Зборник радова Факултета техничких наука, Нови Сад

УДК: 004.738.1:766
ДОИ: https://doi.org/10.24867/16BE10Kevac

СТЕГАНОГРАФИЈА И СТЕГОАНАЛИЗА

STEGANOGRAPHY AND STEGANALYSIS

Елена Кевац, *Факултет техничких наука, Нови Сад*

Област – ЕЛЕКТРОТЕХНИКА И РАЧУНАРСТВО

Кратак садржај – *У овом раду описана је стеганографија као техника скривеног записа. Детаљно су објашњени типови стеганографије, као и алати који се користе да би се ова техника спровела у дјело. Такође, у наставку рада описана је стегоанализа која представља метод откривања стеганографије, као и алати који се користе у те сврхе.*

Кључне речи: *стеганографија, стегоанализа, дигитална форензика*

Abstract – *This paper describes steganography as a technique of hidden notation. The types of steganography are explained in detail, as well as the tools used to put those technique into use. Also, in the continuation of the paper, steganalysis is described as a method of detecting steganography, as well as the tools used for that purpose.*

Keywords: *steganography, steganalysis, digital forensics*

1. УВОД

Један од најважнијих фактора информационих технологија и комуникација јесте безбједност информација. Криптографија је настала као техника осигуравања тајности комуникације. Развијене су многе методе шифровања и дешифровања порука, али понекад није довољно да садржај поруке буде тајан, већ и да постојање поруке буде тајна за неауторизоване кориснике. Развијена је научна дисциплина чији је основни задатак управо то, а њен назив јесте стеганографија.

Назив потиче од грчке ријечи *steganós* (στεγανός) што значи прикривен или тајни, и *–graphia* (γραφή) што значи писање. Стеганографија има врло широке могућности примјене, од прикривене размјене података у приватне и пословне сврхе па до заштите ауторских права у облику воденог жига. Ипак, због свог темељног принципа „невидљивости" често се користи и у илегалне сврхе.

За стегоанализу се може рећи да је она за стеганографију оно што је криптоанализа за криптографију или антивирусни софтвер за рачунарски вирус. То је у ствари процес откривања малих промјена у очекиваном шаблону структуре мултимедијалне датотеке. Дигитална форензика се фокусира на очување и анализу дигиталних доказа. Дефиниција дигиталне форензике је: „Употреба научно изведених и доказаних метода за очување, прикупљање, валидацију, идентификацију, анализу, тумачење, документацију и представљање дигиталних доказа изведених из дигиталних извора у сврху олакшавања или унапређења реконструкција догађаја за које се утврди да су кривични или помаже у предвиђању неовлаштених случајева акције за које се показало да ремете планиране операције" [1].

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

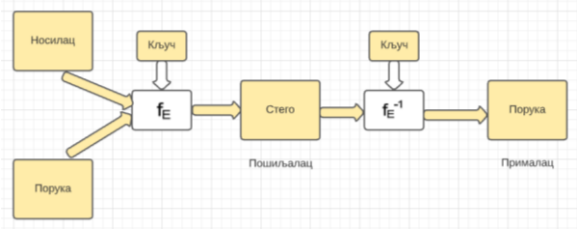
2. СТЕГАНОГРАФИЈА

2.1. Појам и класификација стеганографије

Стеганографија подразумијева прикривање тајне поруке, али не и чињенице да двије стране комуницирају међусобно. Стога, процес стеганографије обично укључује уметање тајне поруке унутар неког преносног медија који се назива носилац и има улогу прикривања постојања тајне поруке. Носилац треба да буде такав скуп података који је саставни дио свакодневне комуникације те као такав не привлачи посебну пажњу на себе. Најчешћи примјери су:

- Слике (.bmp, .gif, .jpeg и сл.)
- Видео записи (.avi, .mpg, .vob и сл.)
- Звучни записи (.mp3, .midi, .wav, .wma и сл.)
- Датотеке (.doc, .xls, .ppt, .txt и сл.)

Пошиљалац кориштењем кључа и стеганографске функције (f_E) утискује поруку у носиоца. Као резултат добија се стеганографски објекат (стего). Стего је комбинација поруке и носиоца (и евентуално кључа). Носилац ће бити видљив свима и неће изазвати сумњу у постојање тајне поруке. Кориштењем стего кључа, пошиљалац маскира поруку у носиоца. Истим кључем прималац издваја поруку из носиоца. Стего кључ се може појавити у више различитих облика. Он може да буде обична лозинка или може да буде позиција у носиоцу. Нападач има могућност пресретања поруке и манипулације стего објектом. Откривањем тајне поруке, нападач је може уништити, измијенити или издвојити.



Слика 1. *Стеганографски систем*

На слици бр. 1 приказан је начин функционисања стеганографског система, гдје је:

- Носилац – медиј унутар којег се сакрива тајна порука
- Порука – тајна порука која треба бити сакривена
- Кључ – стеганографски кључ, параметар функције f_E
- f_E – стеганографска функција „ уграђивање”
- Стего – стеганографска датотека
- ${f_E}^{-1}$ – стеганографска функција „издвајање”

Исти носилац никада не би требало да се користи два пута, јер нападач који има приступ двјема верзијама једне те исте слике може лако детектовати и евентуално реконструисати поруку. Да би се избјегла случајна поновна употреба, и пошиљалац и прималац би требало да униште носиоце које су већ користили за пренос информација.

2.3 Класификација техника стеганографије

Стеганографске технике се у глобалу дијеле на техничку и лингвистичку.
Техничка стеганографија користи научни приступ да би се сакрили подаци. Ова техника се огледа у употреби специјалних уређаја, инструмената и метода у скривању поруке. Техничкој стеганографији припадају сљедеће технике: невидљиво мастило, скривена мјеста, микрофотографије као и дигитална стеганографија. Због своје опширности и фокуса у овом раду, дигитална стеганографија обрађена је у сљедећем одјељку.

2.3.1 Дигитална стеганографија

Код дигиталне стеганографије порука се сакрива у неком од дигиталних медијума попут слике, видеа, звука, текстуалног документа или унутар мрежних пакета. Централни концепт сликовне стеганографије је поступак скривања поруке унутар слике тако да она буде невидљива оку у оригиналној слици. У звучној стеганографији звучна датотека се користи као носилац за прикривање повјерљивог садржаја уз помоћ људског слушног система.

Видео стеганографија је проширење стеганографије слика. Видео снимци нуде нове могућности за скривања података, попут скривања поруке у компонентама покрета. Звучна компонента видео садржаја се такође може искористити за сакривање поруке. Текстуална стеганографија се сматра врло често и најтежом због недостатка сувишних података у текстуалној датотеци. Када је у питању мрежна стеганографија, она се односи на технике уградње скривених информација унутар порука које се шаљу преко мреже унутар TCP/IP заглавља. У наставку текста детаљно су објашњене поменуте технике.

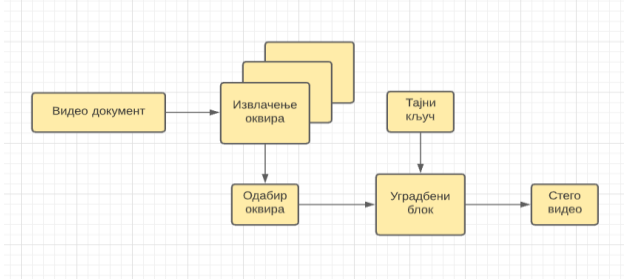
2.3.1.1 Звучна стеганографија

Технике скривања порука у звучној датотеци ослањају се на два корака. Први корак је означавање битова који се понављају у звучној датотеци. Други корак је уметање повјерљиве поруке замјеном ових битова са битовима поруке. Најчешће су три технике звучне стеганографије:

1. Фазно кодирање (енг. *phase encoding*)
2. Ширење спектра (енг. *spread spectrum*)
3. Сакривање одјека (енг. *echo data hiding*).

2.3.1.2 Видео стеганографија

Видео датотека која садржи различите оквире слика користи се као носач за покривање података. Велика количина тајних података може се сакрити у видео датотекама као што су MPEG, MP4, AVI итд.



Слика 2. Основни блок дијаграм за видео стеганографију

Потребни кораци изведени у видео стеганографији су сљедећи:

- Одабир одређеног видео записа у који желимо да уградимо поруку
- Подјела видеа у мале оквире
- Одабир одређене структуре у коју желимо да се тајни подаци убацују
- Тајни кључ је постављен за уграђивање са одређеним оквиром, а затим се стего видео шаље пошиљаоцу

2.3.1.3 Мрежна стеганографија

Односи се на технике уградње скривених информација унутар порука које се шаљу преко мреже унутар *TCP/IP* заглавља. *TCP/IP (*енг. *transmission control protocol/internet protocol).*

3. СЛИКОВНА СТЕГАНОГРАФИЈА

Код овог типа стеганографије, датотеке са екстензијама JPEG, GIF, BMP, PNG итд. користе се за складиштење битова тајне поруке. Најпознатије технике сликовне стеганографије су технике просторног домена, технике фреквентног домена и кориштење формата слике.

3.1 Кориштење формата слике

Најједноставнији метод за скривање информације јесте употреба формата слике код којег се на крај датотеке са сликом убацује текстуална датотека. Порука се додаје након EOF-а. EOF је ознака за крај датотеке. Када се слика отвори у неком програму за преглед фотографија чита се само онај дио до EOF-а, а остатак се занемарује. Кориштењем овог метода не смањује се квалитет слике, али је поруку врло лако открити, односно довољно је отворити слику у било којем уређивачу текста.

3.2 Технике просторног домена

У технике просторног домена спадају замјена бита најмање важности, филтрирање и маскирање, сортирање палета и деградација слике.

3.2.1 Замјена бита најмање важности (LSB алгоритам)

LSB алгоритам (енг. *least significant bit substitution*) је најпопуларнија и најчешће кориштена техника сликовне стеганографије. Идеја ове технике се заснива на

растављању оригиналне поруке у битове, који се потом убацују на позицију бита најмање важности. Појам бит најмање важности се односи на нумеричку вриједност бита у октету, односно на његову тежинску вриједност. Октет заједно са садржавајућим битовима и њиховим тежинским вредностима приказан је на слици 3.

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
1	0	1	1	0	0	1	1

Слика 3. *Октет*

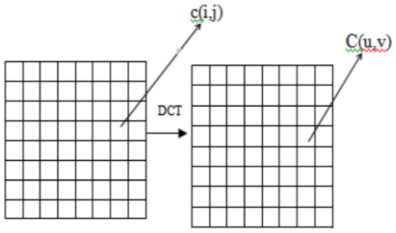
Из претходног објашњења лако је закључити да промјена бита најмање вриједности има најмањи утицај на промјену укупне вриједности октета. Из овога се закључује да промјене бита на најмањим тежинским позицијама у октетима изазивају најмањи утицај на промјену изгледа оригиналне слике.

3.3 Технике фреквентног домена

Технике фреквентног домена користе алгоритме и трансформације, односно математичке функције које се користе и код техника компресије. Најпознатији су алгоритми дискретне косинусне трансформације и дискретне таласне трансформације.

3.3.1 Дискретна косинусна трансформација

Основна улога дискретне косинусне трансформације (енг. *discrete cosine transform – DCT)* је да трансформише сигнал или слику из просторног у фреквентни домен као што је приказано на слици 6. Корисна је при дијељењу слике на различите дијелове различитог значаја, у односу на квалитет слике. Слика се дијели у високофреквентне, средњефреквентне или нискофреквентне компоненте.



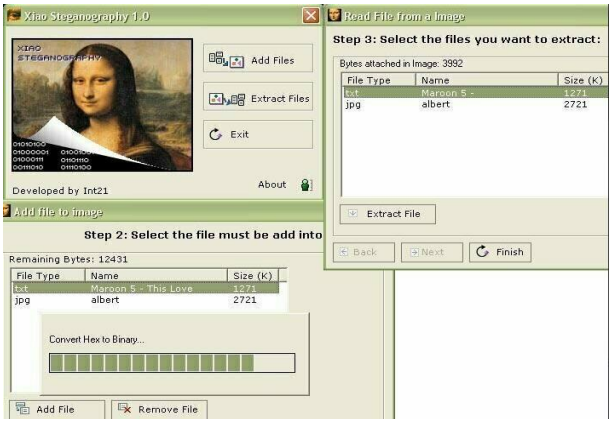
Слика 4. *Дискретна косинусна трансформација слике [3]*

4. АЛАТИ ЗА СТЕГАНОГРАФИЈУ

Постоје многи алати који нуде могућност стеганографије. Неки од њих нуде само стеганографију, док други нуде криптографију прије сакривања података. Примјер алата који се користи у ове сврхе је Xiao Steganography.

4.1 Xiao Steganography

Xiao Steganography је бесплатан софтвер који се може користити за скривање тајних датотека у *BMP* сликама или *WAV* датотекама. Коришћење алата се заснива на томе да се учита било која *BMP* или *WAV* датотека, а затим се дода датотека која треба да буде сакривена. Овај алат подржава и шифровање. Даје могућност бирања алгоритма за шифровање као што су: *RC4, Triple DES, DES, Triple DES 112, RC2* и *hashing SHA, MD4, MD2* и *MD5.* Изабере се било који од њих и сачува се циљна датотека. Да би се прочитала скривена порука из ове датотеке, користи се поново исти софтвер. Овај софтвер ће прочитати датотеку и декодирати скривену датотеку из ње. *Xiao Steganography* има интуитиван изглед који олакшава коришћење као што је приказано на слици 5.



Слика 5. *Изглед алата Xiao Steganography [2]*

5. СТЕГОАНАЛИЗА

5.1 Дефиниција

Стегоанализа (енг. *steganalysis*) је процес детектовања стеганографског садржаја који се заснива на проучавању варијација узорака битова и необично великих датотека.

5.2 Циљеви Стегоанализе

Стегоанализа је обрнути процес у односу на стеганографију. Док је код стеганографије циљ сакрити податке у носиоца, код стегоанализе циљеви су:

- идентификација сумњивих скупова података (сигнали или датотеке), унутар којих се потенцијално налазе скривене поруке,
- утврђивање да ли су подаци уметнути у носиоца шифровани прије процеса стеганографије,
- утврђивање постојања шума или небитних података унутар сигнала или датотеке и
- издвајање и дешифровање уметнуте поруке из стего објекта.

5.3 Облици Стегоанализе

Напади и анализе скривених података које изводи аналитичар укључују различите активности попут детекције, издвајања, онемогућавања или уништавања скривених података. Врста напада који ће бити изведен зависи од информација које су доступне аналитичару. У зависности од тога, постоје облици напада у којима је познато сљедеће

- само стеганографска датотека (енг. *steganography-only attack*) – доступна је само стеганографска датотека над којом се потом изводе различите анализе,
- познати носилац (енг. *known-carrier attack*) – доступна је стеганографска датотека и носилац, а упоређивањем двају датотека се долази до скривеног садржаја. Најбољи примјер је употреба *LSB* технике за скривање тајне поруке у

логоу *Google*-а. Пошто је носилац познат, а доступан је нападачу, он врло лако упоређивањем добијене и оригиналне фотографије може да екстрахује скривене информације,

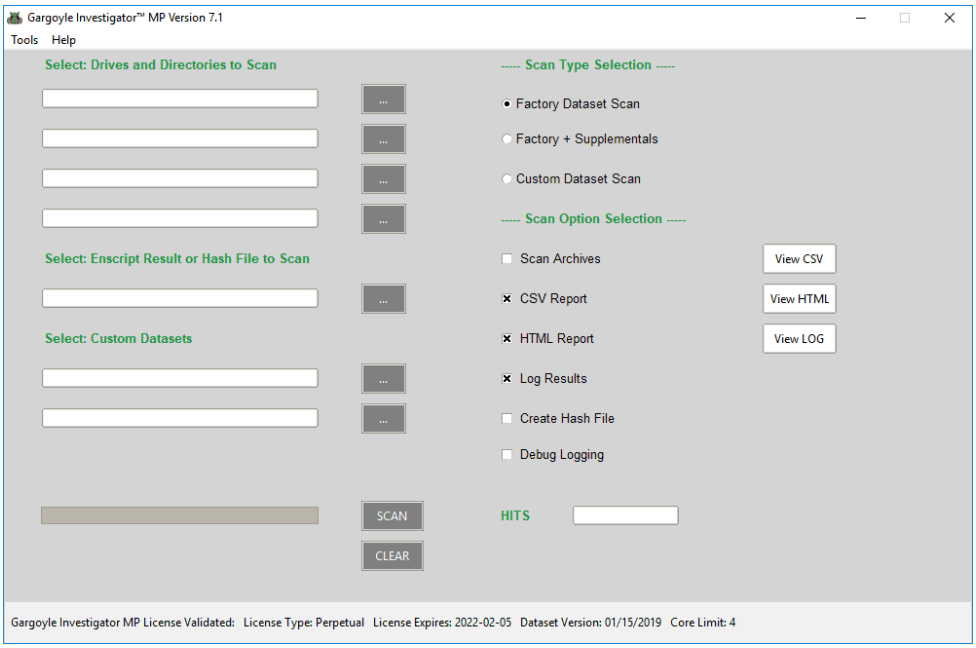
- позната порука (енг. *known-message attack*) – код овог напада доступна је тајна порука,
- изабрана стеганографска техника (енг. *choosen-steganography attack*) – позната је и стеганографска датотека и стеганографска техника, односно алгоритам који је кориштен за уметање поруке,
- изабрана порука (енг. *chosen-message attack*) – позната је порука и стеганографски алгоритам кориштен за креирање стеганографске датотеке која ће се користити за будућу анализу и упоређивање,
- познати носилац и стеганографска техника (енг. *known-steganography attack*) – расположива је стеганографска датотека, стеганографски носилац, као и алгоритам кориштен за уметање тајне поруке. Сврха овог напада јесте утврђивање одговарајућих узорака у стеганографској датотеци који могу указати на кориштење одређеног стеганографског алгоритма.

6. АЛАТИ ЗА СТЕГОАНАЛИЗУ

Постоје многи алати који нуде могућност стегоанализе. У овом одјељку дат је примјер једног алата који се користи у те сврхе, а то је Gargoyle.

6.1 Gargoyle

Gargoyle је програм развијен од стране *WetStone technologies* 2004. године (раније *StegoDetect*), који се може користити за детекцију присуства стеганографских садржаја. Овај алат користи заштићени скуп података свих датотека из познатих стеганографских алата, упоређујући их са помијешаним датотекама предмета који се истражује. *Gargoyle* скуп података може бити кориштен и за детекцију присуства криптографије, хитних порука, кључа за записивање у оперативни регистар, тројанских коња и других злонамјерних софтвера. Изглед алата Gargoyle приказан је на слици 6.



Слика 6. *Изглед алата Gargoyle [3]*

7. ЗАКЉУЧАК

Иако се стеганографски алати могу користити за легитимне примене као што је заштита тајности пословних или приватних информација, постали су предмет интересовања форензичких истраживача који се баве њиховом злонамјерном и незаконитом употребом. Како поменути алати постају све доступнији и лакши за употребу, заштита од злонамјерне употребе захтијева све већу пажњу. Такође, равнотежа између заштите од незаконите употребе и мијешање у легитимну употребу појављују се као нови изазов.

8. ЛИТЕРАТУРА

[1] Sadhana Rathore, "Steganography: Basics and digital forensics", *International Journal of Science, Engineering and Technology Research (IJSETR),* Volume 4, Issue 7

[2] XiaoSteganography (https://xiao-steganography.en.softonic.com/)

[3] Gargoyle (https://www.wetstonetech.com/products/gargoyle-malware-detection-dfir/)

Кратка биографија:

Елена Кевац рођена је 10.05.1994. године у Бањалуци. Мастер рад на Факултету техничких наука из области Рачунарство и аутоматика – Софтверско инжењерство одбранила је 2021.год. контакт: elenakevac@gmail.com