Зборник радова Факултета техничких наука, Нови Сад

UDK: 004.738.1:766
DOI: https://doi.org/10.24867/32BE7Ristic

СТЕГОАНАЛИЗА АУДИО ЗАПИСА

AUDIO STEGANALYSIS

Марк Ристић, *Факултет техничких наука, Нови Сад*

Област – ЕЛЕКТРОТЕХНИКА И РАЧУНАРСТВО

Кратак садржај – *Стеганографија, стеганографске технике и стегоанализа означавају појмове везане за технике сакривања информација унутар наизглед безазлене комуникације. Први део рада упознаје читаоца са основним појмовима и дефиницијама стеганографије и стегоанализе. Након тога, описане су основне стеганографске и стегоаналитичке технике. Практична имплементација овог рада је уско везана за аудио фајлове, технику супституције бита најмање важности и технику кодирања парности. Описан је стеганографски процес кроз употребу већ постојећих и ручно имплементираних алгоритама. Извршена је стегоаналитичка класификација употребом различитих класификационих модела.*

Кључне речи: *стеганографија, стегоанализа, аудио стеганографија, кодирање парности, супституција бита најмање важности, вештачка интелигенција*

Abstract – *Steganography, steganographic methods and steganalysis signify terms connected to information hiding techniques inside innocent seeming communication. The first part of this paper introduces the reader with basic steganography and steganalysis concepts and definitions. The practical implementation of this paper is tightly coupled to audio files, the least significant bit substitution method and the parity coding method. This paper also describes the steganographic process via usage of already existing and manually implemented algorithms and steganalitical classification via different classification models.*

Keywords: *steganography, steganalysis, audio steganography, parity coding, least significant bit substitution, artificial intelligence*

1. УВОД

Двадесет и први век, окарактерисан као четврта индустријска револуција [1], сведочи експоненцијалном технолошком напретку човечанства, напретку који је утемељио „информацију“ као основну и највреднију валуту дигиталног друштва. Новонастала учесталост електронске комуникације довела је у питање безбедност њене употребе, где су се као одговор на овај новонастали проблем појавиле различите технике шифровања података. Шифровање података подразумева криптографски процес, где је циљ сакривање садржаја, тј. његово претварање у нечитљив скуп знакова, читљив једино од стране особа које поседују кључ за дешифровање. Иако је модерно шифровање веома робусно, крајњи учесници комуникације, као и присутност тајне комуникације су још увек очигледни. Идентитет учесника могуће је сакрити употребом анонимних римејлера (енг. *anonymous remailers*) [2] који прослеђују поруке без прослеђивања пошиљаоца. Нажалост, сама употреба ове методе не сакрива постојање тајне комуникације, те се нападом на ове посреднике могу открити крајњи учесници. Постоје одређене политичке, службене (нпр. тајна операција) па и криминалне ситуације [2], где је неопходно сакрити само постојање комуникације. Техника скривања тајних порука на такав начин да нико осим предајне и пријемне стране није свестан постојања комуникације назива се стеганографија. Технике откривања постојања скривених порука унутар наизглед бескорисних информација назива се стегоанализа [3].

2. СТЕГАНОГРАФИЈА

Масивна дигитализација модерног света омогућила је инстант комуникацију између било која два дела планете. Помоћу ове „тренутне комуникације“ креиране су нове врсте заједница, нове врсте услуга и наравно нове врсте послова. Поред свих позитивних новина, главни носилац дигиталне комуникације, интернет, постао је мета експлоатације у виду пресретања информација дељених његовим путем. Као што је споменуто у самом уводу, шифровање у великој мери осигурава интернет комуникацију користећи робусне и доказане протоколе као што су HTTPS, SSH и FTPS. Главна мана, и притом главна разлика између шифровања и стеганографских процеса јесте у чињеници да шифровање по својој природи не сакрива само „постојање комуникације“ из чега настаје и главни разлог примене стеганографије.

2.1. Примена стеганографије

Претходно смо навели политичке, криминалне и службене домене као домене употребе стеганографије. У овом делу одељка биће конкретизована примена стеганографских процеса кроз реалне примере из модерног дигиталног друштва. Преласком са аналогних на дигитална складишта уметности као што су филм, сликарство и музика, настао је проблем противзаконите расподеле дигиталних добара. Како би се заштитило ауторско право или интелектуална својина, креирана је техника означавања дигиталних фајлова воденим жигом (енг. *watermarking*) [2]. Како

НАПОМЕНА:
Овај рад проистекао је из мастер рада чији ментор је био др Стеван Гостојић, ред. проф.

би се спречила пиратизација ових материјала, на њега се ставља жиг који јасно приказује коме припада дата својина (слика 1).

Слика 1. *Пример воденог жига [4]*

2.2. Основни појмови

Примарни циљ стеганографије лежи у сакривању постојања скривене комуникације помоћу наизглед безазлене комуникације. Насупрот, употреба воденог жига се често не сакрива, па чак и наглашава у циљу застрашивања од незаконите употребе означених материјала. Битно је напоменути да стеганографија и означавање воденим жигом деле теоријску основу на којој се темеље, али су њихова примена и фактори који утичу на њихову примену, различити [2].

Основна мера квалитета система воденог жига јесте ефективност уграђивања и она представља шансу да детектор жига погреши тј. не верификује постојање очекиваног жига одмах након уграђивања пре било какве дисторзије као што је компресија. Позитивна (не нула) шанса за ову грешку означава присуство ограничавајућих фактора уграђивања као што је верност (енг. *fidelity*). Другим речима, комбинација датог преносиоца и датог уграђивача не могу беспрекорно да угради жиг у медијум. У случају стеганографије, не користи се мера ефективности уграђивања зато што стеганографија најчешће није везана за конкретан медијум преноса, док водени жиг означава конкретан (без могућности промене) медијум (филм, слику, песму итд.) [2].

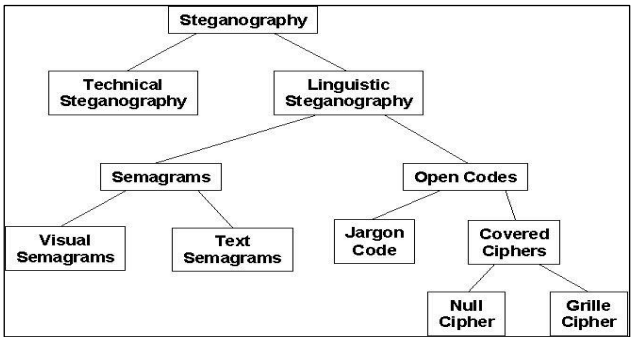
Споменута мера верности, често није примењива у области стегоанализе зато што стегоаналитичари често немају приступ оригиналном преносиоцу у који је уграђена порука како би се проценила верност медијума са поруком у односу на чист медијум. Као што се може приметити из претходног дела, стеганографија акценат ставља на поруку која се уграђује, док маркирање воденим жигом мари једино за медијум преноса, а од поруке очекује једино да докаже власништво медијума.

Иако стеганографија не садржи медијумска ограничења (није везана за специфичан фајл, често ни за врсту фајла), постоје друга ограничења која треба узети у обзир, као на пример капацитет уграђивања. Капацитет уграђивања дефинише се као максималан број битова који може да се модификује у циљу уграђивања поруке у дати медијум за дату методу. У случају употребе методе најмање битног бита и слике као медијума, капацитет уграђивања представља укупан број пиксела дате слике. Наравно, што се више битова модификује већа је шанса за оштећење преносиоца и евентуалну детекцију од стране стегоаналитичких алата. Много бољу меру представља стеганографски капацитет, који представља максималан број битова који могу бити употребљени за сакривање поруке, да се при том минимализује могућност детекције присутности скривене поруке. Стеганографски капацитет је много мањи од капацитета уграђивања, и веома га је тешко израчунати и за веома просте стеганографске системе. Што је порука мања/краћа мање су шансе за детекцију – порука од неколика битова је можда корисна као водени жиг, али не представља корист као скривена порука коју прималац треба да интерпретира и искористи. Циљ модерних стеганографских алата је сакривање што веће поруке уз помоћ што мање модификација преносиоца поруке. Баланс овог односа представља стеганографска ефикасност [2].

2.3. Технике стеганографије

Популарност стеганографије која је доживела нагли раст крајем претходног и почетком тренутног века се још увек шири. Све је више стеганографских алата који кроз неколико корака могу да сакрију поруку у неки медијум. Иако се већина техника бави манипулацијом битова, постоје стеганографске технике које претходе дигиталном добу.

Кеслер је 2004. поделио стеганографске технике на следећи начин (слика 2):



Слика 2. *Кеслерова подела стеганографије [5]*

Техничка стеганографија користи научне методе као што су невидљиво мастило, воштане табле, микро тачкице и друге методе сакривања поруке путем маскирања или смањивања величине.

Лингвистичка стеганографија представља сакривање тајне поруке помоћу неке наизглед безначајне/безазлене поруке путем неког од преносиоца. Даље се категорише кроз семаграме и отворене кодове.

Семаграми сакривају поруке користећи симболе или знакове. Визуелни семаграми сакривају поруку користећи безазлене или свакодневне објекте као што су цртежи, распоред ствари на слици једног стола или веб страница. Текстуални семаграми сакривају поруке модификацијом текста који преноси поруку, као што су промена фонта (стил, величина), модификацијом празних поља између слова, различито украшеним словима и сл.

Жаргонски код означава поруку где само намењени примаоци могу да схвате значење.

Скривене шифре сакривају поруку као подскуп свеукупног текста преноса. Овај подскуп није могуће идентификовати без познавања „тајне“, односно кључа од кога зависи логика закључавања и откључавања. Решеткаста шифра подразумева стављање одређеног обрасца преко текста преноса, где решетка наглашава поруку. Нулте шифре прате раније уговорену логику писања и читања поруке као што је „прочитај сваку реч након речи која почиње са сугласником“ или нешто простије као „прочитај сваку седму реч сваке друге реченице“.

Дигитална стеганографија обухвата техничку стеганографију и делове лингвистичке стеганографије. Дигитална стеганографија користи дигиталне фајлове као преносиоце скривених порука.

Учестала места за сакривање поруке јесу [6]:

- сакривање унутар текста – програмски код, текст текстуалних докумената (нпр. .docx, .pdf, .txt, .py фајлови),
- сакривање унутар диск простора – фајлови често не заузимају читав алоциран диск простор, вишак диск простора (енг. *slack space*) се може искористити за сакривање тајних порука,
- сакривање унутар мрежних пакета – заглавља TCP/IP пакета поседују просторни вишак у који је могуће уградити поруке,
- сакривање унутар електричних кола – распоред електричних кола на плочи може да представља маркер за валидност хардвера и
- сакривање унутар сликовних, аудио и видео фајлова – поруке могу да се сакрију у информације ових медија као што су контраст, фреквенција, боја итд.

2.3.1. Аудио стеганографија

Аудио стеганографија подразумева модификацију дигиталног звучног сигнала, тако да се минимизује шанса да човек или рачунар примете промену. Све технике аудио стеганографије се ослањају на принципе и особине људског слушног система (енг. *human auditory system – HAS*) и чињеницу да иако људски слух има велики динамички опсег (осетљивост на гласноћу), људи поседују мали диференцијални опсег (осетљивост на разлике између две узастопне тачке аудио сигнала) [7].

Супституција бита најмање важности може се применити на било какав бинарни фајл, па тако и на аудио фајлове. Техника сакрива поруку кроз бите најмање важности, пратећи унапред договорену логику. Овакве промене, све док поштују ограничења стеганографског капацитета, не утичу превише на звук садржаја, али могу бити препознате од стране напредних стегоаналитичких алата.

Техника кодирања парности дели сигнал на одвојене области узорака и кодира сваки бит тајне поруке у биту парности тренутне регије узорка. Уколико се бит поруке и бит парности не подударају, окреће се бит најмање важности једног од узорака у регији.

3. СТЕГОАНАЛИЗА

Стегоанализа представља скуп техника које деле заједнички циљ препознавања присутности тајних порука унутар неког стего преносног медијума. Детекција у домену стегоанализе, често дефинисана као стегоаналитички напад, представља класификациони проблем, обично у више нивоа. Примарни задатак јесте класификација у две класе, чист објекат и стего објекат. Секундарни задатак јесте препознавање конкретног стеганографског алгоритма. Терцијални задатак јесте откривање садржаја поруке. Разликујемо циљану и слепу стегоанализу у зависности од тога да ли нам је познат стеганографски алгоритам или не.

3.1. Аудио стегоанализа

Технике аудио стегоанализе се базирају на идентификацији аномалија и несагласности у приказима медијума у различитим доменима као што су фреквентни и просторни домен. Аудио сигнали се ређе користе као медијум од слика, али имају ту стеганографску предност да људски слух не може да примети све фреквенције и амплитуде доступне стего комуникаторима. Наравно, постоје и боје и друге сликовне мере које човек не може да процесира, али би оне изазвале визуелне очигледности, док су у аудио снимцима просто занемарене.

4. МЕТОДОЛОГИЈА

Ово поглавље описује методологију коју имплементира софтверски алат који стеганографски уграђује текстуалну поруку унутар .wav аудио фајла преко више алгоритама и употребом различитих класификационих модела класификује тестни фајл у N+1 класа где је N број алгоритама за уграђивање. Нулта класа представља чист фајл без скривене поруке.

Класификатор базиран на статистичким особинама врши статистичку анализу аудио сигнала. Екстрахују се особине сигнала и додају се лабеле за сваки ред унутар скупа података. Екстраховане особине се чувају у фајл и употребом генетског алгоритма се налази гранична вредност за сваку посматрану особину. Вредности изнад или испод ове вредности се сматрају сумњивим, након N од M сумњивих вредности фајл проглашавамо прљавим (N – подесив број тренутно сумњивих особина, M – број укупних посматраних особина.

Класификатор базиран на моделима вештачке интелигенције такође издваја особине сигнала. Разлика је у начину тренирања где се код претходних модела употребом генетског алгоритма тражио скуп оптималних граница, док се код модела вештачке интелигенције тренира конкретан математички модел над скупом података.

Поред класификатора базираних на статистичким особинама, имплементирана су три модела вештачке интелигенције: Support Vector Machine (Classifier), алгоритам случајних шума (енг. *random forest*) [8] и XGBoost алгоритам [9]

4.1. Скуп података

Као извор аудио фајлова коришћен је „Freesound General-Purpose Audio Tagging“ [10] скуп података. Овај скуп података садржи око 11.000 аудио фајлова у .wav формату. Скуп података је означен у сврхе идентификације жанра и инструмента употребљених у фајлу. Пројекат не користи ове лабеле, врши процесирање над основним скупом фајлова и задаје му сопствене лабеле које употребљава за класификацију.

Коначан скуп података (укупно 27.142 фајлова) састоји се од три групе фајлова: чистих (из оригиналног скупа података), креираних кодирањем парности и креиране супституцијом бита најмање важности употребом већ имплементираног алгоритма. Код креирања коначног скупа података примењен је и на тестни скуп и на скуп намењен за тренирање.

5. РЕЗУЛТАТИ

Класификација у три класе (чист, lsb, фајл кодирања парности) путем класификатора базираног на статистичким особинама постигла је тачност од 0,4611, док је класификација у две класе (чист, прљав) постигла тачност од 0,6039.

Резултате три имплементирана модела вештачке интелигенције могуће је видети у табели 1:

Табела 1. *Компарација резултата модела вештачке интелигенције*

Model	Accuracy	Weighted Avg Precision	Weighted Avg Recall	Weighted Avg F1-Score	Support
SVC	0,80	0,82	0,80	0,79	5429
Random Forest	0,88	0,91	0,88	0,88	5429
XGBoost	0,87	0,89	0,87	0,86	5429

6. ДИСКУСИЈА

Модел случајних шума представља најбалансиранији модел који кроз читав скуп података показује једнако добре перформансе. Идентификација употребе супституције бита најмање важности се показала као најлакши задатак где су сва три модела показала веома високу тачност. SVC модел иако даје веома добре перформансе је још увек најмање перформантан од три имплементирана модела. Перформансе модела могуће је унапредити проширењем скупа издвојених особина аудио записа и анализом релевантних особина. Ресурсе је могуће појачати употребом Гугл или Амазон сервера за тренирање модела вештачке интелигенције, што би омогућило брже тренирање, бољу хипероптимизацију параметара и експериментисање са више врста модела.

7. ЗАКЉУЧАК

Модернизацијом комуникације модернизовали су се и комуникациони захтеви, где неки од њих захтевају не само заштиту садржаја ове размене, већ и сакривање самог постојања исте. Стеганографија представља решење за претходно поменуте захтеве. Њен главни циљ јесте маскирање тајне комуникације у оквиру неке безазлене комуникације употребом слика, филмова, текста или музике. Напретком науке и технологије, сваким даном појављују се нови стеганографски и стегоаналитички приступи, који ће уједно повећати доступност стеганографских алата и побољшати њихов квалитет.

8. ЛИТЕРАТУРА

[1] K. Schwab, The Fourth Industrial Revolution, Geneva, Switzerland: World Economic Forum, 201

[2] I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, Digital Watermarking and Steganography, 2nd ed., Burlington, MA: Morgan Kaufmann, 2008.

[3] М. Веиновић и С. Адамовић, Криптологија I: Основе за анализу и синтезу шифарских система, Београд: Машински факултет, 2013.

[4] Before and after example of AI watermark. [Online]. Available: https://www.shutterstock.com/image-photo/before-after-example-ai-watermark-600w2259074049.jpg. [Приступљено: Октобар 2024].

[5] G. C. Kessler, "An Overview of Steganography for the Computer Forensics Examiner," Int. J. Digital Evidence, vol. 3, no. 2, Feb. 2004.

[6] N. F. Johnson, Z. Duric, and S. Jajodia, Information Hiding: Steganography and Watermarking – Attacks and Countermeasures, Norwell, MA: Kluwer Academic Publishers, 2003.

[7] K. P. Adhiya and S. A. Patil, "Hiding Text in Audio Using LSB Based Steganography," in Proceedings of the 2012 Int. Conf. Comput. Comm. Inf. Sci., Pune, India, 2012, pp. 1-4.

[8] Scikit-learn, Scikit-learn Documentation, 2023. [Online]. Available: https://scikitlearn.org/stable/api/index.html. [Приступљено: Јул 2024].

[9] XGBoost, XGBoost Documentation, 2023. [Online]. Available: https://xgboost.readthedocs.io/en/stable/python/sklearn_estimator.html. [Приступљено: Јул 2024].

[10] Kaggle, Freesound Audio Tagging Challenge, 2018. [Online]. Available: https://www.kaggle.com/c/freesound-audio-tagging/overview. [Приступљено: Мај 2024].

Кратка биографија:

Марк Ристић рођен у Суботици 1998. год. дипломирао је 2021.год. на ФТН-у, смер Рачунарство и аутоматика са темом „Примена фази логике у управљању безбедности информационих система“ контакт: risticmark1337@gmail.com