STEGANOGRAFIJA I NJENE IMPLIKACIJE NA FORENZIČKE ISTRAGE
STEGANOGRAPHY AND ITS IMPLICATION OF FORENSIC INVESTIGATION

Ćosić Jasmin, *Ministarstvo unutrašnjih poslova Unsko-sanskog kantona, Bihać*
Bača Miroslav, *Sveučilište u Zagrebu, Fakultet organizacije i informatike, Varaždin, Republika Hrvatska*

Sadržaj – *Pojam „steganografija“ se obično veže za skrivanje ili prikrivanje podataka i informacija. Veliki dio informatički pismenog osoblja niti nezna pravo značenje ovoga pojma, dok čak i IT stručnjaci za sigurnost veoma rijetko dolaze u dodir sa steganografijom i stegoanalizom. Razvojem tehnike i tehnologije, a naročito posljednjih 15-tak godina Steganografija je postala velika opasnost. U svojim namjerama koriste je hackeri, zlonamjerni korisnici na internetu , sajber kriminalci, a nakon „11.septembra“ i napada na SAD čak i teroristi. Često se pojam Steganografija mješa i stavlja u pogrešan kontekst sa Kriptografijom iz prostog razloga što se obje tehnike upotrebljavaju za skrivanje informacija (podataka). U ovom radu će autori predstaviti pojam steganografije i stegoanalize, analizirati mogućnosti šire upotrebe ove tehnike s akcentom na kompjutersku forenziku i istrage, te softverske alate i način otkrivanje ovako skrivenih podataka u slikama, audio-video falovima ili običnim tekstualnim fajlovima.*

Abstract – *The term "steganography" is usually associated to hiding or covering data and information. Most of IT personnel do not know a true meaning of this term, even though IT security specialists rarely come into contact with steganography and steganalysis. The steganography has become a great danger through development of techniques and technology, especially in the last 15 years. Hackers, malicious users of the Internet, cyber criminals, use it in their evil intentions and after 9/11, attacks on the United States, even terrorists use it too. The term steganography is often confused with Cryptography, for the simple reason that both techniques are used to hide information (data). In this paper the authors will present the concept of steganography and steganalysis, analyze the possibilities to use these techniques with emphasis on computer forensic and investigation , and software tools used to detect hidden data in images, audio-video files, or even plain text files.*

KLJUČNE RIJEČI: steganografija, stegoanaliza, digitalna forenzika, kompjuterski kriminal, sajber kriminal

KEY WORDS: steganography, steganalysis, digital forensic, computer crime, cyber crime

1. UVOD

Razvoj informacijsko-komunikacijskih tehnologija nametnuo je širu upotrebu kompjutera u skoro svim sferama društvenog života. Danas skoro da i ne postoji neki aspekt ljudskog djelovanja gdje računar ne igra značajnu ulogu. U ovakvim uslovima, pojavio se problem sigurnosti informacionih sistema, jer se informacije prenose putem raznih medija u digitalnom obliku i lako se može doći u njihov posjed.

Za zaštitu ovakavih informacija najčešće se koriste metode kao što su kriptografija, kodiranje ali i steganografija [1]. Svaka od ovih metoda ima svoje prednosti i/ili nedostake . U radu se opisuje stegonografija jer je u posljednjih nekoliko godina ova metoda postala veoma raširena. Često se steganografija i kriptografija stavljaju u pogrešan kontekst ali često i postovjećuje, iz jednostavnog razloga što se obje tehnike upotrebljavaju za skrivanje informacija, što je potpuno pogrešno. Kod upotrebe kriptografije je vidljivo da strane komuniciraju kroz kriptovan kanal, te da postoji neka poruka unutar kriptovanog fajla, a kada je u pitanju steganografija uopšte se ne vidi postojanje te komunikacije i skrivene datoteke jer je ona obično “umetnuta” i skrivena u drugu datoteku [2]. Zbog ovoga , mogućnosti primjene steganografije su pored legalnog korištenja kod zaštite vlasništva (vodeni žig) uvidjeli hackeri, cyber-kriminalci, teroristi i drugi zlonamjerni korisnici na internetu. Njihovo svakodnevno korištenje ove tehnike zadalo je velike muke kako stručnjacima zaduženim za sigurnost, tako i kompjuterskim forenzičarima ali i sudskim vještacima prilikom istraga kriminalnih djela.U nastavku rada naglasak će se staviti na na pojam, način funkcioniranja ali i moguće zloupotrebe steganografije, kao i načine njenog otkrivanja i stegoanalizu.

2. POJAM I TIPOVI STEGANOGRAFIJE

Nastanak i prva upotreba steganografije seže još u daleku prošlost u vrijeme starih Grka. Sam pojam predstavlja kovanicu riječi Steganos (grčki prikriveno) i Graptos (grčki pisati), što bi značilo “skriveno pisanje”. U to vrijeme, kada su željeli poslati skrivenu poruku, stari grci bi glasniku obrijali glavu, na nju istetovirali poruku, zatim čekali da mu naraste kosa i onda ga slali da na taj način prenese tajnu poruku [3]. U II svjetskom ratu se upotrebljavala “nevidljiva” tinta sačinjena od voćnog soka, urina, mlijeka ili vinskog sirćeta sa kojom su se pisale poruke koje su trebale biti nevidljive. Kada bi se papir na kom je napisana takva poruka zagrijao, tinta bi potamnila i poruka bi bila čitljiva [4].

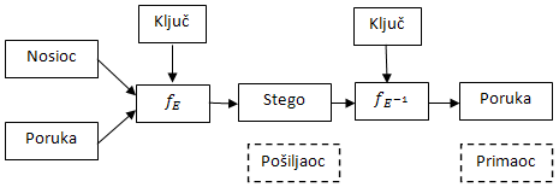
Danas se situacija nije mnogo promjenila u pogledu bitnosti prenosa informacija, i dalje se informacije prenose, ali na drugačiji način. Snaga interneta se ogleda u tome da se u kratkom roku mogu prenijeti ogromne količine informacija sa kraja na kraj svijeta. Ključno pitanje koje se ovdje postavlja je kako, na koji način ali i zašto zaštiti odnosno “skrivati” ove informacije ?

Pomoću steganografije informacije je moguće skriti unutar:

- Slike-fotografije (.bmp, .gif, .jpeg i sl.)
- Video fajla (.avi, .mpg, .vob i sl.)
- Audio fajla (.mp3, .midi, .wav, .wma i sl.)
- Datoteke (.doc, .xls, .ppt, .txt i sl.)
- ali i bilo kog binarnog fajla

Proces steganografije se odvija na taj način da se skrivena poruka umetne u neki transportni posrednik, koji se zove nosioc. Skrivena poruka je proširena u nosiocu i formira se steganografski posrednik. Nakon toga se dodaje steganograski ključ kako bi se fajl dodatno kriptovao .Proces se može pokazati kao :

steganografski_medij = tajna_poruka + nositelj + steganografski_ljuc [Kessler, 2004]



Slika 1: Steganografski sistem

Na slici br.1 prikazan je način funkcioniranja steganografskog sistema, gdje je:

• Nosioc - medij unutar kojeg se sakriva tajna poruka
• Poruka - tajna poruka koja treba biti sakrivena
• Ključ - steganografski ključ; parametar funkcije fE
• fE - steganografska funkcija "ugrađivanje"
• Stego - steganografski fajl
• fE -1 : steganografska funkcija "izdvajanje"

Često se nosioc u literaturi naziva i carrier, poruka je „payload“ a „package“ je konačni fajl u koji je ukomponovan i nosilac i payload.

Danas je najčešći način skrivanja fajlova je unutar slike (fotografije) iz niza razloga koji će se razmotriti u nastavku. Metode koje se najčešće upotrebljavaju su:

- LSB (Least Significant Byte) ili substitucija bita najmanje važnosti,
- Injection ili umetanje i
- Modifikacija svojstava datoteke (slike,fotografije)

ASCII [5] (The American National Standard Code for Information Interchange) predstavlja standard za prezentovanje teksta i karaktera u digitalnom svijetu. ASCII upotrebljava 7 bitova i 1 paritativan bit za predstavljanje bilo kog znaka-karaktera. Npr. Znak “S” je predstavljen kao niz bitova - (0)1010011.

Slika na kompjuteru je takodjer predstavljena nizom znakova koji predstavljaju intezitet svjetline u tačkama ili “pikselima”.
Tipična 8-bitna slika rezolucija 640x480 pixela je veličine cca 307 KB (640x480=307.200). 24-bitna slika rezolucije 1024x768 pixela je veličine cca 2.3 MB (1024x768x3=2359296) i ona je veoma pogodna kao nosioc skrivenog podatka.
Naime, svaki byte se sastoji od 8 bitova, npr. u našem primjeru znaka „S“ (0)1010011, prva pozicija 0 predstavlja bit najmanje važnosti . U 24-bitnoj slici postoje 3 ovakva bit-a i mogu se kodirati u svakom pixelu (24 bits/8 (1 byte) = 3 bytes) [6] . To praktično znači da se u sliku veličine 1024x768 može skriti informacija u količini od cca 288 KB ((((1024x768x3)/8)/1024)=288 KB). To svakako nije zanemarljivo malo ako se uzme u obzir da su promjene u originalnom fajlu minorne i jedva primjetne.

Steganografija se obično djeli na 2 vrste Fragile (lomljiva, krhka) i Robust (robusna, snažna).
Pomoću fragilne steganografije informacija se umeće u fajl pri čemu ukoliko dođe do promjena na fajlu nosiocu, dolazi do potpunog gubitka informacije. Kod robusne steganografije informacija se umeće u fajl pri čemu je veoma teško ovakvu informaciju uništiti ili oštetiti. Ovaj tip steganografije je mnogo teži za implementaciju ali su mu i mogućnosti primjene mnogo veće.

3. (NE)LEGALNE MOGUĆNOSTI PRIMJENE

Upotreba steganografije se najčešće odvija u 2 pravca:

1. Zaštita protiv otkrivanja (skrivanje informacija)
2. Zaštita od uklanjanja:

    a. Watermarking (vodeni žig) svi objekti se obilježavaju na isti način
    b. Fingerprinting (otisak prsta) svaki objekt je obilježen specifično [7].

Digitalni vodeni žig se obično koristi kod zaštite autorskih prava i vlasnišva nad multimedijalnim fajlovima (audio-video fajlovi), zaštite od kopiranja, te dodavanja dodatnih informacija izvornom fajlu,provjeru autentičnosti fajlova.
Vodeni žig se može koristiti i kao zamjena za neke funkcije koje se koriste za generisanje hash sažetaka (fingerprint)[17].
Pored “legalnih” aktivnosti ono što najviše brine Agencije za sprovođenje zakona u cijelom svijetu je upotreba steganografije u nelegalne svrhe i kriminalne aktivnosti. Veoma čest slučaj u kriminalnoj praksi je da se steganografija upotrebljava za distribuciju zabranjenih sadržaja ali i izdavanje naloga za tajne transfere novca, slanje tajnih podataka od strane špijunskih organizacija, krađu povjerljivih inforacija, krađu identiteta, finanijske pronevjere i sl.
Veoma često kriminalci i teroristi koriste ovu metodu za skriveno komuniciranje (“*covert communication*”).
U praksi je poznat slučaj [8] djelovanja jedne kriminalne organizacije koja je shodno prethodnom dogovoru vršila distribuciju fotografija na kojima su zlostavljana djeca, na “legalan” način putem eBay servera. Grupa je bila uredno registrirana na eBay-u, sa tačnim podacima o ponudama i plaćanjima. Predmeti trgovine su takodjer bili tačni i uredno registrirani. Radilo se o raznim fotografijama koje su se smjenjivale u vremenskim intervalima. Shodno ranijem dogovoru i planu sa članovima organizacije, na eBay su postavljane i fotografije koje su unutar sebe sadržavale tajne, zabranjene sadržaje-skrivene fotograije. Članovi organizacije

su tačno znali kada će se pojavljivati ovakve fotografije i vršili su njihovo "download-anje" sa servera. U istragama koje su usljedile bilo je veoma teško identificirati i napraviti razliku između ljudi koji su bili legalni kupci na eBay-u i nisu znali za skrivene sadržaje unutar fotografija i osumnjičenika koji su imali unaprijed dostavljen plan pojavljivanja ovakvih fotografija.

Drugi način korištenja ove tehnike u nezakonite svrhe ogleda se u kreiranju tipičnih spam poruka unutar kojih se skrivaju nelegalni sadržaji-tekstualne poruke.
U ove svrhe se koriste posebno kreirani algoritmi čiji se rad temelji na "gramatički baziranom ponašanju" [9]. Neki web servisi [10] nude usluge kreiranja spam poruka oponašajući željeni tekst. Tekst se unese u formu aplikacije, kreira se novi tekst-obično nalik spam poruci, u koji se "umetne" naša poruka, te na taj način omogući slanje putem interneta ili nekog drugog prenosnog medija.
Ukoliko se još proces kodiranja "pojača" sa passwordom ili još bolje Private Key Infrastrukturom, proces dekodiranja postaje noćna mora za kompjuterske forenzičare.

Ovaj način prenosa informacija predstavljao je pravu muku istražiteljima sigurnosnih agenicija u SAD-u naročito poslije 11.septembra 2001.g. i terorističkih napada na WTC. U to vrijeme teroristi su koristili steganografiju i razne sportske, političke pa čak i porno portale kako bi na forumima postavljali slike i druge sadržaje unutar kojih su skrivali tajne planove za napade.
Napad izvršen u julu mjesecu prošle godine na turistički hotel u Mumbai-u u Indiji je takodjer planiran i izvršen upotrebljavajući skrivane i kodirane poruke koje su bile umetane u regularne e-mailove kojim su komunicirali teroristi putem Yahoo servera [11].
Istražiteljima su trebali mjeseci mukotrpnog rada kako bi otkrili ove poruke.

Danas cyber-kriminalci koriste steganografiju za distribuciju nelegalnih sadržaja kao što su brojevi ukradenih kreditnih kartica, lažni nalozi bankama za plaćanja, distribuiranje korisničkih imena i lozinki za web stranice u koje su upali, te u novije vrijeme distribuciju baza podataka građana sa matičnim brojevima, brojevima osiguranja, zdravstvenih kartona itd. Čest slučaj je i korištenje u špijunske svrhe, gdje tzv. "*intruderi*" iz ciljanih firmi u kojima su zaposleni i koje špijuniraju, izvještavaju nalogodavce o svojim špijunskim aktivnostima.

4. STEGOANALIZA I NAČINI OTKRIVANJA

Za stegoanalizu se može reći da je ona za steganografiju ono što je kriptoanaliza za kriptografiju. IT stručnjaci zaduženi za sigurnost je zovu i "kontramjera steganografiji" ili "napad na steganografiju". Ovo je relativno mlado istraživačko područje, prvi puta se pojavljuje kanih 1990tih godina. Steganografija ne podrazumjeva samo otkrivanje skrivenih podataka, nego i izdvajanje skrivenog sadržaja, onemogućavanje pregleda sadržaja-uništavanje , te preuređivanje sadržaja kako bi se primaocu poruke poslala pogrešna informacija [12].

Tehnike stegoanalize mogu se klasificirati slično kao i tehnike kriptoanalize, zavisno koliko informacija imamo [13]:

- "Steganography-only" napad – kada nam je dostupan samo steganografski medij za analizu
- "Known-carrier" napad – kada nam je dostupan nosioc i medij za analizu
- "Known-message" napad – kada nam je poznata skrivena poruka
- "Chosen-steganography" napad – kada nam je poznat medij i algoritam
- "Chosen-message" napad – kada nam je poznata poruka i algoritam
- "Known-steganography" napad - kada nam je poznat i nosilac, medij i algoritam

Jedan od načina otkrivanja steganografskih sadržaja koje kompjuterski forenzičari upotrebljavaju je pregled računara u cilju pronalaska ovakvog software-a ili pristupa web servisima koji nude ove usluge. Ukoliko se na računaru pronađu ovakvi sadržaji nakon toga se identificiraju eventualni fajlovi nosioci – najčešće se sumnja na 24-bitne .bmp fajlove rezolucije 1024x768 ali i druge grafičke i audio-video fajlove. Fajlovi se pregledaju vizualno a nakon toga sa posebnim programima namjenim za ove svrhe. Ono što prilikom vizualnog pregleda forenzičar može primjetiti je kod sumnjivih slika "neprirodni" kontrasti, manje izobličenje slike. Kod tekstualnih fajlova može biti sumnjivo postojanje više nego je normalno razmaka (space) između slova ili riječi, te riječi kojima nije mjesto u tekstu koji je napisan. Posebnim alatima se filtrira saobraćaj i neispravni "headeri" unutar TCP/IP peketa, te izdvajaju dijelovi koji sadrže sumnjivi sadržaj.
Problem se može javiti u tome što neki programi namjenjeni za steganografiju ne zahtjevaju instalaciju , te se pokreću direktno sa prenosnih memorija (usb memory stick) te je i samo korištenje ovakvih programa teško pronaći jer na računaru ne ostavljaju nikakve tragove. U ovakvim sučajevima je potrebno pristupiti drugačijem načinom u odnosu na tradicionalni.
Proces oktrivanja ovih sadržaja je mnogo komplikovaniji i kompleksniji nego kod kriptoanalize, jer se kod kroptoanalize zna da se u predmetnom fajlu koji se istražuje nalazi neki podatak ili informacija, dok se kod stegoanalize uopšte nezna da li se u sumnjivom fajlu nalazi neki drugi sadržaj. Ovakvi skriveni sadržaji mogu biti umetnuti bilo gdje (npr. na internetu na web-u) u:

- Tekstu web stranice
- Slici na web-u
- Audio-video sadržaju na web stranici
- Unutar bilo kog linka (proširen HTML)
- Komentari na forumima
- Okvir (frame) web stranice [CERT, PUBDOC,2006]

Najčešće upotrebljavana stegnografska tehnika je korištenje LSB -a jer može da sadrži skrivene uzorke. Statistička analiza LSB podatka je široko raspostranjena metoda za otkrivanje ovih uzoraka. Jedan od najčešćih uzoraka je korelacija između HOB-a (High Order Bits) i LSB-a, koji je obično predstavljen u hardveru, kao što je kamera, koji se upotrebljava da generira originalne podatke. Ova vrsta

napada je najuspješnija jer najviše steganografskih algoritama funcionira pod pretpostavkom da je LSB slučajan. Statistička analiza može detektirati promjene učinjene na LSB-u [14].

Danas postoji na stotine različitih programa, od komercijalnih do "open-source" licenci koji omogućavaju stegoanalizu na Windows, Unix/Linux/OpenBSD, Macintosh, OS/2, DOS i drugim operativnim sistemima.
Stegoarchive [15] je on-line arhiva oko 120 programa za sve operativne sisteme za steganografiju i stegoanalizu.
Od strane SARC (Steganography Analysis and Reasearch Centre) identificirano je preko 725 steganografskih aplikacija [16].
Gruba podjela ovih programa je na:

- Komercijalne
- Besplatne (freeware) i one koji se distribuiraju pod open-source licencom.

Među najpopularnije se mogu svrstati: F5, S-Tools, JP Hide&Seek, Stegomagic, Gif-It-Up, Stegomagic, S-Tools, Mp3Stego, StegHide Itd.

Što se tiče stegoanalitičkih programa većina ih koristi "signature-based" –sistem otkrivanja baziran na potpisima, slično kao i antivirusna i antimalware zaštita.
Forenzički stručnjaci najčešće koriste isprobane profesionalne programe za kompjutersku i digitalnu forenziku kao što su EnCase firme Guidance software i FTK – Forensic data ToolKit firme AccessData.
Ova dva moćna programska alata imaju u sebi tzv. "Steganography Application Fingerprint Database", baze podataka steganografskih aplikacija bazirane na upisanim HASH funkcijama (CRC-32, MD5, SHA-1, SHA-224, SHA-256, SHA-384, i SHA-512), zavisno od licence, a ove baze se mogu nabaviti i posebno i izvršiti uvoz u ove aplikacije [16].
Također korisni alati su i StegDetect, Gargoyle i StegoSuite koji se sastoji od nekoliko modula (StegoHunter, StegoWatch, StegoAnalyst i StegoBreak).

5. ZAKLJUČAK I BUDUĆA ISTRAŽIVANJA

Staganografija je razvojem interneta i cyber-kriminala promjenila prvotnu ulogu. Samo jednim dijelom se koristi u legalne svrhe (vodeni žig, fingerprinting), dok je nažalost najviše koriste zlonamjerni korisnici na internetu koji su u njoj pronašli dobar način za ostvarivanje svojih nezakonitih ciljeva. Ovdje se najviše misli na teroriste, cyber-kriminalce, distributere sadržaja dječije pornografije i sl. Forenzička istraživanja ovih sadržaja se moraju planirati i sprovoditi permanentno i planski. Iako je tehnički gledano ovako skrivene sadržaje veoma teško pronaći , ukoliko se planski pristupi ovom problemu, rezultati nemogu izostati. Forenzički stručnjaci moraju dobro poznavati alate i načine funkcioniranja pojedinih alata za stegoanalizu kako bi se mogli nositi u koštac sa ovim rastućim problemom. Na prostorima BiH ali i okruženja se još uvijek ne vrše sistamatska istraživanja u cilju identificiranja i otkrivanja sadržaja na internetu kako bi se moglo doći do zaključka kakvo je stanje na polju upotrebo steganografije. Budući rad i istraživanja autori će usmjeriti u tom pravcu. Na reprezentativnom uzorku će se analizirati web sadržaji (tekst, slike, video, audio i ostalo) uz pomoć dostupnih alata, te pokušati utvrditi postojanje (ne)zakonitih skrivenih sadržaja.

LITERATURA

[1] S.Channalli, A.Jadhav, „Steganography-An Art of Hiding Data", International Journal of Computer Science and Engineering, 2009

[2] J.Cummins, P.Diskin, S.Lau, R.Parlett, „Steganography and Digital Watermarking", 2004

[3] Herodotus, The Hisories, chap 5," 7 – The seventh book entitled Polymnia", 1992

[4] Second Lieutenant J.Caldwell, "Steganography", United States Air Force, 2003

[5] Basement Computing, dostupno na: http://www.neurophys.wisc.edu/comp/docs/ascii/ (pogledano 07.01.2010.godine)

[6] S.R.Betancourt, „Steganography:A New Age of Terrorism", GSEC Practical Version, SANS Institute,2004

[7] R.Popa, „An Analysis of Steganographics Technique", The Politehnica University of Timisoare, Faculty of Automatics and Computers, Department of Computer Science and SE, 1998

[8] G.C.Kessler, „Steganography:Implications for the Prosecutors and Computer Forensics Examiner", American Prosecution Reasearch Institute, 2004

[9] P.Wayner, „Dissappearing Cryptography , Information hiding:Steganography , Watermarking", Third Edition 2009

[10] Spam Mimic, dostupno na: http://www.spammimic.com (pogledano 12.01.2010.godine)

[11] DNA, Read The World, dostupno na: http://www.dnaindia.com/mumbai/report_mumbai-police-fail-to-crack-july-11-suspects-mail_1058716 (pogledano 05.12.2009.godine)

[12] J.T.Jackson, H.Gregg, H.Gunsch... „Steganography detection using a computational immune syste",International Journal of Digital Evidence,Spring, 2003

[13] K.Curran, K.Bailey, „An evaluation of image-based steganography methods", International Journal of Digital Evidence, 2003

[14] A.Ibrahim, Steganalysis in Computer Forensic, School of Compuzter and Information Science, Edith Cowan University, 2007

[15] StegoArchive.com, dostupno na: www.stegoarchive.com, (pogledano 29.12.2009.godine)

[16] Steganography Analyst and Reasearch Centre, dostupno na: http://www.sarc-wv.com/safdb.aspx, (pogledano 25.01.2010.godine)

[17] M. Bača, Uvod u računalnu sigurnost, Narodne novine, Zagreb, 2004