KAUNO TECHNOLOGIJOS UNIVERSITETAS

INFORMATIKOS FAKULTETAS

Lilija Stoškutė

STEGANOGRAFIJOS METODŲ ANALIZĖ

Baigiamasis magistro darbas

Vadovas
Prof. dr. Algimantas Venčkauskas

KAUNAS, 2016

KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ KATEDRA

TVIRTINU
Katedros vedėjas
(parašas) Prof. dr. Algimantas Venčkauskas
(data)

STEGANOGRAFIJOS METODŲ ANALIZĖ

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

Vadovas
(parašas) Prof. dr. Algimantas Venčkauskas
(data)

Recenzentas
(parašas) Prof. dr. Rimantas Butleris
(data)

Projektą atliko
(parašas) Lilija Stoškutė
(data)

KAUNAS, 2016

KAUNO TECHNOLOGIJOS UNIVERSITETAS

(Fakultetas)

(Studento vardas, pavardė)

(Studijų programos pavadinimas, kodas)

Baigiamojo projekto „Steganografijos metodų analizė“

AKADEMINIO SĄŽININGUMO DEKLARACIJA

20 ___ m. _____ ____ d.

Kaunas

Patvirtinu, kad mano, **Lilijos Stoškutės,** baigiamasis projektas tema „.....“ yra parašytas visiškai savarankiškai. Įstatymų nenumatytų piniginių sumų už šį darbą niekam nesu mokėjusi, 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.

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

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

Stoškutė, Lilija. Steganografinių metodų analizė. Magistro baigiamasis projektas / vadovas prof. dr. Algimantas Venčkauskas; Kauno technologijos universitetas, Informatikos fakultetas, kompiuterių katedra.

Kaunas, 2016. 65 p.

SANTRAUKA

Žmonėms vis daugiau laiko praleidžiant prie kompiuterių, steganografija tampa vis populiaresnė slepiant skaitmeninius duomenis. Dauguma failų, elektroninių dokumentų, garso ir vaizdo įrašų turi neišnaudotų bitų. Šiuolaikinė steganografijos technologija išnaudoja šių tuščių informacijos plotų galimybes, įrašant tam tikrą informaciją į tuščias vietas arba pakeičiant dalį originalo informacijos žmogui negirdima, nematoma informacija.

Darbo tikslas - palyginti, kaip veikia skirtingi steganografijos metodai slepiant ir ieškant informacijos. Šiame darbe bus analizuojami steganografijos metodai ir įrankiai, atliekamos steganografijos atskleidimo ir įveikimo analizės, sudaryta tyrimo metodika. Parinkti tyrimui reikalingi dangų ir paslapčių failai. Ištirus dangos atvaizdus, pateikti jų slaptumo įverčiai. Su pasirinktais steganografiniais įrankiais sudaryti stego atvaizdai. Nustatyta įrankių greitaveika, atvaizdų dydžių pasikeitimai, talpumas. Skaičiuojami stego atvaizdų slaptumo įverčiai. Darbo pabaigoje pateikti atliktos analizės rezultatai. Palyginimo būdu pasiūlytas efektyviausias steganografijos metodas. Taip pat nustatyta kokiu įrankiu naudojantis galima slėpti informaciją su mažiausia aptikimo galimybe.

Stoškutė, Lilija. Analysis of Steganography Methods: Master‘s thesis in Informatics / supervisor. prof. dr. Algimantas Venčkauskas. The Faculty of Informatics, Kaunas University of Technology.

Kaunas, 2016. 65 p.

SUMMARY

Stenography is going more and more popular for hiding digital information while people are working more with computers. There are a lot of unused bits in audio files, electronic documents, videos, photos and all other documents. These days stenography uses potencial of those unused bits by saving specific information in those empty slots or replacing part of original file information with its hidden information.

The goal is to compare how diferent methods of stenography work on hiding and searching information. There will be analysed methods and tools of stenography, stenography exposure and steganalysis, made methodics of research. There will be chosen cover carriers and secret messages, needed for the research. There are shown scale numbers of secrets after researches was made. There were made stego images using selected stenographic tools. Bandwitdth of tools set, changes of stego image sizes, capacity. Counted scale numbers of stego images. Results of analysis are shown in the end of this work. Most effective stenographic method was offered, which was found by comparing diferent stenographic methods. Also it was cleared out which tool used can best hide information with lowest risk of being found.

TURINYS

LENTELIŲ SĄRAŠAS

PAVEIKSLŲ SĄRAŠAS

TERMINŲ IR SANTRUMPŲ ŽODYNAS

Steganografija – mokslas apie informacijos slėpimo būdus.

Stegoanalizė – mokslas apie tai, kaip aptikti paslėptą informaciją arba patį slėpimo faktą.

Stegoanalitikas – asmuo, kuris bando perskaityti paslėptą tekstą atsiųstame pranešime.

Kriptografija – mokslas, tiriantis informacijos užšifravimo ir iššifravimo metodus.

TK – tiesinė kriptoanalizė.

DK – diferencialinė kriptoanalizė.

Feistelio struktūra – tai iteratyvusis blokinis šifras. Bet kuris blokinis šifras, naudojantis šią struktūrą, yra grįžtamasis ir garantuoja duomenų dešifravimo galimybę kiekviename cikle. Dešifravimas vyksta taip pat, kaip užšifravimas, tik subraktai naudojami atvirkštine tvarka.

ĮVADAS

Magistro baigiamajame darbe nagrinėjami steganografijos ir stegoanalizės metodai. Taip pat steganografijos įrankiai, kuriems padedant galima paslėpti norimą informaciją daugiaformačiuose failuose arba surasti jau paslėptą. Bandant perskaityti paslėptą tekstą atliekami trys žingsniai. Pirmiausiai, gavęs failą, stegoanalitikas turi nustatyti, kuris steganografijos metodas buvo pritaikytas. Gautas failas apdorojamas ir sudaromas galimų steganografijos metodų, kuriais galėtų būti užkoduotas pranešimas, sąrašas. Remdamasis šiuo sąrašu stegoanalitikas gali atskleisti slaptą pranešimą. Vėliau jis nagrinėja steganografijos metodų, kuriais galėjo užkoduoti tą informaciją, ypatybes. Sėkmingai atpažinus ir išnagrinėjus steganografijos metodą, stegoanalitikas gali išgauti iš failo slaptą pranešimą.

Kaip ir duomenų šifravimas, taip ir steganografija laikoma vienu iš pagrindinių informacijos konfidencialumo saugojimo principų.

Pats terminas „steganografija“ kilo iš graikų kalbos („stegonos“ – paslaptis ir „graphy“ – raštas) ir reiškia slaptaraštis, paslėptas raštas. XV amžiuje steganografijos terminas pavartotas vokiečių autoriaus Johano Trihemijaus (Johannes Trithemius) išleistoje knygoje „Steganografija“. Steganografijai skirta daugelis slaptumo įrankių, tokių, kaip permatomas rašalas, mažos nuotraukos, paslaptingi kanalai, ženklų pasiskirstymas ir t.t.

Steganografija yra mažiau svarbi duomenų saugojimo atžvilgiu, nes ji ne pakeičia, o papildo kriptografiją. Pranešimo slėpimas steganografijos metodais sumažina tikimybę jį aptikti, tačiau jeigu pranešimas dar bus ir užšifruotas kriptografijos metodais, tai saugumo lygis smarkiai padidės.

Kaip ir dauguma saugumo įrankių, steganografija gali būti naudojama skirtingiems tikslams. Tai gali būti:

- apsauginiai ženklai ant valiutų;
- skaitmeniniai parašai, tokie, kaip pirštų antspaudai, kurie patvirtina žmogaus tapatumą, autorines teises.
- podėlio (angl. Cache) reikšmės keitimas – imamas įvesto kintamojo ilgis ir keičiamas į statinį eilutės ilgį tam, kad būtų patvirtinta, jog įvestas kintamasis nebuvo pakeistas vykdymo metu;
- parašas, patvirtinantis autorines teises, ant internete patalpinto paveiksliuko;
- slaptos informacijos saugojimas tam, kad būtų apsisaugota nuo vagysčių ir nesankcionuotos peržiūros.

Tačiau steganografija yra naudojama ir neteisėtiems veiksmams. Pavyzdžiui, bandant išsiųsti pavogtą informaciją, ji įrašoma kitame faile arba failuose ir elektroniniu paštu siunčiama kaip paprastas failas ar paveiksliukas. Be to, steganografiją galima naudoti slepiant informaciją kietajame diske arba norint slaptai bendrauti su tam tikrais žmonėmis.

Dažnai steganografija yra naudojama kartu su kriptografija. Kriptografijos pagalba stengiamasi apsaugoti pranešimą nuo įsilaužėlių ir pristatyti jį tik tam asmeniui, kuriam jis buvo skirtas. Tuo tarpu steganografija slepia ne tik siunčiamą pranešimą, bet ir patį pranešimo slėpimo faktą. Dėl šių priežasčių kartais yra efektyviau šias metodikas naudoti kartu. Steganografija sukuria saugų persiuntimo kanalą, o kriptografija – duomenų apsaugą. Tokiu būdu pranešimas nukeliauja saugiu kanalu.

Steganografijos metodika negali būti tiesiogiai priskirta kriptografijai. Jų bendras bruožas yra tai, kad abi metodikos stengiasi kiek įmanoma daugiau išlaikyti originalios informacijos, tai yra, kuo mažiau ją iškraipyti.

DARBO PROBLEMATIKA IR AKTUALUMAS

Žmonėms vis daugiau laiko praleidžiant prie kompiuterių, steganografija tampa vis populiaresnė slepiant skaitmeninius duomenis. Dauguma failų, elektroninių dokumentų, garso ir vaizdo įrašų turi neišnaudotų bitų. Šiuolaikinė steganografijos technologija išnaudoja šių tuščių informacijos plotų galimybes, įrašant tam tikrą informaciją į tuščias vietas arba pakeičiant dalį originalo informacijos žmogui negirdima, nematoma informacija.

DARBO TIKSLAS IR UŽDAVINIAI

Darbo tikslas: palyginti, kaip veikia skirtingi steganografijos metodai slepiant ir ieškant informacijos.

Darbo uždaviniai:

- atlikti steganografijos metodų analizę;
- išanalizuoti steganografijos įrankių veikimą;
- išanalizuoti, kokiais steganografijos metodais yra patikimiau slėpti informaciją, kad būtų sunkiau aptikti jos buvimą;
- išanalizuoti, kokie stegoanalizės metodai aptinka daugiau skirtingais būdais paslėptos informacijos.

DARBO REZULTATAI IR JŲ SVARBA

Darbo pabaigoje pateikiami atliktos analizės rezultatai. Palyginimo būdu bus pasiūlytas efektyviausias steganografijos metodas, stegoanalizės metodas. Taip pat pasiūlyta, kokiu įrankiu naudojantis galima slėpti informaciją su mažiausia aptikimo galimybe.

DARBO STRUKTŪRA

Šiame darbe yra šeši skyriai. Pirmame skyriuje yra aprašyta steganografijos metodų ir įrankių analizė, kurią sudaro: steganografijos įgyvendinimo, atskleidimo įveikimo įrankių analizė. Sekančiame skyriuje yra aprašyta tyrimo eiga:

- Parinkti dangos failus;
- Parinkti paslaptis;
- Ištirti dangos failus;
- Parinkti steganografijos įrankius;
- Sudaryti stego atvaizdus;
- Ištirti sudarytus stego atvaizdus;
- Palyginti stego atvaizdus tarpusavyje;
- Surasti paslaptis stego atvaizduose.

Trečiame skyriuje pateikiami atlikto tyrimo rezultatai. Pateikiami parinkti dangos atvaizdai ir jų slaptumo įverčiai. Tuomet, atliekus paslapčių slėpimus dangos failuose su kiekvienu tyrimo metodikos dalyje nurodytu steganografijos įrankiu, pateikiama jų veikimo greitaveika, failo dydžio pasikeitimai, talpumas. Toliau šiame skyriuje pateikiami gautų rezultatų palyginimas tarp skirtingais įrankiais sudarytų stego atvaizdų. Taip pat skaičiuojami slaptumo įverčiai ir palyginami gauti rezultatai. Pabaigoje apskaičiuojamos stegoanalizės greitaveikos ir lyginami gauti rezultatai.

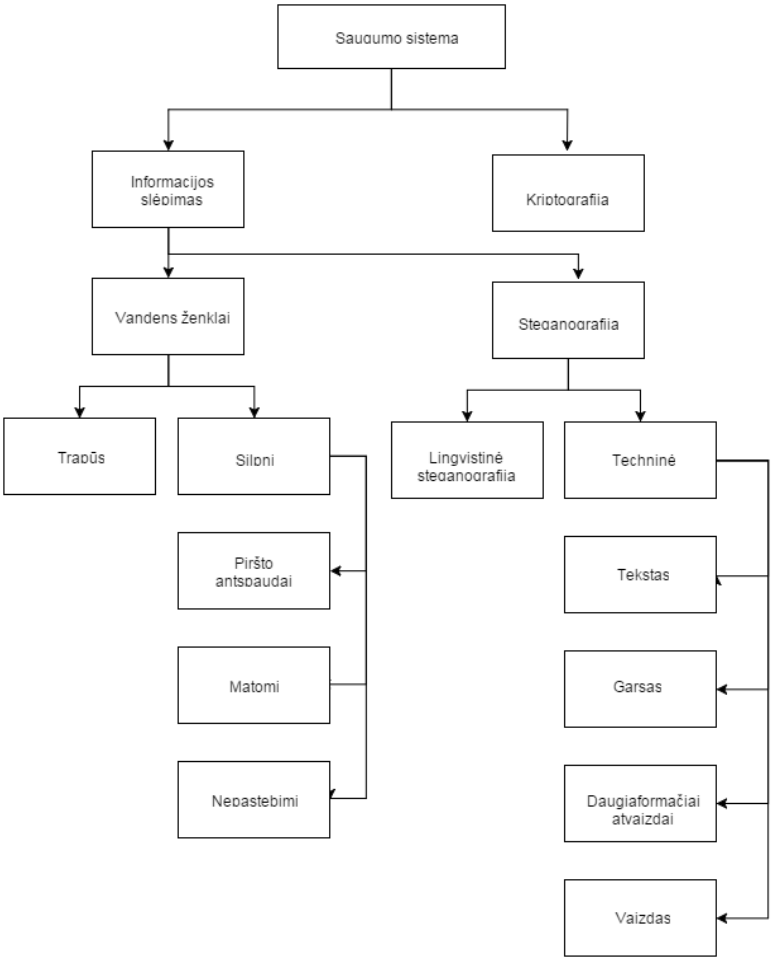
Išvadose aprašomi tyrimo metu gauti rezultatai ir išrenkamas efektyviausias steganografijos metodas ir įrankis, kuris efektyviausiai slepią bei ieško informacijos atvaizduose.

Literatūros sąraše pateikiami moksliniai straipsniai, kuriais remiantis buvo atliekama steganografijos metodų ir įrankių analizė.

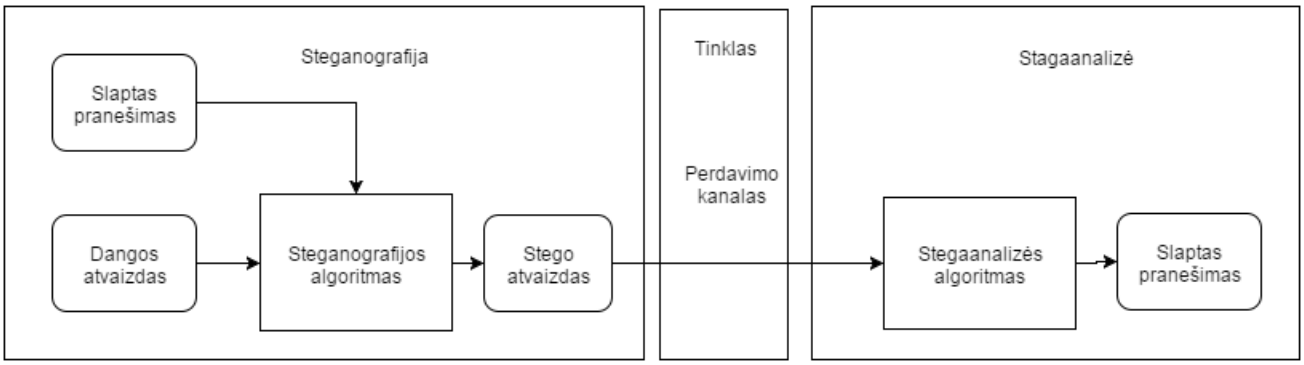
Prieduose pateikiami tyrimo metu naudotų paslapčių tekstai.

1. STEGANOGRAFIJOS METODŲ IR ĮRANKIŲ ANALIZĖ

Žmonėms vis daugiau laiko praleidžiant prie kompiuterių, steganografija tampa vis populiaresnė slepiant skaitmeninius duomenis. Dauguma failų, elektroninių dokumentų, garso ir vaizdo įrašų turi neišnaudotų bitų. Šiuolaikinė steganografijos technologija išnaudoja šių tuščių informacijos plotų galimybes, įrašant tam tikrą informaciją į tuščias vietas arba pakeičiant dalį originalo informacijos žmogui negirdima, nematoma informacija. Steganografijos būdu dažniausiai informacija slepiama paveikslėliuose ir garso failuose, iš pradžių užšifruojant, o po to įdiegiant į slepiantį vaizdą. Pranešimas gali būti paprastas tekstas arba kitas vaizdas. Kaip pavaizduota Pav. 2 [1], sujungus slepiantį vaizdą ir slepiamą pranešimą, gaunamas stegovaizdas. Stegorakto pagalba, kuris yra įvedamas specialia steganografijos programine įranga, pranešimas yra paslepiamas arba atidengiamas. Tik tas asmuo, kuris žino, kaip yra įdiegtas pranešimas, gali iššifruoti ir perskaityti jį.



Pav. 1 Steganografija saugos atžvilgiu [17]

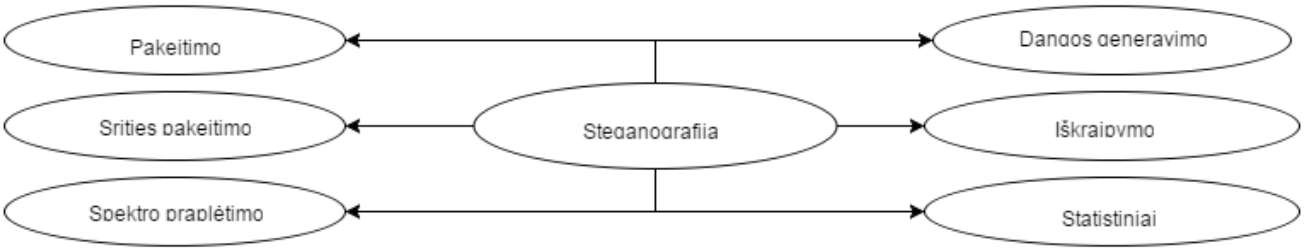


Pav. 2 Steganografijos ir stegoanalizės procesas

Steganografija skirstoma 3 kategorijas [1]:

- lengva steganografija, kur nėra stego rakto. Pagrindinė sąlyga, kad jokia kita pusė nežino apie komunikacijas;
- Slapto rakto steganografija, kur stego raktu yra apsikeičiama prieš komunikuojant;
- Viešo rakto steganografija, kur viešas ir privatus raktai naudojami saugiai komunikacijai.

Steganografijos metodus galima skirstyti į 6 pagrindines kategorijas [17]:



Pav. 3 Steganografijos metodų kategorijos

- Pakeitimo metodai pakeičia likusias dangos dalis su slaptu pranešimu (erdvinė sritis).
- Srities pakeitimo technikos įdeda slaptą informaciją į pakeistą signalo vietą (dažnio sritis).
- Praplėtimo spektro technika priima mintis iš praplėsto spektro komunikacijos.
- Statistiniai metodai koduoja informaciją keisdami kelias statistines slėpimo ypatybes ir naudoja hipotezės bandymą ištraukimo procese.
- Iškraipymo technikos kaupia informaciją apie signalo iškraipymą ir matuoja nukrypimą nuo originalios dangos iššifravimo žingsnyje.
- Dangos generavimo metodai koduoja informaciją tuo būdu, kuriuo slaptas komunikavimas buvo sukurtas.

1.1. Steganografijos įgyvendinimo analizė

Pagrindiniai steganografijos, apimančios kompiuterių sistemas, metodai remiasi:

- kompiuterinių failų formatų savybėmis;
- daugialypės terpės objektų (garso, vaizdo, paveikslų) informacijos pertekliškumu.

Toliau aprašyti su kompiuterinių failų formatų savybių pritaikymu susiję metodai.

Išplėtimo skyrių naudojimas. Daug daugialypės terpės failų turi išplėtimo skyrius papildomai informacijai ar papildomam funkcionalumui įterpti. Paprastai šie skyriai nenaudojami ir yra laisvi. Įterpus slaptą informaciją į šiuos skyrius, pati priedangos terpė, išskyrus plėtimo, nekinta, todėl skirtumus galima pastebėti tik pasitelkus specialią programinę įrangą. Tačiau žinant, jog terpė naudojama slaptai informacijai slėpti, aptikti pakeistus skyrius nesudėtinga. Be to, dažnai perduodamos slaptos informacijos kiekis yra ribotas, nes paprastai šių skyrių dydis ribojamas. [20]

Specialių skyrių naudojimas. Slaptą informaciją saugo ne tekstas, o jo formatavimo atributai (pvz., informacijai saugoti gali būti pasitelkiami skirtingo dydžio šriftai). Informacija turi būti koduojama, ir tam dažnai naudojamas dvejetainis kodas (tam, kad formatavimo pokyčiai būtų sunkiau pastebimi). [20]

Specialus tekstų išdėstymas. Slapta informacija saugoma pačiame tekste, o siekiant nustatyti slaptos infomacijos žodžius, vartojami tam tikri žodžių (ar raidžių) junginiai (prieš slaptus žodžius gali būti papildomas tarpas). Pavyzdžiui, toks būdas taikomas naudingai slaptai informacijai šlamšto tipo laiškuose perduoti. [20]

Nuliniai šifrai. Slaptą informaciją identifikuoja padėtis (pvz., informacijai paslėpti gali būti vartojamos pirmosios sakinių raidės). [20]

Specifinių vaizdavimo savybių išnaudojimas. Atsižvelgiama į tai, kaip tam tikra programinė įranga perteikia informaciją ekrane. Gali būti vartojami specialūs formatavimo simboliai ir kodai, kad vaizduojamosios informacijos nebūtų galima pamatyti pasitelkus tam tikrą programinę įrangą. Paprasčiausiu atveju tai gali būti balto teksto pateikimas balto fono tinklalapyje. [20]

Diskinių laikmenų savybių išnaudojimas. Mėginama padaryti taip, kad standartinėmis priemonėmis nebūtų galima nuskaityti visos laikmenoje esančios informacijos. Paprasčiausiu atveju tai daroma keičiant informacijos (failų) išdėstymo lentelę, sudėtingesniais atvejais – kuriami specialūs disko formatai ir atitinkamos tvarkyklės. Šis metodas populiarus žaidimų pramonėje – būtent tokiomis priemonėmis siekiama apsaugoti originalias kompaktines plokšteles nuo kopijavimo. [20]

Failų identifikacinės informacijos šalinimas. Slapti duomenys užšifruojami, pašalinama failo identifikacinė informacija. [20]

Paslaptys gali būti paslėptos visose dangos informacijos rūšyse: teksto, atvaizdų, garso, vaizdo ir kt. Dauguma šių dienų steganografinių sistemos įrankių paslepia informaciją atvaizduose, kadangi tai palyginti lengva įgyvendinti. Tačiau yra pasiekiamų įrankių, kaupiančių paslaptis viduje beveik bet kokiame dangos šaltinyje. Taip pat galima paslėpti informaciją, pavyzdžiui, tekstuose, garsuose ir vaizdo filmuose. Svarbiausia dangos šaltinio savybė yra duomenų kiekis, kuris gali būti jame sukauptas nekeičiant pastebimų dangos ypatybių. Kai atvaizdas yra iškraipytas, ar muzikos kūrinys atrodo kitoks negu originalas, dangos šaltinis bus įtariamas ir gali būti kruopščiau tikrintas.[16]

Kadangi kiekvienas gali skaityti, koduoti tekstą neutraliuose sakiniuose yra abejotinai efektyvu. Informacijos paprastame tekste slapstymas gali būti padarytas keliais skirtingais būdais.

Pirmos raidės metodo naudojimas nėra labai saugus, nes žinant sistemą, kuri yra panaudota, automatiškai išduodama paslaptis. Daugelis technikų apima sustatymo teksto pasikeitimą, taisykles, kaip kiekvieno n-tojo simbolio naudojimas, ar pakeičia tarpų kiekį po linijų ar tarp žodžių. Naujausia technika sėkmingai panaudojama praktiškai ir net po to, kai tekstas būna išspausdintas ir nukopijuotas popieriuje dešimt kartų, slapta žinutė gali vis dar būti atkurta. Kitas galimas būdas patalpinti slaptą pranešimą į tekstą – naudoti viešai pasiekiamą dangos šaltinį, knygą ar laikraštį, ir naudoti kodą, kuris susideda, pavyzdžiui, iš puslapio numerio, linijų skaičiaus ir simbolių skaičiaus kombinacijos. Taip jokia dangos šaltinyje patalpinta informacija neprives prie paslėptos žinutės. Žinutės atradimas galimas tik žinant slaptą raktą. [16]

Šiuo metu paslėpti pranešimą atvaizde yra populiari technika. Atvaizdas su slaptu pranešimu gali būti lengvai siunčiamas per žiniatinklį ar žinių grupes. Steganografijos panaudojimas žinių grupėse buvo atrastas vokiečių steganografijos eksperto Nielso Provos, kuris sukūrė skenavimo klasterį, aptinkantį paslėptą pranešimą atvaizde, patalpintame į tinklą. Tačiau po 1 mln. atvaizdų tikrinimo, nebuvo rastas nei vienas paslėptas pranešimas, todėl praktiškai naudojama steganografija išlieka ribota. [16]

Slepiant pranešimą atvaizde nepakeičiant jo pastebimų savybių, dangos šaltinis gali būti keičiamas į „triukšmų“ laukus su daugybe spalvų variacijų, taigi mažiau atkreipiant dėmesį į modifikuotas vietas. Mažiausiai reikšmingo bito (LSB - angl. *Least significant bit*), užmaskavimo, filtravimo ir transformacijos dangos atvaizde yra įprastinės metodikos. Šita technika gali būti panaudota su skirtingais pasisekimo laipsniais ant skirtingų atvaizdo rinkmenų tipų. [16]

Plačiausiai panaudota duomenis paslėpianti technika yra LSB vartojimas. Nors yra kelios šio metodo kliūtys, įgyvendinimo paprastumas daro jį populiarų. Kad paslėptų slaptą žinutę atvaizde, deramas dangos atvaizdas yra būtinas. Kadangi šis metodas naudoja bitus kiekvieno vaizdo elemento atvaizde, tai nebūtina, kad panaudotų mažiau prarandamo suspaudimo formatą, kitaip paslėpta informacija dings suspaudimo algoritmo transformacijoje. [18]

Kai naudojamas 24 bitų spalvos atvaizdas, kiekvieni raudonos, žalios ir mėlynos spalvos bitų komponentai gali būti panaudojami, taigi visi trys bitai gali būti patalpinti į kiekvieną vaizdo elementą. 800 x 600 vaizdo elementų atvaizdas gali apimti iš viso 1440000 bitus (180000 baitus) slaptų duomenų, pvz.: toliau einantis blokas gali būti skaitomas kaip 3 vaizdo elementai 24 bitų spalvos atvaizde, naudojant 9 baitus atminties [18]:

```
00100111    11101001    11001000
00100111    11001000    11101001
11001000    00100111    11101001
```

Kai simbolis 'A', kurio dvejetainė reikšmė lygi 10000001, įterpiamas, gaunamas blokas [18]:

00100111	11101000	11001000
00100110	11001000	11101000
11001000	00100111	11101001

Šiuo atveju reikėjo keisti tik tris bitus, kad sėkmingai būtų įterptas simbolis. [18]

Vidutiniškai pusė atvaizdo bitų yra modifikuojami slepiant pranešimą, jei naudojamas maksimalus dangos dydis. Pasikeitimai, padaryti naudojant mažiausios reikšmės bitą, yra maži, todėl žmogaus akiai nepastebimi, taigi pranešimas yra efektyviai paslėptas. [18]

Kitas panašus metodas yra LSB metodas – slėpti informaciją mėlynos ir dalyje žalios spalvos komponentų atsistiktiniuose atvaizdo kraštuose esančiuose pikseliuose. Ši LSB steganografija yra paremta duomenų slėpimu raudoname, žaliame ar mėlyname MSB (labiausiai reikšmingame bite) komponente iš atsitiktinės lygios vietos. [18]

Naudojant 24 bitų atvaizdą, gaunama palyginti didelė vieta slėpti pranešimą, taip pat galima naudoti 8 bitų atvaizdą kaip dangos šaltinį. Dėl mažesnės vietos ir skirtingų ypatybių, 8 bitų atvaizdams reikalingas atsargesnis metodas. Ten, kur 24 bitų atvaizdas naudoja tris bitus nusakant vaizdo elementą, 8 bitų atvaizdas naudoja tiktai vieną. Dangos atvaizdas turi būti išrinktas rūpestingai, ir geriau, kad būtų pilkoje skalėje, kadangi žmogaus akis neaptiks skirtumo tarp skirtingų pilkų atspalvių taip lengvai kaip su skirtingomis spalvomis. [18]

Nenaudinga naudoti LSB pokyčio, nes jis reikalauja gana didelės dangos atvaizdo, kad sukurtų tinkamą naudoti erdvę slėpimui. Net šiuo metu nesuspausti 800 x 600 vaizdo elementų atvaizdai yra retai naudojami internete, taigi jų naudojimas galėtų sukelti įtarimų. Kita problema iškils, kai suspaudžiant atvaizdą su paslaptimi, bus naudojamas netekties suspaudimo algoritmas. Paslėpta žinutė neišgyvens šios operacijos ir bus prarasta po transformacijos. [18]

Užmaskavimo ir filtravimo technikos paprastai suvaržo 24 bitų ar pilkos skalės atvaizdus, slėpti pranešimą naudojamas skirtingas metodas. Šitie metodai savo efektyvumu yra panašūs į popieriaus vandenženklius, jais kuriamas žymėjimas atvaizde. Tai gali būti pasiekiama, pavyzdžiui, pakeičiant atvaizdo dalių šviesumą. Tuo metu, kai užmaskavimas tikrai keičia matomas atvaizdo ypatybes, jis gali būti padarytas tokiu būdu, kad žmogaus akis nepastebės anomalijos. [18]

Procesas, kai užmaskuojant naudojami matomi atvaizdo aspektai, yra efektyvesnis negu LSB pasikeitimas dėl suspaudimo, apkarpymo ir įvairių rūšių vaizdo apdorojimo. [18]

Informacija nėra paslėpta „triukšmo“ lygmenyje, bet yra matomoje atvaizdo dalyje, kuris daro ją tinkamesnę negu LSB pasikeitimai tuo atveju, jei naudojamas praradimo suspaudimo algoritmas, pvz., kaip JPEG. [18]

Sudėtingesnis būdas paslėpti paslaptį atvaizdo viduje vyksta su naudojimu ir atskiros kosinuso transformacijos pasikeitimais. Atskira kosinuso transformacija (DST) yra naudojama JPEG suspaudimo algoritmo, kad paverstų atvaizdo nuoseklius 8 x 8 vaizdo elemento blokus į kiekvieno

64 DCT koeficientus. Po koeficientų skaičiavimo vykdoma kvantavimo operacija. Paprastas pseudo-kodo algoritmas slėpti pranešimą JPEG atvaizde turėtų atrodyti taip [18]:

įvestis: pranešimas, dengiamas atvaizdas
išvestis: steganografinis atvaizdas su pranešimu
kol yra duomenų, kuriuos reikia įstatyti, **vykdyti,**
    gauti toliau einantį DCT koeficientą iš dengiamo atvaizdo
    jei DCT(6)=0 ir DCT(6)=1 **tada**
        gauti toliau einantį LSB iš pranešimo
        pakeisti DCT LSB su pranešimo bitu
    baigti
    įterpti DCT į steganografinį atvaizdą
baigti

Nors vieno DCT pasikeitimas paveiks visus 64 atvaizdo vaizdo elementus, kvantuoto DCT koeficiento LSB gali būti panaudotas, kad paslėptų informaciją. Mažiausio praradimo suspausti atvaizdai bus įtartini žmogaus regai, kai LSB bus pakeisti. To nebus su anksčiau apibūdintu metodu, kadangi tai vyksta atvaizdo dažnio srityje vietoj erdvinės srities, ir todėl nebūna jokių matomų pakeitimų dangos atvaizde. [18]

Steganografija, išnaudojanti paveikslėlio formatą. Pranešimo paslėpimas gali būti lengvai atliekamas „Windows OS“ komandinėje eilutėje: „C:\> copy Cover.jpg /b + Message.txt /b Stego.jpg“. Šis kodas slaptą pranešimą, esantį tekstiniame faile Message.txt, prijungia prie JPEG vaizdo failo Cover.jpg ir pateikia stega vaizdo failą Stego.jpg. Slaptas pranešimas yra įpakuojamas ir įterpiamas po failo pabaigos žymės (**EOF** – angl. *End Of File*). Kai atvaizdas Stego.jpg yra atidaromas peržiūrėti naudojant bet kokį nuotraukų peržiūros įrankį, jis parodo atvaizdą ignoruodamas viską, kas yra už EOF žymės. Tačiau, kai Stego.jpg bus atidaromas, pavyzdžiui, naudojant „Notepad“ įrankį, paslėptas pranešimas bus matomas failo pabaigoje. Slepiamas pranešimas nepakeičia nuotraukos kokybės ar matomo vaizdo. Nors šis metodas yra paprastas, internete galima rasti programinę įrangą, kuri jį naudoja („Camouflage“, „JpegX“, „Data Stash“). [19]

Kitas steganografijos metodas apima duomenų slėpimą išplėstos informacijos failų vaizduose (**EXIF** – *Extended File Information*). EXIF paprastai naudojamas skaitmeninių kamerų gamintojų saugoti tikrai informacijai vaizdo faile: kameros gamintojas ir modelis; laikas, kada nuotrauka buvo padaryta ir suskaitmeninta; vaizdo rezoliucija; ekspozicijos laikas; židinio nuotolis. Tai yra metaduomenų informacija apie vaizdą ir jo šaltinį, esanti failo antraštėje.

Bloko sudėtingumo pagal duomenų įdėjimą (ABCDE – angl. *A Block Complexity based Data Embedding*) metodas. Įdėjimas vyksta keičiant pasirinkto triukšmo bloko atitinkamų pikselių duomenis į atvaizdą su kitu triukšmo bloku, tada gauti pikseliai konvertuojami ir įdedami duomenys.

Informacijos girdimosiose rinkmenose slapstymas gali būti padarytas keliais skirtingais būdais. Galima naudoti mažiausio reikšmingumo bitą, kadangi pasikeitimai paprastai nekuria girdimų pakeitimų garse. Kitas metodas turi pranašumą prieš žmogaus apribojimą. Galima užkoduoti žinutes naudojant dažnius, kurie yra negirdimi žmogaus ausiai. Naudojant bet kokius dažnius aukštesnius nei 20.000 Hz, žinutės bus paslėptos garso failų viduje ir nebus aptiktos tikrinant žmogui.

Taip pat žinutė gali būti užkoduota naudojant muzikinius tonus su pakeitimo planu. Pavyzdžiui, F tonas atstovauja 0, ir C tonas atstovauja 1. Normali muzikinė dalis gali būti sudaryta aplink slaptą žinutę arba egzistuojanti dalis gali būti išrinkta kartu su kodavimo planu, kuris atstovaus žinutei.

Vaizdo failai yra atvaizdų ir garsų kolekcija, taigi dauguma pristatytos technikos atvaizdams ir garsui gali būti pritaikomos vaizdo failams. Dideli vaizdo pranašumai yra didelis kiekis duomenų, kurie gali būti paslėpti viduje, ir faktas, kad tai yra judanti atvaizdų ir garsų srovė. Todėl bet kas mažas galėtų praeiti nepastebėtas žmonių dėl informacijos srauto tęstinumo.

Taigi, steganografija naudojama paslėpti informaciją dangos faile, paslepiant ne tik informaciją, bet ir faktą, kad kažkas gali būti paslėpta. Tuo tarpu kritografija užšifruoja slepiamą informaciją, bet jos nepaslepia.

DES metodas

DES yra simetrinis, blokinis šifras, kuriame šifruojami 64-bitų atviro teksto blokai, naudojant 64-bitų raktą. Dešifravimas yra atvirkščias užšifravimui: atliekami užšifravimo veiksmai vykdomi atvirkščia tvarka. Algoritmo saugumas priklauso nuo rakto. DES turi 64 silpnuosius raktus. DES algoritmas – tai dviejų pagrindinių šifravimo metodų, išskaidymo bei sumaišymo, kombinacija. Viename algoritmo etape yra naudojamos vienetinės šių metodų kombinacijos (pakeitimas ir perstatymas), kurios priklauso nuo rakto. DES algoritmas susideda iš 16 etapų: atviram teksto blokui yra taikoma ta pati metodų kombinacija šešiolika kartų. Algoritmo pagrindas – Feistelio struktūra. Užšifravimas susideda iš 64 bitų dokumento (atviro teksto) bloko T perstatymo (Perstatypas IP), 16-os šifravimo etapų (iteracijų) ir gauto bloko bitų atvirkštinio perstatymo IP^{-1}. Lentelės, naudojamos šiame algoritme, yra standartinės ir negali būti keičiamos. Lentelių kodai yra parenkami taip, kad būtų maksimaliai apsunkintas dešifravimas parenkant raktą.

Privalumai ir trūkumai:

- Algoritmas yra paprastas: paprasta ir aiški struktūra, paprastos šifravimo operacijos;
- Funkcionavo 20 kriptoanalizės metų.
- Algoritmo atsparumas TK ir DK yra pakankamai didelis.
- DES algoritmas skirtas aparatinei realizacijai, programinės realizacijos atveju užšifravimo greitis yra mažas.
- Algoritmas paseno. Dėl mažo rakto ilgio visų raktų perrinkimo būdas tapo lengvai pasiekiamas.

3DES algoritmas

Tobulėjant kompiuterinėms technologijoms, DES 56-bitų raktas tapo per trumpas. Vėliau pradėtas naudoti Triple DES (3DES). Tai DES algoritmo versija, kurioje baziniu DES algoritmu atviro teksto blokas šifruojamas tris kartus. Rakto ilgis – 1368 bitai, bloko ilgis 64 bitai. Šis algoritmas paveldėjo visus DES privalumus, kartu padidino atsparumą daugiau nei du kartus (atakos laikas buvo sumažintas iki 108-bitų rakto ilgio lygio). Taip pat 3DES liko silpnųjų ir pusiau-silpnųjų raktų klasės. Tačiau šio algoritmo programinė realizacija tapo dar lėtesnė nei DES programinė realizacija.

Gost algoritmas

GOST yra blokinis algoritmas. Šifruoja 64-bitų blokus, naudodamas 256-bitų raktą. Algoritmas turi 32 etapus. Algoritmo pagrindas – Feistelio struktūra. Algoritmas naudoja aštuonis skirtingus S-blokus, t.y. tiek pat, kiek 4-bitų sekų. Pirmieji 4 bitai – tai pirmojo S-bloko įėjimas, antrieji 4 – tai antrojo S-bloko išėjimas ir t.t. Kiekvienas S-blokas – tai skaičių nuo 0 iki 15 kombinacija. Visi šie blokai yra skirtingi, faktiškai tai papildoma slapta informacija. S-blokai turi būti saugomi. Dažnai S-blokai – tai pačios algoritmo schemos parametrai, vienodi tam tikrai vartotojų grupei.

Algoritmo privalumai:

- Didelis užšifravimo greitis;
- Programinės realizacijos efektyvumas;
- Visų raktų perrinkimo atakos būdo neperspektyvumas;
- Atsparumas tiesinei ir diferencialinei kriptoanalizei.

Algoritmo trūkumai: GOST standartas neaprašo konkrečių S-blokų generavimo algoritmo. Viena vertus, tai yra papildoma slapta informacija, kita vertus, tai neleidžia nustatyti algoritmo kriptoatsparumo lygio.

Twofish algoritmas

Twofish – tai simetrinio rakto blokinio šifravimo algoritmas su 128-bitų blokais ir iki 256-bitų rakto dydžiu. Algoritmo pagrindas – Feistelio struktūra. Algoritmas nuo kitų išsiskiria tuo, kad iš anksto žinomas raktas priklauso nuo S-blokų ir yra pakankamai sudėtingas raktų išskaičiavimas. Viena dalis n-bitų rakto yra naudojama kaip tikras šifravimo raktas, o kita naudojama atliekant šifravimo algoritmo pakeitimus. Šis algoritmas naudoja kitus metodų elementus, tokius kaip pseudo Hadamard transformaciją (PHT) iš SAFER šeimos algoritmų.

Algoritmo privalumai ir trūkumai:

- Algoritmas veikia lėčiau nei AES su 128-bitų raktais, bet kažkokiais būdais greičiau nei su 256-bitų raktais;
- Algoritmas nebuvo užpatentuotas, o buvo pateiktas viešai, todėl nemokamas visiems be jokių apribojimų.

- Vienas iš kelių, kurie įtraukti į PGP rakto standartą.

Blowfish algoritmas

Blowfish algoritmas šifruoja atviro teksto 64-bitų blokus. Algoritmo rakto ilgis kinta nuo 32 iki 448 bitų. Algoritmo pagrindas – Feistelio struktūra. Užšifravimas susideda iš 16 etapų, kiekviename iš jų su kairiąja 32-bitų dalimi atliekami tokie veiksmai:

*Sub*bloko bitai sudedami *mod 2* su *i*-tojo etapo *sub*rakto K_i bitais. Šios operacijos rezultatas tampa naująja *sub*bloko reikšme. Gautas *sub*blokas transformuojamas, panaudojant funkciją *f*, ir sudedamas *mod 2* su dešiniuoju *sub*bloku. Kiekviename etape, išskyrus paskutinįjį, kairysis ir dešinysis *sub*blokai sukeičiami vietomis. Po 16-os algoritmo etapų kairiojo *sub*bloko bitai sudedami *mod 2* su *sub*rakto K_{17} bitais, o dešiniojo *sub*bloko bitai – su K_{18}*sub*rakto bitais.

Algoritmo privalumai ir trūkumai:

- Didelis užšifravimo greitis, turint praplėstą raktą.
- Algoritmo paprastumas;
- Šešiolikos etapų Blowfish yra atsparus žinomiems kriptoanalizės atakos būdams.
- Algoritmas netinka tada, kai reikalingas dažnas raktų pakeitimas.
- Dėl didelių atminties reikalavimų algoritmas negali būti realizuotas intelektualiosiose kortelėse.
- Algoritmo rakto praplėtimo ir užšifravimo operacijos nėra lygiavertės, jos atliekamos atskirai.

RC2 algoritmas

RC2 algoritmas šifruoja atviro teksto 64-bitų blokus. Algoritmo rakto ilgis kinta nuo 8 iki 1024 bitų (didėja po 8 bitus). Algoritmo pagrindas – Feistelio struktūra. Užšifravimas susideda iš 16 etapų, kiekviename iš jų vykdomi maišymai.

AES algoritmas

Tai keitimo – permutacinis simetrinio šifravimo algoritmas. Kiekvieną raktą sudaro tam tikras skaičius žodžių (Nk), kuris tiesiogiai priklauso nuo rakto dydžio. Taip pat ir AES algoritmo ciklų skaičius (Nr) priklauso nuo rakto.

Užšifravimą bei dešifravimą sudaro keturios transformacijos:

- Būsenos baito pakeitimas naudojant pakeitimų S-lenteles;
- Būsenos eilučių cikliniai postūmiai;
- Būsenos stulpelių maišymas;
- Būsenos sudėtis su vis kitu subraktu kiekviename šifravimo cikle.

Žemiau esančioje lentelėje (Lentelė 1) palyginti anksčiau išanalizuoti šifravimo metodai, kurių pagalba galima gaunamas stego atvaizdas. Šie metodai buvo lyginami pagal tai:

- kokio ilgio šifravimo raktus naudoja,

- kokio dydžio šifravimo blokas,
- kokia metodo veikimo struktūra
- bei keliais etapais vyksta šifravimo procesas.

Metodas	Rakto ilgis (bitais)	Šifruoto bloko dydis (bitais)	Struktūra	Etapų skaičius
Twofish	128, 192, 256	128	Feistelio	16
Gost	256	64	Feistelio	32
DES	56	64	Feistelio	16
3DES	56, 112, 168	64	Feistelio	48
Blowfish	32-448	64	Feistelio	16
RC2	8-1024	64	Feistelio	16

Lentelė 1 Šifravimo metodų palyginimas

Kadangi visi šie metodai veikia pagal Feistelio struktūrą ir galima sakyti, kad naudoja tokio paties dydžio šifro blokus, tai vėliau, atliekant jų veikimo tyrimą, aiškiai matysis, kuris metodas veikia efektyviau ar tiksliau.

1.2. Steganografijos atskleidimo analizė

Kadangi vis daugiau besislepiančios informacijos technikos išvystoma ir pagerinama, metodai aptikti steganograafijos naudojimą taip pat tobulėja. Didžioji dalis steganografijos technikos apima besikeičiančias dangos šaltinio ypatybes ir yra keli būdai aptikti šituos pakeitimus.

Tuo metu, kai informacija gali būti paslėpta tekstuose, kur žinutės buvimas gali būti aptiktas tiktai žinant slaptą raktą, pavyzdžiui, naudojant viešai pasiekiamą knygą ir simbolio padėčių kombinaciją, kad būtų paslėptas pranešimas, dauguma technikų apima dangos šaltinių pokyčius. Šitie pasikeitimai gali būti aptikti ieškant tekstuose modelio ar jį ardant, nelyginiame kalbos vartojime ir neįprastuose baltų tarpų kiekiuose.

Nors atvaizdai gali būti peržiūrėti įtariamomis ypatybėmis pagrindiniu būdu, paslėptų žinučių atskleidimas paprastai reikalauja labiau techninio metodo. Dydžio pasikeitimai, failo formatai, paskutinio pakeitimo laiko žymės ir spalvotos paletės galėtų parodyti paslėptos žinutės egzistavimą, bet taip ne visada yra.

Plačiai panaudota technika atvaizdui peržiūrėti apima statistinę analizę. Dauguma steganografijos algoritmų, kurie dirba ties atvaizdais, mano, kad mažiausio reikšmingumo bitas yra daugiau ar mažiau atsitiktinis. Tai yra klaidinga prielaida. Kai galėtų atrodyti, kad LSB neturėtų daug reikšmės taikant filtrą, kuris tiktai rodo mažiausio reikšmingumo bitus, jis vis dar pagamins atpažįstamą atvaizdą. Šiuo atveju gali būti prieinama išvada, kad LSB nėra atsitiktinis, bet iš tikrųjų turi savyje informaciją apie visą atvaizdą. Įdėdamas paslėptą žinutę į atvaizdą, šią savybę keičia. Ypač su šifruotais duomenimis, kurie turi labai aukštą entropiją. Dangos atvaizdo LSB daugiau neturės savyje informacijos apie originalą, bet dėl pasikeitimų jie dabar bus daugmaž atsitiktiniai.

Su LSB statistine analize skirtumas tarp atsitiktinių verčių ir tikrų atvaizdo verčių gali būti lengvai aptiktas. Naudojant šią techniką taip pat galima aptikti žinutes, paslėptas JPEG failo viduje su DCT metodu, kadangi tai taip pat apima LSB pasikeitimus net nepaisant to, kad jie vyksta dažnio srityje.

Statistinis analizės metodas taip pat gali būti panaudotas prieš girdimąsias rinkmenas, kadangi LSB pasikeitimo technika taip pat gali būti panaudota garsams. Aukšti, negirdimi dažniai gali būti peržiūrėti dėl informacijos ir nelyginių iškraipymų arba struktūra garsuose galėtų parodyti slaptos žinutės egzistavimą. Taip pat metimo, aido ar foninio triukšmo skirtumai gali sukelti įtarimą. Steganografijos vaizdo rinkmenų įgyvendinimui naudojami metodai aptikti paslėptą informaciją taip pat yra kombinacija technikos, panaudotos atvaizdams ir girdimosioms rinkmenoms. Tačiau gali būti panaudota skirtinga steganografijos technika, kuri yra ypač efektyviai naudojama vaizdo filmuose. Ypatingų kodinių ženklų vartojimą ar gestus yra labai sudėtinga aptikti kompiuterine sistema. Šis metodas buvo panaudotas Vietnamo kare. Šiuo būdu karo belaisviai galėjo pranešti žinutes slaptai per vaizdo filmus, priešo kareiviai buvo priversti juos nusiųsti į namų liniją.

1.3. Steganografijos įveikimo analizė

Nors steganogramos gali ne visada būti sėkmingai aptinkamos, yra skirtingų būdų pašalinti paslėptas žinutes iš galimų dangos šaltinių. Žinojimas ar įsitikinimas apie paslėptos žinutės egzistavimą nėra būtini, kadangi žinutės gali būti sunaikintos prieš aptinkant. Nors niekada nebus 100 procentų pasisekimo garantijos, galimų būdų skaičius nusiųsti paslėptas žinutes gali būti lengvai sumažintas naudojant bet kokią steganografijos technikos kombinaciją įveikimui.

Geriausias būdas pašalinti paslėptas žinutes nuo paprasto teksto galėtų būti perrašymas ir iš naujo formuojami turiniai. To perrašymas naudojant skirtingus žodžius ir sakinio struktūras geriausiai pašalins visus būdus atkurti paslėptą žinutę, kadangi pasirūpins beveik kiekvienu galimu būdu, kuriuo duomenys gali būti sukaupti paprastame tekste. Simbolio padėties planas daugiau nebetiks todėl, kad žodžiai buvo pakeisti, ir tas pats galioja skirtingiems baltiems tarpams, kadangi tekstas turės naują sustatymą. Vienintelis metodas, kuris nebus apimtas šios technikos, yra viešai pasiekiamo dangos šaltinio vartojimas. Kadangi šis šaltinis negali lengvai būti pakeistas, nėra jokio efektyvaus būdo sustabdyti šį metodą, išskyrus slapto rakto užkirtimą.

Atvaizdo suspaudimas, naudodamas praradimo suspaudimą panaikins žinutes, kurios yra paslėptos, naudojant LSB pasikeitimo techniką. Tai taip pat įvyks, kai atvaizdui bus pakeistas dydis ar savarankiškai yra pakeistos spalvos. Pakeitus į kitą atvaizdo formatą, kuris dažnai naudoja skirtingą suspaudimo tipą, taip pat bus padedama pašalinti paslėptas žinutes. Ir, pavyzdžiui, šviesos pakeitimas pašalins vandenženklius matomoje atvaizdo dalyje.

Dauguma technikų, kurios gali būti panaudotos atvaizdams, taip pat gali būti pritaikomos girdimiesiems failams. Girdimieji failai su praradimo suspaudimu bus paslėptos žinutės praradimo

priežastis, kadangi tai pakeis visą failo struktūrą. Taip pat keli praradimo suspaudimo planai naudoja žmogaus girdimumo ribas, pašalinami visi dažniai, kurių žmogus negali išgirsti. Tai taip pat pašalinami bet kokie dažniai, kurie yra panaudoti steganografijos sistemos, slepiančios informaciją toje spektro dalyje.

Vaizdams gali būti pritaikyti tie patys metodai, kaip atvaizdams ir girdimiesiems failams, kad pašalintų paslėptą informaciją. Kad nugalėtų naudojamus signalus ar gestus, žmogaus įžvalgumas yra vis dar būtinas, kadangi kompiuterinės sistemos dar nesugeba pačios to aptikti.

1.4. Steganografijos įrankių analizė

Yra daugybė steganografijos įrankių, kurie slepia, tikrina ar ieško informacijos įvairiuose daugiaformačiuose failuose. Vieni naudoja tik tam tikrą slėpimo metodą, kiti kelis ir vartotojui leidžia pasirinkti. Dalis jų skirta daugiaformačiams failams, tačiau yra tokių, kurie pritaikyti tik vienam formatui. Taip pat vieni steganografijos įrankiai yra skirti tik informacijai slėpti, kiti tik paslėptos informacijos paieškai. Taip pat yra tokių, kurie gali ir paslėpti, ir aptikti paslėptą informaciją. Daugumos šių įrankių veikimo principas panašus. Iš pradžių pasirenkamas failas, kuriame bus slepiama informacija, tuomet failas su slepiama informacija. Programa paprašo įvesti slaptažodį ir pasirinkti informacijos šifravimo būdą. Tada sugeneruojamas stego failas su jau paslėpta informacija.

StegoS - šifravimo įrankis, padėsiantis duomenis paslėpti ten, kur niekas net nesugalvos jų ieškoti. Naudojant šį įrankį, informacija yra paslepiama paveikslėlių ar muzikiniuose failuose: juose nesvarbi ir nematoma ar negirdima informacija pakeičiama pranešimo kodu. Naudojamas steganografijos metodas paslepia bet kurį nurodytą failą .bmp paveiksliuke. Paveiksliuko, kuriame slepiama informacija, vaizdo kokybė beveik nepakinta (jeigu paveiksliukas margas, skirtumo išvis neįmanoma pastebėti). Jeigu .bmp failas kelis kartus didesnis nei slepiamas, visai nepasikeičia.

OpenPuff – steganografijos šifravimo įrankis, kuris naudoja 512 bitų simetrinių raktų kriptografiją. Palaiko daugybę failų formatų vaizdo (.bmp, .jpeg, .pcx, .png, .tga), garso (.aiff, .wav), vaizdo (.3gp, .mp4, .mpg, .vob) ir kitų (.flv, .swf, .pdf). Duomenys yra padalinami. Tik teisingai nurodžius seką, leidžiama parodyti informaciją. Naudojami saugumo lygiai: šifravimas, balinimo ir kodavimo.

Steganography Studio įrankis, skirtas mokytis naudoti ir analizuoti steganografinius algoritmus.

Internete galima rasti dešimtis programų, skirtų informacijai slėpti.

QuickStego programinė įranga leidžia paslėpti tekstą atvaizde taip, kad tik kitas asmuo, naudojants QuickStego įrankį, galėtų perskaityti paslėptą pranešimą. Išsaugojus pranešimą atvaizdas lieka „atvaizdu“, jis atidaromas ir uždaromas, kaip bet kuris kitas atvaizdas. Šį atvaizdą galima saugoti, siųsti el. paštu, įkelti į tinklalapį kaip ir anksčiau, vienintelis skirtumas tas, kad jis turi

paslėptą tekstą. Šis įrankis nešifruoja slapto pranešimo teksto, nes jis yra pakankamai gerai pasislėpęs atvaizde.

Kuo didesnis atvaizdas, tuo daugiau teksto galima paslėpti viduje. Jei viršijamas slepiamos informacijos kiekis nurodytam atvaizdui, pranešama, keliais simboliais viršijamas galimas simbolių kiekis. QuickStego nepastebimai keičia atvaizdo pikselius (atskirus atvaizdo elementus), koduodamas slaptą pranešimą, pridėdamas mažų svyravimų spalvotus vaizdus. Žmogaus akis šių nedidelių skirtumų nemato.

Reikalavimai:

- Operacinė sistema - Windows XP, Vista, 7.
- Ekranas - bent 32 bitų spalvų.
- Vaizdo tipai, kuriuos galima atidaryti - .jpg/.jpeg, .gif ir .bmp formatais.
- Saugomas failas su paslėptu pranešimu – tik .bmp formatu.

InvisibleSecrets programinė įranga ne tik slepia informaciją atvaizde, bet ir ją užšifruoja. Vienintelis būdas apsaugoti savo duomenis ir leisti juos peržiūrėti tik autorizuotiems asmenims yra naudoti stiprią kriptografiją ir pakankamo ilgio slaptažodį, kad būtų pasipriešinta brutaliai jėgai. Tačiau ar to tikrai užtenka? Daugelis kriptografijos programų tiesiog transformuoja duomenis į neperskaitomus šifruotus duomenis ir saugo kaip paprastus failus. Jei kažkas atsivers tą failą, greitai supras, kad jis yra užšifruotas ir bandys nulaužti kodą. Šis įrankis siūlo galimybę užšifruoti ir paslėpti failus kituose failuose, kuriuos peržiūrėjus negalima įtarti šifravimo. Iš pradžių bus užšifruojamas slepiamas failas naudojant specifikuotą slaptažodį ir šifravimo algoritmą. Po to šifruotas tekstas bus patalpintas dangos atvaizde. Šis metodas pasižymi tuo, kad pranešimas beveik nepastebimas ir apsunkina darbą tam, kuris bando išgauti slaptą pranešimą. Iš pradžių jis turi surasti teisingą dangos atvaizdą ir ištraukti iš jo užšifruotą pranešimą ir tik tada turi nulaužti šifravimo slaptažodį.

Privalumai:

- Lengva naudoti;
- Lankstus – vartotojas gali patalpinti savo algoritmus ar dangos atvaizdus ir paprastai juos integruoti į programą;
- Naudojami vaizdo tipai - .jpg, .png, .bmp;
- Duomenys suspaudžiami prieš šifravimą/slėpimą;
- Naudojamas šifravimo algoritmas – Blowfish / CBC;
- Suklastotų pranešimų generavimas;
- Gera vietinė apsauga – visi laikini failai, naudoti procese, yra ištrinami.

MP3Stego programinė įranga leidžia slėpti informacija .mp3 formato failuose naudojant suspaudimo procesą. Iš pradžių duomenys yra suspaudžiami, šifruojami ir tada slepiami MP3 bitų sraute. Bet kuris įrankis gali išskleisti bitų srautą ir perspausti, bet tai ištrina slepiamą informaciją.

Slėpimo procesas vyksta viduryje trečio sluoksnio šifravimo proceso, vadinamo *inner_loop,* metu. Vidinė linija suskaitmenina įvesties duomenis ir padidina skaitmens žingsnio dydį iki reikiamo, kad duomenys būtų koduojami su turimu bitų kiekiu. Kitos linijos tikrina, ar įvesti duomenys neiškraipė psicho akustinio modelio nustatytos ribos. Antros ir trečios dalies ilgio kintamasis yra mastelio rodiklio ir Huffman kodo duomenų MP3 bitų srautui *main_data* reikalingų bitų skaičius. Bitai šifruojami kaip lygiaverčiai, keičiant vidinės linijos pabaigos ciklo būklę. Keičiamos tik antros ir trečios dalies ilgio vertės, atranka daroma naudojant pseudo atsitiktinį bitų generatorių pagrįstą SHA-1.

Steghide programinė įranga skirta informacijai slėpti bei rasti atvaizduose ir garso failuose.

Ypatybės:

- Slepiamų duomenų suspaudimas;
- Slepiamų duomenų šifravimas;
- Palaiko .jpeg, .bmp, .wav ir .au formatų failus.

S-Tools programinė įranga, sukurta Andy Browno: duomenys į paveikslų (.bmp) ir garso (.wav) failus įterpiami remiantis ŽSB metodu. Informaciją galima paslėpti laisvuose diskų ir diskelių sektoriuose.

Jsteg programinė įranga: pagal ŽSB metodą duomenys paslepiami JFIF formato failuose (.jpg, .jpeg).

Hide and Seek: duomenys paslepiami GIF tipo paveikslų failuose ir papildomai užšifruojami IDEA šifravimo algoritmu.

PGE (angl. *Pretty Good Envelope*): duomenys supakuojami ir paslepiami GIF arba JPEG tipo paveikslų failuose.

Mandelsteg: pagal duomenis suformuojamas fraktalas ir išsaugomas GIF failuose.

Stego: bet koks failas pakeičiamas beprasmiu tekstu, remiantis laisvai parenkamu žodynu.

Texto: duomenys pakeičiami poetiškais angliškais sakiniais.

Stegovideo programa leidžia paslėpti bet kokio tipo failą vaizdo duomenyse. Nedidelį slepiamos informacijos kiekį galima prarasti vaizdo failą koduojant vienu iš populiarių kodeksų.

Bendras steganografijos principas:

Priedangos terpė + slaptas pranešimas + šifravimo raktas = steganografijos terpė.

Žemiau pateiktoje lentelėje (Lentelė 2) pateikiamas anksčiau išnagrinėtų steganografijos įrankių palyginimas. Joje matoma, kokių formatų dangos failai ir kokie steganografijos metodai naudojami

informacijai slėpti. Taip pat sužinoma, ar šis įrankis papildomai gali naudoti kriptografinius algoritmus ir kokius. Dar pateikiamas saugumo užtikrinimo lygis.

Įrankis	Dangos failo tipas	Steganografijos metodas	Kriptografijos algoritmai	Saugos užtikrinimas
„Windows OS“ komandinė eilutė	.jpg	Slepia informaciją po failo pabaigos simbolio.	Nėra	Aukštas
OpenStego	.jpg/.jpeg, .png, .bmp	Atitiktinis LSB	Neprivalomas (DES)	Aukštas
QuickStego	.jpg/.jpeg, .gif, .bmp	LSB	Nėra	Vidutinis
QuickCrypto	.jpg/.jpeg, .gif, .bmp	LSB	Neprivalomas (Blowfish, AES, 3DES).	Aukštas
OpenPuff	.bmp, .jpg, .png, .mp3 ir kt.	Naudojant pseudo atsitiktinių skaičių generatorių duomenys globaliai sumaišomi su atsitiktiniais indeksais.	AES, Anubis, Camellia, Cast-256, Clefia, FROG, Hierocrypt3, Idea-NXT, MARS, RC6, Safer+, SC2000, Serpent, Speed, 2fish, Unicorn-A.	Aukštas
Steghide	.jpeg/.jpg, .bmp, .wav, .au	Ieško grafinio teoretinio atitikmens.	Neprivalomas (Cast-128, gost, AES, 2fish, ARC4, cast-256, safer+, DES, 3DES, blowfish, RC2 ir kt.).	Aukštas
InvisibleSecrets	.jpg/.jpeg, .bmp, .png, .html, .wav	LSB	Blowfish, AES, 2fish, RC4, Cast-128, gost, diamond2, sapphire2.	Vidutinis

Lentelė 2 Steganografijos įrankių palyginimas

1.5. Analizės išvados

Analizės skyriuje buvo išsiaiškinta, kas yra steganografija ir kaip ji veikia, pagal tai buvo išskirtos jos kategorijos bei metodai. Taip pat buvo išskirti keli šifravimo metodai, tokie kaip: DES, 3DES, gost, twofish, blowfish, RC2 bei LSB. Jie buvo išanalizuoti ir išskirti kiekvieno privalumai bei trūkumai, sudarytos veikimo schemos. Atlikus šiuos veiksmus, metodai buvo palyginti tarpusavyje.

Toliau buvo išanalizuotas steganografijos atskleidimas, kur buvo išsiaiškinta, kaip ištirti stego atvaizdą, kad būtų galima sužinoti, ar ten iš viso kas nors yra paslėpta. Ir tik tuomet, kai atvaizdas bus įtariamas, ieškoma pati paslaptis. Kai kuriais atvejais, kai nepavyksta išgauti paslapties, failas būna daug kartų suspaudžiamas skirtingais metodais ir vėl išskleidžiamas, kad pasikeistų tiek, jog niekas nebegalėtų surasti tos paslapties.

Taip pat šioje dalyje buvo analizuojami įrankiai, kurie slepia, tikrina ar ieško informacijos įvairiuose daugiaformačiuose failuose. Vieni iš jų sukurti taip, kad galėtų naudoti tik vieną metodą, kiti gali naudoti kelis. Buvo išsiaiškinta, kad vieni įrankiai skirti tik informacijai slėpti (Pvz.,*StegoS*,

OpenPuff, *QuickStego*, *MP3Stego*, *S-Tools*, *Jsteg* ir kt.), kiti tik informacijos paieškai. Be abejo, yra tokių, kurie gali ir paslėpti, ir aptikti paslėptą informaciją (Pvz., *Steganography Studio, Steghide*).

2. STEGANOGRAFINIŲ METODŲ TYRIMO METODIKA

2.1. Duomenų slėpimas (steganografija)

Šioje dalyje bus aprašyta steganografinių metodų tyrimo eiga:

- Parinkti dangos failus;
- Parinkti „paslaptis“;
- Ištirti dangos failus;
- Parinkti steganografijos įrankius;
- Sudaryti stego atvaizdus;
- Ištirti sudarytus stego atvaizdus;
- Palyginti stego atvaizdus tarpusavyje;
- Surasti paslaptis stego atvaizduose.

Iš pradžių bus parenkami 5 dangos (atvaizdų) ir 5 „paslapčių“ (tekstų) skirtingo dydžio failai. Tuomet bus ištirti dangos failai, kad vėliau būtų galima palyginti, kiek skiriasi gauti stego atvaizdai nuo originalių failų.

Toliau, naudojant komandinę eilutę, QuickStego, Steghide, OpenStego, OpenPuff įrankius, bus sudaromi stego atvaizdai.

Komandinės eilutės pagalba kopijuosim dangos failą kartu su suglaudinta paslaptimi į stego atvaizdą. Tokiu būdu paslėptą pranešimą bus galima pamatyti su išskleidimo įrankiu atsidarius stego atvaizdą (pvz., WinRar).

QuickStego įrankiu slepiama informacija naudojant 1 bito LSB slėpimo metodą. Kadangi šis įrankis leidžia slėpti be arba su kriptografijos algoritmu, tai bandymus darysim ir su kriptografijos algoritmais (blowfish, AES, 3DES).

Steghide įrankiu taip pat galima slėpti tiek naudojant steganografijos metodą, tiek kartu naudojant šifravimą (blowfish, 2fish, DES, 3DES, gost, RC2 ir kt.). Todėl bandymai taip pat bus atliekami su ir be šifravimo. Šis įrankis taip pat naudoja LSB metodą.

OpenStego įrankiu informacija atvaizduose slepiama naudojant atsitiktinio LSB bitą. Šis įrankis leidžia slėpimą vykdyti naudojant tik steganografijos metodą ir papildomai naudojant DES šifravimo algoritmą, todėl tyrimo metu bandymai taip pat bus atliekami su ir be šifravimo.

Tyrimo metu paslaptys bus slepiamos tiek naudojant steganografijos metodus, tiek steganografijos metodus kartu su kriptografiniais algoritmais. Turint stego atvaizdus iš pradžių bus palyginti failų dydžių pokyčiai nuo dangos failų, taip pat tarpusavyje palyginti gauti greitaveikos

rezultatai, kad būtų galima nustatyti, kurie metodai ar įrankiai veikia greičiau ar lėčiau, kurie efektyviau ar daugiau slepia informacijos. Tuomet bus tikrinama, kiek gauti stego atvaizdai yra „slapti“, t.y. ar pagal aukščiau išvardintus kriterijus gauti rezultatai telpa į normas, o gal kelia įtarimą.

2.2. Slaptumas ir stegoanalizė

Atvaizdų slaptumo skaičiavimui bus naudojama pseudo atsitiktinio skaičiaus sekos testavimo atviro kodo programa ***ent*** 2008 metais parašyta Džono Volkerio (John Walker). Ši programa skaičiuoja:

- kiekvieno faile esančio simbolio pasiskirstymą procentais;
- entropiją;
- Chi kvadrato pasiskirstymą faile;
- duomenų baitų aritmetinį vidurkį;
- Monte Carlo π reikšmę;
- serijos koreliacijos koeficientą.

Chi kvadrato testai, poros palyginimai ir kiti statistiniai metodai gali įvertinti duomenų atvaizde atsitiktinumą. Jei bitai yra pernelyg netvarkingi arba perdaug kompaktiški, gali būti įtarta steganografija. Kuo daugiau duomenų slepiama dangos faile, tuo didesnė entropija. Entropija apskaičiuojama dauginant diskrečiojo rinkinio atsitiktinius įvykius (a_j), iš jų tikimybių ($P(a_j)$). Sumuojant šiuos rezultatus per visus j, ($\sum_j$), renkami vidutinis informacijos atitikmuo šaltinio išvesčiai:

$$H=-\sum_j P(a_j) \log P(a_j)$$ [20]

Naudojame histogramą stebėti atvaizdo įvertinimui ir rasti simbolio tikimybę šaltinyje, kai kinta nuo nulio (0) iki L-1 (paprastai 255):

$$\hat{H}=-\sum_k p_r(r_k) \log_2 p_r(r_k).$$ [20]

Jei gautas procentas didesnis nei 99% arba mažesnis nei 1%, seka yra beveik neabejotinai atsitiktinė. Jei procentas yra 95-99% arba 1-5% - seka yra įtariama. Jei 95-90% arba 5-10% - sekos yra beveik įtartinos.

Aritmetinė reikšmė yra apskaičiuojama paprastai – sumuojami visi baitai, esantys faile, ir dalinami iš failo ilgio. Jei reikšmė artima atsitiktiniam dydžiui (turėtų būti 127,5), tai simbolių seka yra atsitiktinė. Jei gautas rezultatas skiriasi nuo šios reikšmės, rezultatas yra nuosekliai aukštas arba žemas.

Monte Carlo π reikšmė. Kiekviena nuosekli 6 baitų seka yra naudojama kaip 24 bitų X ir Y koordinatės kvadrate. Jei atsitiktinai sugeneruoti taško atstumai yra mažesni už apskritimo, įbrėžto į kvadratą, spindulį, ši šešių baitų seka yra laikoma pažeista. Procentinė pažeidimų dalis gali būti

naudojama apskaičiuoti π reikšmę. Dėl labai didelių srautų (šie priartėjimų skirstymai labai lėti), reikšmė bus artima tiksliai π reikšmei, kei seka bus atsitiktinė.

Serijos koreliacijos koeficientas matuoja mastą, kaip kiekvienas baitas faile priklauso nuo ankstesnių baitų. Atsitiktinėse sekose ši reikšmė (ji gali būti ir teigiama, ir neigiama), žinoma, bus artima nuliui. Neatsitiktiniai baitų srautai, pvz., C programa duos serijos koreliacijos koeficientą artimą 0,5. Nepaprastai nuspėjamų duomenų koeficientas bus artimas vienetui.

Slaptumo rodiklių dydžiai, nekeliantys įtarimo failui:

- Entropija ≥ 7,90;
- Chi kvadrato pasiskirstymas faile ≤ 1% arba ≥ 99%;
- Duomenų baitų aritmetinis vidurkis 120 - 130;
- Monte Carlo π reikšmė ~ 3,14;
- Klaidos <5%;
- Serijos koreliacijos koeficientas < 0,1.

Ištyrus failų slaptumą, bus bandoma tais pačiais įrankiais, kuriais slėptos paslaptys, jas surasti. Tuomet bus tikrinama įrankių greitaveika, taip pat, ar stego atvaizdo parametrai pasikeitė po stegoanalizės pagalba surastos paslapties.

3. STEGANOGRAFINIŲ METODŲ TYRIMAS

Kadangi visi tyrimui parinkti įrankiai gali slėpti informaciją atvaizduose, tai tyrimui parenkami 5 dangos atvaizdai (Lentelė 3). Dangos atvaizdai buvo parinkti skirtingų dydžių ir spalvų, kad galima būtų palyginti kiekvieno metodo sugebėjimą:

- Slėpti didelį kiekį informacijos mažame dangos faile;
- Slėpti mažą kiekį informacijos dideliame dangos faile;
- Slėpti informaciją šviesiame ar tamsiame dangos faile.

danga1 (53,9 KB) 	danga4 (83,5 KB) 
danga3 (30,0 KB) 	danga2 (16,1 KB) 
danga5 (10,2 KB) 	

Lentelė 3 Tyrimo metu naudoti dangos (.jpg, .bmp) failai

Taip pat šio tyrimo metu buvo naudoti tekstiniai failai su skirtingo dydžio paslaptimis (žiūrėti skyrelį Priedai):

- paslaptis1.txt (3,47 MB)
- paslaptis2.txt (5,72 MB)

- paslaptis3.txt (1,95 MB)
- paslaptis4.txt (0,38 MB)
- paslaptis5.txt (0,04 MB)

Parinkus dangos atvaizdus buvo atlikta jų analizė, kad vėliau būtų galima matyti, kiek pasikeitė stego atvaizdų slaptumo įverčiai paslėpus juose informaciją (Lentelė 4). Iš gautų rezultatų matyti, kad dangos failai yra švarūs ir atitinka normatyvus, kurie nekelia įtarimo failams.

Failas	Entropija	Chi kvadratas (%)	Aritmetinis vidurkis	Monte Carlo π reikšmė	Klaidos procentas	Serijos koreliacijos koeficientas
Danga1	7,98	< 0,01	124,4016	3,22	2,35	0,03
Danga2	7,91	< 0,01	120,9497	3,21	2,12	0,10
Danga3	7,96	< 0,01	120,2641	3,27	3,98	0,06
Danga4	7,94	< 0,01	128,0124	3,05	2,96	0,07
Danga5	7,95	< 0,01	123,9481	3,20	1,93	0,04

Lentelė 4 Slaptumo skaičiavimas dangos failuose

3.1. Stego atvaizdų sudarymas

Toliau atliekami paslapčių slėpimai dangos failuose su kiekvienu tyrimo metodikos dalyje nurodytu steganografijos įrankiu ir pateikiama jų veikimo greitaveika, failo dydžio pasikeitimai, talpumas.

3.1.1. **„Windows OS“ komandinė eilutė**

Metodas: paslaptis įterpiama po failo pabaigos simbolio.

Naudoti dangos failai (.jpg) pateikti aukščiau esančioje lentelėje (Lentelė 3). Žemiau pateiktoje lentelėje (Lentelė 5) matome, kad naudojant šį įrankį pavyko paslėpti paslaptis visuose dangos atvaizduose. Taip pat matome, kad slėpimai vykdomi greitai (vidutiniškai 0,016 ms) ir gautų stego atvaizdų dydis dėl slėpimo nežymiai padidėja (vidutiniškai 1,30 KB). Dėl šios priežasties gauname pakankamai didelį gautų atvaidų talpumą (vidutiniškai 92,4 simb./KB).

Danga	Paslaptis	Gauto failo dydis (KB)	Slėpimas	Greitaveika (ms)	Talpumas (simb./KB)	Skirtumas (KB)
1	1	56,0	pavyko	0,15	63,6	2,1
1	2	56,8	pavyko	0,01	102,2	2,9
1	3	55,1	pavyko	0,01	36,0	1,2
1	4	54,3	pavyko	0,01	6,9	0,4
1	5	54,1	pavyko	0,01	0,8	0,2
2	1	18,1	pavyko	0,03	196,7	2,0
2	2	18,9	pavyko	0,02	307,2	2,8
2	3	17,2	pavyko	0,01	115,4	1,1
2	4	16,4	pavyko	0,01	22,9	0,3
2	5	16,2	pavyko	0,01	2,8	0,1

3	1	32,1	pavyko	0,01	110,9	2,1
3	2	32,9	pavyko	0,01	176,5	2,9
3	3	31,2	pavyko	0,01	63,6	1,2
3	4	30,4	pavyko	0,01	12,4	0,4
3	5	30,1	pavyko	0,01	1,5	0,1
4	1	85,6	pavyko	0,01	41,6	2,1
4	2	86,4	pavyko	0,01	67,2	2,9
4	3	84,7	pavyko	0,02	23,4	1,2
4	4	83,8	pavyko	0,01	4,5	0,3
4	5	83,6	pavyko	0,01	0,5	0,1
5	1	12,2	pavyko	0,01	291,9	2,0
5	2	13,0	pavyko	0,01	446,7	2,8
5	3	11,3	pavyko	0,01	175,7	1,1
5	4	10,5	pavyko	0,01	35,8	0,3
5	5	10,3	pavyko	0,01	4,4	0,1

Lentelė 5 Tyrimas naudojant „Windows OS“ komandinę eilutę

3.1.2. **Įrankis: „QuickStego“**

Metodas: 1 bito LSB įterpimas.

Naudoti dangos failai (.jpg) pateikti aukščiau esančioje lentelėje (Lentelė 3). Kadangi šis įrankis turi tik grafinę sąsają ir neturi įrašų žurnalo, tai negalime išmatuoti jo greitaveikos slepiant ir ieškant paslapties. Iš pateiktų rezultatų (Lentelė 6) matome, kad šis įrankis sugebėjo paslėpti visas paslaptis visuose dangos atvaizduose. Tačiau gautų stego atvaizdų dydis gerokai išaugo, vidutiniškai padidėjo apie 16 kartų. Dėl šios priežasties ženkliai sumažėjo failų talpumas (vidutiniškai 7,1 simb./KB). Lyginant su „Windows OS“ komandinės eilutės talpumu, šio įrankio talpumas 13 kartų mažesnis.

Danga	Paslaptis	Gauto failo dydis (KB)	Slėpimas	Talpumas (simb./KB)	Skirtumas (KB)
1	1	868	pavyko	4,1	814,1
1	2	868	pavyko	6,7	814,1
1	3	868	pavyko	2,3	814,1
1	4	868	pavyko	0,4	814,1
1	5	868	pavyko	0,1	814,1
2	1	217	pavyko	16,4	200,9
2	2	217	pavyko	26,8	200,9
2	3	217	pavyko	9,1	200,9
2	4	217	pavyko	1,7	200,9
2	5	217	pavyko	0,2	200,9
3	1	802	pavyko	4,4	772,0
3	2	802	pavyko	7,2	772,0
3	3	802	pavyko	2,5	772,0
3	4	802	pavyko	0,5	772,0
3	5	802	pavyko	0,1	772,0
4	1	800	pavyko	4,5	716,5
4	2	800	pavyko	7,3	716,5

4	3	800	pavyko	2,5	716,5
4	4	800	pavyko	0,5	716,5
4	5	800	pavyko	0,1	716,5
5	1	147	pavyko	24,2	136,8
5	2	147	pavyko	39,5	136,8
5	3	147	pavyko	13,5	136,8
5	4	147	pavyko	2,6	136,8
5	5	147	pavyko	0,3	136,8

Lentelė 6. Tyrimas naudojant „QuickStego“ LSB algoritmą

3.1.3. **Įrankis: „OpenStego“**

Metodas: LSB/ LSB+DES.

Naudoti dangos failai (.png) pateikti aukščiau esančioje lentelėje. Bandymai buvo atliekami naudojant steganografijos metodą be šifravimo ir steganografiją kartu su šifravimo algoritmu (DES). Atliekant šį bandymą gautų stego atvaizdų dydis dėl šifravimo nepakito, skyrėsi tik jų greitaveika (Lentelė 7). Kaip ir ankstesniais atvejais, šis įrankis taip pat sugebėjo paslėpti visus paslapčių failus dangos atvaizduose. Tačiau slėpimas užtruko pakankamai ilgai (vidutiniškai 1,03ms) lyginant su „Windows OS“ komandine eilute. Papildomai naudojant kriptogravimo algoritmą, slėpimo greitaveika vidutiniškai padidėjo apie 0,3 ms. Taip pat ir gautų stego atvaizdų dydis gerokai padidėjo (vidutiniškai apie 11 kartų), dėl to atvaizdų vidutinis talpumas tik 9,1 simb./KB.

Danga	Paslaptis	Gauto failo dydis (KB)	Slėpimas	Greitaveika be kriptografijos (ms)	Greitaveika su kriptografija(ms)	Talpumas (simb./KB)	Skirtumas (KB)
1	1	631	pavyko	1,56	1,78	5,6	577,1
1	2	634	pavyko	1,32	1,83	9,2	580,1
1	3	628	pavyko	1,20	1,72	3,2	574,1
1	4	625	pavyko	1,46	1,69	0,6	571,1
1	5	624	pavyko	1,45	1,68	0,1	570,1
2	1	186	pavyko	0,83	1,18	19,1	169,9
2	2	188	pavyko	0,81	1,16	30,9	171,9
2	3	185	pavyko	0,72	1,17	10,7	168,9
2	4	183	pavyko	0,77	1,17	2,1	166,9
2	5	182	pavyko	0,75	1,16	0,2	165,9
3	1	471	pavyko	1,42	1,42	7,6	441,0
3	2	477	pavyko	1,48	1,65	12,2	447,0
3	3	465	pavyko	1,41	1,45	4,3	435,0
3	4	460	pavyko	1,39	1,67	0,8	430,0
3	5	459	pavyko	1,22	1,68	0,1	429,0
4	1	472	pavyko	1,12	1,57	7,5	388,5
4	2	475	pavyko	1,17	1,50	12,2	391,5
4	3	464	pavyko	0,84	1,31	4,3	383,5
4	4	467	pavyko	1,10	1,29	0,8	380,5
4	5	463	pavyko	0,77	1,00	0,1	379,5
5	1	120	pavyko	0,66	0,70	29,7	109,8

5	2	121	pavyko	0,65	1,04	48,0	110,8
5	3	118	pavyko	0,56	1,00	16,8	107,8
5	4	117	pavyko	0,60	1,11	3,2	106,8
5	5	116	pavyko	0,60	0,88	0,4	105,8

Lentelė 7 Tyrimas naudojant „OpenStego“ įrankio LSB/LSB+DES metodus

3.1.4. **Įrankis: „Steghide“**

Metodas: grafinis teoretinis atitimuo.

Naudoti dangos failai (.jpg) pateikti aukščiau esančioje lentelėje (Lentelė 3). Kaip matome rezultatų lentelėje (Lentelė 8), šis įrankis nesugebėjo paslėpti pirmos, antros ir trečios paslapties antrame ir penktame dangos atvaizde; pirmos ir antros paslapties trečiame dangos atvaizde.Tačiau slėpimus atliko pakankamai greitai (vidutiniškai 0,09ms) ir gauti failai tik nežymiai padidėjo (vidutiniškai 0,9 KB), dėl to gaunamas nemažas talpumas (vidutiniškai 30,9 simb./KB). Tik naudojant didelį dangos failą (83,5 KB), gauti stego atvaizdai buvo penktadaliu mažesni už slėpimo metu naudotą dangos atvaizdą.

Danga	Paslaptis	Gauto failo dydis (KB)	Slėpimas	Greitaveika (ms)	Talpumas (simb./KB)	Skirtumas (KB)
1	1	55,6	pavyko	0,15	64,0	1,7
1	2	55,7	pavyko	0,13	104,3	1,8
1	3	55,5	pavyko	0,07	35,8	1,6
1	4	55,4	pavyko	0,05	6,8	1,5
1	5	55,3	pavyko	0,06	0,8	1,4
2	1	16,1	**nepavyko**	0,04	0,0	0,0
2	2	16,1	**nepavyko**	0,04	0,0	0,0
2	3	16,1	**nepavyko**	0,04	0,0	0,0
2	4	16,2	pavyko	0,05	23,2	0,1
2	5	16,2	pavyko	0,04	2,8	0,1
3	1	30,0	**nepavyko**	0,04	0,0	0,0
3	2	30,0	**nepavyko**	0,04	0,0	0,0
3	3	30,8	pavyko	0,07	64,4	0,8
3	4	30,7	pavyko	0,05	12,2	0,7
3	5	30,7	pavyko	0,06	1,5	0,7
4	1	68,8	pavyko	0,11	51,8	-14,7
4	2	68,9	pavyko	0,13	84,3	-14,6
4	3	68,7	pavyko	0,07	28,9	-14,8
4	4	68,6	pavyko	0,05	5,5	-14,9
4	5	68,6	pavyko	0,05	0,7	-14,9
5	1	10,2	**nepavyko**	0,04	0,0	0,0
5	2	10,2	**nepavyko**	0,04	0,0	0,0
5	3	10,2	**nepavyko**	0,04	0,0	0,0
5	4	10,8	pavyko	0,41	34,8	0,6
5	5	10,8	pavyko	0,05	4,2	0,6

Lentelė 8 Tyrimas naudojant „Steghide“ įrankio LSB metodą

Žemiau pateikiami rezultatai (Pav. 4), kurie buvo gauti slepiant iš eilės visas paslaptis antrame dangos faile. „Plika“ akimi žiūrint net negali pasakyti, kad paveikslėliai kažkuo skiriasi.

Pav. 4 Dangos failas ir stego atvaizdai su skirtingomis paslaptimis

Metodas: grafinis teoretinis atitimuo + Blowfish.

Žemiau pateikiami duomenys gauti naudojant LSB metodą kartu su blowfish šifravimo algoritmu (Lentelė 9). Kaip ir naudojant tik steganografijos metodą, taip ir papildomai naudojant šifravimą, nepavyko paslėpti pirmos, antros ir trečios paslapties antrame ir penktame dangos atvaizduose, taip pat pirmos ir antros paslapties trečiame dangos faile. Dėl papildomai naudoto kriptografijos algoritmo, padidėjo slėpimo greitaveika (vidutiniškai 0,25 ms), tačiau gautų stego atvaizdų dydis ir talpumas išliko toks pat, kaip ir naudojant tik steganografijos metodą.

Danga	Paslaptis	Gauto failo dydis (KB)	Slėpimas	Greitaveika (ms)	Talpumas (simb./KB)	Skirtumas (KB)
1	1	55,6	pavyko	0,34	64,0	1,7
1	2	55,7	pavyko	0,44	104,3	1,8
1	3	55,5	pavyko	0,28	35,8	1,6
1	4	55,4	pavyko	0,28	6,8	1,5
1	5	55,3	pavyko	0,21	0,8	1,4
2	1	16,1	**nepavyko**	0,15	0,0	0,0
2	2	16,1	**nepavyko**	0,17	0,0	0,0
2	3	16,1	**nepavyko**	0,18	0,0	0,0

2	4	16,2	pavyko	0,20	23,2	0,1
2	5	16,2	pavyko	0,17	2,8	0,1
3	1	30,0	**nepavyko**	0,18	0,0	0,0
3	2	30,0	**nepavyko**	0,26	0,0	0,0
3	3	30,8	pavyko	0,26	64,4	0,8
3	4	30,7	pavyko	0,20	12,2	0,7
3	5	30,7	pavyko	0,21	1,5	0,7
4	1	68,7	pavyko	0,45	51,8	-14,8
4	2	68,9	pavyko	0,42	84,3	-14,6
4	3	68,7	pavyko	0,23	28,9	-14,8
4	4	68,6	pavyko	0,21	5,5	-14,9
4	5	68,6	pavyko	0,15	0,7	-14,9
5	1	10,2	**nepavyko**	0,17	0,0	0,0
5	2	10,2	**nepavyko**	0,17	0,0	0,0
5	3	10,2	**nepavyko**	0,13	0,0	0,0
5	4	10,8	pavyko	0,16	34,8	0,6
5	5	10,8	Pavyko	0,13	4,2	0,6

Lentelė 9 Tyrimas naudojant „Steghide“ įrankio LSB+BlowFish metodą

Metodas: grafinis teoretinis atitimuo + GOST.

Žemiau pateikiami duomenys gauti naudojant LSB metodą kartu su gost šifravimo algoritmu (Lentelė 10). Šis įrankis su gost šifravimo algoritmu taip pat nesugebėjo paslėpti pirmos paslapties antrame dangos atvaizde, pirmos ir antros paslapties trečiame dangos atvaizde bei pirmos, antros ir trečios paslapties penktame dangos atvaizde. Gauta vidutinė greitaveika 0,27 ms, kadangi vidutiniškai gauti stego atvaizdai padidėjo 12,1 KB, tai vidutinis atvaizdų talpumas išlieka apie 34,1 simb./KB.

Danga	Paslaptis	Gauto failo dydis (KB)	Slėpimas	Greitaveika (ms)	Talpumas (simb./KB)	Skirtumas (KB)
1	1	55,6	pavyko	0,36	64,0	1,7
1	2	55,7	pavyko	0,43	104,3	1,8
1	3	55,5	pavyko	0,29	35,8	1,6
1	4	55,4	pavyko	0,24	6,8	1,5
1	5	55,3	pavyko	0,32	0,8	1,4
2	1	16,1	**nepavyko**	0,18	0,0	0,0
2	2	55,7	pavyko	0,41	104,3	39,6
2	3	55,5	pavyko	0,30	35,8	39,4
2	4	55,4	pavyko	0,17	6,8	39,3
2	5	55,3	pavyko	0,20	0,8	39,2
3	1	30,0	**nepavyko**	0,15	0,0	0,0
3	2	30,0	**nepavyko**	0,15	0,0	0,0
3	3	30,8	pavyko	0,22	64,4	0,8
3	4	30,7	pavyko	0,18	12,2	0,7
3	5	30,8	pavyko	0,15	1,5	0,8
4	1	68,8	pavyko	0,35	51,8	-14,7

4	2	68,9	pavyko	0,43	84,3	-14,6
4	3	68,7	pavyko	0,28	28,9	-14,8
4	4	68,6	pavyko	0,21	5,5	-14,9
4	5	55,3	pavyko	0,20	0,8	-28,2
5	1	10,2	**nepavyko**	0,16	0,0	0,0
5	2	10,2	**nepavyko**	0,16	0,0	0,0
5	3	10,2	**nepavyko**	0,15	0,0	0,0
5	4	10,8	pavyko	0,18	34,8	0,6
5	5	10,8	pavyko	0,15	4,2	0,6

Lentelė 10 Tyrimas naudojant „Steghide“ įrankio LSB+GOST metodą

Metodas: grafinis teoretinis atitimuo + 2FISH.

Žemiau pateikiami duomenys gauti naudojant LSB metodą kartu su twofish šifravimo algoritmu (Lentelė 11). Kartu naudojant twofish šifravimo algoritmą, nepavyko paslėpti pirmos paslapties antrame dangos atvaizde, pirmos ir antros paslapties trečiame dangos atvaizde bei pirmos, antros bei trečios palapties penktame dangos atvaizde. Vidutiniškai 0,19 ms užtruko sudaryti stego atvaizdą. Sudarytų atvaizdų dydis buvo labai panašus į anksčiau gautus duomenis (LSB metodas su gost algoritmu), vidutiniškai atvaizdai padidėjo 12,1 KB, todėl talpumas išliko 34,0 simb./KB.

Danga	**Paslaptis**	**Gauto failo dydis (KB)**	**Slėpimas**	Greitaveika (ms)	**Talpumas (simb./KB)**	**Skirtumas (KB)**
1	1	55,6	pavyko	0,37	64	1,7
1	2	55,6	pavyko	0,42	104,4	1,7
1	3	55,5	pavyko	0,23	35,8	1,6
1	4	55,4	pavyko	0,27	6,8	1,5
1	5	55,3	pavyko	0,16	0,8	1,4
2	1	16,1	**nepavyko**	0,11	0,0	0,0
2	2	55,8	pavyko	0,27	104,1	39,7
2	3	55,8	pavyko	0,18	35,6	39,7
2	4	55,3	pavyko	0,18	6,8	39,2
2	5	55,3	pavyko	0,13	0,8	39,2
3	1	30,0	**nepavyko**	0,10	0,0	0,0
3	2	30,0	**nepavyko**	0,11	0,0	0,0
3	3	30,8	pavyko	0,15	64,4	0,8
3	4	30,7	pavyko	0,12	12,2	0,7
3	5	30,7	pavyko	0,11	1,5	0,7
4	1	68,8	pavyko	0,20	51,8	-14,7
4	2	68,8	pavyko	0,24	84,4	-14,7
4	3	68,8	pavyko	0,16	28,9	-14,7
4	4	68,6	pavyko	0,16	5,5	-14,9
4	5	55,3	pavyko	0,11	0,8	-28,2
5	1	10,2	**nepavyko**	0,09	0,0	0,0
5	2	10,2	**nepavyko**	0,12	0,0	0,0
5	3	10,2	**nepavyko**	0,09	0,0	0,0
5	4	10,8	pavyko	0,10	34,8	0,6

5	5	10,8	pavyko	0,09	4,2	0,6

Lentelė 11 Tyrimas naudojant „Steghide“ įrankio LSB+2FISH metodą

Metodas: grafinis teoretinis atitimuo + 3DES.

Žemiau pateikiami duomenys gauti naudojant LSB metodą kartu su tripledes šifravimo algoritmu (Lentelė 12). Pavyko sudaryti tuos pačius stego atvaizdus kaip ir ankstesniais atvejais. Vidutinė slėpimo greitaveika padidėjo iki 0,24 ms. Tačiau vidutinis talpumas (34,1simb./KB) ir gautų atvaizdų padidėjimas (12,1 KB) išliko toks pat, kaip ir papildomai naudojant ankstesnius šifravimo algoritmus.

Danga	Paslaptis	Gauto failo dydis (KB)	Slėpimas	Greitaveika (ms)	Talpumas (simb./KB)	Skirtumas (KB)
1	1	55,6	pavyko	0,37	64	1,7
1	2	55,7	pavyko	0,34	104,3	1,8
1	3	55,5	pavyko	0,22	35,8	1,6
1	4	55,4	pavyko	0,26	6,8	1,5
1	5	55,3	pavyko	0,15	0,8	1,4
2	1	16,1	**nepavyko**	0,18	0,0	0,0
2	2	55,8	pavyko	0,38	104,1	39,7
2	3	55,5	pavyko	0,27	35,8	39,4
2	4	55,3	pavyko	0,18	6,8	39,2
2	5	55,3	pavyko	0,16	0,8	39,2
3	1	30,0	**nepavyko**	0,13	0,0	0,0
3	2	30,0	**nepavyko**	0,13	0,0	0,0
3	3	30,8	pavyko	0,17	64,4	0,8
3	4	30,7	pavyko	0,17	12,2	0,7
3	5	30,7	pavyko	0,12	1,5	0,7
4	1	68,8	pavyko	0,36	51,8	-14,7
4	2	68,8	pavyko	0,38	84,4	-14,7
4	3	68,8	pavyko	0,27	28,9	-14,7
4	4	68,6	pavyko	0,25	5,5	-14,9
4	5	55,3	pavyko	0,23	0,8	-28,2
5	1	10,2	**nepavyko**	0,18	0,0	0,0
5	2	10,2	**nepavyko**	0,16	0,0	0,0
5	3	10,2	**nepavyko**	0,16	0,0	0,0
5	4	10,8	pavyko	0,17	34,8	0,6
5	5	10,8	pavyko	0,15	4,2	0,6

Lentelė 12 Tyrimas naudojant „Steghide“ įrankio LSB+3DES algoritmą

Metodas: grafinis teoretinis atitimuo + RC2.

Žemiau pateikiami duomenys gauti naudojant LSB metodą kartu su rc2 šifravimo algoritmu (Lentelė 13). Kaip ir papildomai naudojant ankstesnius šifravimo algoritmus, taip ir naudojant šį, nepavyko sudaryti visų stego atvaizdų. Labai panašūs ir jų gauti rezultatai: vidutinė greitaveika – 0,23 ms, vidutinis talpumas – 34,1 simb./KB, vidutinis gauto atvaizdo padidėjimas – 12,1 KB.

Danga	Paslaptis	Gauto failo dydis (KB)	Slėpimas	Greitaveika (ms)	Talpumas (simb./KB)	Skirtumas (KB)
1	1	55,6	pavyko	0,40	64	1,7
1	2	55,7	pavyko	0,41	104,3	1,8
1	3	55,7	pavyko	0,28	35,6	1,8
1	4	55,7	pavyko	0,24	6,8	1,8
1	5	55,3	pavyko	0,25	0,8	1,4
2	1	16,1	**nepavyko**	0,17	0,0	0,0
2	2	55,7	pavyko	0,33	104,3	39,6
2	3	55,6	pavyko	0,24	35,7	39,5
2	4	55,3	pavyko	0,21	6,8	39,2
2	5	55,3	pavyko	0,16	0,8	39,2
3	1	30,0	**nepavyko**	0,12	0,0	0,0
3	2	30,0	**nepavyko**	0,15	0,0	0,0
3	3	30,8	pavyko	0,21	64,4	0,8
3	4	30,7	pavyko	0,14	12,2	0,7
3	5	30,7	pavyko	0,11	1,5	0,7
4	1	68,8	pavyko	0,23	51,8	-14,7
4	2	68,9	pavyko	0,25	84,3	-14,6
4	3	68,7	pavyko	0,17	28,9	-14,8
4	4	68,7	pavyko	0,20	5,5	-14,8
4	5	55,3	pavyko	0,27	0,8	-28,2
5	1	10,2	**nepavyko**	0,16	0,0	0,0
5	2	10,2	**nepavyko**	0,20	0,0	0,0
5	3	10,2	**nepavyko**	0,14	0,0	0,0
5	4	10,8	pavyko	0,15	34,8	0,6
5	5	10,8	pavyko	0,20	4,2	0,6

Lentelė 13 Tyrimas naudojant „Steghide“ įrankio LSB+RC2 algoritmą

Metodas: grafinis teoretinis atitimuo + DES

Žemiau pateikiami duomenys gauti naudojant LSB metodą kartu su des šifravimo algoritmu (Lentelė 14). Taip pat ir papildomai naudojant des šifravimo algoritmą, gauti rezultatai beveik nesiskiria nuo anksčiau gautų: vidutinė greitaveika – 0,24 ms, vidutinis talpumas – 34,1 simb./KB, vidutinis gauto atvaizdo padidėjimas – 12,1 KB.

Danga	Paslaptis	Gauto failo dydis (KB)	Slėpimas	Greitaveika (ms)	Talpumas (simb./KB)	Skirtumas (KB)
1	1	55,6	pavyko	0,35	64,0	1,7
1	2	55,7	pavyko	0,35	104,3	1,8
1	3	55,5	pavyko	0,24	35,8	1,8
1	4	55,4	pavyko	0,16	6,8	1,8
1	5	55,3	pavyko	0,17	0,8	1,4
2	1	16,1	**nepavyko**	0,16	0,0	0,0
2	2	55,8	pavyko	0,39	104,1	39,6
2	3	55,5	pavyko	0,24	35,8	39,5

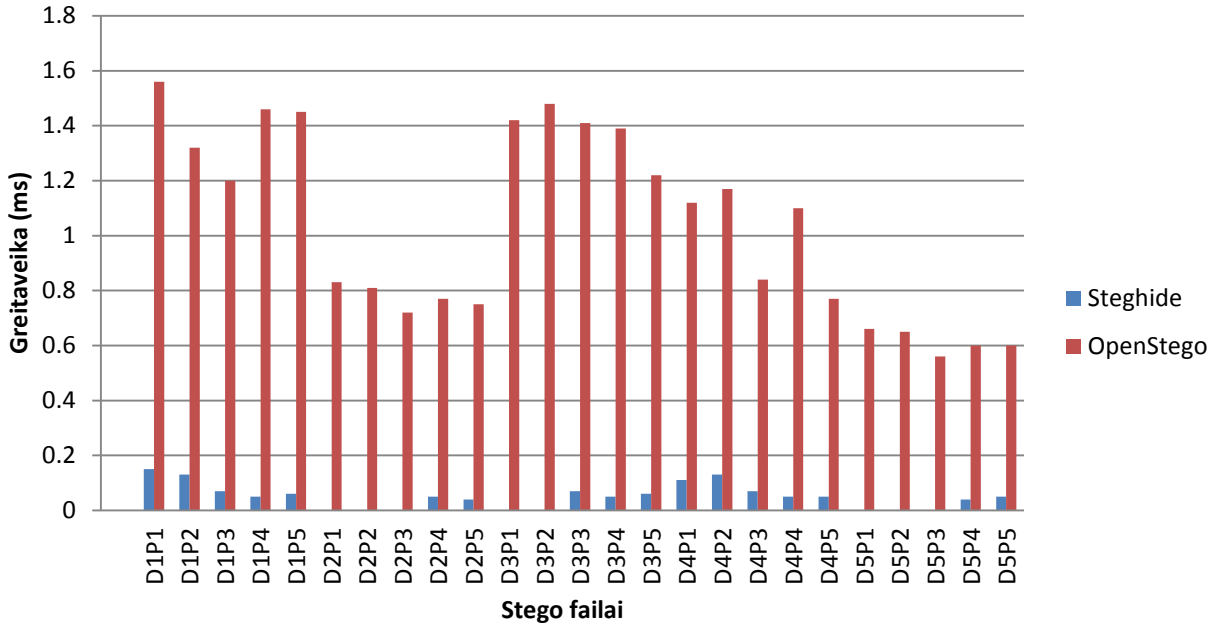
2	4	55,3	pavyko	0,23	6,8	39,2
2	5	55,3	pavyko	0,14	0,8	39,2
3	1	30	**nepavyko**	0,19	0,0	0,0
3	2	30	**nepavyko**	0,17	0,0	0,0
3	3	30,8	pavyko	0,31	64,4	0,8
3	4	30,7	pavyko	0,22	12,2	0,7
3	5	30,7	pavyko	0,16	1,5	0,7
4	1	68,8	pavyko	0,25	51,8	-14,7
4	2	68,8	pavyko	0,34	84,4	-14,6
4	3	68,8	pavyko	0,33	28,9	-14,8
4	4	68,6	pavyko	0,24	5,5	-14,8
4	5	55,3	pavyko	0,16	0,8	-28,2
5	1	10,2	**nepavyko**	0,15	0,0	0,0
5	2	10,2	**nepavyko**	0,15	0,0	0,0
5	3	10,2	**nepavyko**	0,22	0,0	0,0
5	4	10,8	pavyko	0,14	34,8	0,6
5	5	10,8	pavyko	0,12	4,2	0,6

Lentelė 14 Tyrimas naudojant „Steghide“ įrankio LSB+DES algoritmą

3.2. Greitaveika

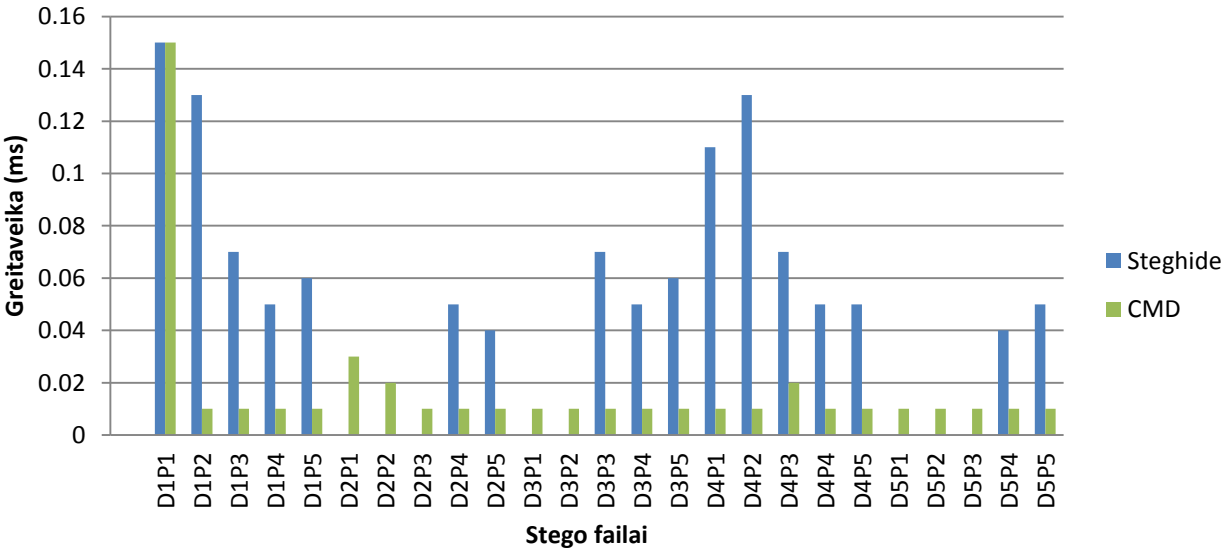
Šioje dalyje pateikiamas greitaveikos palyginimai nadojant tą patį steganografijos metodą su skirtingais įrankiais. Taip pat naudojant tą patį įrankį į pagalbą pasitelkiant kriptografiją.

Kadangi greitaveiką pavyko suskaičiuoti tik dviejų įrankių, kurie naudoja LSB metodą, tai žemiau pateiktoje diagramoje (Pav. 5) matomas tik „OpenStego“ ir „Steghide“ įrankių greitaveikos palyginimas. Joje matyti, kad „Steghide“ įrankis, nors ir ne visuose failuose sugebėjo paslėpti pranešimus, tačiau slėpimą įvykdydavo iki 0,2ms. „OpenStego“ įrankis sugebėjo paslėpti visus pranešimus, tačiau slėpdamas užtrukdavo beveik 8 kartų ilgiau.



Pav. 5 Greitaveikos palyginimo naudojant LSB metodą diagrama

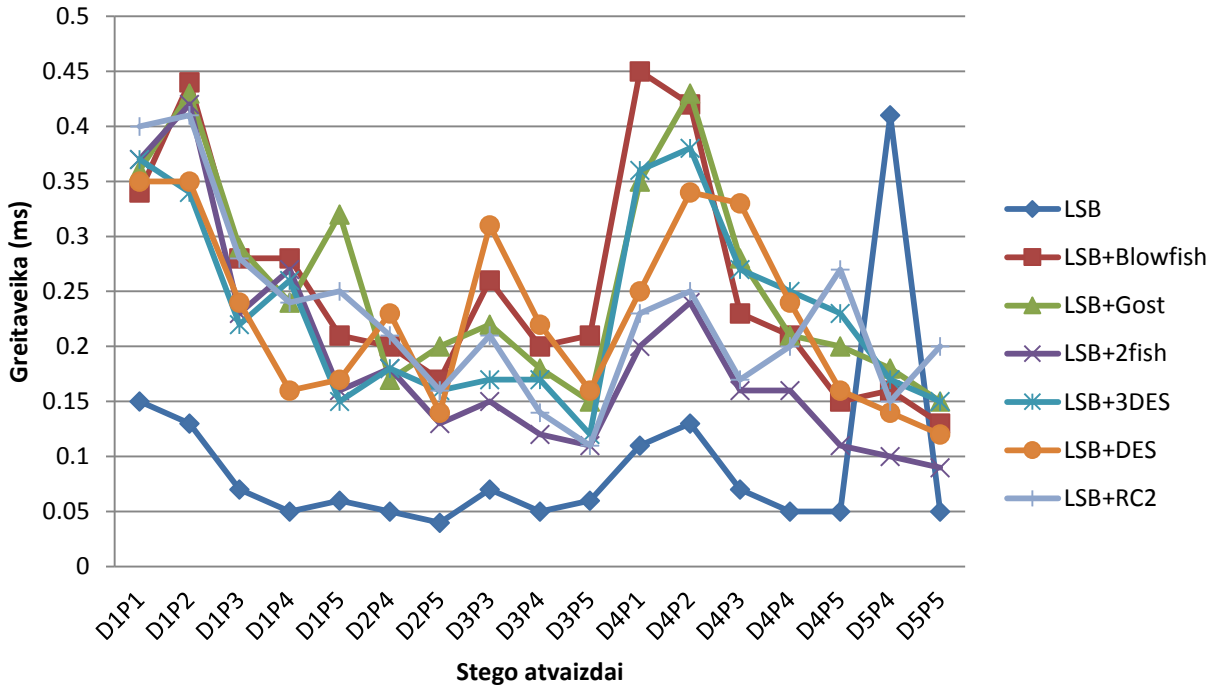
Jei lygintume greitaveiką tarp įrankių, nepriklausomai nuo to, kokį slėpimo metodą jie naudoja su panašiais rezultatais, tai matytume, kad „OpenStego“ užtrukdavo ilgiausiai. „Steghide“ ir komandinė eilutė slėpdamos pranešimus atvaizduose užtrukdavo panašų laiko tarpą (iki 0,15 ms) (Pav. 6). Vidutiniškai „Steghide“ užtrukdavo – 0,09 ms, „OpenStego“ – 1,03 ms, komandinė eilutė – 0,02 ms. Taigi galime teigti, kad greičiausiai slėpimą vykdo komandinė eilutė informaciją įrašydama į dangos failo pabaigą.



Pav. 6 Greitaveikos palyginimo naudojant skirtingus steganografijos metodus diagrama

„Stegohide“ pagalba buvo paslėpti pranešimai ir papildomai naudojant kriptografijos algoritmus (blowfish, gost, twofish, tripledes, des ir rc2). Žemiau pateiktoje diagramoje (Pav. 7)

matomas greitaveikos pasiskirstymas tarp naudotų algoritmų su tais pačiais dangos ir paslapties failais.

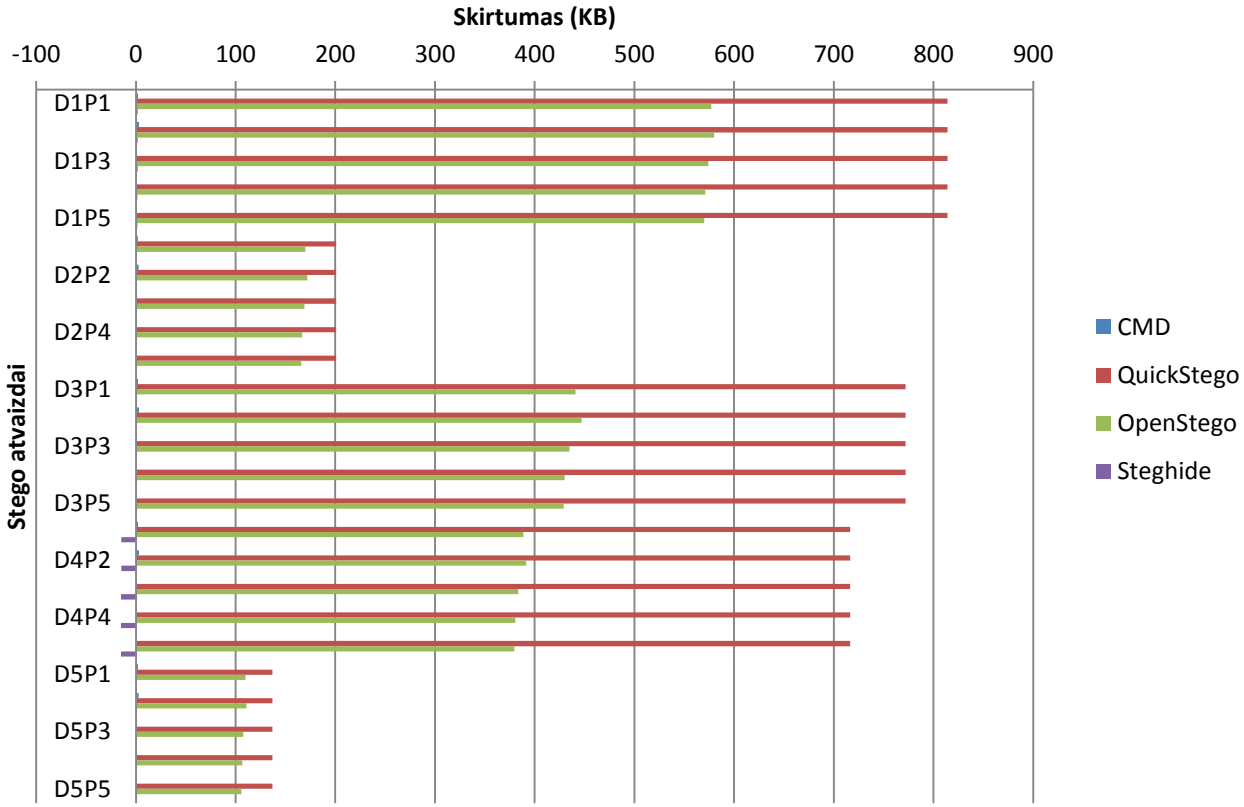


Pav. 7 Greitaveikos palyginimo naudojant „Stegohide“ įrankį diagrama

Kaip ir buvo galima tikėtis, visais atvejais be šifravimo slėpimai vykdavo žymiai greičiau. Tačiau tam, kad būtų užtikrintas aukštesnis paslapties saugumas, naudojami kriptografiniai metodai, tai greitaveika tarp skirtingų šifravimo metodų skiriasi visai nežymiai.

3.3. Failo dydžio pakitimas po slėpimo

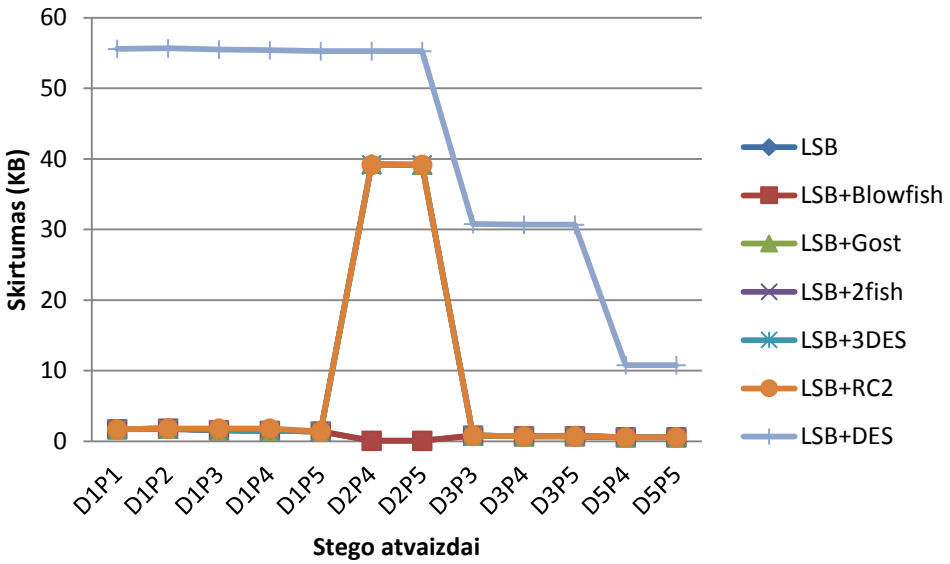
Šioje dalyje palyginama gautų stega atvaizdų dydžio pakitimai po slėpimų. Iš anksčiau pateiktų stego atvaizdų duomenų matyti, kad naudojant „QuickStego“ ir „OpenStego“ gauti atvaizdai beveik 10 kartų didesni už pradinius dangos failus. Tuo tarpu slepimui naudojant komandinę eilutę arba „Steghide“ įrankį, gautų failų dydis tik nežymiai pasikeisdavo (Pav. 8).



Pav. 8 Gautų atvaizdų dydžių pokyčio diagrama

Naudojant komandinę eilutę, failai vidutiniškai padidėdavo 1,3 KB, „QuickStego“ – 528,1 KB, „OpenStego“ – 334,5 KB, „Steghide“ – 1,0 KB.

Jei papildomai slėpimui būdavo naudojama kriptografija, tai dauguma atvejų failo dydis nesiskirdavo nuo tų, kuriuose slėpimui būdavo naudojama tik steganografija. Naudojant „OpenStego“ įrankį, gauti stego atvaizdai slėpimo metu tiek naudojant šifravimą, tiek jo nenaudojant buvo vienodo dydžio. Naudojant „Steghide“ įrankį gauti stego atvaizdai sudaryti su pirma, trečia ir penkta dangomis ir papildomai naudojus 3DES, RC2, 2fish, gost ar blowfish šifravimo algoritmus, beveik nesiskyrė nuo stego atvaizdų, kurie sudaryti naudojant tik steganografijos metodą (Pav. 9). Naudojant papildomai naudojant DES šifravimo algoritmą, failų dydžiai akivaizdžiai padidėjo. Taip pat atvaizdai labai padidėdavo, kai buvo slepiama santykinai mažas paslapties failas dideliame dangos faile.



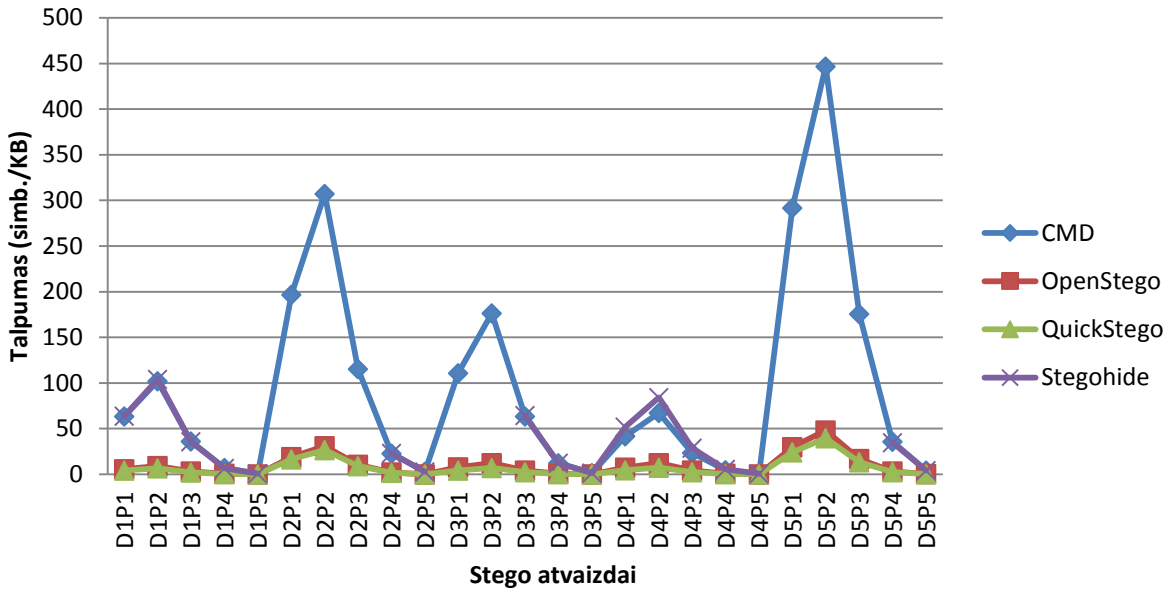
Pav. 9„Steghide“ įrankio sukurtų atvaizdų dydžių pasikeitimo diagrama

3.4. Slepiamos informacijos kiekis

Tyrimo metu buvo lyginamas slėpimo įrankių sudarytų stego atvaizdų informacijos talpumas dangose. Diagramoje nematome visų stego atvaizdų informacijos kiekio talpinimo naudojant „Steghide“ įrankį, nes šis įrankis nesugebėjo paslėpti:

- pirmos (3,47 KB), antros (5,72 KB) ir trečios (1,92 KB) paslapties antrame paveikslėlyje (16,1 KB);
- pirmos (3,47 KB) ir antros (5,72 KB) paslapties trečiame paveikslėlyje (30 KB);
- pirmos (3,47 KB), antros (5,72 KB) ir trečios (1,92 KB) paslapties penktame paveikslėlyje (10,2 KB);

Ankstesnėje diagramoje (Pav. 8) matėme, kad slepiant labai mažą failą su paslaptimi (0,04 KB) bet kokiame dangos faile naudojant „OpenStego“ arba „QuickStego“ įrankį, gaunami stego atvaizdų failai yra daug didesni už dangos failus. Todėl žemiau pateiktoje diagramoje (Pav. 10) šių įrankių sukurtuose stego atvaizduose labai mažas talpumas. Taip pat matoma, kad kuo didesnis failas, tuo daugiau informacijos jame galima paslėpti.



Pav. 10 Slepiamos informacijos kiekio stego atvaizduose diagrama

3.5. „Slaptumas“

Kai žinomas steganografijos metodas, kuriuo buvo įdėta paslaptis, paslapties paieškos metodas gali būti nesunkiai pritaikytas, t.y. pasirenkama *specifinė* stegoanalizė. Kai metodas yra nežinomas, paieškos technikos dažniausiai yra paprastos. Tai vadinama „akla“ stegoanalizė. Dažniausi srities metodai geriau išlaiko dangos ir paslapties integralumą, apsaugo atvaizdą nuo suskleidimo ir filtravimo metu atsirandančių pakitimų.

Toliau lyginsime gautų failų slaptumo įverčius, aprašytus antrame šio darbo skyriuje.

„Windows OS“ komandinės eilutės pagalba sudarytų stego atvaizdų slaptumo rodikliai pateikti žemiau esančioje lentelėje (Lentelė 15). Joje matome, kad visi stego atvaizdų gauti slaptumo įverčiai atitinka normatyvus, todėl galima teigti, jog šio įrankio naudojamas slėpimo metodas užtikrina aukštą saugos lygį.

Dan-ga	Pas-lap-tis	Entropija	Chi kvadratas	Aritmetinis vidurkis	Monte Carlo π reikšmė	Klaidos procentas	Serijos koreliacijos koeficientas
1	1	7,98	< 0,01	124,4392	3,21	2,21	0,03
1	2	7,98	< 0,01	124,4406	3,22	2,45	0,03
1	3	7,98	< 0,01	124,3442	3,22	2,38	0,03
1	4	7,98	< 0,01	124,3480	3,22	2,36	0,03
1	5	7,98	< 0,01	124,2947	3,22	2,40	0,03
2	1	7,92	< 0,01	121,4619	3,20	1,89	0,09
2	2	7,93	< 0,01	121,5894	3,21	2,24	0,09
2	3	7,92	< 0,01	121,0004	3,21	2,10	0,10
2	4	7,91	< 0,01	120,8435	3,21	2,28	0,10
2	5	7,91	< 0,01	120,6188	3,21	2,22	0,10
3	1	7,96	< 0,01	120,5982	3,26	3,71	0,06
3	2	7,96	< 0,01	120,6923	3,25	3,50	0,06

3	3	7,96	< 0,01	120,3178	3,26	3,88	0,06
3	4	7,96	< 0,01	120,2143	3,26	3,90	0,06
3	5	7,95	< 0,01	120,0890	3,27	4,05	0,06
4	1	7,94	< 0,01	127,9490	3,05	2,88	0,07
4	2	7,94	< 0,01	127,9181	3,05	2,76	0,07
4	3	7,94	< 0,01	127,9251	3,05	2,89	0,07
4	4	7,93	< 0,01	127,9632	3,05	2,91	0,07
4	5	7,93	< 0,01	127,9381	3,05	2,93	0,07
5	1	7,96	< 0,01	124,1969	3,19	1,64	0,05
5	2	7,96	< 0,01	124,2177	3,19	1,59	0,04
5	3	7,95	< 0,01	123,7163	3,19	1,53	0,04
5	4	7,95	< 0,01	123,6865	3,21	2,18	0,04
5	5	7,95	< 0,01	123,3930	3,21	2,16	0,05

Lentelė 15 „Windows OS“ komandinės eilutės sukurtų atvaizdų slaptumo analizė

Toliau pateikiami „QuickStego“ įrankiu sukurtų stego atvaizdų slaptumo įverčių rezultatai (Lentelė 16). Joje matome, kad pagal entropijos dydį visi stego atvaizdai, sudaryti su ketvirtu ir penktu dangos atvaizdu, yra žemiau normatyvo. Aritmetiniai vidurkiai su pirma, ketvirta ir penkta dangomis taip pat neatitinka normatyvų. Monte Carlo π reikšmės atitinka normatyvus tik tų stego atvaizdų, kurie sudaryti su antru dangos atvaizdu. Gauti klaidos procentai įtartinai dideli atvaizdų, sudarytų su pirma, trečia, ketvirta ir penkta dangomis. O žiūrint serijos koreliacijos koeficientų reikšmes, visi sudaryti atvaizdai patenka į rėžį, kai atvaizdai kelia labai didelį įtarimą.

Dan-ga	Pas-lap-tis	Entropija	Chi kvadratas	Aritmetinis vidurkis	Monte Carlo π reikšmė	Klaidos procentas	Serijos koreliacijos koeficientas
1	1	7,75	< 0,01	162,8468	2,57	18,04	0,81
1	2	7,75	< 0,01	162,8466	2,57	18,06	0,81
1	3	7,75	< 0,01	162,8467	2,57	18,05	0,81
1	4	7,75	< 0,01	162,8466	2,57	18,05	0,81
1	5	7,75	< 0,01	162,8466	2,57	18,05	0,81
2	1	7,90	< 0,01	121,1410	3,28	4,46	0,93
2	2	7,90	< 0,01	121,1429	3,28	4,45	0,93
2	3	7,90	< 0,01	121,1426	3,28	4,46	0,93
2	4	7,90	< 0,01	121,1423	3,28	4,46	0,93
2	5	7,90	< 0,01	121,1424	3,28	4,46	0,93
3	1	7,91	< 0,01	129,6434	2,91	7,25	0,74
3	2	7,91	< 0,01	129,6433	2,91	7,25	0,74
3	3	7,91	< 0,01	129,6435	2,91	7,25	0,74
3	4	7,91	< 0,01	129,6434	2,91	7,25	0,74
3	5	7,91	< 0,01	129,6434	2,91	7,25	0,74
4	1	7,34	< 0,01	94,2497	3,92	24,81	0,89
4	2	7,34	< 0,01	94,2495	3,92	24,81	0,89
4	3	7,34	< 0,01	94,2509	3,92	24,81	0,89
4	4	7,34	< 0,01	94,2512	3,92	24,81	0,89
4	5	7,34	< 0,01	94,2512	3,92	24,81	0,89
5	1	7,57	< 0,01	111,8219	3,73	18,75	0,84
5	2	7,57	< 0,01	111,8205	3,73	18,74	0,84
5	3	7,57	< 0,01	111,8213	3,73	18,74	0,84

5	4	7,57	< 0,01	111,8296	3,73	18,76	0,84
5	5	7,57	< 0,01	111,8297	3,73	18,76	0,83

Lentelė 16 „QuickStego“ įrankiu sukurtų atvaizdų slaptumo analizė

Taigi visi atvaizdai, sudaryti su šiuo įrankių, neatitinka normatyvų,visi jie kelia didelį įtarimą failams.

„OpenStego“ įrankiu sukurtų failų su paslaptimis analizės rezultatai. Žemiau pateiktoje lentelėje (Lentelė 17) pateikiami ištirti atvaizdai, kuriuos kuriant buvo naudojamas tik steganografijos metodas, ir tie, kuriuos kuriant buvo papildomai naudojamas DES šifravimo algoritmas.

Failai, sudaryti naudojant tik steganografijos metodą, beveik visi atitinka normatyvus, kurie nekelia įtarimo failams. Monte Carlo π reikšmės įverčiai failams trečia ir penkta dangomis yra kiek žemiau normos, todėl jie yra beveik nekeliantys įtarimo. Tačiau su trečia danga sudarytų atvaizdų gauti klaidos procentai viršija normatyvus, kurie nekelia įtarimo failams. Žiūrint į serijos koreliacijos koeficientus, nei vienas atvaizdas nekelia įtarimo, kad jame galėtų būti kas nors paslėpta.

Visi failai, sudaryti papildomai naudojant des šifravimo algoritmą, atitinka normatyvus, kurie nekelia įtarimo failams. Todėl galima teigti, jog šio įrankio naudojamas slėpimo metodas kartu su des šifravimo algoritmu užtikrina aukštą saugos lygį.

Dan-ga	Pas-lap-tis	Entropija	Chi kvadratas	Aritmetinis vidurkis	Monte Carlo π reikšmė	Klaidos procentas	Serijos koreliacijos koeficientas
LSB metodas							
1	1	7,98	< 0,01	129,9460	3,03	3,71	-0,003
1	2	7,97	< 0,01	129,8592	3,07	2,23	-0,003
1	3	7,97	< 0,01	130,4848	3,06	2,54	0,007
1	4	7,97	< 0,01	129,9581	3,06	2,61	0,000
1	5	7,97	< 0,01	129,6398	3,07	2,27	-0,003
2	4	7,95	< 0,01	129,8342	3,06	2,57	0,020
2	5	7,95	< 0,01	128,9797	3,02	3,71	0,010
3	3	7,91	< 0,01	133,2251	2,93	6,89	-0,020
3	4	7,91	< 0,01	133,0970	2,96	5,76	-0,020
3	5	7,91	< 0,01	133,7019	2,96	5,71	-0,030
4	1	7,98	< 0,01	130,3065	3,04	3,14	-0,010
4	2	7,97	< 0,01	130,4626	3,03	3,47	-0,010
4	3	7,98	< 0,01	130,5272	3,07	2,37	-0,010
4	4	7,98	< 0,01	130,9634	3,05	3,03	-0,020
4	5	7,98	< 0,01	130,4857	3,05	2,96	-0,020
5	4	7,91	< 0,01	127,8314	2,99	4,89	0,040
5	5	7,91	< 0,01	127,8314	2,99	4,89	0,040
LSB metodas su DES algoritmu							
1	1	7,99	< 0,01	127,63	3,11	1,06	0,07
1	2	7,99	< 0,01	127,78	3,10	1,20	0,07
1	3	7,99	< 0,01	127,73	3,11	1,03	0,07
1	4	7,99	< 0,01	127,63	3,11	1,01	0,07
1	5	7,99	< 0,01	127,83	3,10	1,25	0,06

2	4	7,99	< 0,01	128,58	3,10	1,38	0,10
2	5	7,99	< 0,01	128,63	3,09	1,52	0,11
3	3	7,98	< 0,01	130,76	3,05	2,89	0,04
3	4	7,98	< 0,01	130,96	3,04	3,37	0,03
3	5	7,98	< 0,01	131,01	3,04	3,11	0,03
4	1	7,99	< 0,01	128,68	3,09	1,49	0,08
4	2	7,99	< 0,01	128,54	3,10	1,29	0,08
4	3	7,99	< 0,01	128,30	3,10	1,28	0,08
4	4	7,99	< 0,01	128,26	3,10	1,27	0,08
4	5	7,99	< 0,01	128,44	3,10	1,19	0,07
5	4	7,99	< 0,01	127,93	3,10	1,37	0,07
5	5	7,99	< 0,01	127,93	3,11	1,05	0,07

Lentelė 17 „OpenStego“ įrankiu sukurtų atvaizdų slaptumo analizė

Toliau pateikiami rezultatai gauti skaičiuojant slaptumą stego atvaizdų, kuriuos pavyko sukurti naudojant „Steghide“ įrankį slepiant informaciją dangos atvaizduose.

Beveik visi atvaizdai, sudaryti naudojant tik steganografijos metodą, atitinka normatyvus, kurie nekelia įtarimo failams (Lentelė 18). Monte Carlo π reikšmės įverčiai failams trečia ir penkta dangomis yra kiek žemiau normos, todėl jie yra beveik nekeliantys įtarimo. Tačiau su trečia danga sudarytų atvaizdų gauti klaidos procentai viršija normatyvus, kurie nekelia įtarimo failams. Žiūrint į serijos koreliacijos koeficientus galima teigti, jog nei vienas atvaizdas nekelia įtarimo, kad jame galėtų būti kas nors paslėpta.

Dan-ga	Pas-lap-tis	Entropija	Chi kvadratas	Aritmetinis vidurkis	Monte Carlo π reikšmė	Klaidos procentas	Serijos koreliacijos koeficientas
1	1	7,97	< 0,01	129,7769	3,06	2,52	0,001
1	2	7,97	< 0,01	129,7831	3,06	2,71	0,001
1	3	7,97	< 0,01	129,6283	3,03	3,44	-0,002
1	4	7,97	< 0,01	129,7315	3,06	2,46	-0,01
1	5	7,97	< 0,01	129,5419	3,06	2,54	-0,002
2	4	7,95	< 0,01	129,2642	3,08	1,93	0,01
2	5	7,95	< 0,01	129,1286	3,06	2,53	0,03
3	3	7,91	< 0,01	132,9633	2,94	6,34	-0,03
3	4	7,91	< 0,01	133,0559	2,92	7,17	-0,02
3	5	7,91	< 0,01	133,1926	2,92	7,04	-0,02
4	1	7,98	< 0,01	130,7313	3,03	3,56	-0,02
4	2	7,98	< 0,01	130,1773	3,06	2,51	-0,01
4	3	7,98	< 0,01	130,6860	3,04	3,13	-0,02
4	4	7,98	< 0,01	130,1119	3,06	2,62	-0,02
4	5	7,98	< 0,01	130,4994	3,04	3,30	-0,02
5	4	7,91	< 0,01	128,6255	2,97	5,55	0,03
5	5	7,91	< 0,01	128,3842	3,02	3,78	0,04

Lentelė 18 „Steghide“ įrankiu naudojant LSB metodą sukurtų atvaizdų slaptumo analizė

Atvaizdų, sukurtų su „Steghide“ įrankiu papildomai naudojant blowfish šifravimo algoritmą (Lentelė 19), slaptumo įverčiai tik labai nežymiai skiriasi nuo tų, kurie buvo sudaryti papildomai nenaudojant šifravimo algoritmo. Entropijos, Chi kvadrato ir serijos koreliacijos įverčiai visiems

failams atitinka normatyvus, kurie nekelia įtarimo failams. Tačiau aritmetiniai vidurkiai atvaizdų, sudarytų su trečiu dangos atvaizdu, yra keliantys įtarimą, nes viršija normatyvus. Taip pat ir šių atvaizdų bei penktoje dangoje paslėptos ketvirtos paslapties Monte Carlo π reikšmės ir klaidų procentų įverčiai neatitinka normatyvų. Taigi, vos 25% sukurtų failų neatitinka slaptumo normatyvų ir kelia jais įtarimą.

Danga	Paslaptis	Entropija	Chi kvadratas	Aritmetinis vidurkis	Monte Carlo π reikšmė	Klaidos procentas	Serijos koreliacijos koeficientas
1	1	7,97	< 0,01	129,7769	3,06	2,52	0,001
1	2	7,97	< 0,01	129,7831	3,06	2,71	0,001
1	3	7,97	< 0,01	129,6283	3,03	3,44	-0,002
1	4	7,97	< 0,01	129,7315	3,06	2,46	-0,01
1	5	7,97	< 0,01	129,5419	3,06	2,54	-0,002
2	4	7,95	< 0,01	129,2642	3,08	1,93	0,01
2	5	7,95	< 0,01	129,1286	3,06	2,53	0,03
3	3	7,91	< 0,01	132,9633	2,94	6,34	-0,03
3	4	7,91	< 0,01	133,0559	2,92	7,17	-0,02
3	5	7,91	< 0,01	133,1926	2,92	7,04	-0,02
4	1	7,98	< 0,01	130,7313	3,03	3,56	-0,02
4	2	7,98	< 0,01	130,1773	3,06	2,51	-0,01
4	3	7,98	< 0,01	130,6860	3,04	3,13	-0,02
4	4	7,98	< 0,01	130,1119	3,06	2,62	-0,02
4	5	7,98	< 0,01	130,4994	3,04	3,30	-0,02
5	4	7,91	< 0,01	128,6255	2,97	5,55	0,03
5	5	7,91	< 0,01	128,3842	3,02	3,78	0,04

Lentelė 19 „Steghide“ įrankiu naudojant LSB metodą su blowfish algoritmu sukurtų atvaizdų slaptumo analizė

Atvaizdų, sukurtų su „Steghide“ įrankiu papildomai naudojant gost šifravimo algoritmą (Lentelė 20), slaptumo įverčiai taip pat tik labai nežymiai skiriasi nuo tų, kurie buvo sudaryti papildomai nenaudojant šifravimo algoritmo. Entropijos, Chi kvadrato ir serijos koreliacijos įverčiai visiems failams atitinka normatyvus, kurie nekelia įtarimo failams. Tačiau aritmetiniai vidurkiai atvaizdų, sudarytų su trečiu dangos atvaizdu, yra keliantys įtarimą, nes viršija normatyvus. Trečioje dangoje slepiant ketvirtą ir penktą paslaptis bei penktoje dangoje slepiant penktą paslaptį gauti stega atvaizdų Monte Carlo π reikšmės ir klaidų procentų įverčiai neatitinka normatyvų. Taigi, vos 18% sukurtų failų neatitinka slaptumo normatyvų ir kelia jais įtarimą.

Danga	Paslaptis	Entropija	Chi kvadratas	Aritmetinis vidurkis	Monte Carlo π reikšmė	Klaidos procentas	Serijos koreliacijos koeficientas
1	1	7,97	< 0,01	130,0218	3,08	2,09	-0,01
1	2	7,97	< 0,01	130,0839	3,07	2,43	-0,002
1	3	7,97	< 0,01	129,7274	3,06	2,56	-0,003
1	4	7,97	< 0,01	129,8189	3,07	2,40	-0,003
1	5	7,97	< 0,01	129,6614	3,07	2,29	0,001
2	4	7,97	< 0,01	129,8242	3,07	2,24	-0,004

2	5	7,97	< 0,01	129,7056	3,10	1,40	0,003
3	3	7,91	< 0,01	132,7704	3,00	4,57	-0,03
3	4	7,91	< 0,01	133,0738	2,95	6,22	-0,02
3	5	7,91	< 0,01	133,0109	2,93	6,58	-0,03
4	1	7,98	< 0,01	130,7218	3,06	2,56	-0,01
4	2	7,98	< 0,01	130,0245	3,06	2,64	-0,02
4	3	7,98	< 0,01	130,6218	3,06	2,64	-0,01
4	4	7,98	< 0,01	130,4562	3,04	3,20	-0,02
4	5	7,97	< 0,01	129,7353	3,10	1,46	0,001
5	4	7,91	< 0,01	128,5276	3,01	4,23	0,02
5	5	7,91	< 0,01	128,2825	2,98	5,19	0,04

Lentelė 20 „Steghide“ įrankiu naudojant LSB metodą su gostalgoritmu sukurtų atvaizdų slaptumo analizė

Atvaizdų, sukurtų su „Steghide“ įrankiu papildomai naudojant twofish šifravimo algoritmą (Lentelė 21), slaptumo įverčiai taip pat tik labai nežymiai skiriasi nuo tų, kurie buvo sudaryti papildomai nenaudojant šifravimo algoritmo. Entropijos, Chi kvadrato ir serijos koreliacijos įverčiai visiems failams atitinka normatyvus, kurie nekelia įtarimo failams. Tačiau aritmetiniai vidurkiai atvaizdų, sudarytų su trečiu dangos atvaizdu, yra keliantys įtarimą, nes viršija normatyvus. Taip pat su trečia danga sudarytų stega atvaizdų Monte Carlo π reikšmės ir klaidų procentų įverčiai neatitinka normatyvų. Taigi, net 82% sukurtų failų atitinka slaptumo normatyvus ir nekelia jais įtarimo.

Dan-ga	Pas-lap-tis	Entropija	Chi kvadratas	Aritmetinis vidurkis	Monte Carlo π reikšmė	Klaidos procentas	Serijos koreliacijos koeficientas
1	1	7,97	< 0,01	130,0636	3,04	3,23	-0,004
1	2	7,97	< 0,01	129,9733	3,04	3,31	-0,003
1	3	7,97	< 0,01	129,8650	3,06	2,67	-0,002
1	4	7,97	< 0,01	129,9833	3,08	2,11	-0,001
1	5	7,97	< 0,01	130,0946	3,09	1,70	-0,001
2	4	7,97	< 0,01	130,0120	3,07	2,36	-0,00004
2	5	7,97	< 0,01	129,6793	3,07	2,38	-0,001
3	3	7,91	< 0,01	133,0481	2,91	7,49	-0,03
3	4	7,92	< 0,01	133,1129	2,97	5,49	-0,02
3	5	7,91	< 0,01	133,3561	2,96	5,93	-0,02
4	1	7,98	< 0,01	130,8541	3,03	3,44	-0,02
4	2	7,98	< 0,01	129,9889	3,07	2,26	-0,02
4	3	7,98	< 0,01	130,3378	3,03	3,46	-0,02
4	4	7,97	< 0,01	130,1968	3,06	2,60	-0,02
4	5	7,97	< 0,01	129,7181	3,08	2,05	-0,01
5	4	7,91	< 0,01	128,7125	3,03	3,58	0,03
5	5	7,91	< 0,01	127,8576	3,03	3,56	0,02

Lentelė 21 „Steghide“ įrankiu naudojant LSB metodą su twofish algoritmu sukurtų atvaizdų slaptumo analizė

Atvaizdų, sukurtų su „Steghide“ įrankiu papildomai naudojant tripledes šifravimo algoritmą (Lentelė 22), slaptumo įverčiai taip pat tik labai nežymiai skiriasi nuo tų, kurie buvo sudaryti papildomai nenaudojant šifravimo algoritmo. Kaip ir ankstesniu atveju, kai papildomai buvo

naudotas twofish algoritmas, gauti slaptumo įverčiai labai panašūs. Entropijos, Chi kvadrato ir serijos koreliacijos įverčiai visiems failams atitinka normatyvus, kurie nekelia įtarimo failams. Tačiau aritmetiniai vidurkiai atvaizdų, sudarytų su trečiu dangos atvaizdu, yra keliantys įtarimą, nes viršija normatyvus. Taip pat su trečia danga ir penkta danga su ketvirta paslaptimi sudarytų stega atvaizdų Monte Carlo π reikšmės įverčiai mažesni už normatyvus. Tačiau tik su trečiu dangos atvaizdų sudarytų stega atvaizdų klaidos procentų slaptumo įverčiai viršija normatyvus. Net 23% sukurtų failų neatitinka slaptumo normatyvų ir kelia jais įtarimą.

Dan-ga	Pas-lap-tis	Entropija	Chi kvadratas	Aritmetinis vidurkis	Monte Carlo π reikšmė	Klaidos procentas	Serijos koreliacijos koeficientas
1	1	7,97	< 0,01	129,9556	3,03	3,57	-0,01
1	2	7,97	< 0,01	130,1787	3,05	2,79	0,0003
1	3	7,97	< 0,01	129,9362	3,07	2,26	-0,004
1	4	7,97	< 0,01	129,8539	3,07	2,39	-0,004
1	5	7,97	< 0,01	130,4248	3,06	2,74	0,002
2	4	7,97	< 0,01	129,8121	3,07	2,32	-0,003
2	5	7,97	< 0,01	130,1855	3,08	1,87	0,004
3	3	7,91	< 0,01	133,2266	2,93	6,80	-0,03
3	4	7,91	< 0,01	133,2267	2,97	5,50	-0,02
3	5	7,91	< 0,01	132,8953	2,93	6,70	-0,03
4	1	7,98	< 0,01	130,8641	3,04	3,25	-0,02
4	2	7,98	< 0,01	130,2555	3,05	2,90	-0,01
4	3	7,98	< 0,01	130,3483	3,09	1,70	-0,02
4	4	7,98	< 0,01	130,5415	3,06	2,61	-0,01
4	5	7,97	< 0,01	129,8934	3,07	2,12	-0,003
5	4	7,91	< 0,01	127,6116	2,99	4,68	0,03
5	5	7,91	< 0,01	128,2312	3,02	3,94	0,02

Lentelė 22 „Steghide“ įrankiu naudojant LSB metodą su tripledes algoritmu sukurtų atvaizdų slaptumo analizė

Atvaizdų, sukurtų su „Steghide“ įrankiu papildomai naudojant dešifravimo algoritmą (Lentelė 23), slaptumo įverčiai išlieka labai panašūs į tuos, kurie buvo sudaryti papildomai nenaudojant jokio šifravimo algoritmo. Kaip ir ankstesniu atveju, kai papildomai buvo naudotas šifravimo algoritmas, gauti slaptumo įverčiai labai panašus. Entropijos, Chi kvadrato ir serijos koreliacijos įverčiai visiems failams atitinka normatyvus, kurie nekelia įtarimo failams. Tačiau aritmetiniai vidurkiai atvaizdų, sudarytų su trečiu dangos atvaizdu, yra keliantys įtarimą, nes viršija normatyvus. Taip pat trečioje dangoje slepiant ketvirtą ir penktą paslaptis bei penktoje dangoje slepiant penktą paslaptį gauti stega atvaizdų Monte Carlo π reikšmės ir klaidų procentų įverčiai žemesni už tuos, kurie nekelia įtarimo failams. Net 76% sukurtų failų atitinka slaptumo normatyvų reikalavimus ir nekelia jais įtarimo.

Dan-ga	Pas-lap-tis	Entropija	Chi kvadratas	Aritmetinis vidurkis	Monte Carlo π reikšmė	Klaidos procentas	Serijos koreliacijos koeficientas
1	1	7,97	< 0,01	129,5338	3,09	1,60	-0,00003
1	2	7,97	< 0,01	130,3411	3,06	2,45	0,004

1	3	7,97	< 0,01	129,8350	3,06	2,75	-0,001
1	4	7,97	< 0,01	129,7917	3,07	2,33	-0,001
1	5	7,97	< 0,01	129,9161	3,07	2,30	0,01
2	4	7,97	< 0,01	130,4295	3,05	2,99	0,001
2	5	7,97	< 0,01	130,0415	3,06	2,69	-0,004
3	3	7,91	< 0,01	132,9447	3,00	4,62	-0,03
3	4	7,91	< 0,01	132,8194	2,96	5,72	-0,03
3	5	7,91	< 0,01	132,8030	2,95	6,22	-0,03
4	1	7,98	< 0,01	130,6111	3,02	4,02	-0,01
4	2	7,98	< 0,01	130,0149	3,05	2,89	-0,01
4	3	7,98	< 0,01	130,3326	3,04	3,35	-0,01
4	4	7,98	< 0,01	130,5358	3,06	2,60	-0,01
4	5	7,97	< 0,01	130,1192	3,06	2,46	0,0002
5	4	7,91	< 0,01	127,8270	3,00	4,46	0,04
5	5	7,90	< 0,01	128,7682	2,91	7,26	0,03

Lentelė 23 „Steghide“ įrankiu naudojant LSB metodą su des algoritmu sukurtų atvaizdų slaptumo analizė

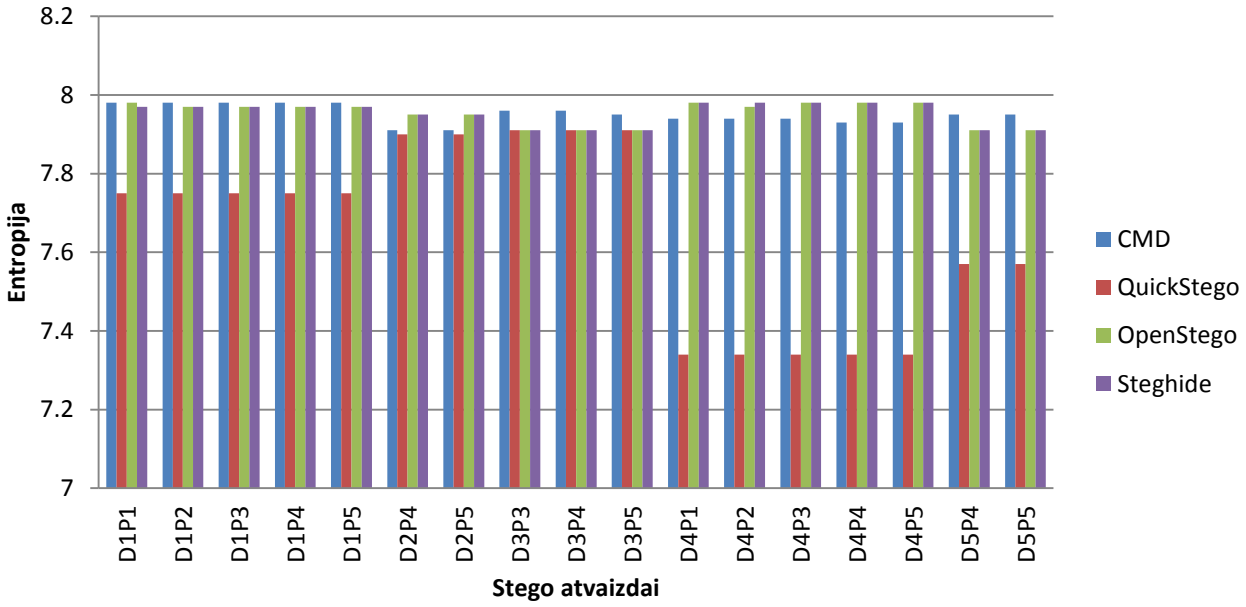
Atvaizdų, sukurtų su „Steghide“ įrankiu papildomai naudojant rc2šifravimo algoritmą (Lentelė 24), slaptumo įverčiai taip pat tik labai nežymiai skiriasi nuo tų, kurie buvo sudaryti papildomai nenaudojant šifravimo algoritmo. Kaip ir ankstesniu atveju, kai papildomai buvo naudoti kiti šifravimo algoritmai, gauti slaptumo įverčiai labai panašus. Entropijos, Chi kvadrato ir serijos koreliacijos įverčiai visiems failams atitinka normatyvus, kurie nekelia įtarimo failams. Tačiau aritmetiniai vidurkiai atvaizdų, sudarytų su trečiu dangos atvaizdu, yra keliantys įtarimą, kadangi viršija normatyvus. Taip pat su trečia danga sudarytų stega atvaizdų Monte Carlo π reikšmės ir klaidų procentų įverčiai neatitinka normatyvų. Net 82% sukurtų failų atitinka slaptumo normatyvus ir nekelia jais įtarimo.

Dan-ga	Pas-lap-tis	Entropija	Chi kvadratas	Aritmetinis vidurkis	Monte Carlo π reikšmė	Klaidos procentas	Serijos koreliacijos koeficientas
1	1	7,97	< 0,01	130,0272	3,05	2,86	-0,003
1	2	7,97	< 0,01	130,2270	3,06	2,46	0,002
1	3	7,97	< 0,01	129,7543	3,10	1,54	0,001
1	4	7,97	< 0,01	129,8880	3,10	1,36	-0,01
1	5	7,97	< 0,01	129,7625	3,08	1,90	-0,01
2	4	7,97	< 0,01	129,8834	3,08	2,03	0,001
2	5	7,97	< 0,01	129,7446	3,07	2,33	-0,0001
3	3	7,91	< 0,01	133,4659	2,94	6,37	-0,02
3	4	7,91	< 0,01	132,7210	2,67	5,56	-0,02
3	5	7,91	< 0,01	133,0084	2,97	5,37	-0,03
4	1	7,98	< 0,01	130,2934	3,05	2,79	-0,02
4	2	7,98	< 0,01	130,3555	3,02	3,91	--0,01
4	3	7,98	< 0,01	130,3337	3,05	2,93	-0,02
4	4	7,98	< 0,01	130,4515	3,04	3,19	-0,01
4	5	7,97	< 0,01	130,1625	3,07	2,24	-0,004
5	4	7,91	< 0,01	128,8230	3,02	3,72	0,02
5	5	7,90	< 0,01	128,4412	2,99	4,85	0,02

Lentelė 24 „Steghide“ įrankiu naudojant LSB metodą su rc2 algoritmu sukurtų atvaizdų slaptumo analizė

Taigi, su „Steghide“ įrankiu visų sudarytų stego atvaizdų entropijos, Chi kvadrato ir serijos koreliacijos slaptumo įverčiai atitinka normatyvus, failai atrodo švarūs. Tačiau naudojant visus slėpimo būdus, su trečia danga sudarytų atvaizdų Monte Carlo π reikšmės, aritmetinio vidurkio ir klaidos procento slaptumo įverčiai kelią įtarimą failams. Net 17 % sudarytų failų nepraėjo slaptumo patikros.

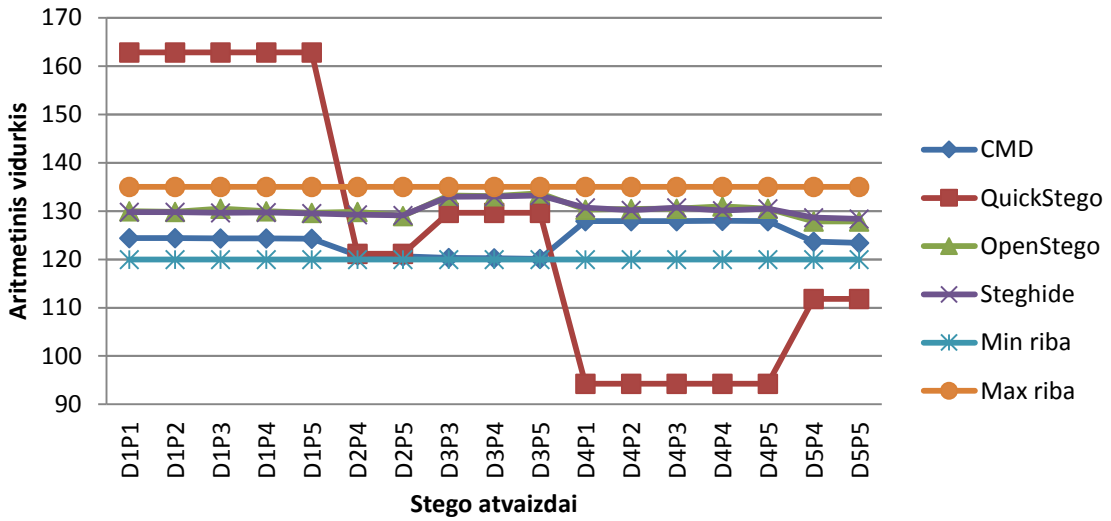
Lyginant gautus duomenys tarpusavyje, kai slėpimas būdavo vykdomas be kriptografijos, tik su ketvirta ir penkta dangomis sudaryti atvaizdai naudojant „QuickStego“ įrankį kelią didelį įtarimą. Šiuo įrankiu sudaryti atvaizdai su pirma danga yra ant ribos tarp neįtartinų ir keliančių nedidelį įtarimą. Kiti atvaizdai, atsižvelgiant tik į entropijos rodiklį, jokio įtarimo nekelia (Pav. 11).



Pav. 11 Stego atvaizdų entropijos palyginimo diagrama

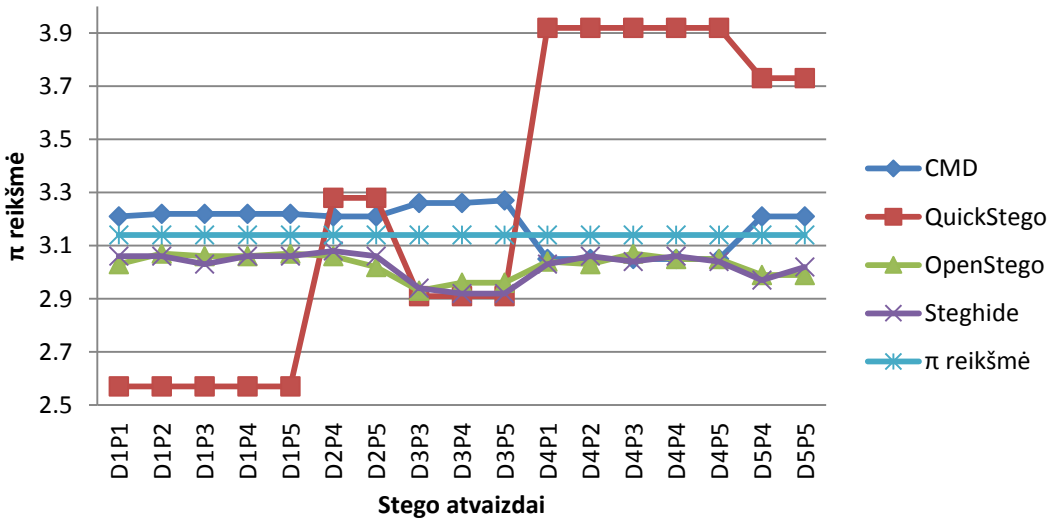
Taip pat nepriklausomai nuo naudoto slėpimo metodo ar įrankio, Chi kvadrato procentinė reikšmė mažesnė nei 1%, tai reiškia, kad visos sekos yra beveik neabejotinai atsitiktinės.

Daugumos aritmetiniai vidurkiai irgi yra labai panašūs, kadangi slėpimo metodai labai panašūs. Jei vidurkis yra nuo 120 iki 135, tai failas nekelia įtarimo. Žemiau pateiktoje diagramoje (Pav. 12) matyti, kad tik „QuickStego“ įrankiu sudaryti stego atvaizdai su pirma ir ketvirta dangomis kelia didelį įtarimą, nes jų aritmetiniai vidurkiai yra gerokai aukščiau arba žemiau normalaus.



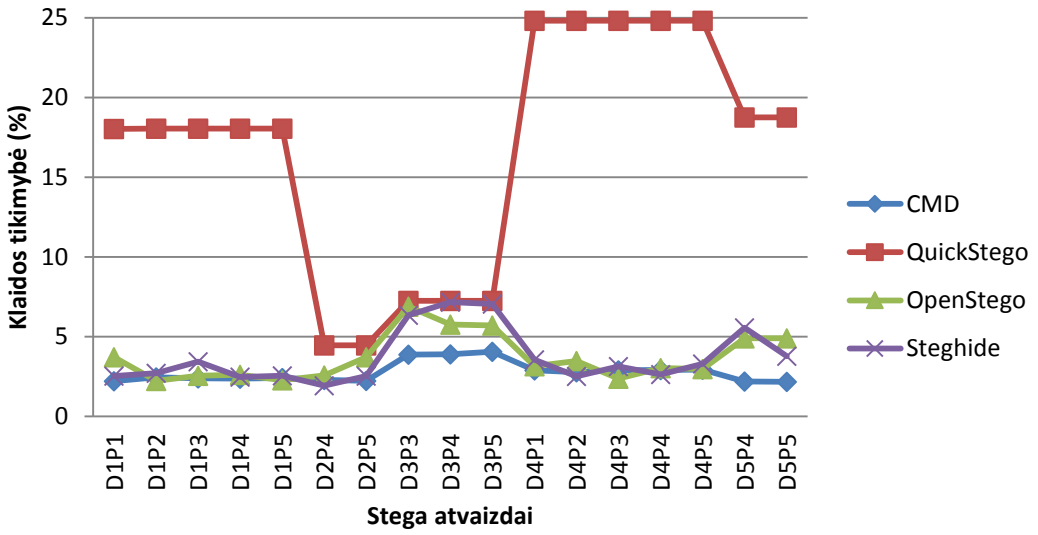
Pav. 12 Aritmetinių vidurkių palyginimo diagrama

Žiūrint tolesnio kriterijaus – Monte Carlo π reikšmės – duomenis, matomi skirtingi rezultatai, tačiau dauguma jų tolygiai pasiskirstę aukščiau arba žemiau standartinės π reikšmės (π= 3,14), kas parodo failuose esančios informacijos slaptumą. Tik stego failai, sukurti naudojant „QuickStego“ įrankį su pirma, ketvirta ir penkta dangomis, kelią didelį įtarimą, kad failuose yra kažkas paslėpta. Su trečia danga sudaryti failai naudojant „QuickStego“, „OpenStego“ ir „Steghide“ įrankius yra beveik neįtartini (Pav. 13).



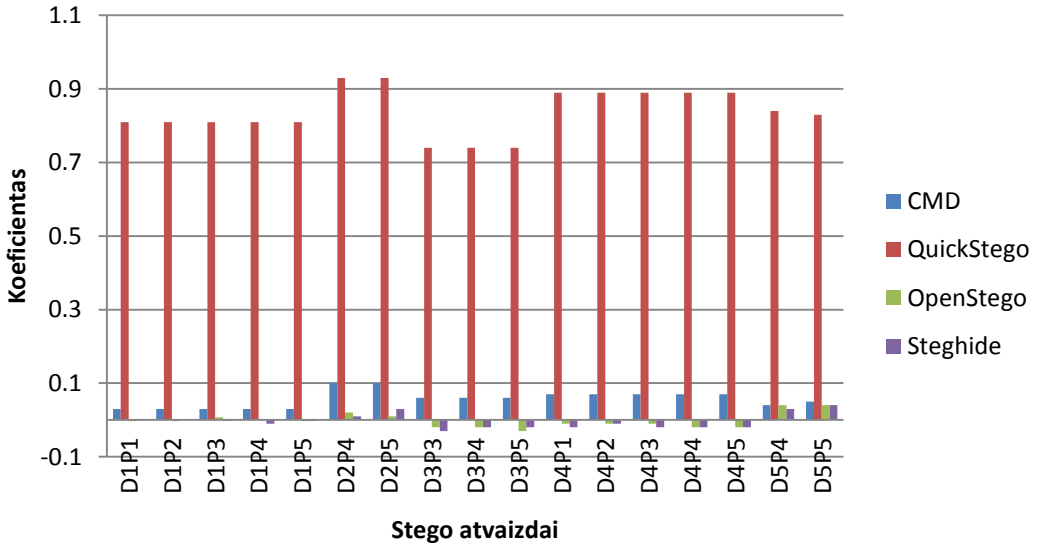
Pav. 13 Monte Carlo π reikšmės palyginimo diagrama

Taip pat šiuose failuose matoma padidėjusi klaidos atsiradimo tikimybė, kas irgi jiems kelią didelį įtarimą. Slepiant paslaptis trečioje dangoje visi failai yra beveik neįtartini, nesvarbu, kokiu įrankiu jie buvo sukurti. Kaip ir ankstesnėse slaptumo diagramose, taip ir šioje, galima matyti, kad „QuickStego” įrankiu sukurti failai (išskyrus naudojant antrą ir trečią dangas) kelią didelį įtarimą (Pav. 14).



Pav. 14 Klaidos tikimybės palyginimo diagrama

Gautuose rezultatuose taip pat matyti, kad serijos koreliacijos koeficientai visais atvejais (išskyrus „QuickStego“ įrankio) artimi nuliui, svyruoja nuo -0,03 iki 0,10, kas reiškia, jog atvaizdai nekelia jokio įtarimo. Net ir tiems failams, kurie kelia įtarimą dėl klaidų tikimybės ar nutolusios π reikšmės, šio koeficiento reikšmė vis tiek artima nuliui. Tačiau, kaip ir ankstesniais atvejais, „QuickStego“ įrankiu sukurti visi atvaizdai kelia didelį įtarimą (Pav. 15).



Pav. 15 Serijos koreliacijos koeficientų palyginimas

Taigi, lyginant šiuos duomenų su dangos failų rezultatais, galima daryti išvadą, kad daugumos gautų failų slaptumas yra didelis, abejonių kelia tik su trečia ir penkta dangomis sudaryti stego atvaizdai, bei visi atvaizdai, kurie sudaryti naudojant „QuickStego“ įrankį. Visų kitų sugeneruotų failų tiek dangos, tiek stega atvaizdų su atitinkamos dangos ir skirtingų paslapčių rezultatai yra panašūs, nežymiai skiriasi. Tačiau visi patenka į ribas, kuomet failai nekelia įtarimo dėl to, jog gali būti kažkas juose paslėpta.

3.6. Stegoanalizės galimybės

Nesvarbu, ar stego atvaizdas sukėlė įtarimų, ar ne, buvo bandoma faile surasti paslėptą informaciją. Kai paslaptis buvo slepiama naudojant „Steghide“ įrankį, šis įrankis surasdavo paslėptą failą, nesvarbu, kokiu metodu buvo paslėpta. Suvedus slaptažodį, rastos paslapties failas išimamas iš stego atvaizdo, t.y. stego atvaizdas tampa pirminiu dangos failu.

Žemiau pateikiami stego atvaizdai prieš (Pav. 16) ir po (Pav. 17) stegoanalizės. Atvaizdai atrodo visiškai vienodi, nors viename iš jų (Pav. 16) yra paslėptas failas su paslaptimi.

Pav. 16 Stego atvaizdas po steganografijos

Pav. 17 Stego atvaizdas po stegoanalizės

Toliau pateikiamos „Steghide“ įrankiu ieškomų paslėptų failų greitaveikos (Lentelė 25). Iš pateiktų rezultatų matyti, kad ilgiausiai paieška trukdavo, kai informacijos slėpimui buvo naudojamas LSB metodas kartu su rc2 šifravimo algoritmu (vidutiniškai 0,08 ms), trumpiausiai – kai slėpimui papildomai buvo naudojami tripledes ir teofish šifravimo algoritmai (vidutiniškai 0,06 ms). Visais kitais atvejais paslapties ieškojimas vidutiniškai užtrukdavo 0,07 ms. Taip pat greičiausiai paieška vykdavo, kai buvo palėptas nedidelis informacijos kiekis (vidutiniškai 0,04 ms). Kai buvo ieškoma didelio kiekio paslėptos informacijos, vidutiniškai greitaveika išaugdavo iki 0,09 ms. Dideliame faile paslapties paieška vidutiniškai užtrukdavo 0,07 ms, mažame – 0,06 ms.

Danga	Paslaptis	Greitaveika (ms)						
		LSB	LSB su Blowfish	LSB su DES	LSB su GOST	LSB su RC2	LSB su 3DES	LSB su 2FISH
1	1	0,08	0,07	0,08	0,10	0,10	0,12	0,07
1	2	0,06	0,07	0,08	0,08	0,07	0,06	0,06
1	3	0,04	0,06	0,06	0,05	0,05	0,06	0,05
1	4	0,04	0,06	0,05	0,04	0,04	0,05	0,04
1	5	0,04	0,04	0,06	0,05	0,04	0,04	0,04
2	4	0,07	0,11	0,06	0,11	0,10	0,05	0,09
2	5	0,12	0,04	0,06	0,05	0,04	0,04	0,04
3	3	0,11	0,09	0,10	0,12	0,15	0,15	0,09
3	4	0,04	0,04	0,05	0,06	0,04	0,05	0,04
3	5	0,04	0,04	0,05	0,05	0,03	0,04	0,05
4	1	0,11	0,12	0,11	0,11	0,06	0,07	0,07
4	2	0,06	0,07	0,09	0,08	0,06	0,08	0,07
4	3	0,11	0,07	0,05	0,05	0,05	0,05	0,11
4	4	0,07	0,04	0,05	0,04	0,13	0,05	0,05
4	5	0,14	0,05	0,04	0,05	0,13	0,04	0,06
5	4	0,04	0,12	0,09	0,05	0,18	0,07	0,08
5	5	0,04	0,04	0,03	0,07	0,03	0,04	0,04

Lentelė 25 Stegoanalizė naudojant „Steghide“ įrankį

Vėliau buvo iš naujo atliktas „slaptumo“ patikrinimas stego atvaizdams, kuriuose buvo rastos paslaptys. Lentelėje (Lentelė 26) pateikiami „slaptumo“ rezultatai pradinio dangos failo ir aukščiau pateiktiems atvaizdams. Iš šių rezultatų matome, kad visi atvaizdų slaptumo įverčiai atitinka normatyvūs, kai failai nekelia įtarimo.

Parametrai	Dangos failas	Stego atvaizdas (Pav. 16)	Stego atvaizdas (Pav. 17)
Entropija	7,98	7,97	7,95
Chi kvadratas (%)	< 0,01	< 0,01	< 0,01
Aritmetinis vidurkis	120,9497	129,8242	129,2642
Monte Carlo Pi reikšmė	3,21	3,07	3,08
Klaidos procentas	2,12	2,24	1,93
Serijos koreliacijos koeficientas	0,10	-0,004	0,01

Lentelė 26 Slaptumas prieš ir po steganalizės „OpenStego“

Žemiau esančioje lentelėje (Lentelė 27) pateikiama „OpenStego“ įrankiu sukurtų stego atvaizdų stegoanalizės greitaveikos. Iš pateiktų rezultatų matome, kad paieškos greitaveika atvaizduose, sudarytuose naudojant tik stegoanalizės metodą, svyruoja nuo 0,38 iki 1,45 ms. Tuo tarpu paieškos greitaveika atvaizduose, sudarytuose papildomai naudojant šifravimo algoritmą svyruoja nuo 0,72 ms iki 1,69 ms. Žiūrint greitaveikų vidurkius, paieška užšifruotuose atvaizduose pailgėdavo iki 0,24 ms. Tačiau lyginant šio ir „Steghide“ įrankių stegoanalizės greitaveikas, „OpenStego“ įrankis vidutiniškai užtrukdavo iki 13 kartų ilgiau.

Danga	Paslaptis	Greitaveika be kriptografijos (ms)	Greitaveika su kriptografija (ms)	Skirtumas
1	1	1,04	1,25	0,21
1	2	0,60	1,27	0,67
1	3	1,01	1,22	0,21
1	4	1,00	1,27	0,27
1	5	0,98	1,22	0,24
2	1	0,55	0,79	0,24
2	2	0,88	0,81	-0,07
2	3	0,38	0,79	0,41
2	4	0,55	0,82	0,27
2	5	0,54	0,75	0,21
3	1	1,04	1,29	0,25
3	2	1,02	1,24	0,22
3	3	1,03	1,27	0,24
3	4	1,02	1,23	0,21
3	5	0,98	1,20	0,22
4	1	1,41	1,64	0,23
4	2	1,45	1,61	0,16
4	3	1,40	1,69	0,29
4	4	1,39	1,68	0,29
4	5	1,38	1,63	0,25
5	1	0,55	0,79	0,24
5	2	0,54	0,78	0,24
5	3	0,53	0,76	0,23
5	4	0,54	0,76	0,22
5	5	0,57	0,72	0,15

Lentelė 27 Stegoanalizė naudojant „OpenStego“ įrankį

Iš pateiktų rezultatų matyti, kad ne su visiais įrankiais pavyko paslėpti visus pranešimus atvaizduose. Taip pat ir ne įrankių naudojami metodai sugebėjo paslėpti informaciją taip, kad nesukeltų įtarimo failams. Vieni metodai nekėlė įtarimo failais arba tie įtarimai nebuvo taip paprastai pastebimi, t.y. matomi tik atlikus slaptumo įverčių skaičiavimus. Kitų metodų sukurti atvaizdai iš karto kėlė įtarimą jais, dėl labai išaugusių atvaizdų dydžio. Greitaveikos palyginimo metu buvo palyginta, kuriuos metodus ir įrankius naudojant buvo greičiausiai atliekami slėpimai. Atlikus slaptumo įverčių skaičiavimus pasimatė, kurie sukurti failai nekelia jokio įtarimo failais, o kurie kelią net ir labai didelį įtarimą. Taip pat steganalizės galimybių tyrimo metu buvo nustatyta kurie įrankiai greičiausiai suranda paslaptis, o kurie lėčiausiai.

4. IŠVADOS

Atlikus tyrimą su „švariais“ dangos atvaizdas slepiant skirtingo dydžio paslaptis, buvo pastebėta, kad ne visi įrankiai gali tai padaryti. Steghide įrankio naudojamas grafinis teoretinis atitikmens metodas negalėjo paslėpti daugiau nei 1 MB informacijos 5 KB dydžio dangos atvaizde net ir papildomai slėpimui naudodamas šifravimo algoritmą. Visi kiti įrankiai, naudodami LSB, atsitiktinio LSB ir slėpimą po failos pabaigos simbolio metodus, gebėjo sudaryti visus stego atvaizdus su parinktais dangų ir paslapčių failais.

Buvo testuojami du įrankiai naudojantys LSB metodą be šifravimo (Steghide, OpenStego), todėl palyginus jų greitaveikas, akivaizdžiai matėsi, kad Steghide įrankis dirba iki 8 kartų greičiau. Lyginant greitaveikas, nepriklausomai nuo naudojamo metodo, buvo pastebėta, kad atsitiktinio LSB metodas veikdavo ilgiausiai (vidutiniškai 1,03 ms). Grafinis teoretinis metodas ir slėpimas po pabaigos simbolio užtrukdavo kur kas trumpiau (grafinis teoretinis metodas vidutiniškai – 0,09 ms; slėpimas po pabaigos simbolio – 0,02 ms). Kadangi įrankio, naudojančio LSB metodą, greitaveikos nustatyti nepavyko, tai negalime palyginti su kitais.

Lyginant atvaizdų dydžių pakitimus po slėpimo, buvo matyti, kad įrankiais, naudojančiais LSB metodą, sukurti atvaizdai buvo beveik 10 kartų didesni už dangos failus. Toks failo dydis kelia įtarimą, kad jame gali bti kas nors paslėptą. Tuo tarpu slepimui naudojant komandinę eilutę arba „Steghide“ įrankį, gautų failų dydis tik nežymiai pasikeisdavo. Naudojant komandinę eilutę, failai vidutiniškai padidėdavo 1,3 KB, „QuickStego“ – 528,1 KB, „OpenStego“ – 334,5 KB, „Steghide“ – 1,0 KB. Net ir papildomai naudojant šifravimo algoritmus, gautų atvaizdų dydis tik nežymiai skyrėsi nuo tų, kurie buvo sudaryti naudojant tik steganografijos metodą. Taip pat atvaizdai labai padidėdavo, kai buvo slepiama santykinai mažas paslapties failas dideliame dangos faile.

Tyrimo metu buvo lyginamas slėpimo įrankių sudarytų stego atvaizdų informacijos talpumas dangose. Kadangi paslapčių slėpimui naudojant įrankius su atsitiktiniu LSB ir LSB metodais gautų atvaizdų dydis gerokai padidėjo, tai šių metodų sukurtų atvaizdų talpumo lyginti negalėjome. Likusių ėrankių pagalba buvo paslėptas panašus informacijos kiekis, slėpiant po pabaigos simboliu, vidutiškai galima paslėpti 29 simb./KB, o grafinio teorinio atitikmens metodu – 31 simb./KB.

Lyginant gautų atvaizdų slaptumo įverčius, pamatėme, kad slepiant po pabaigos simboliu, visi gauti atvaizdai atitiko normatyvus, kai nėra jokio įtarimo failams. Taip ir dauguma atvaizdų sudarytų naudojant atsitiktini LSB metodą irgi nekėlė įtarimo. O papildomai naudojant DES šifravimą, visi atvaizdai atitiko normatyvus. Naudojant grafinį teorinį atsitikmens metodą, visi sudaryti failai, kurie slėpė ne daugiau nei 1MB informacijos 5KB atvaize, atitiko normatyvūs, kurie nekelia įtarimo. Tuo tarpu LSB metodu sudaryti atvaizdai visi kėlė didelį įtarimą failams.

Paslapčių paieškos visų atvaizdu vyko panašiu greičiu, ilgiau užtrukdavo, jei papildomai buvo naudojamas šifravimas.

Kriterijus	Slėpimas po failo pabaigos simbolio („Windows OS“ komandinė eilutė)	Atsitiktinis LSB („OpenStego“)	LSB („QuickStego“)	Grafinis teoretinis atitikmuo („Steghide“)
Greitaveika	4	2		3
Failo dydžio pakitimas po slėpimo	3	2	1	4
Slepiamos informacijos kiekis	3			4
Slaptumas	4	3	1	2
Stegoanalizė	4	4	4	4
Viso	18	11	6	17

Lentelė 28 Steganografijos metodų palyginimo lentelė

Taigi bendrai palyginus visu kriterijus, pateiktus aukščiau esančioje lentelėje (Lentelė 28), matoma, kad efektyviausia naudoti slėpimo po failo pabaigos simboliu metodą. Jei slėpiamas informacijos ir dangos failo santykis yra 1024:5, kada tokį patį efektyvumą galima pasiekti ir naudojant grafinį teoretinį atitikmens metodą. Atsitiktinis LSB ir LSB metodai dėl žymiai padidėjusio stego atvaizdo dydžio yra mažai efektyvūs, nors atsitiktinio LSB metodų ir užtikrinamas slaptumas.

5. LITERATŪRA

[1] M. Badr, I. Salama, M. I. Selim, H. Khalil, „A review on steganalysis techniques: from image format point of view“, International Journal of Computer Applications, nr. 4, pp. 0975-8887, 2014.

[2] Hung-Min Sun, Chi-Yao Wng, Chin-Feng Lee, Cheng-Hsing Yang, „Anti-Forensics with steganographic data embedding in digital images“, Selected areas in communications, nr. 7, 2011

[3] „Digital steganalysis: review on recent approaches“, Global research in computer science, nr. 1, 2011

[4] R. Din, H. S. Hussain, S. Shuib, „Hiding secret messages in images: suitability of different image file types“, WSEAS TRANSACTIONS on COMPUTERS, nr. 6(1), pp. 127 -132, 2006.

[5] W. Luo, F. Huang, J. Huang, „Edge adaptive image steganography based on LSB matching revisited“ , Information forensics and security, nr. 2, 2010

[6] J. Harmsen and W. Pearlman, “Steganalysis of additive-noise modelable information hiding,” *Proc. SPIE Electronic Imaging*, nr. 5020, pp. 131–142, 2003.

[7] A. D. Ker, “Steganalysis of LSB matching in grayscale images,” *IEEE Signal Process. Lett.*, nr. 6, pp. 441–444, 2005.

[8] J. Kodovsky, J. Fridrich „Effect of imade downsampling on steganographic security“, Information forensics and security, nr. 5, 2014

[9] R. Böhme, “Weighted stego-image steganalysis for JPEG covers,” *Proc. 10th Int. Workshop Inf. Hiding*, pp. 178–194, 2007,

[10] V. Holub, J. Fridrich, “Optimizing pixel predictors for steganalysis,” *Proc. SPIE*, nr. 8303, pp. 1–13, 2012.

[11] J. Kodovský J. Fridrich, “Steganalysis in resized images,” *Proc.IEEE Int. Conf. Acoust., Speech, Signal Process.*, pp. 2857–2861, 2013,

[12] W. Luo, Y. Wang, and J. Huang, “Security analysis on spatial ±1 steganography for JPEG decompressed images,” *IEEE Signal Process. Lett.*, no. 1, pp. 39–42, 2011.

[13] T. Quach, „Extracting hidden messages in steganographic images“, Digital Investigation, pp. S40-S45, nr. 11, 2014

[14] Yao Lu „Investigating steganography in audio stream for network forensic investigation“, 2014

[15] J. Silman „Steganograhpy and steganalysis: an Overview“, 2001

[16] Bret Dunbar „A detailed look at Steganographic Techniques and their use in an Open-Systems Environment“, SANS Institute, 2002

[17] C. P. Sumathi, T. Santanam, G. Umamaheswari „A Study of various steganographic techniques used for information hiding“, International Journal of Computer & Engineering Survey, nr. 6, 2013.

[18] M. Nosrati, R. Karimi, M. Hariri, „An introduction to steganography methods“, World Applied Programming journal, nr. 3, 2011.

[19] A. Cheddad, J. Condell, K. Curran, P. Mc Kevitt, „Digital image steganography: Survey and analysis of current methods“, Journal of Signal Processing, nr. 90, pp. 727-752, 2010.

[20] G. Corser, „Entropy as an estimate of image steganografy“, Computer science and engineering Oakland University, 2012

[21] R. Poisel, S. Tjoa, „Forensics investigations of multimedia data: a review of the State-of-the-Art“, Insertnational conference on IT security incident management and IT forensics, 2011.

[22] T. Pevny, J. Fridrich, „Multiclass detector of current steganographic methods for JPEG format“, Journal of IEEE transactions on intermation forensics and security, nr. 4, 2008.

6. PRIEDAI

Šiame priede pateikiami bandymų metu naudotų slepiamų paslapčių failų, kurie buvo naudoti skyrelyje „Steganografinių metodų tyrimas“, turiniai.

PASLAPTIS1.TXT:

„Brangi Mamyte, brangus Tėtukai! Man čia gera.

Tikiuos, kad jūs, dėdė Juozas, podė Liucė, dėdė Antans, teta Stasė, dėdė Prans, teta Bronikė, dėdės Rička ir Vacius, Steps, Broniuks, Moncikė, Macijauckų Rimutė, Zosikė, Stefa, Vanda su savo Zeniuku ir mano Zigmuks tai pat sveiki. Pasakykit visiem, ka ta tarnyba yr superinis reikals. Nėr ka lygint su mūsų Varputėnais. Tegu jie greičiau atvara užsirašyti, kol da te yr vietų.

Iš pradž jaučiaus kvailai, mat iki šešių reik voliotis lovoj, tai blemba net nepatogu…. Nei tau galvijų šert, nei karvių melžt, nei mėšlo vežiot, nei krosnies kurt neverč… Pasakykit Vaciui ir Stepukui, kad reik tik sava lovą paklot (prie to galim i priprast) ir iki pusryčių kelis daiktus pavalyt. Visiem vyrukam kasdien reik skustis, bet tai nėr baisu, nes yr karšts vanduo. Visą laik, bet kurią valandą! Pasakykit mana Zigmukui, ka tik pusryčiai čia juokingi, tipo europietiški. Prasti popieriai matyt toj Europoj, oi, prasti… Tik viens kiaušins, pora permatomų riekelių kumpia i sūria. I da kažkokių grūdų, kurių net vištos nelestų, su pienu. Nei tau bulbų, nei lašinių, nei zacirkas! Laimei, bent duonos gali pasimt, kiek širdis trokšt (todėl draugeliai mane Kepaliuku ir praminė…). Su pietum tai jau bėdos nėr. Tiesa, porcijas vaikiškas kai daržely, ale tie miestiečiai arba valga nedrūčiai, arba išvis mėsas net nelieč… Kiba jie kokie ligoniai..? Tad ko nesuvalga, man ataneša, i tada jau gerai.

Tie miestiečiai išvis kažkokie keisti… Bėgiot tie lepūnėliai nesugeb. Muštis taip pat… Mum če reik bėgiot su manta. Nu, kap pas mumi namuos kožną rytą, tik be viedrų. Trumpiau. Kap nuo mūsų stubos iki bažnyčios. Parbėgę tai jie tik akis pastata ir šnopuoja kaip šernai. Nesuprantu ko jie apsivemia, da i su kraujais kartais. Juk tai tik 5 kilometrai i da su dujokauke! Tad reik juos po to į kareivines sunkvežimiu parvežt, nes iš jų jau jokias naudas. Per kovos pratybas tik paspaudi tokį trupučiuką …ir jau lūža kokia ranka! Matyt čia nuo tas kavas, kur litrais lak, i da dėl tas mėsas, katros jie nevalga…! Stipriausias pas mumi tai tokis Kazlauskas iš Alizavas prie Kupiškio. Bet jisai tai 2 metrų ilgio ir sveria kokius 120 kilų, o aš tai vos 1,66 m ir gal 72 kg…mat priaugau trupučiuką nuo to gera kareiviška maista…

O daba žiūrėkit, juokingiausias dalykas! Būtinai papasakokit apie tai dėdei Ričkai, Broniui ir mana Zigmukui. Jau turiu pirmą medalę už šaudymą!!! Ale žinokit nesuprantu, už ką… Tas juočkis balvons, kur ant jų skyda nupaišyc, didelis kai kokia jaučia galva. I nejud visai, ne taip, kai miške šernai ar kiškiai. Ir į tavi nieks nešauda, kaip pas mumi broliai Šapalai per medžioklę iš sava berdankių. Kulipkos – kai daina… i da patiem jų gamint nereik! Tik paėmei naujų, pakrovei ir, jei nesi akls, pataikai nesitaikęs!

Mūsų seržanc kažko primena matiekos mokytoją Vyšniauckienę. Šnek, rėk, nervinas be krašto, ir vis tiek nesuprasi, ko ans nori. Iš pradžių ant manęs kažko užsisėda ir liepė vien su maike lakstyt per lietų po aikštę. Ale kartą daviau čierką samagono, to, kur dėdė Prans atsiuntė, tai vos kojų nepakratė. Lakstė visas raudons po tą aikštę, o po to pusdienį šikinyke tūnojo. Kitą dieną prisakė man bonkę to Prana samagona iki dugna išgert. Iškart visą. Nu i ką? I nieka! Samagons gers, visai kai nuo vaikystės žinau. Seržanc tik akis pastatė, o daba vis žiūr į mane kaip kažką įtardams, ale jau nustoja kabinėtis.

Pasakykit visiem, kad ta tarnyba yr superinis dalyks. Tegu greičiau atvara užsirašyt, kol da yr vietų. Bučkiai visiems (ypač mano Zigmukui) Jūsų dukra Marytė“

PASTAPTIS2.TXT

„Trečiadienį Didžiosios Britanijos teisme 38 metų Lietuvos pilietis Viktoras Bružas prisipažino pernai lapkritį per šešias minutes mirtinai subadęs 55 metų Patricką ir 54 metų Gillianą Kettyle'us jų namuose Felčame. Už šį nusikaltimą teismas jam skyrė 33 metus nelaisvės, praneša britų žiniasklaida.Teisme paaiškėjo, kad V.Bružas nusikaltimui ryžosi įtardamas, kad P.Kettyle'as flirtavo su jo buvusia žmona ir paskatino ją skyryboms.

Pareigūnai išsiaiškino, kad V.Bružas prieš šį nusikaltimą kelis kartus buvo P.Kettyle'ui grasinęs. Policija dėl to buvo jį įspėjusi.

Tačiau pernai lapkričio 27-osios naktį, prieš tai gausiai išgėręs, V.Bružas pasiėmė didelį virtuvinį peilį ir atvyko į Kettyle'ų namus įvykdyti, kaip paaiškino pats žudikas, revanšo už sužlugdytą santuoką.

Du žmones nužudė per 6 minutes

Kelią į šeimininkų miegamąjį V.Bružas puikiai žinojo, nes anksčiau buvo remontavęs jų vonios kambarį. Į namą jis pateko perlipęs per tvorą ir išdaužęs langą pirmajame pastato aukšte.

Name vyras užtruko vos šešias minutes. Per tiek laiko jis mirtinai subadė P.Kettyle'ą ir jo žmoną. Prokuroras Alanas Kentas teigė, kad užpuolimas buvo labai žiaurus. P.Kettyle'as buvo subadytas į galvą, krūtinę, nugarą ir net kojas. Pasak prokuroro, Gillianos žudyti V.Bružas nesiruošė, tačiau moteris stojo ginti savo vyro, todėl smūgių peiliu į nugarą ir krūtinę kliuvo ir jai.A.Kento teigimu, moteris kurį laiką dar buvo gyva ir sugebėjo paliepti kitame kambaryje pasislėpusiam šešiolikmečiui sūnui paskambinti policijai. Atvykę pareigūnai pamatė šiurpų vaizdą – nužudyta pora gulėjo kraujo klane savo miegamajame.

Netrukus netoli Kettyle'ų namų buvo rastas ir nužudymo įrankis – peilis su žudiko pirštų atspaudais. Po 18 val. V.Bružas buvo sulaikytas.

Prokuroro teigimu, sulaikomas lietuvis nesipriešino ir elgėsi ypač ramiai. „Jis tik paklausė, kiek metų nelaisvės Didžiojoje Britanijoje skiriama už tokį nusikaltimą“, – pasakojo prokuroras.

Tačiau pirmose apklausose V.Bružas dar mėgino kaltę neigti. Lietuvio prisipažinimą aukų artimieji išgirdo tik trečiadienį teismo salėje. Jo advokatas teigė, kad prisipažinti vyras nutarė dėl to, kad byla būtų greičiau išnagrinėta ir nereikėtų apklausti egzekucijos metu name buvusio ir viską girdėjusio šešiolikmečio.

Kettyle'ų sūnus kraupią lapkričio 27-osios naktį buvo užsirakinęs savo kambaryje ir pasislėpęs. Subadęs aukas V.Bružas dar priėjo prie jo kambario durų ir pasakė nenorintis nieko blogo jam ir Gillianai ir kad „dėl visko kaltas Patrickas“.
Grasino keliskart

Teisme paaiškėjo, kad V.Bružas prieš nusikaltimą ne kartą buvo grasinęs P.Kettyle'ui. 2013 m. sausį dėl lietuvio žinučių britas buvo kreipęsis į policiją, prie namų įrengęs stebėjimo kameras, kurios lemtingą lapkričio naktį fiksavo V.Bružo įsibrovimą.Tai nebuvo pirmas kartas, kai V.Bružas laužėsi į Kettyle'ų namus. 2012 m. laidydamasis įžeidimais jis jau buvo įsiveržęs pas buvusius darbdavius.

V.Bružas Kettyle'ų įmonėje įsidarbino 2007-aisiais, kai su žmona Kristina iš Kauno persikraustė į Didžiąją Britaniją. Bendradarbiai lietuvį apibūdino kaip gerą statybininką.
Šefas paskatino skirtis

37 metų K.Bružienė taip pat dirbo Kettyle'ams. Ji buvo jų valdomos statybų ir nekilnojamojo turto įmonės sekretorė.

Teisme teigta, kad P.Kettyle'as vadovavo verslui iš namų. Tačiau jis gana artimai bendravo su K.Bružiene. Teigiama, kad ji savo viršininkui atviravo apie savo netikusią santuoką, apie vyro agresiją ir buvo jo raginama ryžtis skyryboms.

„P.Kettyle'as buvo tikrai žavingas vyras. Panašu, kad kaltinamojo žmona su juo galėjo atvirai pasikalbėti apie savo santuoką. Ji pasiskundė dėl vyro smurto ir kontrolės, kurią nuolat kentė“, – sakė prokuroras.

Pašnekesiai ir flirtas su šefu moterį įkvėpė skyryboms.

„Gal Patrickas flirtavo su darbuotoja, gal ji atsakė tuo pačiu ir gal tai suteikė tvirtumo K.Bružienei nutraukti kankinančius santykius“, – pripažino A.Kentas.

Pasak jo, V.Bružas apie draugiškus žmonos santykius su vadovu sužinojo perskaitęs jos elektroninius laiškus 2012 m. Vos tai padaręs V.Bružas paryčiais atlėkė pas Kettyle'us rėkdamas, kad Patrickas bando atimti jo žmoną. Dar vieną grasinančią žinutę Patrickui lietuvis elektroniniu paštu išsiuntė 2013 m. Tuomet verslininkas kreipėsi į policiją, o pareigūnai įspėjo V.Bružą liautis persekiojus buvusį darbdavį.

Advokatas: „Norėjo išsaugoti santuoką“

Advokatas Peteris Wilcockas teismą bandė įtikinti, kad žmogžudystės V.Bružas iš anksto neplanavo.
Jo teigimu, su peiliu rankose Kettyle'ų miegamajame V.Bružas pasirodė tik norėdamas pagąsdinti Patricką.

„Akivaizdu, kad vyras visaip bandė išsaugoti savo santuoką“, – gynė lietuvį advokatas.

Jis pabrėžė, kad moters žudyti V.Bružas nė nenorėjo. Taip pat atkreipė dėmesį, kad V.Bružas buvo jautrus šešiolikmečiui ir pripažindamas kaltę apsaugojo jį nuo liudijimų teisme.

Prisipažinimas ketveriais metais sutrumpino ir V.Bružui skirtą laisvės atėmimo bausmę.

Jam kalėjime teks praleisti ne 37, o 33 metus.

Teisėjas: „Santuoką sugriovė pats“

Teisėjas Robinas Spenceris skelbdamas nuosprendį pareiškė, kad Kettyle'ai buvo laiminga sutuoktinių pora, o Patricko flirtas su K.Bružiene buvęs labai nekaltas.

„Manei, kad tavo santuoką sugriovė Patrickas. Tačiau iš tikrųjų ji baigėsi dėl to, kad tu smurtavai prieš savo buvusią žmoną“, – į nuteistąjį kreipėsi teisėjas.
Teisėjas pažymėjo netikintis, kad peilį į verslininkų namus V.Bružas atsinešė tik norėdamas apsiginti nuo šunų ir siekdamas pagąsdinti Patricką.

„Visa istorija rodo, kad buvai apsėstas minties nužudyti vyrą, kuris drįso flirtuoti su buvusia tavo žmona“, – sakė teisėjas.

Aukų artimieji teisme kalbėti atsisakė dėl per didelio skausmo. Tačiau šeimos atstovas Markas Prestonas teigė, kad šeimą tenkina teismo skirta bausmė žudikui.“

PASLAPTIS3.TXT

„Verslininko Aurimo Rapalio nužudymu įtariamas nepilnametis buvo pažįstamas ne tik su savo auka, bet ir policija. Jaunuolio atžvilgiu buvo pradėti ikiteisminiai tyrimai dėl vagystės ir plėšimo. Žiauraus nusikaltimo aplinkybes tiriantys prokurorai sako, kad 17-metis prisipažino subadęs A.Rapalį ir tai padaręs iš savanaudiškų paskatų.
Sėkmingai verslą IT srityje vysčiusio 31 metų kauniečio A.Rapalio gyvybei pavojus iškilo penktadienį paryčiais, kai jis buvo subadytas prabangiame savo bute I.Kanto gatvėje. Praėjus daugiau nei parai Kauno klinikose gydytas vyras mirė.

Tyrimo duomenys rodo, kad „Bokštu“ vadinamame pastate gyvenęs A.Rapalis nužudymu įtariamą jaunuolį į namus įsileido pats. Pareigūnų teigimu, jiedu buvo pažįstami ir anksčiau – bendravo apie 4 metus.

Kas siejo verslininką ir moksleivį, neaišku. Pareigų duomenimis, darbo ryšiais jie nebuvo susiję.
Nusikaltimo motyvai neaiškūs
Pasak įvykį tiriančių pareigūnų, žmogžudyste įtariamas jaunuolis prisipažįsta tai padaręs, tačiau motyvai, dėl ko įvykdytas nusikaltimas, lieka neaiškūs.

Pirmadienį surengtoje spaudos konferencijoje Kauno apygardos prokuratūros vyriausiasis prokuroras Darius Valkavičius ir Kauno apygardos prokuratūros Pirmojo baudžiamojo persekiojimo skyriaus vyriausiasis prokuroras Vitoldas Guliavičius teigė, jog tiriamos kelios versijos. Tačiau pagrindinė – nužudymas iš savanaudiškų paskatų.

„Pirmiausia buvo byla tiriama dėl sunkaus sveikatos sutrikdymo. Vėliau nukentėjusiajam mirus, byla perkvalifikuota į nužudymą“, – spaudos konferencijoje kalbėjo prokuroras D.Valkavičius.
Prokurorų teigimu, peiliu į krūtinę, nugarą ir kaklą sunkiai sužeistas verslininkas dar įstengė nusileisti į prabangaus namo pirmąjį aukštą ir paprašyti pagalbos. Ten budintis apsaugos darbuotojas iškvietė greitosios medicinos pagalbos ekipažą.

Atvykę medikai nukentėjusįjį skubiai išgabeno į Kauno klinikas. Antruoju ekipažu į tą pačią gydymo įstaigą išvežtas ir nusikaltimu įtariamas nepilnametis.“

PASLAPTIS4.TXT

„Tikiuos, kad jus, dede Juozas, pode Liuce, dede Antans, teta Stase, dede Prans, teta Bronike, dedes Ricka ir Vacius, Steps, Broniuks, Moncike, Macijaucku Rimute, Zosike, Stefa, Vanda su savo Zeniuku ir mano Zigmuks tai pat sveiki. Pasakykit visiem, ka ta tarnyba yr superinis reikals. Ner ka lygint su musu Varputenais. Tegu jie greiciau atvara uzsirasyti, kol da te yr vietu.“

PASLAPTIS5.TXT

„Brangi Mamyte, brangus Tetukai! Man cia gera.“