

ANALIZA STEGANOGRAFSKIH TEHNIKA I METODA

Miroslav Čajić¹, Mladen Veinović², Bogdan Brkić³

Sadržaj — U ovom radu izvršena je analiza aktuelnih steganografskih tehnika i metoda, i ukazano je na prednosti i nedostatke postojećih tehnika koje se koriste u steganografiji. Kao primjeri za datoteke sa slikama upotrebljen je JPEG, a za audio datoteke MP3 format. Primjenom određenih steganografskih tehnika na originalnu datoteku dobija se steganografski obrađen nosač podataka koji se naziva stego-datoteka. U zavisnosti od količine utisnutog otvorenog teksta u određenoj stego-datoteci moguće su određene varijacije koje se manifestuju kroz razlike u veličini i kvalitetu u odnosu na originalnu datoteku. Tehnike koje se koriste su: ubacivanje, zamjena i generisanje.

Ključne riječi — steganografija, steganoanaliza, stego-datoteka, kapacitet, bit, piksel.

1. UVOD

SKRIVANJE podataka iz bezbjedonosnih razloga danas je uobičajena pojava u svim organizacijama čije se poslovanje bazira na zaštićenom prenosu podataka. Skrivenje informaciju znači ne dozvoliti da informacija bude čitljiva trećim licima. Poslovni sistemi koji funkcionišu preko računarske mreže povećavaju međuzavisnost između informacija i komunikacionog kanala, te na taj način postaju meta mnogih zlonamjernih korisnika. To svakako dovodi do potrebe zaštite podataka u poslovnom okruženju. Za rješenje problema, pored primjene određenih kriptografskih algoritama kao što su RSA, DES, AES i sl., moguća je i upotreba steganografskih metoda koje omogućavaju prikrivanje podataka iza bezazlenih objekata u slikama, audio, video snimcima, ali na taj način da originalni nosilac podatka ostane vjerodostojan. U današnjem poslovanju postoji povećana zabrinutost zbog velikog broja zloupotrebe računarskih sistema, pa je zbog toga upotreba kriptološke zaštite u stalnom porastu. Na žalost, većina kriptoloških tehnika postale su ranjive na napade koji se izvode od strane hakera. To se takođe odnosi i na napredne šifarske metode. Cilj svake kripto-metode je da pronađe najbrži i najpovoljniji način da prenesena informacija bude sačuvana. Jedna od takvih metoda koje se danas koriste zasniva se na upotrebi steganografije.

Steganografija je nauka koja se bavi sakrivanjem informacija u drugim podacima, tako da je i samo postojanje šifrata sakriveno u nosiocu podatka. Riječ steganografija je kovanica od dvije riječi grčkog porijekla, *στεγανος* (steganos) i *γραφo* (grafo), što u prevodu znači pisati skriveno. Cilj steganografije je da prenese informacije od pošiljaoca do primaoca tako što se podatak utisne u nosioca podatka, koji mora da bude čitljiv i razumljiv za odredište.

Za razliku od kriptografije gdje je neprijatelju omogućeno da presretne poruku, da je pokuša promijeniti, odnosno, narušiti njen integritet, steganografija je nauka i umjetnost razmjene osjetljivih ili privatnih podataka koja skriva postojanje komunikacije. Čak, iako neprijatelj prepozna da se prenosi neka informacija, cilj je da se steganografska poruka sakrije

¹Miroslav Čajić dipl.ing.inf.-master, MikroByte doo, Vesa Rackovića 16, 73220 Rogatica, tel.: +387 65/631-675, fax: 387 58/417-517, e-mail: miroslavcagic@gmail.com

²prof. dr Mladen Veinović, Univerzitet Singidunum, Bulevar Zorana Đinđića 44, Novi Beograd, Tel: +381 11/31-21-349, e-mail: mveinovic@singidunum.ac.rs

³Bogdan Brkić dipl.ing.inf.-master, Ministarstvo finansija Republike Srpske, Kralja Petra I Karađorđevića, 78000 Banja Luka, tel.: +387 65/567-941, e-mail: bbogdan@teol.net

unutar drugih poruka na način koji ne dozvoljava neprijatelju prepoznavanje postojanja tajne poruke. Steganografija se često miješa s tajnom, jer se oba dva termina koriste za zaštitu važnih informacija. Jedina razlika između njih je to što steganografija uključuje skrivanje informacija. Ako objekat u kom je poruka skrivena bude presretnut, na osnovu vizuelnog pregleda nije moguće da se uoče razlike koje ukazuju na prisustvo steganografije.

2. STEGANOGRAFSKE TEHNIKE

Sa gledišta nauke, steganografija se može podijeliti na tehničku i lingvističku. Tehnička se bavi metodama za otkrivanje steganografskog uzorka u pisanom tekstu ili mikrofilmovima, dok lingvistička steganografija obuhvata tehnike skrivanja podatka u datoteci na način da originalna datoteka bude vjerodostojna stego-datoteci. Lingvistička steganografija se može podijeliti na semagrame i otvorene kodove.

Semagrami se baziraju se na upotrebi simbola i znakova za skrivanje poruka, a mogu biti vizuelni i tekstualni. Vizuelni semagrami za generisanje skrivene poruke koriste svakodnevni raspored predmeta i objekata u prostoru, dok tekstualni za skrivanje koriste različite modifikacije teksta na nosiocu podataka. To može biti suvišan razmak između riječi, promjena veličine i boje fonta i sl.

Otvoreni kodovi koriste razne načine prenosa skrivene poruke. Dije se na žargonski kod i skrivene šifre. Žargonski kod koristi predefinisane fraze pri komunikaciji koje su poznate samo osobama koje komuniciraju. To mogu biti unaprijed dogovoreni pojmovi i sl.

Skrivene šifre predstavljaju steganografsku tehniku kod koje se skrivena poruka može izdvojiti iz stego-datoteke samo u slučaju ako je poznata metoda kojom je skrivena informacija utisnuta u datoteku. Skrivene šifre se dijele na rešetkaste i na nulte kodove.

Princip rada rešetkastih šifara bazira se na šablonima koji se koriste za skrivanje poruke u nosiocu, dok se metoda nultog koda bazira na usvajanju određenog pravila za umetanje podataka u nosiocu podataka. To može biti izuzimanje svakog neparnog reda ili svake parne riječi u redu i sl.

U steganografiji postoji nekoliko različitih tehnika koje se mogu koristiti za skrivanje informacija u datotekama. To su:

- Ubacivanje (*Injection* ili *Insertion*)
- Zamjena (Substitucija) i
- Generisanje (*Generation*)

2.1. UBACIVANJE

Ova tehnika omogućava skrivanje postojanja podataka u dijelovima datoteka koji su od manjeg značaja za zlonamjernog korisnika. Tehnika se bazira na dodavanju bitova u datoteke tako da površinski dio datoteke ostane savršeno čist. Dodavanjem određenog broja dodatnih bezopasnih bitova u izvršnu datoteku neće bitno uticati na proces koji se izvršava, a prisustvo metode neće se odraziti na konačan ishod metode, tako da krajnji korisnik ne može osjetiti prisustvo skrivenog podatka u datoteci. Međutim, upotreba tehnike umetanja mijenja veličinu datoteke u zavisnosti od ukupnog broja utisnutih bitova, što može dovesti da neuobičajeno velika datoteka izazove određenu pažnju kod zlonamjernog korisnika.

2.2. ZAMJENA

Pristup zamjene zasniva se na zamjeni najmanje značajnih bitova datoteke, i to na takav način da primjena ove metode ima što manji efekat na izobličenje originalne datoteke. Glavna prednost ove tehnike je u tome što se veličina datoteke ne mijenja prilikom primjene kriptografskog algoritma. S druge strane, ova metoda ima i dva nedostatka. Prvi je degradacija steganografski obrađene datoteke i ograničenje broja manje značajnih bitova koji se mogu upotrijebiti za primjenu ove metode.

2.3. GENERISANJE

Nedostatak kod prethodno pomenute dvije tehnike ubacivanja i zamjene je taj što se originalna slika može porediti sa stego slikom i tom prilikom moguće je otkriti razlike. Tehnika generisanja ne zahtijeva originalnog nosioca podataka, već sama generiše datoteku u kojoj će biti sadržana poruka. Kada se koristi tehnika generisanja konačan rezultat je originalna datoteka koja je imuna na komparaciju sa drugim datotekama.

3. STEGANOGRAFSKE METODE

U suštini, steganografija koristi ograničene sposobnosti našeg vizuelnog sistema. Bilo koji otvoreni ili šifrovani tekst, slika i sl., korišćenjem određenih metoda može biti utisnut u određenu sliku nosioca podataka, a da to ne bude vidljivo prostim okom. Postoji više metoda koje se koriste za skrivanje informacija unutar teksta, slike, audio ili video datoteke. Neke od metoda koje se koriste u steganografiji su:

- HTML stego
- LSB (least significant bit)
- SS (Spread Spectrum)
- DCT (Diskretna Kosinusna Transformacija) i
- WS (White Space) metoda

3.1. HTML STEGO METODA

Ova metoda koristi tehniku zamjene. Bazira se na skrivanju informacija u izvornom HTML kôdu tako da podaci koji se prezentuju korisniku ostaju nepromijenjeni. Tehnika se zasniva na zamjeni bitova manje važnih identifikatora decimalnog oblika koji se odnosi na boju teksta sa njihovim ekvivalentima u tekstualnom obliku. Sledeći primjer pokazuje kako se steganografija koristi prilikom pisanja HTML koda.

Dat je izvorni tekst:

*Your quest objective is Erratic Sentries,
which roam the northeast section of the Isle. font>
After you have killed them,
use the provided Attuned Crystal Cores.
This will reactive the Arcane Sentries
to turn them into friendly units.*

Izvorni kôd u HTML jeziku bi bio sledeći:

```
<font color="#01001100">Your quest objective is Erratic Sentries,</font><br>  
<font color="#01000000">which roam the northeast section of the Isle. font><br>  
<font color="#01010010">After you have killed them,</font><br>  
<font color="#01000001">use the provided Attuned Crystal Cores.</font><br>  
<font color="#01000110">This will reactive the Arcane Sentries</font><br>
```

Steganografski obrađen kôd bi bio ovakav:

```
<font color="#01001110">Your quest objective is Erratic Sentries,</font><br>
<font color="#01000001">which roam the northeast section of the Isle.</font><br>
<font color="#01010000">After you have killed them,</font><br>
<font color="#01000001">use the provided Attuned Crystal Cores.</font><br>
<font color="#01000100">This will reactive the Arcane Sentries</font><br>
```

Skrivena poruka glasi: 01001110 01000001 01010000 01000001 01000100, što u prevodu znači: NAPAD.

HTML metoda se najviše koristi za obmanu računara koji u potrazi za informacijama pretražuju Internet.

3.2. LSB METODA

LSB (*Least Significant Byte*), ili bit najmanje težine, je metoda koja koristi tehniku zamjene vrijednosti najmanje značajnih piksela u binarnom obliku. U datoteci se obično nalazi nekoliko bitova koji nisu stvarno potrebni, ili na određeni način nisu toliko važni. Ti bitovi u datotekama mogu poslužiti za prenos skrivenih informacija na taj način da neće bitno mijenjati datoteku ili je oštetiti. LSB metoda najbolju primjenu je našla u slikovnim datotekama koje imaju visoku rezoluciju uz upotrebu različitih boja, i u audio datotekama koje reprodukuju različite zvukove na velikim brzinama. LSB metoda obično ne povećava veličinu datoteke, ali zavisno od veličine informacije koja se skriva, može primjetno deformisati datoteku.

Za skrivanje informacija u slikama upotrebom LSB metode najčešće se koriste 24-bitne BMP slike. Slika treba da bude različitih boja i inteziteta svjetlosti na različitim djelovima. Razlog tome je što je u sliku visokog kvaliteta i rezolucije mnogo lakše sakriti informacije nego u sliku niskog kvaliteta. Iako je 24 bitna slika najbolja za skrivanje informacija, zbog svoje veličine i česte primjene može se za upotrebu uzeti i 8-bitna BMP slika ili eventualno drugi format slike, kao što je GIF. Razlog tome je što postavljanje slika velikih formata na Internetu može probuditi sumnju potencijalnih napadača i samim tim ugroziti komunikaciju. Važno je napomenuti, da će skrivena informacija unutar slike biti izgubljena ako se izvrši konverzija slike iz jednog formata u drugi.

Ako je slika veličine $3264 \times 1840 = 6.005.760$ piksela, i ako se uzme u obzir da se za svaki kanal uzima po jedan bajt, a u ovom slučaju se koriste R, G i B kanali, onda je za skladištenje 6.005.760 piksela potrebno 18017280 bajtova, odnosno 144138240 bitova. Upotrebom svakog osmog bajta za skrivanje sadržaja dokumenta koji se utiskuje u nosioca podataka dobija se rezultat do 2252160 bajtova, odnosno 2,14 MB prostora za skrivanje podataka. Ako se pomoću ove računice uzme slika iz primjera čija stvarna veličina iznosi 5.454.969 bitova, odnosno, 5.20 MB, dolazimo do zaključka da je koeficijent iskorišćenja slike 41 %, tj., $2.252.160 / 5.454.969 = 0.412863$.



Slika br. 1. Originalna i steganografski obrađena slika

3.3. SPREAD SPECTRUM METODA

Ova metoda koristi tehniku ubacivanja a zasniva se na širenju frekvencijskog spektra signala u određenom domenu. Koristi slabosti koje imaju ljudski organi čula. Takođe, koristi se i za kontrolu bezbjednosti komunikacionog kanala, povećanje otpornosti na prirodne smetnje, sprečavanje otkrivanja i za ograničenje snage određenih prenosnih linkova. U audio steganografiji implementacija je moguća pažljivim biranjem audio sadržaja u koji se utiskuju podaci. Trenutne steganografske aplikacije koje koriste ovu metodu su prije svega ograničene na potvrdu dokaza o autorskim pravima, kao i garancijama integriteta sadržaja. Ova metoda se koristi i u audio steganografiji i to za WAV i AIFF formate koji koriste 16-bitnu linearnu kvantizaciju primjenjenu za distorziju prenosnog signala. Pošto se koristi tehnika zamjene niskih talasa, slično kao kod LSB metode, problem kod ove metode je što su niski talasi uočljivi za ljudsko uho tako da je ovo praktično prilično ranjiva metoda. Ova metoda radi na dodavanju šumovi u slučajne odabrane signale. Informacije se kriju unutar nosača i širi se preko frekvencijskog spektra.

Slična ovoj metodi je i ECHO metoda koja takođe koristi tehniku ubacivanja podataka. Ova metoda za skrivanje informacija koristi odjeke u audio datotekama. Princip rada se zasniva na jednostavnim ubacivanjem dodatnog zvuka jeke unutar audio datoteka u kom je sadržana informacija. Ono što čini ovu metodu izdvaja od ostalih audio-steganografskih metoda je to da se zapravo audio zvuk unutar datoteke može dodatno poboljšati.

3.4. WHITE SPACE METODA

White Space metoda je još jedna steganografska metoda koja se bazira na tehnici ubacivanja. Dodatnim dodavanjem bijelog prostora unutar pisanog teksta na listovima papira jednostavnim pritiskom tastera "*space*" na tastaturi, običnom korisniku vjerovatno neće izazvati pažnju. Prazni prostori su uobičajena pojava u svim dokumentima koji se svakodnevno koriste, pa je primjena ove metode veoma efikasna za većinu tekstualnih datoteka. Ova metoda se može primjenjivati u skoro svim datotekama u kojima je smješten tekst za čitanje: doc, pdf, rtf. Za detekciju *white space* metode koristi se program koji se zove SNOW.

4. DIGITALNI VODENI PEČAT (WATERMARK)

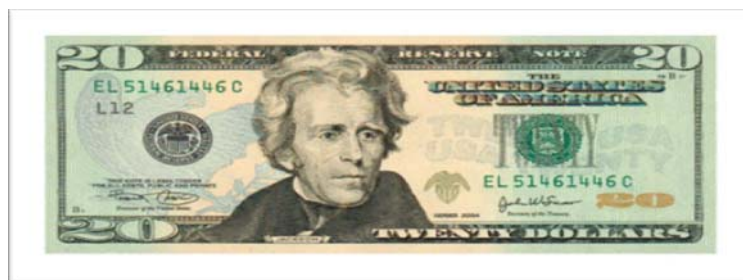
Digitalni vodeni pečat (*wathermark*) predstavlja digitalni identifikator ili digitalni pečat na podatku, koji se koristi zbog autorizacije izvora nosioca podataka. Najčešće se koristi radi odbrane od softverske i muzičke piraterije. Postoji više vrsta *wathermark-a*:

- nevidljivi,
- vidljivi,
- robustni i
- osjetljivi.

Nevidljivi *wathermark* se utiskuje u nosioca podataka tako da on za korisnika nije vidljiv prostim okom. Vidljivi *wathermark* je vidljiv prostim okom i on može da nosi neku konkretnu oznaku kao što je TOP SECRET ili sl. Robustni *wathermark* je čitljiv za korisnika i u slučaju napada ne mijenja svoju strukturu. Osjetljivi *wathermark* je sličan robustnom, samo što kod njega u slučaju napada dolazi do samouništenja samog pečata.

Wathermark se može ugrađivati i u digitalnu sliku. Nevidljivi *wathermark* veličine jednog kvadratnog inča je dovoljan da cijela fotografija dimenzija 1024x768 stane u njega. Prilikom oštećenja, iz neoštećenog dijela fotografije može se izvaditi nevidljivi *wathermark* i na osnovu njega rekonstruisati cijela slika. Naša moneta sadrži zaštitnu nit kao zaštitno sredstvo protiv kopiranja, ali samo U.S. moneta sadrži *wathermark* u obliku slike koji se vidi pod odgovarajućim svjetlom.

Na domaćem tržištu još uvijek je u određenoj mjeri prisutna softverska i muzička piraterija. Internet nudi neiscrpnu bazu nelegalnog digitalnog materijala. Uvođenjem digitalnih vodenih pečata u izvorne nosioce podataka sigurno će se redukovati broj piratskog materijala koji se može naći na crnom tržištu. Utiskivanjem robustnog nevidljivog pečata u digitalnu muziku može se ući u trag originalnom izvoru ako se piratska muzika pojavi na Internetu. Ako je u audio fajl dodat osjetljivi nevidljivi pečat kopiranjem DVD-a pečat se neće kopirati. Kopiranjem se narušava integritet podatka zbog toga što osjetljivi nevidljivi pečat nije kopiran i fajl neće biti čitljiv. Često se primjenjuje kombinacija više pečata, npr. nevidljivi i vidljivi robustni.



Slika br. 2. US moneta sa vidljivim robustnim *wathermarkom*

5. STEGOANALIZA

Umjetnost ili vještina otkrivanja steganografski obrađenih datoteka naziva se stegoanaliza. Cilj svake steganalize je da otkrije mogući umetnuti podatak koji je pomoću određene steganografske tehnike i metode ubačen u nosioca podatka. Postoji više metoda koje se koriste pri stegoanalizi datoteka. Najčešće korišćene su:

- Metoda vizuelnog pregleda,
- Audio-reproduktivna i
- Softverska metoda.

Metoda vizuelnog pregleda se odnosi na slikovne i tekstualne datoteke. Zasniva na pronalaženju istih detalja iz različitih izvora podataka, njihovom poređenju sa potencijalnom stego-datotekom i sumiranjem razlika.

Audio-reproduktivna metoda sa zasniva na uzastopnom preslušavanju istih audio datoteka na različitim brzinama. Pri izboru audio datoteka mora se voditi računa o stepenu kompresije koji je upotrebljen pri kompresiji u potencijalnoj steganografski obrađenoj audio datoteci (MP3).

Ako se dođe do zaključka da se prostim okom ne mogu utvrditi bitne razlike između potencijalne steganografske i originalne datoteke, u tu svrhu se može primijeniti softverska metoda, koja podrazumjeva upotrebu određenog steganografskog alata. Neki od njih su:

Xsteg, Jsteg, Stegoanalysis, Camouflage, Stegalyzer, ImageHide, TiPi, Steganography i sl.

6. ZAKLJUČAK

Iz navedenih primjera se vidi da postoje određene razlike između originalnih i steganografski obrađenih datoteka. Dakle, određena steganografska metoda može biti upotrebljiva za skrivanje samo određene količine teksta. Zbog prevazilaženja nedostataka u postojećim steganografskim metodama, poželjna je kombinacija različitih metoda koje se zasnivaju na zamjeni ili umetanju određenih bitova. Takođe, u steganografiji je moguće izvršiti i dodatno šifrovanje određenom šifarskom metodom, kako bi mogućnost preuzimanja podataka od strane drugih korisnika bila svedena na minimum. Budući da se pomenute tehnike zasnivaju na umetanju ili zamjeni sličnih bitova, razlika između originalne i stego slike je neprimjetna. Važno je napomenuti i to da je vrijeme hakerisanja skrivene poruke izuzetno dugo i da se podaci koji su otkriveni u stego-datoteci ne mogu lako dešifrovati. U radu nisu analizirane inovatorske steganografske metode.

LITERATURA

- [1]. Chen, B. i Wornell, G.W., *Quantization Index Modulation: A Class of*
- [2]. Cole, E., *Hiding in Plain Sight, Steganography and the Art of Covert Communication*, Wiley, 2003.
- Embedding*, IEEE Trans. Information Theory, Vol. 47, No. 4, pp. 1423-
- [3]. Gopalan, K., *Audio steganography using bit modification*", *Proceedings*
- [4]. Katzenbeisser, S., *Information Hiding Techniques for Steganography and Digital Watermarking*, Artech House, 1999.
- [5]. Milosavljević, M. i Grubor, G., *Osnovi bezbednosti i zaštite informacionih sistema* Univerzitet Singidunum, 2006.
- of the IEEE International Conference on Acoustics, Speech, and Signal Processing*, (ICASSP '03), Vol. 2, pp. 421-424, April 2003.
- Provably Good Methods for Digital Watermarking and Information*
- [6]. Schneier, B., *Applied Cryptography*, John Wiley & Sons, 1996.
- [7]. Stallings, W., *Cryptography and Network Security*, Prentice Hall, 2005.
- [8]. Veinović, M., Jevremović, A., Šimić, G., *Uticaj formata nosećih podataka na efikasnost steganografskih metoda*, Sinergija 2009.
- [9]. Wnang, H. i Wang Sh., *Cyber Warfare: Steganography vs. Steganalysis*, COMMUNICATIONS OF THE ACM, October 2004/Vol. 47, No. 10. 1443, 2001
- [10]. www.garykessler.net
- [11]. www.jjtc.com

Abstract — In this paper performed the analysis of current steganographics techniques and method and pointed out the advantages and disadvantages of existing techniques in steganography. As examples of image file format used is JPEG, and MP3 audio files. Applying certain steganography techniques getting the original file steganography's processed data carrier, which is called a stego-file. Depending on the amount of inserted open text in a particular stego-file can be certain variations that are manifested through the difference in size and quality to the original file. The techniques used are: insertion, replacement and generation.

Key words —steganography, steganoanalysis, stego-file, capacity, bit, pixel.