Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 004.738.1:766
DOI: https://doi.org/10.24867/20BE32Turkovic

ИМПЛЕМЕНТАЦИЈА СТЕГАНОГРАФСКОГ СИСТЕМА УПОТРЕБОМ ТЕХНИКЕ СУПСТИТУЦИЈЕ БИТА НАЈМАЊЕ ВАЖНОСТИ

IMPLEMENTATION OF A STEGANOGRAPHICS SYSTEM USING THE LEAST SIGNIFICANT BIT SUBSTITUTION TECHNIQUE

Емина Турковић, *Факултет техничких наука, Нови Сад*

Област – ЕЛЕКТРОТЕХНИКА И РАЧУНАРСТВО

Кратак садржај – *Појам „стеганографија“ обично се везе за скривање или прикривање података и информација. У првом делу рада описан је историјски развој стеганографије, њени основни појмови и њена примена. Затим је извршена класификација стеганографије на основу техника коришћених за скривање података, на техничку, лингвистичку и дигиталну стеганографију. Акценат је стављен на подврсту дигиталне стеганографије чији носилац је слика – сликовну стеганографију. Детаљно је описана њена LSB метода, коришћена за имплементацију система који је израђен у оквиру овог рада. Приказани су дизајн и имплементација стеганографске апликације која имплементира LSB методу. Коначно, имплементирани систем је демонстран помоћу низа слика графичког корисничког интерфејса.*

Кључне речи: *стеганографија, LSB метода, сликовна стеганографија, стеганографски медијум*

Abstract – *The term "steganography" is usually associated to hiding or covering data and information. The first part of the paper describes the historical development of steganography, its basic concepts and its use. Steganography was then classified based on the techniques used to hide data, into technical, linguistic and digital steganography. Emphasis is placed on a subtype of digital steganography whose carrier is an image – image steganography. Its LSB method, used to implement the system presented in this paper, is described in detail. This paper also presents the design and implementation of steganographic application that implements the LSB method. Finally, the implemented system is demonstrated using a series of graphical user interface (GUI) images.*

Keywords: *steganography, LSB method, image steganography, steganographic medium*

1. УВОД

Развој информационо-комуникационих технологија наметнуо је ширу употребу рачунара у скоро свим сферама друштвеног живота. У оваквим условима, појавио се проблем сигурности информационих система, јер се информације преносе путем различитих несигурних канала и малициозни корисници врло лако могу доћи у њихов посед. Криптографија је креирана као техника за обезбеђивање тајности комуникације и развијено је много различитих метода за шифровање и дешифровање података како би се поруке одржале у тајности. Нажалост, понекад није довољно чувати само садржај поруке у тајности, већ може бити потребно и да чињеница да порука постоји – буде сакривена. Техника која имплементира ову „невидљиву“ комуникацију назива се стеганографија.

У стеганографији, могући носиоци скривених информација делују наивно (слике, аудио, видео, текст или нека друга информација у дигиталном облику). Порука је сакривена информација која може бити обичан текст, шифровани текст, слика, или било шта што се може уградити у ток битова (енг. *bit stream*). Носилац поруке заједно са поруком креира стего-носиоца. За скривање информација може бити потребан и стего кључ који је додатна тајна информација, као што је лозинка, која је неопходна за уграђивање поруке. Постоје разне стеганографске технике које ће у наставку бити описане, са акцентом на LSB (енг. *least significant bit*) методу, која је коришћена за имплементирање апликације која подржава стеганографско сакривање и детектовање порука, а која је израђена уз обрађивану тему.

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

2. СТЕГАНОГРАФИЈА

У овом одељку су описани појам, начин функционисања, примена и могуће злоупотребе стеганографије. Стеганографија је научна дисциплина која се бави прикривеном разменом информација. Појам стеганографија (енг. *steganography*) долази од грчких речи „*steganos*“ – прикривено и „*grafia*“ – писање, што би у буквалном преводу значило „скривено писање“ [1]. Њен основни принцип почива на прикривању самог постојања информације која се преноси унутар неког наизглед безазленог медијума или скупа података.

2.1. Основни стеганографски појмови

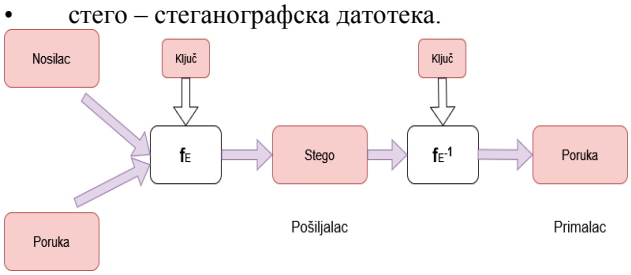
Процес стеганографије укључује уметање тајне поруке унутар неког преносног медијума који се у том случају назива носилац и има улогу прикривања постојања тајне поруке. Носилац мора бити скуп података који је саставни део уобичајене свакодневне комуникације, те као такав не би требало да привлачи посебну пажњу. Целина сачињена од тајне поруке и носиоца унутар којег је та порука уметнута, назива се

стеганографски медијум или стего. У сврху додатне заштите, могућа је и употреба стеганографског кључа којим се тајна порука криптује пре уметања у носиоца. Стеганографски медијум се стога може приказати у следећем облику:

стеганографски_медијум = тајна_порука + носилац + стеганографски_кључ

На слици 1 приказан је начин функционисања стеганографског система, којег чине:

- f_E – стеганографска функција (функција уметања),
- f_E^{-1} – инверзна стеганографска функција (функција издвајања),
- носилац – медиј унутар кога се скрива тајна порука,
- порука – тајна порука која треба да буде сакривена,
- кључ – стеганографски кључ; параметар функције f_E,
- стего – стеганографска датотека.



Слика 1. *Стеганографски систем*

2.2. Примена стеганографије

Као и многе друге сигурносне методе и алати, стеганографија се може користити у различитим подручјима и активностима, како легалним тако и илегалним. Легалну примену највећим делом сачињава коришћење дигиталног воденог печата у сврху заштите ауторских права и власништва над мултимедијалним датотекама. Стеганографија се такође користи као замена за генерисање једносмерне хеш (енг. *hash*) вредности. На тај начин се након обраде промењиве величине информација као резултат добија излазни скуп података фиксне величине, на основу којег се потом може утврдити постојање било каквих додатних измена над изворним скупом података. Такође, стеганографијом је могуће додати различите белешке мултимедијалним датотекама тако да се њихов формат не мења, чиме се не ствара потреба за коришћењем специјализованих програма за њихово манипулисање. Напослетку, далеко најлогичнија примена стеганографије је управо очување поверљивости и тајности важних информација, те њихова заштита од потенцијалне саботаже, крађе или неовлашћеног приступа.

Због своје посебности као средства тајне комуникације, стеганографија често налази примену и у илегалним активностима, пошто омогућава скривање доказа о таквим активностима. Илегална примена стеганографских техника најчешће се везује уз крађу поверљивих информација (на пример у индустрији и пословном сектору), финансијску проневеру, размену дечије порнографије, крађу идентитета, коцкање, кријумчарење, хаковање и тероризам.

3. ТЕХНИКЕ СТЕГАНОГРАФИЈЕ

У овом одељку је описана подела стеганографије, као и карактеристике различитих стеганографских метода у односу на тип носиоца поруке, с нагласком на сликовну стеганографију, због тога што је она коришћена приликом имплементације стеганографског система израђеног у оквиру овог рада. С развојем дигиталне технологије и све већом количином података који се похрањују на рачунарима и размењују преко рачунарских мрежа, стеганографија је такође ушла у ново доба.

Развијен је велики број различитих стеганографских алата који омогућавају скривање било какве бинарне датотеке унутар друге бинарне датотеке. С обзиром на коришћене технике скривања података, постоје три основна типа стеганографије: техничка, лингвистичка и дигитална стеганографија.

3.1. Техничка стеганографија

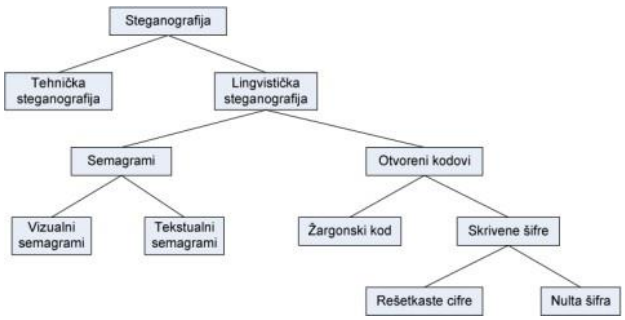
Техничка стеганографија (енг. *technical steganography)* обухвата научне методе које тајну поруку скривају коришћењем алата, уређаја или хемикалија. Верује се да се ова стеганографија први пут практиковала током Златног доба у Грчкој. Древни грчки записи описују праксу топљења воштаних плоча (комади дрвета преливени воском) које су се користиле за писање порука, а затим уписивање поруке у дрво испод плоче. Наиме, да би пренели поруку, Грци би одстранили восак са плочице, написали поруку директно на дрво те поново нанели восак на плочицу. Таква воштана плоча се чинила празном и неупотребљеном, те је одлично служила за скривено слање порука [2].

Невидљиво мастило је још једна од техника коришћена за уметање и пренос скривених порука, која датира још из раздобља Другог светског рата, али с једнаким учинком може се употребити и дан данас. Наиме, у наизглед безазлено писмо уметала се тајна порука – испод видљивог текста, између редова или на неким другим празним површинама папира.

Мастило којом је тајна порука била написана правило се од млека, воћних сокова или урина. Све наведене супстанце имале су исти ефекат приликом загревања – тамњење. Услед развоја технологије и све чешћих појава разоткривања порука писаних невидљивим мастилом, осмишљене су софистицираније супстанце која постају видљиве тек након реаговања на различите хемијске састојке.

3.2. Лингвистичка стеганографија

Лингвистичка стеганографија (енг. *linguistic steganography)* користи методе скривања тајне поруке у неважне информације. Информације су језичког садржаја. Дели се у две групе: семаграми и отворени кодови. На слици 2 приказана је таксономија стеганографских техника.



Слика 2. *Преглед стеганографских техника*

3.3. Дигитална стеганографија

Дигитална стеганографија (енг. *digital steganography*) представља скривање порука кроз битове, у дигиталним медијима (слици, аудио или видео запису).

Стеганографија се данас све више користи у мултимедијалним датотекама како би се пренео тајни садржај. У највећем броју случајева слике се користе као могући медијуми за пренос уграђеног тајног садржаја. У дигиталном свету боје се приказују као комбинације црвене, плаве и зелене вредности – RGB боје (енг. *red-green-blue*). Унутар RGB система, свака боја се приказује помоћу релативног интензитета сваке од 3 постојеће компоненте – црвене, зелене и плаве. Недостатак свих компоненти резултира појавом црне, док присуство свих компоненти резултира добијањем беле боје. Свака RGB компонента специфицирана је једним октетом, тј. низом од 8 битова, тако да вредност интензитета сваке од три боје може варирати од 0 до 255. Пошто RGB систем садржи 3 компоненте, дотичном методом презентације, добија се 24-битна шема која подржава 16,777,216 јединствених боја. То значи да је сваки пиксел унутар слике кодиран с 24 бита.

3.3.1. Сликовна стеганографија

Слике данас представљају најраспрострањенији медиј стеганографског преноса информација. Да бисмо сакрили поруку унутар слике без промене њених видљивих својстава, носилац тајне поруке се може променити у својим „бучним“ деловима који садрже много варијација боја, тако да би његове модификације привукле минимално пажње. Најчешћи методи за прављење ових измена укључују коришћење супституције бита најмањег значаја или LSB-а, сортирање палета, маскирање, филтрирање и трансформације на насловној слици. Ове технике се могу користити са различитим степеном успеха на различитим типовима сликовних датотека и неке од њих биће детаљније описане у наставку.

3.3.1.1. Супституција бита најмање важности (LSB)

Супституција бита најмање важности (енг. *LeastSignificant Bit Substitution; LSB Substitution*) најчешћа је стеганографска техника коришћена у раду с мултимедијалним датотекама. Појам „бит најмање важности“ везан је за нумеричку важност битова у октету. Стога промена бита најмање важности има најмањи учинак на промену укупне вредности октета, а промена бита најмање важности у свим октетима који сачињавају мултимедијалну датотеку има најмањи учинак на промену изгледа саме датотеке. Описани принцип још је делотворнији због чињенице да човеков оптички систем није довољно осетљив за детектовање таквих промена у боји. Идеја стеганографске технике супституције бита најмање важности базира се на растављању тајне поруке на битове, који се потом похрањују на место бита најмање важности у одабраним октетима. Као једноставан пример LSB супституције приказано је скривање слова 'G' унутар следећег низа октета:

10010101 00001101 11001001 10010110

00001111 11001011 10011111 00010000

Слово 'G' се према ASCII (енг. *American Standard Code for Information Interchange*) стандарду записује као бинарни низ 01000111. Ових 8 битова записује се на место битова најмање важности у изворном скупу октета:

1001010<u>0</u> 0000110<u>1</u> 1100100<u>0</u> 1001011<u>0</u>

0000111<u>0</u> 1100101<u>1</u> 1001111<u>1</u> 0001000<u>1</u>

LSB супституција је једноставна стеганографска техника, али њена примена често и није тако једноставна. Наиме, ако се скуп октета у које се умеће по бит тајне поруке одабере на једноставан начин, нпр. низ суседних октета на почетку датотеке, врло је вероватно да ће тај део слике имати другачије статистичке карактеристике од остатка слике, те ће као такав привући пажњу на себе и компромитовати тајност скривене поруке.

Стога се скуп циљних октета најчешће дефинише неком методом насумичног одабира, што је један од фактора који детекцију стеганографских порука чине изразито компликованом [3]. Нажалост, LSB супституција осетљива је и на најмање операције над сликом, као што су компресија или уклањање неких делова слике. На пример, конвертовање GIF или BMP стеганографске датотеке у JPEG формат, те конвертовање назад у изворни формат може довести до уништавања информација садржаних у битовима најмање важности.

4. СТЕГОАНАЛИЗА

За стегоанализу се може рећи да је она за стеганографију оно што је криптоанализа за криптографију [4]. ИТ стручњаци задужени за сигурност је зову и „контрамера стеганографији” или „напад на стеганографију”. Наука која се бави откривањем стеганографски скривених порука назива се стегоанализа (енг. *steganalysis*). Ова вештина темељи се на проучавању варијација у шаблонима битова и необично великим датотекама. Циљевистегоанализе су:

- Идентификовање сумњивих скупова података, као што су сигнали или датотеке, унутар којих се потенцијално налази скривена тајна порука.
- Утврђивање да ли су тајни подаци уметнути у стеганографску датотеку претходно криптовани.

• Утврђивање постојања шума или небитних података унутар сумњивог сигнала или датотеке.

• Издвајање и декриптовање уметнуте поруке из стеганографске датотеке.

5. СПЕЦИФИКАЦИЈА ЗАХТЕВА И ДИЗАЈНА

Апликација израђена уз обрађивану тему подржава следеће функционалне захтеве:

• Стеганографско уметање тајне поруке унутар неког преносног медијума (слике) применом одабраног алгоритма.

• Утврђивање да ли су тајни подаци уметнути у стеганографску датотеку.

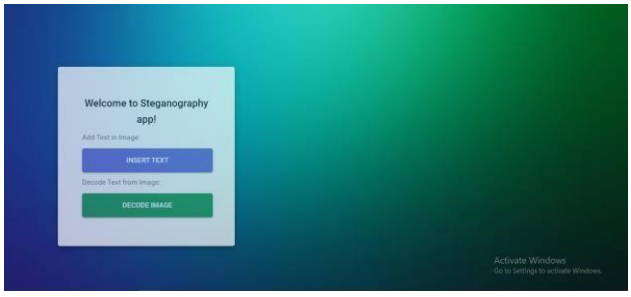
• Издвајање уметнуте поруке из стеганографске датотеке (уколико се претходно утврди да њена присутност).

6. ИМПЛЕМЕНТАЦИЈА

Након стицања доменског знања, одлучено је да се акценат стави на сликовну стеганографију, односно да носилац скривених информација буде слика у PNG (енг. *Portable Network Graphics*) формату, док би саме поруке биле у текстуалном формату. Слике данас представљају најраспрострањенији медијум стеганографског преноса информација, због чега су оне и одабране као средство за скривање тајних порука. Супституција бита најмање важности је одабрана стеганографска техника за уметање тајне поруке у носиоца.

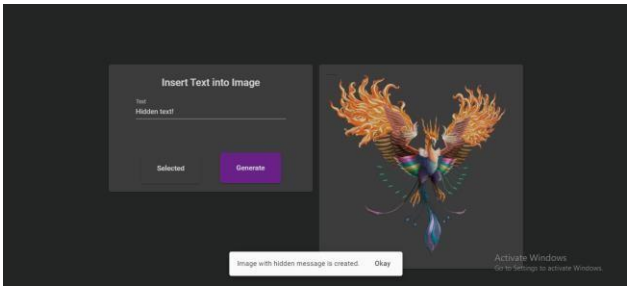
7. ДЕМОНСТРАЦИЈА

Након покретања серверске и клијентске апликације, уношењем адресе *http://localhost:4200* у веб прегледач, стижемо до почетне странице апликације. Изглед почетне странице приказан је на слици 3.



Слика 3. *Почетна страница*

Кликом на дугме *Insert Text* присутпа се форми за стеганографско уметање која се састоји од текстуалног поља које се мора попунити тајном поруком, и од једног дугмета *Pick Data* које служи за уметање слике која ће бити стеганографски носилац информација, у коју ће се у процесу стеганографије уметнути унета тајна порука. Када унесемо све потребне податке, кликом на дугме *Generate* прослеђујемо их серверу, који кориснику враћа стеганографски медијум (стего), који он може скинути на свој локални систем (слика 4).



Слика 4. *Приказ слике која представља стеганографски медијум*

8. ЗАКЉУЧАК

Стеганографија комбинована с криптографијом, представља додатни сигурносни слој у заштити информација. Стеганографска технологија врло је једноставна за употребу, а изразито се тешко детектује. У последњих неколико година, стеганографија је била тема многих дискусија везаних за њену злоупотребу, нарочито у терористичким активностима. С друге стране, постоји велики број предности коришћења стеганографије у легалном контексту, као што су дигитални водени печати за утврђивање власништва и ауторских права или сигурније методе складиштења важних и поверљивих информација, због чега се у будућности очекује још интензивнији развој ове технологије, као и њена широка могућност примене.

9. ЛИТЕРАТУРА

[1] Sara Khosravi, Mashallah Abbasi Dezfoli, Mohammad Hossein Yektaie, *A new steganography method based HIOP (Higher Intensity Of Pixel) algorithm and Strassen's matrix multiplication*, Journal of Global Research in Computer Science, Vol.2, No. 1, 2011.
[2] "Steganografija", 2006. – https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-04-154.pdf [pristupljeno: jul 2022.]
[3] M. Hariri, R. Karimi, M. Nosrati, *An introduction to steganography methods*, World Applied Programming. 2011 Aug.
[4] Stevan Gostojić, „09 Kriptologija" 2022.

Кратка биографија:

Емина Турковић рођена је у Прибоју 1998. год. Дипломирала је 2021. год. на ФТН-у, смер Рачунарство и аутоматика, са темом „Логичко прогамирање у програмском језику Prolog".
контакт: eminaturkovic600@gmail.com