STEGANOGRAFIJA KAO ANTIFORENZIČKI ALAT

Manja Đuričkov, dipl. inž. informatike

Sažetak: U analizi je obuhvaćena steganografija kao jedna od disciplina digitalne forenzike. Poznavajući steganografiju i steganoanalizu možemo na verodostojan način dokazati da je neki kompjuter korišćen u svrhe kompjuterskog kriminala. Da bi se stekao uvid u oblasti primene steganografije neophodno je klasifikovati je i definisati metode za primenu steganografije nad različitim digitalnim nosiocima tajnih poruka. Najteži deo u istražnom postupku predstavlja detekcija postojanja steganografije posebno u velikim mrežama poput Interneta gde je prisutan veliki protok informacija. U okviru steganoanalize predstavljeni su metodi zasnovani na uočavanju promena između originala, bio on slika, zvuk, dokument isl. i stego nosioca i tehnike steganoanalize koje su bazirane na to koliko informacija znamo o delovima skupa koji čine steganografiju.

Ključne reči: Steganografija, steganoanaliza, stegano nosioc, digitalni vodeni pečat, digitalna forenzika, najmanje značajan bit.

1. STEGANOGRAFIJA I STEGANOANALIZA

1.1. Steganografija kroz istoriju

Steganografija datira još od 200. god. pre Hrista, iako ne u obliku u kakvom nam je danas poznata. Jedan od takvih primera su Naska linije u Peruu[1]. Na suvoj ravni je izgrebano više od 80 km linije između dva grada Naska i Palpe, od kojih su mnoge vidljive tek iz vazduha.

Tragovi steganografije mogu se pronaći u delima Džon Tritemius (1462-1516) koji bio je opat Nemačkog porekla („Steganografija: umetnost koja zahteva otkrivanje skrivenog pisanja misaonim aktivnostima čoveka[2].“). Kraljica Marija od Škotske[3] je koristila kombinaciju kriptografije i steganografije da sakrije pisma. Ona je svoja pisma krila u rupi za zapušavanje bureta piva, koje je neometano ulazilo i izlazilo iz njenog zatvora. Herodot je u 5. veku pre rođenja Hrista brijao glave nosiocima poruka, pisao je ohrabrujuće poruke

[1] Wikipedia [13]

[2] Najpribližniji prevod do kog je moglo da se dođe, original glasi : “*Steganographia:hoe est ars per occultam scripturam animi sui voluntatem absentibus aperiendi certa*.”

[3] The Science of Secrecy, Steganography [21]

Aristagoras iz Mileta, koje su podsticale na revolt protiv kralja Persije. Nakon što glasniku poraste kosa, on biva otpremljen primaocu. Kada bi glasnik stigao na predodređeno odredište, glava bi mu ponovo bila obrijana i na taj način bi se došlo do skrivene poruke.
480. godine pre Hrista grk po imenu Demaratus je poslao Spartancima poruku upozorenja o neizbežnoj invaziji Kserksa. Herodot opisuje metod koji je koristio Demarat[4]: „*Kako je opasnost od otkrivanja bila velika, postojao je samo jedan način na koji je mogao da posalje poruku preko: tako što je sa drvene table strugan vosak, zatim ispisivana na njemu poruka šta Kserks planira da uradi, a onda je poruka sakrivana ponovo voskom. Na ovaj način table, naizgled čiste, ne bi prouzrokovale problema sa stražarima duž puta...*“. Podataka o drugim ranim radovima na steganografiji i kriptologiji mogu se pronaći na web strani koju je postavio Fabian Petitkolas[5].

U novijoj istoriji, neke od steganografskih metoda korišćene su tokom Drugog svetskog rata[6]. Mikrotačke razvijene od strane nacista su delovi mikrofilma, napravljene pod velikim uveličanjem, najčešće preko 200 puta. Ove tačke mogu sadržavati stranice informacija, slika itd. Nacisti su, takođe, upotrebljavali nevidljivo mastilo i bezšifarnu tehniku. Bezšifarna tehnika (ili kodiranje) se koristi da se sakrije jedna poruka u drugu bez korišćenja komplikovanog algoritma. Još jedan od primera steganografije uključuje upotrebu Kardano rešetke[7].

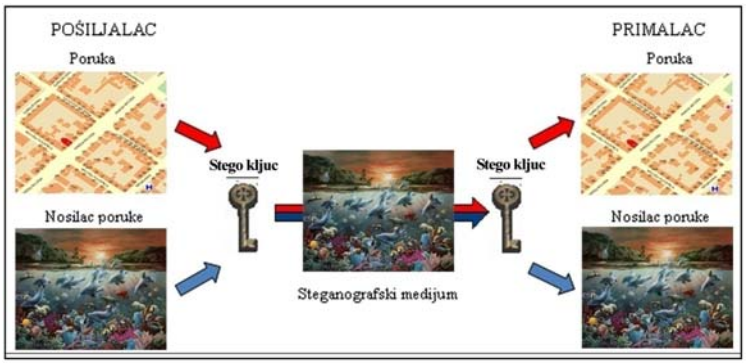
Naučni pristup izučavanja steganografije praktično je započet 1983[8]. Do 11. septembra 2001. godine, steganografija se smatrala bezopasnom. Odjednom, posle više od dve hiljade godina postojanja postala je predmet opšteg interesovanja. Za njenu upotrebu zainteresovala se i Vlada najrazvijenije zemlje sveta SAD. Zbog mogućnosti opšte upotrebe, svojstva maskiranja, mogućnosti korišćenja u oblasti industrijske špijunaže, čini je interesantnom i za poslovni svet. Teroristi Al Kaide organizovali su i izvršili napad na Svetski trgovinski centar i Pentagon komunicirajući putem nekoliko pornografskih Web sajtova. Plan terorističkog napada, u obliku šaljivih komentara, bio je „utisnut“ u slike koje su prenošene putem Interneta. Iako naizgled zastareo i naivan, steganografski metod prenosa poruka se pokazao krajnje efikasan. Bezbednosni sistem SAD je bio potpuno nemoćan. Teroristi su nadmudrili eksperte i američke bezbednosne agencije.

1.2. Savremena steganografija

Savremeni pojam steganografije, odnosno steganografskog sistema (stegosistema)[9] podrazumeva skup sredstava i metoda koji se koriste za formiranje ***skrivenog kanala*** prenosa informacija. Opšti proces steganografije (slika 1.) dat je ralacijom:

Steganografski medijum= skrivena poruka + nosilac poruke + steganografski ključ

[4] Singh Simon [20]
[5] Petitcolas Fabien A. P. [17]
[6] “Hidden in Plain Sight-Steganography”, Izdanje 2, Jun 1998 [11]
[7] Cardano Grille, „Classical Steganography“ [5]
[8] Reč je o „Problemnu zatvorenika“ [19]
[9] Na konferenciji ***Information Hiding: First InformationWorkshop 1996 godine*** (Baltimor) predložena je upotreba jedinstvene terminologije i definisani su osnovni pojmovi steganografije.



Slika 1. Opšti process steganografije - stegosistem[10]

U svojstvu podataka može se koristiti bilo koja informacija (tekst, audio podaci ili slika), pa je bolje koristiti termin ***poruka*** (engl. *message*) umesto informacija. ***Noslilac poruke***[11] (engl. *carrier, cover, cover medium*) je bilo koja informacija namenjena da kao „nosilac" prenese skrivenu poruku. *Ugrađena* ili *tajna poruka*, (engl. *embedded message*) je poruka koja se implementira u nosioca poruke.

Stego ključ (engl. *steg-key*) je tajni ključ pomoću koga se tajna poruka implementira u nosioca poruke. U stegosistemu može postojati jedan ili više stego ključeva, a po analogiji sa kriptografijom, razlikujemo stego sisteme sa tajnim i javnim ključem. ***Steganografski medijum*** (engl. *steganography medium, stego-medium*) je posrednik koji sadrži implementiranu poruku koja se tajno prenosi. *Steganografski kanal* (stegokanal) je komunikacioni kanal preko kojeg se šalje stego nosilac poruke.

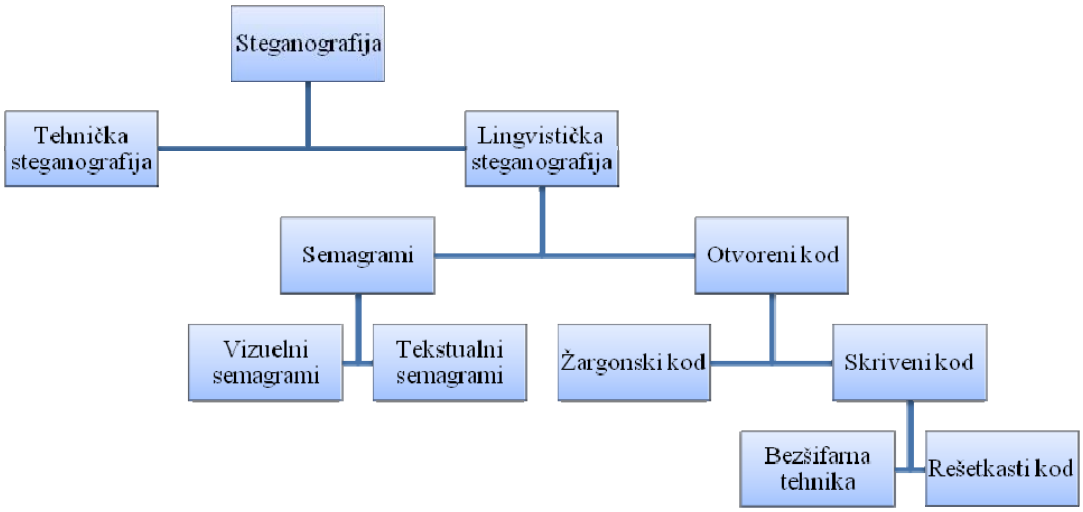
Primena steganografije se najčešće bazira na sledećem principu: pošiljalac tajne poruke bira nasumično nosioca poruke; u izabrani nosilac poruke implementira se tajna poruka uz pomoć stego ključa; primaocu se šalje steganografski medijum, a primaoc na drugoj strani obrnutim postupkom dolazi do sadržaja tajne poruke. Da tajna poruka ne bi bila vidljiva, bitno je da nosilac poruke sadrži dovoljno redundantnih bitova, koji mogu biti zamanjeni tajnom porukom. Važno je napomenuti da nisu svi digitalni formati pogodni za prenošenje tajnih poruka, jer se npr. promenom bitova u nekom izvršnom fajlu dovodi do toga da program ne radi ili javlja greške pri radu.

1.3. Klasifikacija steganografskih tehnika

Na slici 2. predstavljena je podela steganografskih tehnika. ***Tehnička steganografija*** koristi naučne metode za sakrivanje poruka, kao što je upotreba nevidljivog mastila ili mikrotačaka i druge metode smanjenja veličine tajnih poruka. ***Lingvistička steganografija*** krije poruke u nosioce na neki neuobičajan način i dalje ih kategoriše kao semagrame ili otvorene kodove. ***Semagrami*** kriju informacije kroz simbole ili znakove. *Vizuelni semagrami* koriste naizgled bezopasne ili svakodnevne fizičke oblike za prenos poruka, kao što su postavljanje detalja na desktop ili web sajt. *Tekstualni semagrami* kriju poruke modifikujući izgled nosioca teksta, kao što je vešta promena tipa ili veličine slova, dodavanjem dodatnih praznih mesta, ulepšavanjem slova ili dodavanje ručno pisanog teksta

[10] Чековский, С., Овсянников, В., 2002 [8]

[11] Nosioca poruke često možemo susreti još pod nazivima kontejner, paket, prenosnik itd.



Slika 2. Klasifikacija steganografskih tehnika[12]

Otvoren kod krije poruke u legitimne nosioce poruka na način koji nije očit nekom nesumnjičavom posmatraču. Nosilac poruke se ponekad zove javno saopštenje, s obzirom na to da je skrivena poruka prikriveno saopštenje. Ova kategorija je podeljena na *žargonski kod* i *sakriveni kod*. ***Žargonski kod***, kao što mu ime kaže, koristi jezik koji je razumljiv grupi ljudi ali je beznačajan drugima. Žargonski kod uključuje simbole koji se koriste da ukažu na prisustvo i vrstu signala bežične mreže, podzemnu terminologiju, ili bezazlenu konverzaciju koja prenosi posebno značenje zato što su činjenice poznate samo govorniku. Podskup žargonskog koda je i znakovni kod u kome se izvesnim preuređenjem fraze menja značenje. ***Sakriveni*** ili ***tajni kod*** krije poruku javno u nosećoj poruci tako da ona može biti otkrivena od bilo koga ko zna na koji način je ona sakrivena. *Rešetkasti kod* koristi šablon koji je korišćen za prikrivanje u nosiocu poruke. Reči koje se pojave pri otvaranju šablona je sakrivena poruka. *Bezšifarna* tehnika krije poruku prema nekom preuređenom setu pravila, poput "čitaj svako petu reč" ili " traži svako treće slovo u svakoj reči".

1.4. Kompjuterska steganografija

Da bi se sakrila poruka u digitlnom fajlu koristeći bezšifarnu tehniku nisu potrebni specijalni alati ili posebne veštine. Slika ili tekstualni blok može biti sakriven u drugoj slici u PowerPoint fajlu, na primer. Poruka može biti sakrivena u atributima Word fajla, u komentaru na Web stranici ili u nekom drugom formatu kojeg Web browser-a[13] ignoriše. Tekst može biti sakriven kao stilizovana linija u dokumentu tako što se tekstu dodeljuje boja pozadine, a zatim se on postavlja u drugi crtež koji je u prvom planu. Primalac može da povrati skriveni tekst tako što će mu promeniti boju[14]. Ovo su sve svakako nisko-tehnički mehanizmi, ali su veoma efektni.

Kompjuterska steganografija je deo steganografije koja se bavi realizacijom stegosistema upotrebom kompjuterske tehnike[15]. Savremeni metodi kompjuterske

[12] Bauer, 2002 [3] i dorađena od strane Arnold-a 2003 [1]
[13] Artz, 2001 [2]
[14] Seward, 2004 [18]
[15] Curran, K., 2003 [6]

steganografije zasnivajum se na: korišćenju specijalnih svojstava kompjuterskih formata i statističkom preobilju informacija u audio i video digitalnim signalima.

*Specijalna svojstva kompjuterskih formata***,** manje se koristi kao metod[16] za realizaciju kompjuterske steganografije namenjene zaštiti informacija, a više kao metod napada, ubacivanjem malicioznih programa. Npr. virus *W32/Perrun* je vrlo prost virus obima 18 kb, ubacuje se u fajlove sa .jpg ekstenzijom tako što se samo nadoda na njih formirajući dvokomponentni program.

Preobilje informacija u audio i video digitalnim signalima je osnovni pravac razvoja metoda kompjuterske steganografije. Digitalna fotografija, digitalna muzika i digitalni video predstavljaju matricu brojeva koji kodiraju intenzitet (jačine svetlosti kod fotografije, intenzitet jačšine zvuka kod muzike) u diskretnom trenutku u vremenu i prostoru. Kako biti sa najmanjim značenjem sadrže malo korisnih informacija, to njihova zamena sa tajnom porukom ne utiče značajno na kvalitet reprodukovanog zvuka ili slike. Kako zbog grešaka kvantizacije17, digitalne signale već prati šum kvantizaciji, neznatno se pogoršava i ne registruje čovekovim čulima. Metodi iz ove grupe mogu se podeliti na:

1. Metod zasnovan na zameni najmanje značajnim bitova - **LSB** (engl. *least significant bits*) i
2. Metod zasnovan na transformaciji slika, najčešće diskretnoj kosinusnoj transformaciji - **DCT** (engl. *Discrete Cosine Transformation*), ili slaganju različitih talasa (engl. *Wavelet transformation*)[18].

Primer: Kolor fajl po LSB metodu omogućava da se u fajlu veličine 800 kb smesti skrivena poruka i do 100 kb. S druge strane, samo jedna sekunda digitalnog zvuka, po LSB metodu, omogućava prenos tajne poruke do 10 kb[19] . Tipična 8-bitna slika dimenzija 640 x 480 sa 256 nijansi boja omogućava skrivanje poruke od 300 kb, odnosno 24-bitna slika 1024 x 768 do 2 Mb.

1.1.1. Steganografija u video formatima

Kada se informacija krije unutar video fajla, program ili osoba kriju informaciju uglavnom koristeći metod DCT, koji neznatno menja svaku sliku u videu, toliko da ne bude vidljivo ljudskim okom. DCT menja vrednost određenih delova slike, uglavnom ih zaokružujući. Na primer, ako deo slike ima vrednost 6.667 zaokružiće se najviše na 7. Steganografija u video fajlovima je slična steganografiji u slikama, osim što je informacija sakrivena u svakom frejmu videa. Kada je samo mali deo informacije sakriven unutar videa generalno nije uočljiv uopšte, u svakom slučaju, što je više informacija sakriveno postaće manje uočljive.

---

[16] Format PE (*portable executable*) ima osobinu da je razbijen u više sekcija. U svakoj od sekcija ima slobodnog prostora u koji je moguće umetnuti neke druge podatke

[17] Kvantizacija je jedan od dva postupka koji se primenjuje na analogni signal kako bi se dobili digitalni signali.

[18] Curran K., [6]

[19] Чековский, С., Овсянников, В., 2002 [8]

1.1.2. Steganografija u audio formatima

Kada se informacija krije u audio fajlu, uglavnom se koristi tehnika kodiranja na *slabom bitu* koja ima sličnosti sa LSB koji se generalno koristi u slikama. Problem kodiranja slabog bita u audio formatu je uočljivost ljudskom sluhu, pa je to donekle rizičan metod. Metod proširenog spektra (engl. *Spread spectrum*) koji se koristi za sakrivanje informacija u audio fajlu funkcioniše tako što se dodaju slučajni šumovi informacijama koje su sakrivene u nosiocu i raširene kroz spektar frekvencija. Metod sakrivanja podataka uz pomoć eha (engl. *Echo data hiding*) koristi eho u muzičkim fajlovima takvim redom da se kriju informacije koje taj fajl nosi. Informacija se može sakriti jednostavnim dodavanjem dodatnog zvuka izvesnom ehu u audio fajlu. Ovaj metod je bolji od drugih zato što poboljšava zvuk audio fajla.

1.1.3. Steganografija u dokumentima

Korišćenje steganografije u dokumentima funkcioniše jednostavnim dodavanjem praznih mesta i tabova na krajevima linija u dokumentima. Ovaj vid steganografije je veoma efikasan, zato što korišćenje praznih mesta i tabova nije vidljivo ljudskom oku uopšte, bar u najvećem broju tekstualnih editora. Prazna mesta i tabovi nalaze se prirodno u dokumentima, pa ne postoji bilo koji mogući način da korišćenje ove metode steganografije bude nekome sumnjivo.

1.1.4. Steganografija u slikama

Za skrivanje informacija u slikama najčešće se koristi metod LSB. Za kompjuter slika predstavlja jednostavan fajl koji pokazuje različite boje i intezitete svetlosti u različitim delovima slike. Najbolji format slike za sakrivanje informacija je 24-bitna BMP slika, kao najveći tip fajla, a samim tim i najkvalitetniji. Mnogo je lakše sakriti informacije u slici visokog kvaliteta i rezolucije. U BMP formatu, boja je predstavljena kao kombinacija crvene, zelene i plave boje. Svaku od ovih boja predstavlja 1 bajt. Kombinacija od po jednog Bajta crvene, zelene i plave daje 3 Bajta (24 bita) koji predstavljaju 1 piksel. 24-bitna šema podržava 16.777.216 (2^{24}) jedinstvene boje[20]. Iako je 24-bitna slika najbolja za sakrivanje informacija, zbog njene veličine mnogi se odpredeljuju za 8-bitni BMP, ili npr. GIF. Jedan od razloga je taj što slanje velikih slika preko Interneta može izazvati sumnju.

Najveći broj aplikacija za digitalne slike danas podržava 24-bitne slike, gde je svaki piksel kodiran u 24. bita. Druge aplikacije kodiraju boje koristeći 8 bita/pikselu. Svaki piksel je kodiran sa 8 bita gde vrednost tačke u 24-bita boje ulazi u paletu. Ovaj metod ograničava jedinstven broj boja u datoj slici na 256 (2^8). Izbor kodiranja boje svakao utiče na veličinu slike. Slika dimenzija 640 x 480 piksela koristeći 8-bitni slikovni format zauzima otprilike 307 KB (640x480 = 307.200 bajta), dok bi slika dimenzija 1400x1050 koristeći 24-bitni slikovni format zauzela 4.4 MB (1400x1050x3 = 4.410.000 bajta). Paleta boja i 8-bitni slikovni format su obično korišćeni u GIF (*Graphics Interchange Format*) i BMP formatu. GIF i BMP se generalno uzimaju u obzir da bi se obezbedila idealna kompresija zato što obnovljena slika posle kodiranja i kompresije je identična u bit originalnoj slici[21].

JPEG (*Joint Photographic Experts Group*) format slike koristi DCT, pre nego kodiranje piksel-po-piksel. U JPEG formatu, slika je podeljena na 8x8 blokova za svaku odvojenu

[20] Curran, K. and Bailey, K, 2003 [7]
[21] Johnson and Jajodia, 1998A [15]

komponentu boje. Cilj je pronaći blok gde bi promena vrednosti piksela bila najmanja. Ako je vrednost prevelika, blok se deli na 8x8 podblokova, sve dok vrednost ne bude dovoljno niska. Svaki 8x8 blok, ili podblok, je transformisan u 64 DCT koeficijenta koji su približni osvetljenju (svetlosti, tami i kontrastu) i signalu boje tog dela slike. JPEG se generalno smatra lošim formatom za kompresovanje, jer slika obnovljena iz kompresije je blizu originalnoj slici, ali nije i identična[22]. Da bi stavili što veću količinu podataka u sliku, koriste se dve vrste kompresujai podataka: bez gubitaka (*Lossless*) i sa gubicima (*Lossy*) kompresija. Pravi predstavnik lossless komprsije su .ZIP i .RAR, a *lossy* kompresije - JPEG. Za kompresiju podatka može se koristiti bilo koji algoritam.

Za poprvaku mutnjikavosti, šarenila i „usamljenih tačaka“ na slici, mogu se koristiti različiti, pažljivo odabrani filteri i efekti za obradu slike. *Maskiranje i filtriranje* je jedna od najzastupljenijih tehnika u steganografiji. Ako se primeti u nekom delu slike mutnjikavost posle ubacivanja skrivenih podataka, onda se original slike može malo potamniti i nakon toga ubaciti podaci u nju. Uspeh se zasniva na činjenici da ljudsko oko slabije raspoznaje razlike među bojama slabije sjajnosti. *Dodavanje „šuma“* je jedan od veoma efektnih tehnika. Zasniva se na dodavanju belih tačaka ili izbeljivanju nekih tamnijih. Sve ovo krajnjem korisniku stvara utisak da je slika skenirana i da je slabijeg kvaliteta i takvu sliku retko ko uzima u detaljno razmatranje. Pri dodavanju šuma, važno je da se ne menjaju bitovi koji nose skriveni podatak. *Korekcija boje piksela* je, dosad, najsavršenija tehnika. Funkcioniše tako što se skriveni podatak upisuje npr. u svaki drugi piksel, a pikseli koji ostanu slobodni, koriguju se prema bojama susednih piksela. Korekcija slobodnog piksela se vrši tako što se, pored njegove originalne boje, gledaju i one susedne (slika bolje izgleda ako se gleda nekoliko susednih), a potom se nađe srednja vrednost boje. Tako će slika izgledati skoro isto kao i original, odnosno približnije nego pre. Nedostatak tehnike je što se koristi svaki drugi piksel za skrivanje podataka, pa ima duplo manje prostora za podatke. Velika prednost je to što se šanse za otkrivanje tajnog sadržaja svode na minimum. Slika će još bolje izgledati ako se podaci sakrivaju u svakom trecem pikselu itd., ali će biti srazmerno manje mesta. Korekcija boje piksela može se koristiti na slikama velikog formata za skrivanje podataka male dužine.

1.2. Detekcija steganografije - STAGANOANALIZA

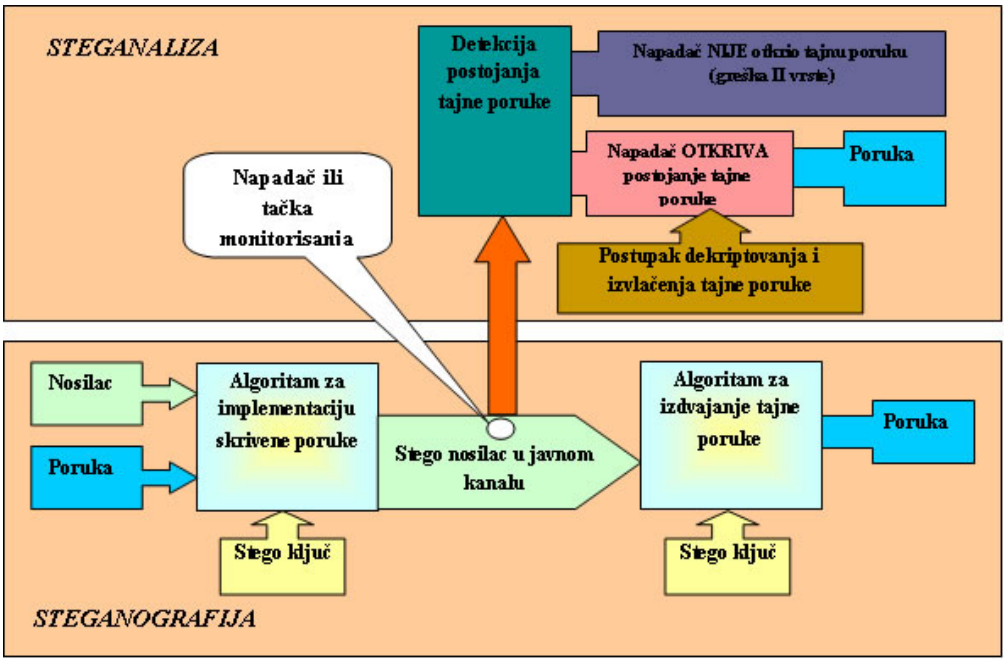
Steganoanaliza, detekcija steganografije od treće strane, relativno je mlada istraživačka disciplina o kojoj su se prvi članci pojavili 1990-tih godina. Zasniva se na otkrivanju sakrivenih informacija posmatranjem nekog prenosa podataka, bez pretpostavke koji steganografski algoritam je korišćen[23], ili na izvlačenju skrivene poruke da se onemogući prijem poruke, ili na promeni tajne poruke radi dezinformacije primaoca. Detekcija steganografije i izvlačenje skrivene poruke vrše se u procesu skupljanja dokaza kompjuterskog kriminalom. Uništavanje i/ili zamena tajne poruke može, takođe, biti pravno legitimna tokom istrage aktivnosti kriminalne ili terorističke grupe. U suštini **steganonaliza** treba da reši tri osnovna zadatka: *detekciju, definisanje i dekodiranje skrivene poruke*.

Za razliku od kriptoanalize, gde je evidentno da dobijeni šifrat sadrži tajnu poruku, steganoanaliza uglavnom startuje sa smanjivanjem skupa nekoliko sumnjivih informacionih

[22] Johnson and Jajodia, 1998A [15]

[23] Chandramouli , 2002 [4]

tokova, podskup najverovatnije izmenjenih informacionih tokova, ali je neizvesno da li neki od njih sadrži skrivenu poruku. To se najčešće realizuje statističkom analizom korišćenjem napredne statističke tehnike. Najjednostavniji metod detekcije modifikovanih fajlova je njihovo upoređivanje sa originalima. Suština detektovanja informacije je kretanje kroz grafičke prikaze na *Web* sajtovima. Analitičar može sačuvati poznate čiste kopije tih materijala i uporediti ih sa aktuelnim sadržajima na sajtu. Razlike, pod pretpostavkom da je nosilac isti, će sačinjavati skrivenu tajnu informaciju. Generalno, upotreba visokog nivoa kompresije čini steganografiju teškom za otkrivanje, ali ipak ne nemogućom. Dok postupak kompresije obezbeđuje dobro mesto za skrivanje podataka, visoka kompresija ipak smanjuje količinu podataka raspoloživih za skrivanje tajne poruke. Skrivanje informacija unutar jednog elektronskog nosioca podataka uzrokuje promene osobina nosioca koje mogu rezultirati nekim oblikom degradacije ili neuobičajenom karakteristikom. Odnos steganografije i steganalize prikazan je na slici 3.



Slika 3. Odnos steganografije i steganoanalize

Za detekciju postojanja skrivenih poruka, u stegoanalizi se koriste *metodi uočavanju promena*: *vizuelna detekcija (*fajlovi sa ekstenzijom *jpeg, bmp, gif), zvučna detecija (*fajlovi sa ekstenzijom *wav, mpeg), statistička detekcija (*promena u šablonu piksela ili *LSB*) ili analiza histograma i *strukturna detekcija* ili detekcija neobičnih struktura (pregled sadržaja fajla, njegove dužine, promena datuma i vremena, modifikacije sadržaja i provera sume-graničnog broja bita).

Steganografski metodi za digitalne medije mogu se široko klasifikovati kao *operateri u domenima slike* i *transformatorski domeni*. Alati u domenima slike kriju poruku u nosiocu manipulacijom bitovima, poput zamene LSB. Alati za transformacijske domene manipulišu steganografskim algoritmima, poput DCT koeficijenata u JPEG slikama. Dakle, steganoanaliza prati način na koji funkcionišu steganografski algoritmi. Drugi pristup je traženje strukturalnih anomalija koje sugerišu manipulaciju. LSB u slikama baziranim na

paletama najčešće su razlog velikog broja dupliranih boja, gde identične, ili najbliže identične, boje se dva puta pojavljuju i ne slažu se jedino u najmanje važnom bitu. Steganografski programi koji kriju informaciju jedino manipulacijom reda boja u paleti prouzrokuju strukturalne promene, koje često kreiraju potpis korišćenog steganografskog algoritma[24].

Statistička analiza se obično koristi za detekciju sakrivenih poruka, posebno kada se analiza radi na slepo[25]. Steganografske tehnike menjaju statistiku nosioca i velike ili duge sakrivene poruke će više promeniti nosioca nego one manje. Statistička analiza slika i audio fajlova može pokazati da li su statističke osobine fajla deformisane u odnosu na očekivanu normu. Ova tzv., statistika prvog reda, varijacija, *hi kvadrat test* (X^2), meri vrednost suvišnih informacija i/ili deformaciju u medijumu. Iako ova merenja mogu doprineti prognozi da li je sadržaj menjan ili je sumnjiv, ona nisu konačna[26]. Statistička steganoanaliza je teško izvodljiva zato što se neki steganografski algoritmi muče da bi očuvali nosioca fajla statistike prvog reda kako bi izbegli ovu vrstu detekcije. Šifrovanje tajne poruke takođe čini detekciju težom zato što šifrovani podaci imaju visok stepen slučajnosti, jedinice i nule se pojavljuju sa jednakim mogućnostima[27]. Obnavljanje tajne poruke dodaje nov sloj kompleksnosti u poređenju sa jednostavnom detekcijom prisutnosti tajne poruke. Obnavljanje poruke zahteva poznavanje ili procenu dužine poruke i, ako je moguće, šifrovani ključ i poznavanje kripto algoritma.

Specifičnost algoritma nosioca fajla može analizu učiniti jasnijom. JPEG je privukao veliku pažnju istraživača zbog načina na koji različiti algoritmi deluju na ovaj tip fajla. JPEG je loš medijum kada se koristi jednostavno ubacivanje LSB, zato što promena u fajlu olakšava detekciju skrivenih informacija. Postoji par algoritama koji kriju informacije u JPEG fajlovima i oni funkcionišu na drugačiji način: *Jsteg* senkvencijalno ugrađuje sakrivene podatke u najmanje važne bitove, *JP Hide&Seek* koriste slučajne procese za selekciju LSB, *F5* koristi matrično šifrovanje bazirano na *Hamingovom* kodu, dok *OutGuess* brani statistiku prvog reda.

Napredni statistički testovi koriste statistiku višeg reda, linearnu analizu, Markovljeva slučajna polja, statistiku različitih talasa itd. Diskusije koje su vođene na ovu temu nisu dostupne javnosti iz bezbednosnih razloga, ali se rezultati istih mogu uočiti u pojedinim alatima za detekciju steganografije.

Mnoge savremene steganoanalitičke tehnike su bazirane na *potpisu*, sličnom antivirusima i sistemina za detekciju upada (IDS/IPS). Steganoanalitički sistemi bazirani na *anomalijama* tek dolaze. Iako su raniji sistemi precizni i otporni, noviji će biti fleksibilniji, bolji i brže će moći da odgovore novim steganografskim tehnikama. Forma zvana „*slepa steganografska detekcija*“ raspoznaje razlike između čiste i steganografske slike koristeći statistiku baziranu na dekompoziciji različitih talasa ili ispitivanjem prostora, orjentacije i razmera kroz podskup većih slika[28]. Opšti alati koji mogu detektovati i klasifikovati setganografiju su još uvek u razvoju, ali polako postaju dostupni u softverskim alatima.

Tehnike steganoanalize, u najvećoj meri zasnovane na tome koliko informacija znamo[29], mogu se klasifikovati na sličan način kao kriptoanalitički metodi, na bazi napada na:

[24] Wayner, 2002 [21], Jackson idr, 2003 [23]
[25] Jackson i sar., 2003 [14]
[26] Wayner, 2002 [23]
[27] Farid, 2001 [9]
[28] Jackson i sar., 2003 [23], Farid, 2001 [14]

[29] Curran i Bailey, 2003 [7] , Johnson and Jajodia 1998 [15]

- *steganografiju*: steganografski medijum je jedina stavka dostupna za analizu,
- *poznatog nosioca*: nosilac tajne poruke i steganografski medijum su stavke dostupne za analizu,
- *poznatu poruku*: poznata je tajna poruka,
- *odabranu steganografiju*: steganografski medijum i algoritam su poznati,
- *odabranu poruku*: poznata poruka i steganografski algoritam su korišćeni za kreiranje steganografskog medija za dalju analizu i poređenje,
- *poznatu steganografiju*: poznati su nosilac, steganografski medijum i steganografski algoritam.

1.3. Tipovi napada na steganografske sisteme

Napadi na skrivene informacije mogu imati nekoliko oblika: detekcija, izdvajanje i/ili uništavanje i/ili dešifrovanje skrivene informacije. Sistem je već postao nesiguran ako je napadač u stanju samo da dokaže postojanje tajne informacije. Polazna pretpostavka je da napadač poseduje neograničene računarske resurse i u stanju je da primeni raznovrsne algoritme napada. Napadi na steganografske sisteme u odnosu na krajnji cilj napadača, mogu se teoretski podeliti na tri vrste: *pasivne*, *aktivne* i *namerne*.

U *pasivne napade* spadaju tehnikae koje samo detektuju postojanje tajne poruke, npr., statističko testiranje hipoteze u kojoj postoje dve mogućnosti greške: *greška I-vrste* nastaje kada se detektuje postojanje tajne poruke u nosiocu, a ona stvarno ne postoji, a g*reška II-vrste* nastaje kada se ne detektuje postojanje tajne poruke, a ona stvarno postoji. Steganografski sistemi maksimizuju verovatnoću da napadač napravi *grešku II-vrste*.

Aktivni napadači su u stanju da modifikuju stego nosioca u toku prenosa, ali ne previše, jer će u tom slučaju perceptulane i semantičke osobine biti narušene. Steganografski sistemi su često jako osetljivi na modifikacije stego-paketa (npr., digitalno procesiranje, filtriranje, usrednjavanje, komprimovanje, prebacivanje iz formata u format), pa čak i kompresiju sa minimalnim gubicima, koje mogu izazvati potpuni gubitak tajne informacije, jer uklanjaju baš one neprimetne komponente signala u kojima se najčešće vrši utiskivanje tajne poruke. Aktivni napadač, koji često nije u stanju ni da detektuje postojanje tajne poruke, može dodati slučajan signal u stego nosioc i uništiti tajnu informaciju. Napači mogu biti slučajni i namerni. Kao primer slučajnog napadača može se navesti slučajan šum koji se akumulira prilikom emitovanja signala nekim od spojnih puteva. Zbog toga jedan od značajnih zahteva koje steganografski sistem mora da ispuni je robusnost, tj., da se utisnuta tajna informacija ne može oštetiti bez drastičnih promena stego nosioca. Potrebno je naglasiti da postoji kompromis između sigurnosti (tajnosti) i robusnosti. Sigurnost zahteva da tajnu informaciju sakrijete u oblasti koje su perceptulano neprimetne, dok robusnost zahteva da tajnu informaciju sakrijete u oblasti koje su perceptualno primetne jer će tako biti teže oštetiti informaciju bez velike degradacije kvaliteta nosioca. Mnogi sistemi se dizajniraju tako da budu robustni na određene karakteristične tipove napada (kompresija, dekompresija, filtriranje, dodavanje belog šuma), a idealan sistem bi trebao da bude robustan na sve vidove napada. Generalno postoje dva principa da se napravi robustan steganografski sistem. Kod prvog sistema vrši se predviđanje mogućih napada i zatim se projektuje takav postupak implementacije tajne poruke koji je robustan na tu vrstu modifikacija, tako da modifikacija ne uništi u potpunosti informaciju. Druga strategija je da se primene inverzne modifikacije, od onih koje su korišćene tokom napada, kako bi se rekonstruisala originalna tajna informacija.

Namerni napadači pokušavaju da falsifikuju poruku ili da startuju steganografski protokol lažno se predstavljajući kao komunikacioni partner. U namernom napadu robusnost nije dovoljna. U slučajevima kada proces implementacije ne zavisi od neke tajne informacije koju poznaju samo pošiljaoc i primaoc, namerni napadač može falsifikovati poruku, s obzirom da primaoc nije u mogućnosti da verifikuje ispravnost identiteta pošiljaoca. Da bi se ovo predupredilo, alogritam za utiskivanje mora biti robustan i siguran. Zbog toga se pred siguran steganografski sistem postavljaju četiri osnovna zahteva koje mora da ispuni i to:

1. Poruke se moraju implementirati u nosioce korišćenjem javnih algoritama i tajnih ključeva,
2. Jedino vlasnik ispravnog ključa može detektovati, izdvojiti i dokazati postojanje tajne poruke.
3. Iako napadač uspe da selektuje sadržaj jedne skrivene poruke, ne može da detektuje ostale i
4. Kompjuterski je neizvodljivo detektovati tajnu poruku.

2. Studija slučaja I: Detekcija i izvlačenje tajne poruke iz *.bmp* formata

U ovoj studiji slučaja, za nosioca je izabrana 24-bitna slika BMP formata[30], dok je tajna poruka slika JPEG formata[31] /slika 4a). Veličina slike je 56 KB. Softver korišćen za primenu steganografije je *wbStego 4.3* (slika 4b). Kao fajlove nosioce ovaj program koristi .bmp fajlove, tekstualne fajlove, HTML i PDF fajlove. Kriptografija je primenjena pre šifrovanja i na taj način obezbeđena je visoka sigurnost. Iako neko ima saznanja da je sakrivena poruka u nosiocu, ne može je dešifrovati bez šifre. *WbStego4* nudi šifrovanje i razne algoritme koji su kompatabilni sa ranijim verzijama ovog programa, wbStego 2.x i 3.x, kao i četiri algoritma za jaku kriptografiju: *Blowfish, Twofish, CAST128, Rijndael (AES)*. Ovim se omogućava zaštita šifrom koja može imati i do 2 biliona karaktera, u ranijim verzijama do 256 karaktera. Ako se iskoristi jak algoritam za šifrovanje, ključ se generiše iz šifre korišćenjem heš algoritma SHA-1. Što je šifra duža i što više različitih karaktera i brojeva sadrži veća je sigurnost. Za šifrovanje je korišćen *Blowfish*, jak kriptološki algoritam koji koristi 160-bitni ključ za šifrovanje (*passphrase*[32]) i SHA-1 (*Secure Hash Algoritam*) u CBC (*Cipher Block Chaining*) modu.

[30] Prikaz stegonosioca dat je na slici 5.
[31] Prikaz tajne poruke (slike) dat je na slici 6.
[32] Relativno duga lozinka koja sadrži seriju reči kao što su fraze i pune rečenice


(a)


(b)

Slika 4. Tajna poruka „vojska 1.jpg"- (a) i izgled prozora wbStego programa u poslednjem koraku - (b)

Da bi se utvrdilo da li je na neku sliku primenjena steganografija, potrebno je izvršiti: *vizuelnu analizu, analizu promena u osobinama fajla, analizu heksadecimalnih podataka i analizu histograma*. *Vizuelnom analizom* ne mogu se uočiti razlike između stego nosioca i stego medijuma (slike 5 i 6), čak i kada se slika 6 uveća i posmatra nezavisno od slike 5.



Slika 5. Nosilac tajne poruke .bmp fromata



Slika 6. Steganografski medijum .bmp formata

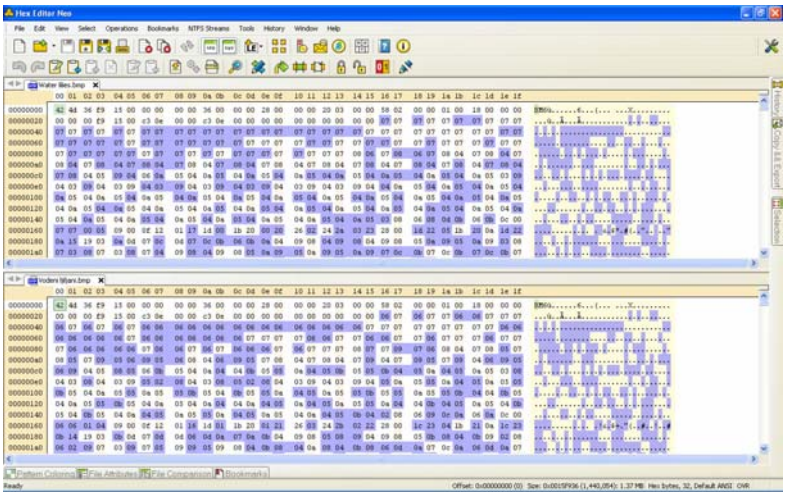
Promene u osobinama fajlova prikazane su u tabeli 1. Detekcija steganografije je u ovom slučaju je veoma teška. Jedan od razloga jeste taj što su softveri za detekciju u najvećoj meri osposobljeni za detekciju samo pojedinih digitalnih formata, kao i detekciju primene pojedinih steganografskih softvera. S obzirom na to da nakon primene steganografije, nije došlo do promene u veličini fajla, detekcija je teška čak i u slučaju da strana koja istražuje poseduje original.

Tabela 1. Osobine fajlova *.bmp* ekstenzije

Naziv fajla	Datum kreiranja	Vreme kreiranja	Veličina fajla
Water lilies.bmp	22/10/2009	12:02:03 pm	1,37 MB
Vodeni ljiljani.bmp	22/10/2009	12:05:12 pm	1,37 MB

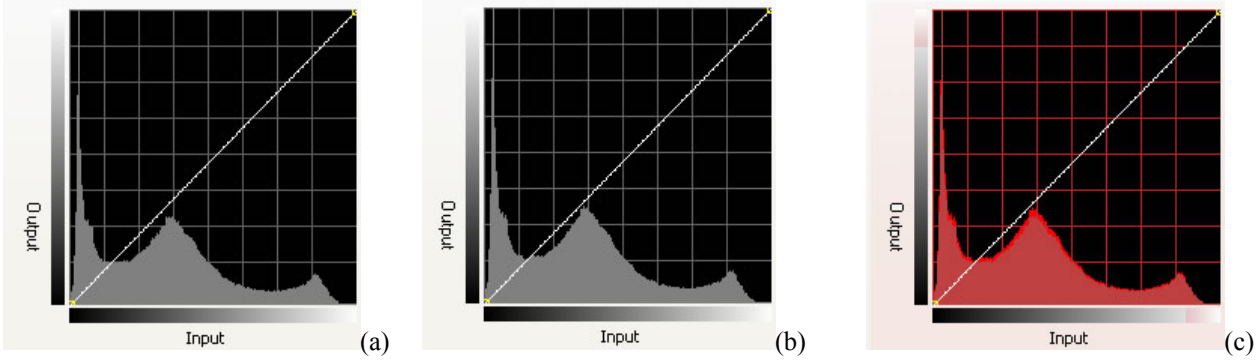
Analiza heksadecimalnih podataka ilustrovana je na slici 7, gde su predstavljene razlike u heksadecimalnom zapisu. Analiza je vršena u programu „Hex Editor Neo", upoređivanjem fajlova „Water lilies.bmp" i „Vodeni ljiljani.bmp". Plavom bojom su obeleženi bajtovi koji se razlikuju u fajlovima. U ovoj analizi prvi put nailazimo na čvrste dokaze da je na slici „Water lilies.bmp" primenjena steganografija. Treba napomenuti da je ovu analizu nemoguće izvršiti ukoliko osoba koja ispituje stego medijum ne poseduje original sliku, odnosno stego nosioca. Pored toga, u okviru

stegomedijuma identifikovan je format sakrivenog fajla kao *.bmp* format. Heksadecimalni zapis ovog formata je *42 4D*, dok je ASCII *BM*.



Slika 7. Razlika u bitovima između slike „Water lilies.bmp“ i „Vodeni ljiljan.bmp“

U *analizi histograma* (slika 8) upoređivani su histogrami stegonosioca i stego medijuma histograma koji su prikazani na slikama 8a i 8b. Preklapanjem histograma uočavamo razliku koja je na slici 8c predstavljena tamno crvenom bojom. Kao i u prethodnoj analizi heksadecimalnih podataka i ovu analizu je nemoguće sprovesti ukoliko ne posedujemo originalnu sliku, odnosno, stego nosioca.



Slika 8. Histogram slike „Water lilies.bmp“- (a), Histogram slike „Vodeni ljiljan.bmp“ - (b), Upoređivanje histograma slika „Vodeni ljiljani.bmp i „Water lilies.bmp“ – (c)

Iz prethodnih analiza sledi da je lako utvrditi da li je neka slika stegonosioc ukoliko nam je dostupna originalna slika. Problem se javlja kada u toku istrage ne posedujemo original, ili računar na kom je izvršen prestup. Dodatni problem kod ove analize predstavlja format slike **.bmp**, jer je većina softwera za detekciju steganografije usko specijalizovana za detekciju slika sa **.jpg** ekstenzijom. Da bi se u slikama drugih formata detektovala prisutnost tajne poruke, na te slike se može primeniti napad na

najmanje važne bitove (LSB napad). Postoji nekoliko podkategorija ovog napada, a s obzirom da nam je cilj da detektujemo primenjenu steganografiju, primenićemo ***hi-kvadrat*** test.

2.1. Hi-kvadrat test

Za LSB ugrađivanje, vrednost paranih piksela ostaje ili nepromenjena ili je podignuta za 1, dok je vrednost neparnih ili ostala nepromenjena ili je smanjena.

Neka $T_C[l], l = 0, \ldots, 255$ označava intenzitet histograma stego nosioca i T_s odgovarajući histogram stego slike nakon ugrađivanja qn bita, gde je n ukupan broj piksela i $0 \leq q \leq 1$. Iz ovoga sledi da ugrađujemo q bitova po pikselu (bpp-*bits per pixels*) ili da je q *relativma dužina poruke*.

Da bismo izračunali Ts kao funkciju od Tc i q pretpostavićemo da je poruka slučajni niz bitova, što je razumna pretpostavka ako je poruka šifrovana ili kompresovana. Očekivani broj piksela $2i$ će biti promenjen u $2i+1$ i iznosiće $\frac{q}{2}T_c[2i]$ iz razloga što će prosečno jedna polovina bitova već odgovarati najmanje važnim bitovima u pikselima. Slično tome, očekivani broj piksela $2i+1$ koji će biti promenjen u $2i$ je $\frac{q}{2}T_c[2i+1]$.

S toga, možemo napisati:

$$E[T_s[2i]] = \left(1 - \frac{q}{2}\right)T_c[2i] + \frac{q}{2}T_c[2i+1]$$

$$E[T_s[2i+1]] = \frac{q}{2}T_c[2i] + \left(1 - \frac{q}{2}\right)T_c[2i+1] \qquad \text{Jednačina 1}$$

Za ugrađivanje cele slike, gde je $q=1$, sledi da je $E[T_s[2i]] = E[T_s[2i+1]]$

Drugim rečima, histogramski intervali (*histograms bins*) $2i$ i $2i+1$ će imati približno jednaku vrednost i to će prouzrokovati promenu stepenika u histogramu.

Značajno je to da je suma $T_s[2i] + T_s[2i+1] = T_c[2i] + T_c[2i+1]$ invarijanta[33] LSB ugrađivanja. Teorijski očekivana vrednost za $T_s[2i]$ s toga iznosi $T_s[2i] = \frac{T_s[2i] + T_s[2i+1]}{2}$.

Iz ovoga sledi da je moguće detektovati ugrađivanje LSB metodom, za q+1, testiranjem da li je $T_s[2i] = T_s[2i+1]$.

Za testiranje možemo koristiti samo parne vrednosti piksela i primenićemo statistički test koji može potvrditi da parne vrednosti $T_s[2i]$ prate poznatu raspodelu $\overline{T}_s[2i]$. U ovom delu ćemo primeniti Parsonsov hi-kvadrat test da bi odredili da li je $T_s[2i] = \overline{T}_s[2i]$.

Hi-kvadrat test počinje izračunavanjem hi-kvadrat statistike S

$$S = \sum_{i=1}^{k} \frac{(T_s[2i] - \overline{T}_s[2i])^2}{\overline{T}_s[2i]} \qquad \text{Jednačina 2}$$

[33] Svojstvo ili vrednost koja pri datim transformacijama ostaje nepromenjena.

sa $(k-1)=127$ stepeni slobode.

Pretpostavimo da parne vrednosti piksela zaista prate verovatnoću iznosa funkcije $T_s[2i]$, statistički test, S, prati hi-kvadrat distribuciju sa $k-1$ stepenom slobode. U praksi je primećeno da slobodni intenziteti (*bins*) moraju biti dodati tako da $T_s[2i] > 4$ da bi se osiguralo da S bude približno hi-kvadrat distribuiran.

Male vrednosti S ukazuju da podaci prate očekivanu distribuciju i iz toga možemo zaključiti da slika sadrži poruku ugrađenu LSB metodom. S druge strane, visoke vrednosti statističkog testa ukazuju na to da nema ugrađene poruke.

Statistički značaj S je meren korišćenjem, tzv. *p-vrednosti*, koja predstavlja mogućnost da bi hi-kvadrat distribuiran slučajnom varijablom sa $k-1$ stepeni slobode dostigao vrednost veću ili jednaku S:

$$p(S) = \frac{1}{2^{\frac{k-1}{2}}\Gamma\left(\frac{k-1}{2}\right)}\int_{S}^{\infty} e^{-\frac{x}{2}} x^{\frac{k-1}{2}-1} dx$$

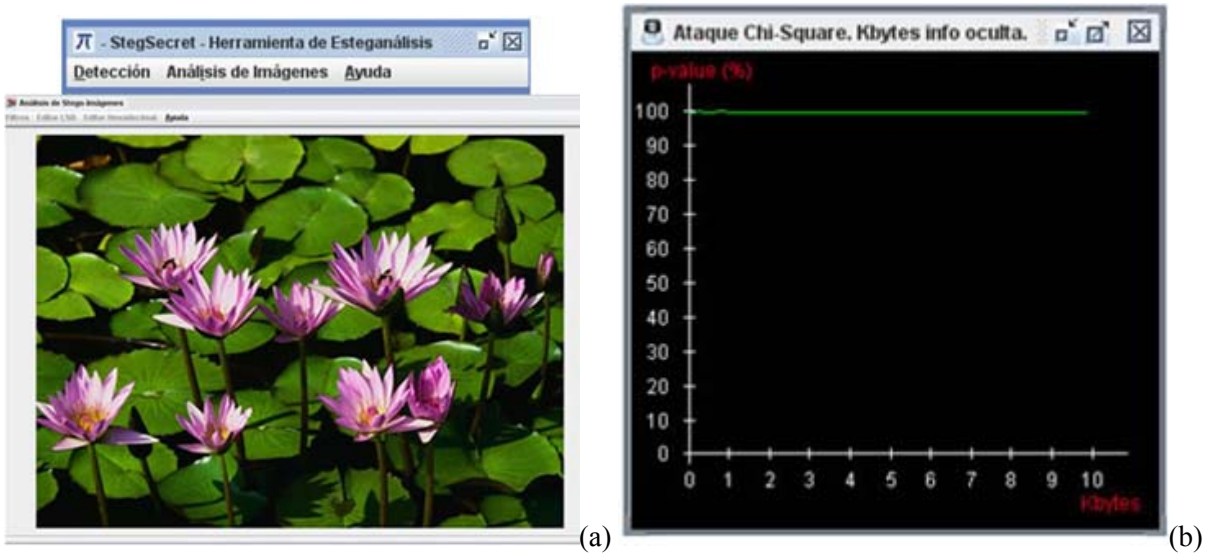
Jednačina 3

Ukoliko slika ne sadrži sakrivenu poruku, S je veliko, a $p(s)\approx 0$. U praksi, računamo prag vrednosti S_{th} tako da $p(S_{th})=\alpha$, gde je α izabran stepen važnosti. Za nivo pouzdanosti, á, odlučujemo da slika sadrži tajnu poruku ako $p(S)>\alpha$, ili, ekvivalentno tome, $S<S_{th}$.

Do sada smo razmatrali potpuno ugrađenu sliku sa $q=1$ bit po pikselu. Ako je stego slika ugrađivana sekvencijalno, ali ne u potpunosti, možemo skenirati stego sliku istim redom kojim smo ugradili poruku i izračunati p za set posećenih piksela. Nakon kratkotrajne inicijalne faze, p-vrednost će biti blizu 1 i uskoro će pasti na 0 kada stignemo na kraj poruke i ostaće na 0 dok ne potrošimo sve piksele. Do ovoga dolazi zbog toga što statistički test S prestaje da prati hi-kvadrat distribuciju. S toga, za sekvencijalno ugrađivanje ovaj test, pored toga što određuje, sa visokom verovatnoćom, da je nasumična poruka ugrađena, procenjuje dužinu ugrađene poruke. Ako su pikseli, koji su nosioci poruke u slici, selektovani pseudoslučajno, a ne sekvencijalno, ovaj test je neefikasan, osim ako je većina piksela zauzeta ugrađenom porukom.

Uz pomoć *freeware*[34] softvera XStegSecret.Beta.v0.1 izvršen je hi-kvadrat napad na sliku "Vodeni ljiljani.bmp". Na slici 9. je dat prikaz rezultata napada, iz čega se može zaključiti da je slika nosioc cele tajne poruke, jer je p-vrednost u najvećem delu grafikona 100% i njegova vrednost se pri kraju poruke ne bliži 0.

[34] stegsecret.sourceforge.net



(a) (b)

Slika 9. Rezultat Hi-kvadrat napada (b) na sliku „Vodeni ljiljani.bmp"(a)

2.2. Softver StegAlyzerSS

StegAlyzerSS **(***Steganography Analyzer Signature Scanner*) je najistaknutiji kompjuterski forenzički alat za istragu, detekciju, analizu i obnavljanje poruke u digitalnoj steganografiji. On forenzičarima omogućava skeniranje celog fajl sistema, pojedinačnih direktorijuma ili individualnih fajlova na prisustvo heksadicimalnih bajtova, ili potpisa određenih steganografskih aplikacija. Kada se detektuje poznati potpis, moguće je izvući sakrivenu informaciju uz pomoć StegAlzyerSS-a, ili korišćenjem udružene steganografske aplikacije. Pretraživanje potpisa i mogućnost automatskog izvlačenja tajne poruke nije moguće nekim drugim steganalitičkim softverom. Pored skeniranja fajlova slepom detekcijom (*blind detection*) ova aplikacija detektuje i potencijalne nosioce sakrivene poruke. StegaAlyzerSS alat koristi operativni system *Microsoft Windows XP Service Pack 2,* a vrši: detekciju sakrivenih korisnih podataka korišćenjem pretrage bazirane na potpisu i sakrivenih korisnih podataka korišćenjem dodatne analize; identifikaciju potencijalnih fajlova nosioca osetljivih na modifikaciju LSB. Za analizu slučaja korišćeni su softveri: *Microsoft Word 2003 Service Pack 3, Microsoft Paint verzija 5.1 Service Pack 2, Microsfot Notepad verzija 5.1 Service Pack 2, WinHex v.11.0, CrypArkan v.1.0, InPlain View v.1.0, wbStego4 v.4.2 / wbStego 4.3 open, wbStego v2.0 / wbStego 2.1, JPegX v.1.00.6, Camouflage v.1.0.4, Camouflage v.1.1.2, Camouflage v.1.2.1, Cloak v.7.0, Data Stash v.1.1, Data Stash v.1.1b, Data Stash v.1.0, Hiderman.* Od hardvera korišćen je*: Gateway E4200, 128MB RAM, Jabil Pentium III BX Motherboard, BIOS Revision P21 i Quantum Fireball Ict10 20GB Hard Drive.*

Analiza ovom aplikacijm detektovala je slike "Vodeni ljiljani.bmp" i "Water lilies.bmp", kao fajlove koji su osetljivi na LSB modifikaciju, što potvrđuje prethodno testiranje hi-kvadrat testom. Problem koji se javlja jeste što *StegAlyzerSS* nije pronašao potpis korišćenog steganografskog alata iako se program *wbStego4 v.4.3* nalazi na listi programa čiji potpis ovaj alat treba da identifikuje.

3. ZAKLJUČCI

1. Steganografija je veoma pouzdana antiforenzička tehnika. Ukoliko se isprate svi zahtevi koje je potrebno da jak steganografski metod ispuni, detekcija je veoma otežana, čak i onemogućena, ako jei skrivena poruka manje od 5% veličine stegonosioca i ako je primenjen jak algoritam.
2. Većina steganografskih alata radi po principu promene LSB, što je jedna od pogodnosti za detekciju primenjene steganografije, pošto većina detektora radi na principu ispitivanja promene i upoređivanja bitova, pa je procenat pozitivne detekcije samim tim veći.
3. Nedostatak većine detektora je što su usko specijalizovani za detekciju tajnih poruka u slikama *.jpg* formata, pa slike drugih formata, poput *.bmp* ili *.gif* mogu proći kroz detektor neidentifikovane kao stegomedijumi. Razumljivo je što su detektori usmereni na detektovanje najzastupljenijih slika na Internetu - *.jpg* formata. Prednost *.bmp* formata je da se u njega može sakriti veća poruka ukoliko za tim postoji potreba.
4. Detekcija steganografije je laka ukoliko postoje dustupna originalna slika i zaplenjen računar. Ukoliko se radi o detekciji u okruženju Interneta, naivna je pretpostavka da će stego nosioc biti dostupan. Dovoljno je samo promeniti mu naziv i tu se mogućnost upoređivanja stegomedijuma i stegonosioca gubi. Ukoliko je dostupan stegonosioc, forenzičar može izvršiti: *vizuelnu analizu, promene u osobinama fajla, analizu heksadecimalnih podataka i analizu histograma.* Vizuelnom analizom nemoguće je detektovanje skrivene poruke u studiji slučaja, jer je kao stegonosioc izabrana slika sa velikim brojem boja i mnogostrukim prelazima. Analizom promena u osobinama fajlova, u *studiji slučaja* nije dobijen podatak da postoji sakrivena poruka, jer se veličine fajlova slažu u bajt. Analizom heksadecimalnih podataka došlo se do prve naznake u *studiji slučaja* da postoji sakrivena poruka, jer se upoređivanjem bajtova vidi da se razlikuje dosta velik broj bajtova. Analiza histograma je u *studiji slučaja* pokazala da je u stegonosicu sakrivena tajna poruka, jer se preklapanjem histograma pokazalo da postoje statističke anomalije.
5. Detektori „Stegdetect“ i „StegSpy V2.1“ su propustili da identifikuju sliku „Vodeni ljiljani.bmp“ kao stegomedijum i ovim je dokazano da *.bmp* format, iako veći, nudi dobru mogućnost za sakrivanje tajne poruke. Detektorom „StegAlyzerSS“ je uspešno detektovano postojanje tajne poruke u fajlu „Vodeni ljiljani.bmp“. Nedostatak free verzije ovog detektora je što, iako po specifikaciji detektuje potpis programa wbStego4, ovaj korak nije uspešno sproveden. Konsultacijom sa osobom iz Centra za analizu i istrazivanje u Sarc-u , izvršeno je ponovno testiranje StegAlyzerSS-a, nakon čega su utvrdili da ovaj program zaista ne moze da detektuje deeklarisan poptis wbStego4 softvera i da samo detektuje tekstualne fajlove u okviru slike kada je steganografija primenjena pomocu programa wbStego4. Primenom ovog softvera je, i pored njihove tvrdnje, detektovan slikovni format sakriven u slikovnom nosiocu, kao i potencijalni stegonosioc, ali zbog nedostataka informacija o tome koji je steganografski program korišćen, nije moguće izvući tajnu poruku iz fajla „Vodeni ljiljani.bmp“.
6. Ukoliko forenzičaru nije dostupan stegonosioc, a nije mu poznato da li je u nekom fajlu sakrivena tajna poruka, potrebno je izvršiti više testova da bi se stekao uvid u postojanje stegomedijuma. Postoji više vrsta testova. U *studiji slučaja* je primenjen hi-kvadrat LSB test. Ova statistika prvog reda, meri vrednost suvišnih informacija i/ili deformaciju u medijumu i može doprineti prognozi - da li je sadržaj menjan ili je sumnjiv. Rezultati ispitivanja su pokazala da se promene na LSB, gde se inače implementira tajna poruka, vrlo jasno uočavaju, te da je p-vrednost, koja pokazuje procenat prognoze zastupljenosti tajne poruke, 100% u najvećem delu grafikona.
7. Na osnovu rezultata ovog istraživanja može se zaključiti da je sakrivanje tajne poruke u *.bmp* formatu mnogo delotvornije i mnogo teže za detektovanje u odnosu na *.jpg* format.

4. LITERATURA

1. Arnold, M., Schmucker, M., and Wolthusen, S. D., *Techniques and Applications of Digital Watermarking and Content Protection*. Artech House, Norwood, Massachusetts, 2003. Dostupno na: http://www.fbi.gov/cgi-bin/outside.cgi?http://www.warchalking.org/
2. Artz, D., *Digital Steganography: Hiding data within data*, ***IEEE Internet Computing*** 5(3):75-80. Dostupno na: http://www.cc.gatech.edu/classes/AY2003/cs6262_fall/digital_steganography.pdf, (2001).
3. Bauer, F. L. *Decrypted Secrets: Methods and Maxims of Cryptology*, 3rd ed. Springer-Verlag, New York, 2002.
4. Chandramouli R., *Mathematical approach to steganalysis*, In: ***Proceedings of the SPIE Security and Watermarking of Multimedia Contents IV***, vol. 4675. International Society for Optical Engineering, San Jose, California, January 21-24, pp. 14-25. Dostupno na : http://www.fbi.gov/cgi-bin/outside.cgi?http://www.ece.stevens-tech.edu/%7Emouli/spiesteg02.pdf, 2002
5. "*Classical Steganography, Cardano Grille*", Dostupno na: http://library.thinkquest.org/27993/crypto/steg/classic1.shtml
6. Curran, K., *An evaluation of image based steganogrphy metods, International journal of digital exidence*, knjiga 2., izdanje 2, decembar 2003. Dostupno na: http://www.fbi.gov/cgibin/outside.cgi?http://www.morecrayons.com/palettes/webSmart/colorcube.php.
7. Curran, K. and Bailey, K., *An evaluation of image-based steganography methods*. ***International Journal of Digital Evidence*** [Online]. (Fall 2003). Dostupno na: http://www.fbi.gov/cgi-bin/outside.cgi?http://www.ijde.org/docs/03_fall_steganography.pdf.
8. Чековский, С., Овсянников В., *Скрытая утечка информации*, ЕПОС публикации : Информационная безопасностъ, 2002.
9. Farid, H., *Detecting Steganographic Messages in Digital Images,* Technical Report TR2001-412, Dartmouth College, Computer Science Department, 2001. Dostupno na : http://www.cs.dartmouth.edu/~farid/publications/tr01.pdf.
10. Fridrich, J. and Du, R., *Secure steganographic methods for palette images,* In: ***Proceedings of the 3rd Information Hiding Workshop,*** Lecture Notes in Computer Science, vol. 1768. Dresden, Germany, September 1999. Springer-Verlag, Berlin, Germany, 2000, pp. 47-60. Dostupno na : http://www.fbi.gov/cgi-bin/outside.cgi?http://www.ws.binghamton.edu/fridrich/Research/ihw99_paper1.dot.
11. "*Hidden in Plain Sight-Steganography*",Counterintelligence News and Developments, Izdanje 2, Jun 1998. Dostupno na: www.nacic.gov/pubs/news/1998/jun98.htm
12. Home and Garden Television, "*Clues in the Quilts*". Dostupno na: http://www.hgtv.com/HGTV/project/0,1158,CRHO_project_7305,00.html
13. http://www.en.wikipedia.org/wiki/Nazca_Lines
14. Jackson, J. T., Gregg, H., Gunsch, G. H., Claypoole, R. L., and Lamont, G. B., *Blind Steganography detection using a computational immune system: A work in progress*, ***International Journal of Digital Evidence*** [Online], (Winter 2003) (December 21, 2003). Dostupno na: http://www.fbi.gov/cgibin/outside.cgi?http://www.ijde.org/docs/02_winter_art4.pdf
15. Johnson, N. F. and Jajodia, S., *Exploring steganography: Seeing the unseen*, ***Computer*** (1998A) 31(2):26-34, Dostupno na : http://www.fbi.gov/cgibin/outside.cgi?http://www.jjtc.com/pub/r2026.pdf.
16. Kahn, D., *Codebreakers: The Story of Secret Writing*, Revised ed., Scribner, New York, 1996.
17. Petitcolas, F. A. P., "*History of Steganography*", Dostupno na: www.cl.cam.ac.uk/~fapp2/steganography/history.html

18. Seward, J., *Debtor's digital reckonings*, ***International Journal of Digital Evidence***, Fall 2003 [Online]. (Januar 3, 2004). Dostupno na : http://www.fbi.gov/cgi-bin/outside.cgi?http://www.ijde.org/docs/03_fall_seward.pdf.
19. Simmons, G.J., *The Prisoner`s Problem and the Subliminal Chanel*, In: Proceedings of CRYPTO ` 83, 1984.
20. Singh, S., "*The Cipher of Mary Queen of Scots*" , Dostupno na: www.arch.columbia.edu/DDL/cad/A4513/S2001/r9/
21. "*The Science of Secrecy, Steganography*". Dostupno na : http://www.channel4.com/plus/secrecy/page1b.html
22. Trithemius, J., "*Steganographia:hoe est ars per occultam scripturam animi sui voluntatem absentibus aperiendi certa*". Dostupno na: http://www.esotericarchives.com/tritheim/stegano.htm
23. Wayner P., *Disappearing Cryptography: Information Hiding: Steganography & Watermarking 2nd. ed*., Morgan Kaufmann, San Francisco, California, 2002.