Архитектура рачунара - Предметни пројекат

Програм Стеганограф

Аутор:
Јоаким Јањатовић

Ментор:
Лазар Стричевић

Факултет техничких наука, Нови Сад, мај 2013.

Стеганографија

Стеганографија је наука о писању сакривених порука на такав начин да нико осим онога ко шаље и онога коме је порука намењена не посумња да порука уопште постоји. Реч стеганографија потиче из грчког језика и значи прикривено писање.

Предност стеганографије у односу на криптографију је што сакривене поруке не привлаче додатну пажњу. Наравно, најбоља би била комбинација стеганографије и криптографије јер би порука тако имала двоструку заштиту.

Један од најстаријих примера забележио је Херодот. Порука о персијским плановима за инвазију на Грчку истетовирана је на обријаној глави роба. Порука је сакривена косом која је касније израсла, а откривена поновним бријањем. Овај начин преношења поруке има очигледне недостатке као што су дугачко време потребно да коса поново израсте, време потребно за човеково путовање и мала дужина поруке.

Основни елементи у стеганографији су носач поруке, сама порука и пакет који се добија сакривањем поруке на носачу.

Замисао

Програм Стеганограф замишљен је као примена стеганографије на дигиталне слике, текст и остале податке. Свака слика састоји се од мноштва обојених тачака односно пиксела који су распоређени у одређеном редоследу. Свака од тих тачака на рачунару је представљена као низ осмоцифрених бинарних бројева односно бајтова. У зависности од формата записа једна тачка може бити представљена различитим бројем бајтова. У овом примеру, биће представљено решење са три броја, односно три боје, црвеном, зеленом и плавом. Дакле, слика је представљена као низ тачака које су разложене на три боје.

С обзиром да осмобитни бинарни број може да има 256 различитих вредности, од 0 до 255, свака од тачака може да буде у једној од 256*256*256=16777216 различитих боја. Овај програм је заснован на томе да људско око не може да препозна разлику између две веома сличне боје, односно да ако боју тачке незнатно променимо, слика ће и даље изгледати исто.

Ако је једна од боја неке тачке представљена бројем 255 (11111111), променом вредности на 254 (11111110) нећемо значајно променити боју, и то је управо оно што ћемо да искористимо.

Податак који се састоји од низа знакова који су представљени са по једним бајтом сакрићемо у слици тако што ћемо најмање значајан бит сваке боје сваке тачке у слици заменити редом са по једним битом (1/8) сваког бајта податка. Укупан број бајтова (слова) који може на тај начин да се сакрије је ((број тачака)*3)/8. Резултат оваквог сакривања је слика која изгледа исто као и почетна, исте је величине као и почетна, а садржи сакривени податак.

Могуће је додатно отежати откривање податка распоређивањем бајтова који се сакривају на несуседне бајтове у одређеном правилном редоследу који зависи од тајне речи коју треба да знају онај ко шаље и онај ко прима поруку. Капацитет слике може се повећати коришћењем два најмање значајна бита, односно променом боје за највише 3 (11) вредности.

Ако желимо да сакријемо број 4 (100) у низу 255,255,255 (11111111,11111111,11111111) променићемо вредности низа на 255,254,254 (11111111,11111110,11111110), а откривање се врши издвајањем последњег бита сваког бајта низа и њиховом поновном комбинацијом. У овом случају, слику у којој је већ сакривен неки податак (текст), није могуће вратити у облик од пре сакривања текста.

Реализација

Стеганограф је написан у програмском језику `C` уз коришћење библиотеке `FreeImage` , доступне на: http://freeimage.sourceforge.net/.

Основне могућности програма су учитавање слике, сакривање неког податка у слици по моделу најмање значајног бита, снимање добијеног пакета и обрнуто, откривање.
С обзиром да нема значајне разлике између текста и неког другог податка (оба су само битови у меморији), овај програм може да сакрије и открије било који тип податка у слици.

Када се покрене са задатим параметрима улазне слике и улазног податка, програм проверава да ли је слика довољно велика да се у њој смести цео податак. Затим величину податка (тридесетдвобитни цео број) сакрива у прва 32 бајта доступног простора слике, а затим сакрива и податак. Добијени пакет снима се као нова слика са тешко уочљивим разликама у односу на стару.

Супротни поступак је отварање слике, читање садржаја последњих битова прва 32 бајта који се тумаче као дужина сакривеног податка. Одатле се учитава податак претходно одређене дужине и снима у нову датотеку.

Корисник није обавезан да дефинише улазну и излазну датотеку. У том случају подразумеван је унос текста преко тастатуре директно у терминал односно испис сакривеног садржаја на екрану.

Теоретски овај програм може да сакрије било који податак, било које величине у слику (под условом да је она довољно велика). Практично ограничење је расположива радна меморија на рачунару, односно успешност операције `malloc`.

Подржани формати слика

Библиотека која је коришћена за учитавање и снимање слика пружа подршку за руковање са `BMP`, `PNG`, и `TIFF` сликама без губитака података приликом компресије. Излазни пакет програм снима у истом формату у којем је и улазна слика. Формат `JPEG` са овом библиотеком није могуће учитати и снимити а да се при томе не губи на квалитету слике односно сакривеним подацима. Због тога овај програм `JPEG` слике може само да учитава, а излазни пакет снима у `PNG` формату.

Компајлирање

Овај програм захтева претходну инсталацију `FreeImage` библиотеке. На Убунту систему то је могуће учинити извршавањем следеће команде у терминалу:

```
sudo apt-get install libfreeimage-dev
```

Затим, потребно је у терминалу прећи у директоријум са Стеганографом и извршити команду `make`. Компајлирани програм могуће је уклонити командом `make clean`. Опција за дебаговање је `make debug`. За компајлирање су неопходне датотеке: `Makefile` и `seganograf.c`

Употреба

Упутство за покретање програма:

`./steganograf [OPCIJA]... [DATOTEKA]...`

Основне опције:

`-w ime_slike`	за сакривање података (слика која се учитава)
`-r ime_slike`	за откривање података (пакет који се учитава)
`-v`	верзија, лиценца
`-h`	упутство

Додатне опције:

`-f ulazno/izlazna_datoteka`	задавање улазне односно излазне датотеке
`-o izlazna_slika`	задавање назива излазне слике

Ако опција `-f` није наведена, подразумевани су улаз са екрана и излаз на екран (`stdin/stdout`). Подразумевано име излазне слике је `izlaz` са одговарајућом екстензијом.

Примери:

`./steganograf -w bmp_24.bmp -f ulaz.txt -o izlaz.bmp`

Учитава слику `bmp_24.bmp`, у њу сакрива податак из `ulaz.txt` и снима га у `izlaz.bmp`

`./steganograf -r izlaz.bmp -f izlaz.txt`

Учитава слику `izlaz.bmp`, у њој открива податак и снима га у `izlaz.txt`

Садржај `Steganograf_v0.5.tar.gz`

Директоријум `Steganograf_v0.5` са следећим датотекама:

`bmp_24.bmp`

`LICENCE.txt`

`Makefile`

`README.txt`

`steganograf.c`

`Steganograf.pdf`

Лиценца