Analiza metoda steganografske zaštite podataka

Kuran, Toni

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI

Toni Kuran

ANALIZA METODA STEGANOGRAFSKE ZAŠTITE PODATAKA

ZAVRŠNI RAD

Zagreb, rujan 2015.

Sveučilište u Zagrebu
Fakultet prometnih znanosti

ZAVRŠNI RAD

ANALIZA METODA STEGANOGRAFSKE ZAŠTITE PODATAKA

ANALYSIS OF STEGANOGRAPHIC DATA PROTECTION METHODS

Mentor: dr. sc. Ivan Grgurević
Student: Toni Kuran, 0135212325
Datum obrane: 15. rujna 2015.

Zagreb, rujan 2015.

ANALIZA METODA STEGANOGRAFSKE ZAŠTITE PODATAKA

SAŽETAK

U završnom radu analiziraju se metode steganografske obrade podataka. Izlaganje teme započinje povijesnim pregledom steganografskih tehnika obrade podataka. Objašnjavaju se razlike između steganografije i kriptografije, a zatim se obrađuju osnovni pojmovi koji čine steganografski sustav. Na primjeru „problema zatvorenika“ detaljno se opisuje princip rada steganografije. Na to se nastavljaju steganografske tehnike koje su razdijeljene i objašnjene te se opisuju načini skrivanja poruke u digitalni nositelj. Zatim se dolazi do glavnog dijela rada u kojem se opisuju steganografske metode s obzirom na medij kojim se stego poruka prenosi. U završnom dijelu rada opisuje se stegoanaliza te se programskim alatima *StegSpy*i *Digital InvisibleInkToolkit* na konkretnim primjerima prikazuje kodiranje, dekodiranje i stegoanaliza tajne poruke.

KLJUČNE RIJEČI: steganografija; steganografske tehnike; steganografske metode

SUMMARY

The final paper analyzes the methods of steganographic data processing. Topic presentation begins with historical overview of steganographic techniques of data processing.The differences between steganography and cryptography are explained, and basic concepts that make steganographic system are then discussed. Using the example of “inmates problem” the working principle of steganography is described in detail. Steganographic techniques build on it, those that are separated and explained, and describe ways of hiding messages into digital carriers. That leads to the main part of the paper which describes steganographic methods based on the medium through which stego-message is transmitted. In the final part of the paper stego-analysis is described and programming tools, StegSpy and Digital InvisibleInkToolkit, show concrete examples of encoding, decoding and analysis of stego-secret messages.

KEYWORDS: steganography; steganographic techniques; steganographic methods

SADRŽAJ

1. Uvod 1
2. Općenito o steganografiji 3
3. Obilježja steganografske obrade podataka 6
4.Pregled steganografskih tehnika 10
4.1. Ubacivanje 13
4.2. Zamjena 13
4.3. Generiranje novih datoteka 14
4.4. Ostale digitalne tehnike 14
5. Pregled steganografskih metoda 15
5.1. Tekstovni zapis 15
5.2. Zvučni zapis 16
5.3. Slikovni zapis 17
5.3.1. Metode prostorne domene 18
5.3.1.1. Supstitucija bita najmanje važnosti – LSB metoda 19
5.3.1.2. Sortiranje paleta 20
5.3.2. Metode transformacije domene 21
5.3.3. HTML metoda 22
6. Analiza steganografskih tehnika i metoda zaštite podataka 24
6.1. Stegoanaliza 24
6.1.1. Oblici napada 26
6.1.2. Osnovne tehnike steganalize 26
6.1.2.1. Neobični uzorci 27
6.1.2.2. Vizualna detekcija 27
6.2. *StegSpy* 28
6.3. *Digital Invisible Ink Toolkit* 29
6.3.1. Kodiranje u DIIT-u 29
6.3.2. Dekodiranje u DIIT-u 31
6.3.3.Analiza u DIIT-u 34
7. Zaključak 36
Literatura 38
Popis kratica i akronima 40
Popis slika i tablica 42

1. Uvod

Povećanjem broja korisnika Interneta povećao se i problem sigurnog prijenosa informacija na daljinu. Informacija se može zaštiti kriptiranjem, ali je kao takva vidljiva trećim osobama i samim time izaziva znatiželju i opasnost od napada.Većina kriptoloških tehnika ranjive su na hakerske napadete uvijek postoji mogućnost curenja i otkrivanja informacija. Drugi način sigurnog prijenosa informacija je steganografija. Informacija se sakrije unutar objekta koji nosi nekakvu informaciju definiranog sadržaja te se prenosi mrežom, a da neovlaštene osobe nisu niti svjesne skrivene poruke. Osim navedenog, postoje programski alati koji kombiniraju tehnike kriptografije i steganografije, a isti će biti prikazani na konkretnim primjerima.

Svrha pisanja ovog završnog rada je autorova motiviranost i intrigiranost skrivenim prijenosom informacija. Cilj je približiti i prikazati prednosti korištenja steganografije te analizirati steganografske tehnike i metode obrade podataka, a sam naslov završnog rada je **Analiza metoda steganografske zaštite podataka**.

Rad je podijeljen u sedam cjelina:

1. Uvod,
2. Općenito o steganografiji,
3. Obilježja steganografske obrade podataka,
4. Steganografske tehnike,
5. Steganografske metode,
6. Analiza steganografskih tehnika i metoda zaštite podataka,
7. Zaključak.

Uvodno poglavlje daje osnovnu sliku o radu te definira cilj i strukturu rada.

U drugom poglavlju pod nazivom *Općenito o steganografiji*opisani su temeljni pojmovi te su navedene najpoznatije primjene steganografije kroz povijest.

Treće poglavlje pod nazivom *Obilježja steganografske obrade podataka* opisuje način prijenosa informacija u steganografskom sustavu te je na primjeru „problema zatvorenika“ prikazan steganografski sustav.

U četvrtom poglavlju pod nazivom *Steganografske tehnike*opisane su steganografske tehnike te je predočena podjela po CERT-u i G.Kipperu.

Peto poglavlje pod nazivom *Steganografske metode* opisuje steganografske metode s obzirom na medij kojim se prenosi odnosno metode umetanja podataka u tekstovni, zvučni i slikovni zapis.

Šesto poglavlje pod nazivom *Analiza steganografskih tehnika i metoda zaštite podataka* opisuje steganografsku analizu, te na konkretnim primjerima prikazuje princip rada steganografksih alata *StegSpy* i *Digital Invisible Ink Toolkit*.

Na temelju prezentiranih činjenica iz prethodnih poglavlja/teza, donesen je zaključak u kojem su ukratko prikazani glavni rezultati završnog rada.

2. Općenito o steganografiji

Steganografija je znanstvena disciplina koja se bavi skrivanjem informacija. Riječ steganografija dolazi od grčkih riječi *steganos* i *graphein*, što u doslovnom prijevodu znači skriveno pisanje. Steganografskim tehnikama tajna se poruka skriva unutar neke druge bezazlene poruke tako da se postojanje tajne poruke ne može uočiti.[1] Steganografija je vrlo slična kriptografiji, obje znanosti se koriste kao sredstva koja prikrivaju informaciju. No za razliku od kriptografije, steganografija ne mijenja samu informaciju, nego ju kamuflira i samim time ne privlači pažnju na nju. Kriptirana informacija, koliko god dobro kriptirana, vidljivo postoji, te budi sumnju i radoznalost. Cilj kriptografije je promijeniti informaciju do te mjere da je ona nerazumljiva trećoj strani, a cilj steganografije je učiniti informaciju nevidljivom trećoj strani. [2]

Premda je pojam steganografija formiran tek krajem 15. stoljeća,[3] najstariji slučaj korištenja steganografije je zabilježen u antičkog Grčkoj (oko 440. godine prije Krista) kada su Grci željeli pokrenuti pobunu protiv Perzije. Grk *Histiaeus* naredio je da se jednom robu obrije tjeme kako bi na njega tetovirali tajnu poruku. Tek kada je robu narasla kosa, poslan je Miletskom kralju *Aristagorasu* koji je ponovno morao obrijati glavu kako bi pročitao tajnu poruku.[4]

Slijedi pregled najpoznatijih primjena steganografije kroz povijest:

- Voštane pločice - u antičkoj Grčkoj su se voštane pločice (komadi drveta preliveni voskom) obično koristile za pisanje. Ali, da bi jedan drugome prenijeli tajnu poruku, Grci bi odstranili vosak s pločice, napisali poruku direktno na drvo te ponovno nanijeli vosak na pločicu. Takva voštana pločica doimala se praznom i neupotrijebljenom pa nije privlačila pažnju prilikom inspekcije. Na taj način je navodno *Demeratus* obavijestio Spartu da *Xerxes* namjerava napasti Grčku.

- Poruke na glasnikovom tijelu - osim voštanih pločica, stari Grci skrivali su poruke i na tijelima svojih glasnika. Tako su na primjer običavali tetovirati svoju tajnu poruku na obrijanu glasnikovu glavu. Kada bi njegova kosa ponovno narasla, poruka je bila uspješno sakrivena te se mogla pročitati samo ponovnim brijanjem glasnikove glave. Najpoznatija priča o opisanoj tehnici skrivene komunikacije odnosi se na upozorenje Grčkoj o perzijskim ofenzivnim planovima.

- Nevidljiva tinta - prvi primjeri korištenja nevidljive tinte datiraju iz razdoblja 2. svjetskog rata, ali s jednakim uspjehom nevidljiva tinta koristila se i do dan danas. U naizgled bezazleno pismo umetala se tajna poruka – ispod vidljivog teksta, između redaka ili na nekim drugim praznim površinama papira. Tinta kojom je tajna poruka bila napisana spravljala se od mlijeka, octa, voćnih sokova ili urina. Sve navedene supstance imale su isti efekt – tamnjenje prilikom zagrijavanja. Uslijed razvoja tehnologije i sve češćih pojava razotkrivanja poruka pisanih nevidljivom tintom, osmišljene su sofisticiranije tinte koje postaju vidljive tek nakon reagiranja na različite kemijske sastojke. Detekcija i čitanje takvih poruka komplicirano je jednako kao i razvijanje fotografija u specijaliziranim laboratorijima.

- Mikrofotografije/mikrotekst - tijekom 2. svjetskog rata, špijuni su koristili mikrofotografije i mikrotekst za prosljeđivanje važnih informacija. Mikrofotografija/ mikrotekst obično je veličine i oblika točke (kao npr. točka u slovima 'i' i 'j') pa kao takvi nisu uočljivi niti čitljivi bez optičkih povećala. Ipak, takvi mikro oblici morali su biti ucrtani posebnom tintom koja se mogla primijetiti ako bi se papir prinio svjetlu ili zakrenuo pod specifičnim kutom.

- Nulta šifra - tajna poruka je zamaskirana unutar druge poruke koja se doima bezazleno i ne privlači pozornost. Jedan od najpoznatijih primjera primjene opisane metode vezan je uz japansku špijunku *Velvalee Dickinson*, poznatiju pod imenom *Doll Woman* (žena lutka). *Velvalee* se tijekom 2. svjetskog rata bavila prodajom i nabavom lutaka, pa je često slala pisma iz New Yorka u neutralnu Južnu Ameriku koja su sadržavala narudžbe za lutke. Dotični tekst narudžbi je zapravo sadržavao sakrivene informacije o kretanjima brodova.[3]

Jedan od najpoznatijih primjera lingvističke steganografije su dva telegrama upućena iz SAD-a u Europu tijekom prvog sjetskog rata. U oba slučaja tekst izgleda kao kratki novinski izvještaj, ali izoliranjem prvog (u prvom telegramu) ili drugog slova (u drugom telegramu) formira se rečenica koja govori o datumu i mjestu isplovljavanja ratne flote.[5]

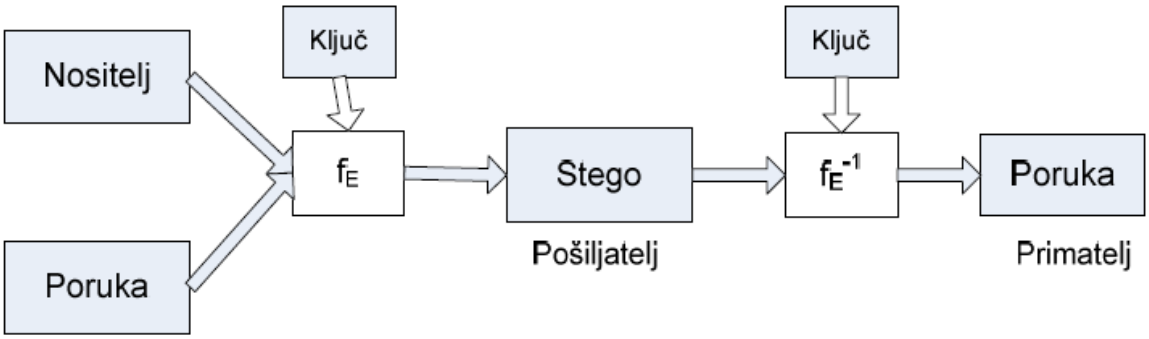
S razvojem digitalne tehnologije i sve većom količinom podataka koji se pohranjuju na računalima i razmjenjuju preko računalnih mreža, steganografija je također ušla u novo doba.[3] Zbog digitalnog formata zapisa podataka, moguće je korištenjem steganografskih aplikacija u strukturu jednog tipa podataka ubaciti dodatne podatke. Zbog strukture zapisa datoteke audio i video zapisi su povoljniji za steganografsku obradu nego tekst ili izvršna

datoteka. Razvija se velik broj različitih steganografskih algoritama koji su specijalizirani za obradu određenog tipa podataka (audio, tekst, izvršne datoteke, datotečni sustav i sl.),[6] od kojih su slike i zvučni zapisi ipak su najuobičajeniji nositelji u kontekstu steganografije.[3] Bez obzira na povijesno razdoblje, steganografska obrada podataka nastoji ispuniti osnovnu zadaću – sakriti postojanje tajne poruke od svakoga kome nije namijenjena.[7]

3. Obilježja steganografske obrade podataka

Steganografija podrazumijeva prikrivanje tajne poruke, ali ne i činjenice da dvije strane međusobno komuniciraju. Stoga proces steganografije obično uključuje umetanje tajne poruke unutar nekog prijenosnog medija koji se u tom slučaju naziva nositelj i ima ulogu prikrivanja postojanja tajne poruke. Nositelj mora biti takav skup podataka koji je sastavni dio uobičajne svakodnevne komunikacije te kao takav ne privlači posebnu pozornost na sebe, npr. tekst, slika, audio ili videozapis. Cjelina sačinjena od tajne poruke i nositelja unutar kojeg je ta poruka ugniježđena, naziva sesteganografski medij ili stego. U svrhu dodatne zaštite, moguća je i uporaba steganografskog ključa kojim se tajna poruka kriptira prije umetanja u nositelj.

Prema [3]steganografski medij se može prikazatiu sljedećem obliku:



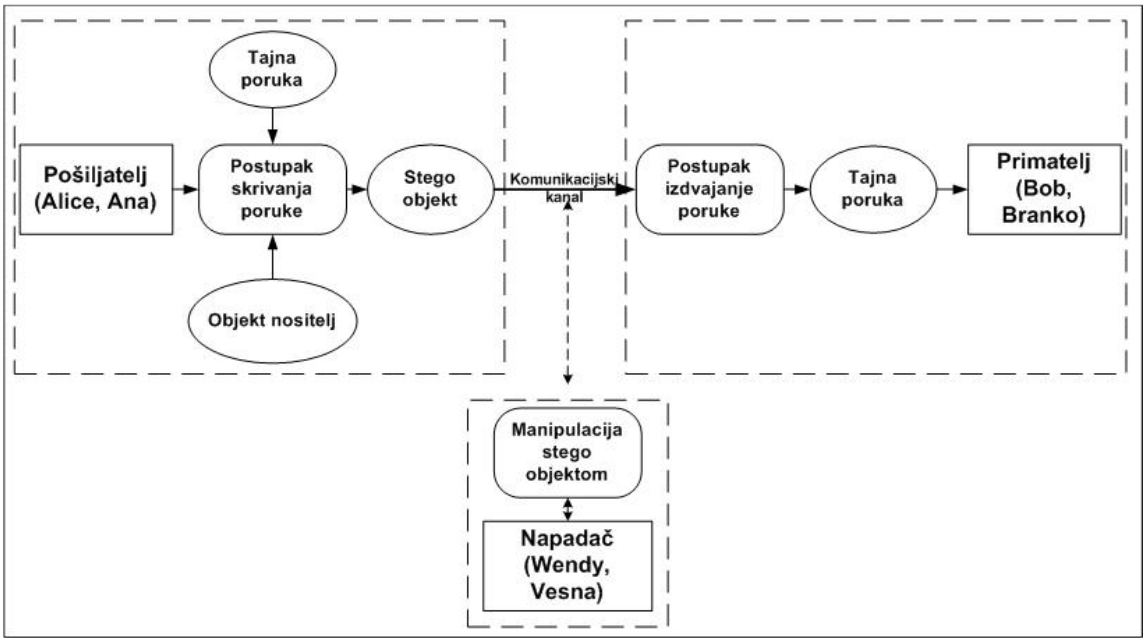
Slika 1. Shema steganografskog sustava, [3]

Pojašnjenje pojmova s prethodne slike koji čine dio steganografskog sustava:

- f_E : steganografska funkcija "ugrađivanje",
- f_E^{-1}: steganografska funkcija "izdvajanje",
- nositelj: medij unutar kojeg se sakriva tajna poruka,
- poruka: tajna poruka koja treba biti sakrivena,
- ključ: steganografski ključ; parametar funkcije f_E,
- stego: steganografska datoteka.[3]

Osim navedenog prikaza steganografskog sustava, prema [2] i [8] steganografski sustav je predočen jednostavnim primjerom nazvanim „problem zatvorenika“.

Neka su Ana (Alice) i Branko (Bob) zatvorenici koji planiraju bijeg iz zatvora i neka je Vesna (Warden) upravitelj zatvora. Nadalje, neka se Ana i Branko nalaze u različitim dijelovima zatvora tako da mogu komunicirati samo pisanim porukama koje kontrolira Vesna. Kako bi se dogovorili o bijegu, Ana i Branko moraju slati poruke koje nisu sumnjivog sadržaja, tj. trebaju koristiti tehnike steganografije. Vesna, koja kontrolira izmjenu poruka, može pri tome pokušati odgonetnuti postoji li kakav sumnjivi sadržaj u njihovim porukama, ali i namjerno ili nenamjerno, mijenjati sadržaje njihovih poruka. Sam pokušaj otkrivanja sumnjivog sadržaja predstavlja pasivni napad, dok mijenjanje sadržaja poruke predstavlja aktivni napad. Vesna može i krivotvorenu poruku predati Ani ili Branku. Takav napad se zove zlonamjeran napad.



Slika 2. Shematski prikaz steganografskog sustava, [2]

Steganografski sustav je prikazan na slici 2. Pošiljatelj (Alice, Ana) šalje primatelju (Bob, Branko) tajnu poruku. Pošiljatelj postupkom skrivanja poruke umeće tajnu poruku u objekt nositelj i time se dobije stego objekt. Stego objekt se prenosi komunikacijskim kanalom do primatelja. Primatelj postupkom izdvajanja poruke dobiva tajnu poruku. U shematskom prikazu postoji i treća osoba zvana napadač (Wendy, Vesna). Napadač ima mogućnost manipulacije stego objektom. On može biti pasivan i samo prisluškivati komunikacijski kanal

ili aktivan i uz prisluškivanje kanala, modificirati stego objekt. Također, napadač može i krivotvorene poruke slati sudionicima komunikacije. Cilj napadača je otkriti sadrži li objekt koji se šalje komunikacijskim kanalom skrivene informacije. U slučaju da napadač otkrije postojanje tajne poruke, on ju može pokušati izdvojiti ili narušiti stego objekt tako da se izgubi tajna poruka.

Postupak skrivanja, odnosno izdvajanja poruke, može biti tajan ili javan. Ukoliko je postupak javan, često se koristi dodatni ključ koji određuje točan slijed umetanja poruke. Taj ključ se razmijeni sigurnim kanalom. Time se izbjegava da napadač jednostavno dođe do skrivene poruke.[2] Steganografski ključ je lozinka koja može biti izvedena kao datoteka ili kao parametar koji korisnik mora upisati kako bi integrirao i ekstrahirao podatke. U većini slučajeva radi se o lozinci u tekstualnom obliku koja se koristi za kodiranje tajne poruke.[7] Osim toga se sama poruka može kriptirati nekim kriptografskim algoritmom čime se postiže dodatna sigurnost u očuvanju tajnosti poruke. Bitno je istaknuti da je osnovni cilj napadača detektirati skrivenu poruku, a ne ju nužno i pročitati. Naime, pretpostavlja se da napadač ima mogućnost manipulacije stego objektom. Stoga on može narušiti komunikaciju primatelja i pošiljatelja i samom izmjenom stego objekta.[2]

Koliko je neki steganografski sustav siguran ovisi o tome koliko se dobro odupire pasivnim, aktivnim i zlonamjernim napadima. Steganografski sustav je robustan ukoliko se skrivena informacija može izmijeniti tek "većim" izmjenama stego objekta. Siguran steganografski sustav ispunjava četiri uvjeta:

- Algoritam skrivanja je javan, ali koristi se tajni ključ,
- Samo onaj tko posjeduje tajni ključ može detektirati, izvaditi i dokazati postojanost tajne poruke. Nitko drugi ne može otkriti nikakav statistički trag o postojanju tajne poruke,
- Čak i kada napadač poznaje sadržaj jedne prenesene poruke, mala je vjerojatnost da će odgonetnuti sadržaj preostalih poruka,
- Detekcija tajne poruke je računalno prezahtjevna.[4]

Iako steganografski sustav koji ima javni algoritam skrivanja, a ne koristi tajni ključ, nije siguran, ponekad je on zadovoljavajući. To se odnosi na sustave koji raspolažu s ogromnom količinom informacija pa se ne mogu analizirati svi objekti nositelji informacija. U tom slučaju nepostojanje ključa može biti i olakotna okolnost s obzirom da nije potrebno prenijeti tajni ključ između sudionika komunikacije.[2]

Steganografiju je moguće detektirati statistički, percepcijom korisnika ili komparacijom sa originalnim zapisom (promjenama u veličini, vremenu i datumu, kontrole sume ili samog sadržaja transportne poruke). Prilikom steganografske obrade cilj je osigurati takvu integraciju podataka da neupućeni korisnik može percipirati i koristiti prijenosnu datoteku, a da za integrirane podatke ne zna da postoje. [7]

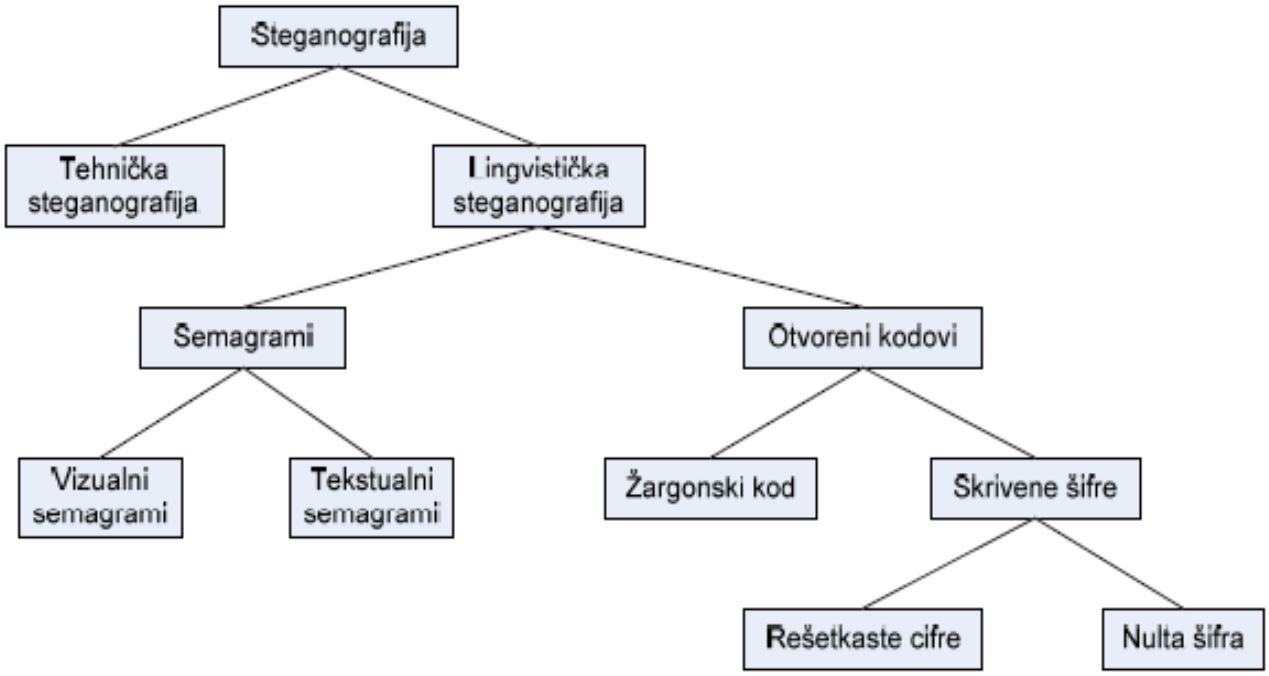
Važno je uočiti da se steganografija u bitnome razlikuje od kriptografije. Naime, kod kriptografije se tajnost poruke postiže modifikacijom poruke odnosno nerazumljivošću sadržaja za treće osobe, dok se kod steganografije tajnost poruke postiže njezinim skrivanjem. Također, bitno je naglasiti da postoje razlike između digitalne steganografije i digitalnog vodenog žiga. Digitalna steganografija ima zadatak skrivenog prijenosa tajne poruke kroz digitalni medij, dok se digitalni vodeni pečat koristi za označavanje digitalnog signala.[2]

4.Pregled steganografskih tehnika

Nakon što su opisane neke od osnovnih tehnika steganografije kroz povijest te princip rada steganografije, slijedi prikaz digitalnih steganografskih tehnika.

Sa znanstvene strane, steganografija se može podijeliti na tehničku i lingvističku. Tehnička se bavi metodama za otkrivanje steganografskog uzorka u pisanom tekstu ili mikrofilmovima, dok lingvistička steganografija obuhvaća tehnike skrivanja podatka u datoteci na način da originalna datoteka bude vjerodostojna stego-datoteci.[9]

Na slici 3 Pregled steganografskih tehnika, prikazana je taksonomija steganografskih tehnika:



Slika 3. Pregled steganografskih tehnika, [3]

Prema[3]steganogafske tehnike dijele se na:

- Tehnička steganografija - koristi znanstvene metode zaskrivanje poruka, kao što su uporaba nevidljive tinte, mikrofotografija i ostale tehnike smanjivanja veličine tajne poruke.

- Lingvistička steganografija - obuhvaća sve tehnike koje skrivaju tajnu poruku unutar nositelja na način da nositelj djeluje kao bezazleni skup informacija. Dotična grana steganografije dalje se dijeli na semagrame i otvorene kodove.

- Semagrami - skrivaju informacije uporabom različitih simbola i znakova. Postoje vizualni i tekstualni semagrami.

- Vizualni semagrami - baziraju se na principu skrivanja poruke uporabom bezazlenih i svakodnevnih fizičkih objekata, npr. specifičnim razmještajem predmeta na stolu ili objekata na web stranici.

- Tekstualni semagrami - skrivaju informacije različitim modifikacijama teksta nositelja, npr. suptilna promjena veličine ili tipa fonta, dodavanje suvišnih razmaka ili korištenje različitih ukrasa u rukopisu.

- Otvoreni kodovi - uključuju sve tipove prijenosa tajne poruke u kojima se koristi legitimna poruka nositelj koja igra ulogu javne, tj. neskrivene komunikacije. Otvoreni kodovi dijele se na žargonski kod i skrivene šifre.

- Žargonski kod - podrazumijeva korištenje jezika koji razumije ograničena skupina ljudi, npr. specifična terminologija određene grupe ljudi ili simboli za indiciranje postojanja i tipa bežičnog mrežnog signala. Podskup žargonskog koda je i znakovni kod u kojem određene predefinirane fraze predstavljaju točno određene pojmove.

- Skrivene šifre - predstavljaju steganografsku tehniku kod koje je umetnutu tajnu poruku moguće izdvojiti iz steganografskog medija samo ako je poznata točna metoda korištena za njeno umetanje u nositelj. Skrivene šifre uključuju rešetkaste i nulte šifre.

- Rešetkaste šifre - temelje se na predlošcima koji se koristi za prikrivanje poruke nositelja. Podaci koji se pojavljuju u otvorima takvih predložaka predstavljaju skrivenu tajnu poruku.

- Nulta šifra - koristi se za skrivanje informacija tako da se definira neki set pravila, npr. „čitaj svaku petu riječ“ ili „čitaj svaki treći znak u svakoj riječi“. Dotična metoda omogućava skrivanje tajnih poruka u svakodnevnim porukama bez uporabe kompliciranih algoritama ili alata. Primjeri umetanja tajnog teksta unutar datoteka su: ispod slike u *PowerPoint* datoteci, u *Properties* dijelu *Word* datoteke, unutar komentara na *web* stranicama, unutar bilo kojeg dokumenta tako da boja teksta odgovara boji pozadine.[3]

Osim navedene podijele, prema [8] steganografske tehnike skrivanja podataka su podijeljene u sljedećih šest kategorija:

- Tehnike supstitucije - suvišni dijelovi nositelja se iskorištavaju za umetanje tajne informacije.

- Tehnike transformacije domene - modifikacija se vrši u transformiranoj domeni. Najčešće se koriste diskretna kosinusna transformacija i diskretna Fourierova transformacija.

- Tehnike raspršenog slijeda - uski signal tajne poruke se nastoji sakriti unutar nositelja. Tajna poruka se modulira signalom šuma te se dodaje u nositelja: isključivo poznavanjem ključa je moguće iz naizgled slučajnog signala šuma dobiti skrivenu poruku. Dvije metode raspršenog slijeda koriste se u stenografiji: tehnika raspršenog spektra direktnog slijeda i tehnika raspršenog spektra frekvencijskog skoka.

- Statističke metode - nositelj se podjeli na onoliko blokova kolika je veličina poruke. Svaki blok služi za skrivanje jednog bita tajne poruke. Ukoliko je bit poruke jednak 1, blok se modificira tako da primatelj može statističkim testiranjem hipoteze otkriti je li taj blok promijenjen. Ukoliko je bit poruke jednak 0, blok se ne mijenja.

- Tehnike izobličavanja - tajna poruka se ne skriva direktno u nositelja, već se stvaraju preinake nositelja kako bi se prenijela tajna poruka. Zahtjeva se da primatelj poznaje originalnu verziju nositelja skrivene poruke.

- Tehnike stvaranja nositelja skrivene informacije - tajna poruka se ne skriva u nositelju, već se na temelju nje stvara nositelj koji joj odgovara.[8]

Postoji tri osnovna načina skirivanja digitalne poruke u nositelj:

- ubacivanje,
- zamjena ,
- generiranje novih datoteka.

4.1. 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, a samim time i otkrivanje iste.[8], [9]

4.2. Zamjena

Pristup zamjene ili supstitucije zasniva se na zamjeni najmanje značajnih bitova datoteke i to na 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 te ograničenje broja manje značajnih bitova koji se mogu upotrijebiti za primjenu ove metode.Ovisno o vrsti nositelja i količini skrivenih podataka, metoda supstitucija može značajno smanjiti kvalitetu izvorne datoteke.[8], [9]

4.3. Generiranje novih datoteka

Nedostatak prethodno navedenih tehnika ubacivanja i zamjene je taj što se originalna slika može usporediti sa stego slikom te je moguće otkriti razlike. Tehnika generiranja novih datoteka ne zahtijeva originalnog nositelja podataka, već sama generira datoteku u kojoj će biti sadržana poruka. Kada se koristi tehnika generiranja konačan rezultat je originalna datoteka koja je imuna na komparaciju sa drugim datotekama.[9]

4.4.Ostale digitalne tehnike

Postoji mnogo različitih tehnika pomoću kojih poruka može biti skrivena unutar digitalnih medija. Jedan od načina je iskorištavanje neupotrijebljenih dijelova datoteka ili nealociranog memorijskog prostora za pohranjivanje tajnih podataka kojima se može direktno pristupiti pomoću za to specijaliziranih alata. Male količine podataka također mogu biti sakrivene unutar neiskorištenih dijelova zaglavlja datoteka. Nadalje, informacije se mogu sakriti i na disku, unutar tajne diskovne particije. Takva particija nije vidljiva u standardnim uvjetima, premda određeni alati istovremeno mogu omogućiti potpuni pristup istoj. Opisana teorija implementirana je u steganografskom *ext2fs* datotečnom sustavu za Linux operacijske sustave. Skriveni datotečni sustav može omogućiti korisniku ograđivanje od posjedovanja određenih informacija ili pojave određenih događaja.

Mrežni protokoli također mogu igrati ulogu digitalnih nositelja. Tako npr. CTCP[1] protokol, osmišljen od strane *Craiga Rowlanda*, formira tajne komunikacijske kanale korištenjem identifikacijskog polja u IP paketima ili polja s brojem sekvence uTCP paketima.

Usprkos velikom broju steganografskih nositelja i metoda koje pruža digitalna tehnologija, slike te zvučni i video zapisi ipak slove kao najprikladniji i najuobičajeniji digitalni nositelji pa je i najveći broj steganografskih tehnika razvijen upravo za njih.[3]

[1] CTCP – (engl. *Covert Transmission Control Protocol*) verzija TCP protokola s tajnim komunikacijskim kanalima

5. Pregled steganografskih metoda

Metoda označava način rada sustava. Postoji jako puno steganografskih metoda te bi bilo teško pobrojati i opisati sve steganografske metode, stoga će u ovom poglavlju biti opisane one metode koje se najčešće koriste.
Steganografske metode su podjeljene s obzirom na medij kojim se prenosi:

- tekstovni zapis
- zvučni zapis,
- slikovni zapis.

5.1. Tekstovni zapis

Tekstualna steganografija postiže se mjenjanjem izgleda teksta ili mjenjanjem odeđenih karakteristika tekstualnih elemenata odnosno znakova. Cilj tekstualne steganografije je razviti promjene koje su pouzdane i nisu uočljive čitatelju. Mali manipulacijski prostor i pouzdanost prijenosa podataka same po sebi su u kontradiktornoj vezi pa predstavljaju izazov u projektiranju stego dokumenta. [10]

Načešće metode tekstualne stego obrade podataka su:

- Metode temeljene na formatu - mijenja postojeći tekst za skrivanje podataka na način da to uključuje umetanje razmaka, promjena veličine i stila teksta, i sl.[11] U tu grupu metoda pripada i *White Space* metoda koja se bazira na tehnici ubacivanja. Dodatnim dodavanjem bijelog prostora unutar pisanog teksta na listovima papira jednostavnim pritiskom na tipku *space* na tipkovnici, običnom korisniku vjerojatno 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, dok se za detekciju *white space* metode koristi se programski alat *Snow*. [9]

- Slučajna i statistička metoda - kod slučajne metode skriveni znakovi se pojavljuju slučajnim redoslijedom, dok statistička metoda određuje statističke podatke kao što su sredina, varijanca i hi kvadrat test kojima se određuje količina redundantnih informacija za skrivanje u tekstu.[11] Funkcionira na principau da se nositelj podijeli na onoliko blokova kolika je veličina poruke. Svaki blok služi za skrivanje jednog bita tajne poruke. Ukoliko je bit poruke jednak 1, blok se modificira tako da primatelj može statističkim testiranjem hipoteze otkriti je li taj blok promijenjen. Ukoliko je bit poruke jednak 0, blok se ne mijenja.[4],[8]

- Lingvistička metoda - kombinira sintaksu i semantiku. Zadatak sintaktičke stegoanalize je osigurati ispravnu gramatičku strukturu, dok je zadatak semantike dodjeljivanje sinonima i podataka koji se impliciraju u orginalni tekst.[11]

5.2. Zvučni zapis

U zvukovnoj steganografiji tajna poruka umetnuta je u digitaliziranom zvukovnom signalu koji za posljedicu ima neznatno mijenjanje binarnog slijeda originalne zvukovne datoteke. [10]

Metode zvukovne steganografije su:.

- LSB[2] kodiranje - metoda kojom se određeni uzorak analognog signala pretvara u digitalni binarni slijed te se tom prilikom bit najmanje važnosti mijenja s binarnim ekvivalentom tajne poruke

- Fazno kodiranje – ova metoda iskorištava činjenicu da ljudski slušni organ ne može prepoznati promjenu faze u zvučnom signalu te kodira tajnu poruku mijenjanjem faznog pomaka u spektru digitalnog signala.[10]

[2]LSB - (engl. *Least Significant Bit substitution*) zamjena bita najmanje važnosti

- Metoda raspršenog slijeda - ova metoda koristi tehniku ubacivanja, a zasniva se na širenju frekvencijskog spektra signala u određenoj domeni. Koristi slabosti koje imaju ljudski slušni organi. Također, koristi se i za kontrolu sigurnosti komunikacionog kanala, povećanje otpornosti na prirodne smetnje, sprječavanje 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 [3] i AIFF [4] formate koji koriste 16-bitnu linearnu kvantizaciju primijenjenu za distorziju prijenosnog signala. Pošto se koristi tehnika zamjene niskih valova, slično kao kod LSB metode, problem kod ove metode je što su niske frekvencije uočljive za ljudsko uho tako da je ovo prilično ranjiva metoda.[9] Dvije se metode raspršenog slijeda koriste u steganografiji: tehnika raspršenog spektra direktnog slijeda - DSSS[5] i tehnika raspršenog spektra frekvencijskog skoka - FHSS[6].[4], [8]

5.3. Slikovni zapis

Slikovni zapis je najčešće korištena podloga u steganografiji pa su samim time slike najzastupljeniji dio steganografske znanonsti. Ovo poglavlje sastoji se od metoda prostorne domene, metoda frekvencijske domene te HTML[7] metode.

Metode steganografske obrade podataka u kojima je slikovni zapis nositelj podataka u osnovi se dijele na:

- prostorno orijentirane metode,
- transformacijski (frekvencijski) orijentirane metode.[9]

[3] WAV - (engl. *Waveform Audio File Format*) valni audio format

[4] AIFF - (engl. *Audio Interchange File Forma*t) izmjenjeni audio format

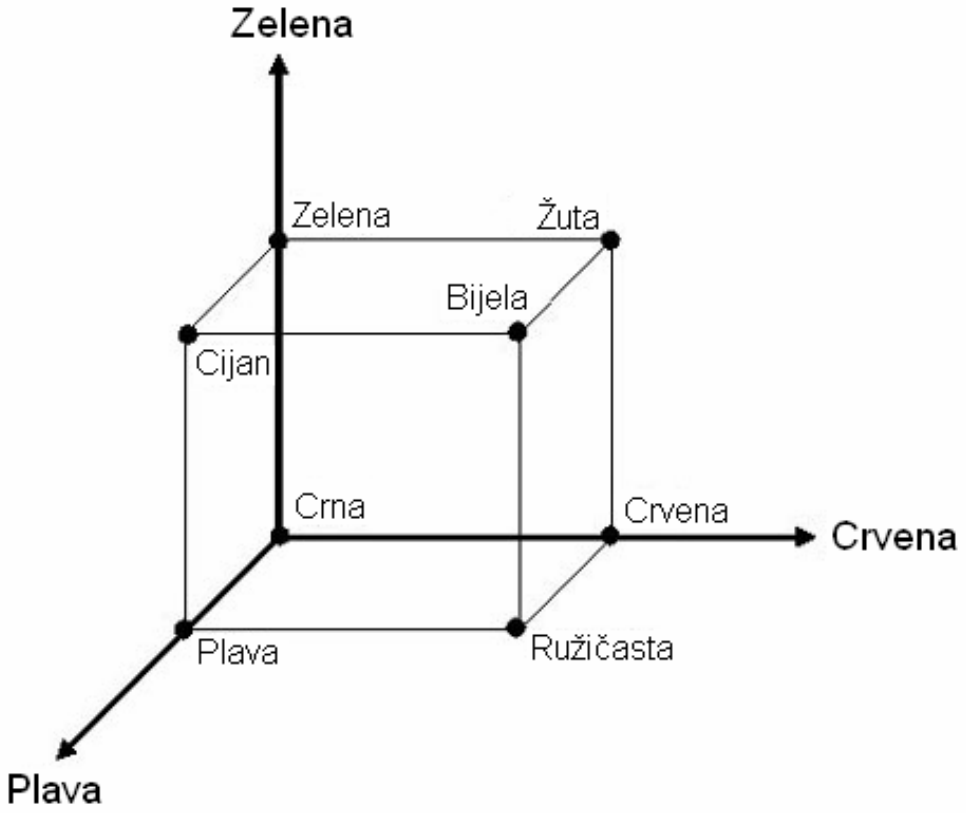
[5] DSSS - (engl. *Direct Sequence Spread Spectrum*) tehnika raspršenog spektra direktnog slijeda

[6]FHSS - (engl. *Frequency Hopping Spread Spectrum*) tehnika raspršenog spektra frekvencijskog skoka

[7] HTML - (engl. *Hyper Text Mark-Up Language*) programski jezik koji osim tekstualnoga zapisa omogućuje postavljanje zvukovnoga, slikovnoga i trodimenzionalnoga prikaza na web stranice

5.3.1. Metode prostorne domene

U prostornoj domeni slika nositelj i tajni podaci modificirani su pomoću metode supstitucije. Osnovni princip sustava baziranih na supstituciji je zamjena redundantnih dijelova slike s tajnim podacima. Kako je za razumijevanje ovog principa bitno poznavanje strukture steganografskog nositelja, slijedi kratak opis RBG[8]sustava. Unutar RGB sustava, svaka boja se prikazuje pomoću relativnog intenziteta svake od tri postojeće komponente – crvene, zelene i plave (slika 4). Nedostatak svih komponenti rezultira pojavom crne, dok prisustvo svih komponenti rezultira dobivanjem bijele boje.



Slika 4.RGB kocka, [3]

[8] RBG – (engl. *Red – Blue – Green*) sustav crvene, plave i zelene boje

Svaka RGB komponenta specificirana je jednim oktetom, tj. nizom od 8 bitova, tako da vrijednost intenziteta svake od triju boja može varirati od 0 do 255. Pošto RGB sustav sadrži 3 komponente, dotičnom metodom prezentacije, dobiva se 24-bitna shema koja podržava 16,777,216 jedinstvenih boja. To znači da je svaki piksel unutar slike kodiran s 24 bita. Većina današnjih aplikacija za obradu i prikaz slika podržava opisanu 24-bitnu shemu, no ipak omogućava i korištenje 8-bitne sheme kako bi se uštedjelo na veličini slike. Takva shema zapravo također koristi 24-bitni prikaz boje piksela, ali dodatno ima i paletu koja specificira boje korištene uslici. Svaki piksel kodiran je s 8 bitova, gdje dotična vrijednost označava indeks zapisa željene boje upaleti. Stoga ova metoda ograničava broj korištenih boja u slici na 256 zbog 8-bitnog prikaza indeksaboje u paleti. 8-bitna shema tipična je za GIF[9] formate slika koji se generalno smatraju kompresijom slike bez gubitaka.[3]

5.3.1.1. Supstitucija bita najmanje važnosti – LSB metoda

Supstitucija bita najmanje važnosti najčešća je steganografska tehnika korištena u radu s multimedijskim datotekama. Pojam „bit najmanje važnosti“ vezan je uz numeričku važnost bitova u oktetu. Bit najveće važnosti je onaj s najvećom aritmetičkom vrijednošću (12810), a bit najmanje važnosti onaj s najmanjom aritmetičkom vrijednošću (110). Stoga promjena bita najmanje važnosti ima najmanji učinak na promjenu ukupne vrijednosti okteta, a promjena bita najmanje važnosti u svim oktetima koji sačinjavaju multimedijsku datoteku ima najmanji učinak na promjenu izgleda same datoteke. Opisani princip još je djelotvorniji zbog činjenice da čovjekov optički sustav nije dovoljno osjetljiv za primjećivanje takvih promjena u boji.[3]

Ideja steganografske tehnike supstitucije bita najmanje važnosti bazira se na rastavljanju tajne poruke na bitove koji se potom pohranjuju na mjesto bita najmanje važnosti u odabranim oktetima. Kao jednostavan primjer LSB supstitucije prikazano je skrivanje slova 'G' unutar sljedećeg niza okteta:

10010101	00001101	11001001	10010110
00001111	11001011	10011111	00010000

[9] GIF - (engl. *Graphics Interchange Format*) grafički format u kojem je jedan piksel prezentiran jednim bajtom

Slovo 'G' se prema ASCII[10] standardu zapisuje kao binarni niz 01000111. Ovih 8 bitova zapisuje se na mjesto bitova najmanje važnosti u izvornom skupu okteta:

1001010**0**	0000110**1**	1100100**0**	1001011**0**
0000111**0**	1100101**1**	1001111**1**	0001000**1**

U navedenom primjeru zapravo je promijenjeno samo pola bitova najmanje važnosti.[3]

Za skrivanje informacija u slikama upotrebom LSB metode najčešće se koriste 24-bitne BMP[11] slike. Slika treba biti različitih boja i intenziteta svjetlosti na različitim dijelovima. Razlog tome je što je u sliku visoke kvalitete i rezolucije mnogo lakše sakriti informacije nego u sliku niske kvalitete. 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. [9]

5.3.1.2. Sortiranje paleta

Kao što je već rečeno, mnoge slike koriste palete boja korištene unutar slike. Palete sadrže samo podskup cjelovitog prostora boja unutar 24-bitnog prikaza.Svaka je boja unutar palete predstavljena s 24-bitnim vektorom koji definira RGB vrijednosti te boje i indeksom, tj. lokacijom u paleti. Taj indeks se pohranjuje unutar svakog piksela slike i pomoću njega se određuje odgovarajuća boja piksela. Prvi korak u primjeni ove steganografske tehnike je izrada kopije izvorne palete boja te promjena lokacija boja u novoj paleti. Novi raspored boja određuje se tako da boje koje se nalaze blizu unutar RGB sustava budu blizu i u paleti. Potom se

[10] ASCII - (engl. *American Standard Code for Information Interchange*) standardni američki kôd za razmjenu informacija

[11] BMP - (engl. *Bitmap image file*) format koji se koristi za pohranu bitmap digitalne slike, neovisno o zaslonu uređaja

primjenjuje standardna LSB supstitucija, tj. bit najmanje važnosti unutar svakog piksela zamjenjuje se bitom tajne poruke. U trećem koraku locira se RGB boja s novo dobivenim indeksom unutar nove palete. Na kraju se dotična RGB boja identificira i u izvornoj paleti pa se njen indeks u izvornoj paleti koristi kao nova vrijednost piksela.[3]

5.3.2.Metode transformacije domene

Steganografska tehnika transformacije domene bazira se na skrivanju podataka pomoću matematičkih funkcija koje se koriste u algoritmima kompresije. Osnovni princip predstavlja umetanje bitova tajne poruke na mjesto koeficijenata najmanje važnosti. Naime, JPEG[12] format slike koristi DCT[13] umjesto kodiranja pojedinačnih piksela. Slika se podijeli u 8x8 blokova za svaku komponentu RGB sustava i nastoje se pronaći blokovi u kojima je količina promjene vrijednosti piksela niska kako bi se čitavi blok zamijenio jednim diskretnim koeficijentom kosinusne transformacije. Ako je količina promjene previsoka, blok se dijeli u 8x8 manjih blokova sve dok količina promjene nije dovoljno niska. Svaki rezultirajući diskretni koeficijent kosinusne transformacije aproksimira luminanciju (svjetlinu, tamnoću i kontrast) i krominanciju (boju) odgovarajućeg dijela slike. JPEG format se smatra kompresijom slike s gubicima pošto slika dobivena konverzijom nije sasvim identična svojoj izvornoj inačici, ali je vrlo bliska aproksimacija iste. Kada se JPEG koristi kao steganografski nositelj, zapravo se vrše promjene relacije spomenutih koeficijenata umjesto bitova koji se zamjenjuju tijekom LSB supstitucije. Većina tehnika transformacije domene ne ovisi o formatu slike tako da umetnuta tajna poruka ostaje sačuvana i nakon konverzije između formata s gubicima i bez gubitaka podataka.[3]
Karakteristike metode transformacije domene jesu:

- koristi redundanciju DCT koeficijenata,
- primjenjiva je prilikom komprimiranih slikovnih sadržaja,
- može utjecati na omjer kompresije slikovnog sadržaja,
- prostorno bazirane steganografske integracije imaju veći steganografski kapacitet.[7]

[12] JPEG - (engl. *Joint Photographic Experts Group*) komprimiranislikovni formatsgubicima izveden iz*bitmape*

[13] DCT - (engl. *Discrete Cosine Transform*) diskretna kosinusna transformacija

5.3.3. HTML metoda

Ova metoda koristi tehniku zamjene. Bazira se na skrivanju informacija u izvornom HTML kôdu tako da podaci koji se prezentiraju 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. [9]

Na primjeru sljedećeg teksta objašnjena je HTML metoda:

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 kod u HTML jeziku bio bi sljedeći:

*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
*

Steganografksi obrađen kod bio bi ovakav:

*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
*

Iz konkretnog primjera vidi se da su promjenjena 4 bita sadržaja poruke, odnosno umetnu je skrivena poruka koja glasi: *01001110 01000001 01010000 01000001 01000100*, što u prijevodu znači: napad.

HTML metoda se najviše koristi za prijevaru korisnika koji u potrazi za informacijama pretražuju Internet.[9]

6. Analiza steganografskih tehnika i metoda zaštite podataka

Nakon što su opisane steganografske tehnike i metode, obraditi će se stegoanaliza te programski alati *StegSpy* i *Digital Invisible Ink Toolkit* sa konkretnim primjerima.

6.1. Stegoanaliza

Steganaliza je znanost i vještina detekcije poruke skrivene steganografskim metodama, odnosno proces detektiranja steganografskih datoteka koji se temelji na proučavanju varijacija uzoraka bitova i neobično velikih datoteka. [2],[3]

Ciljevi stegoanalize su:

- Identificiranje sumnjivih skupova podataka, kao što su signali ili datoteke, unutar kojih se potencijalno nalazi skrivena tajna poruka,
- Utvrđivanje da li su tajni podaci umetnuti u steganografsku datoteku prethodno kriptirani,
- Utvrđivanje postojanja šuma ili nebitnih podataka unutar sumnjivog signala ili datoteke,
- Izdvajanje i dekriptiranje umetnute poruke iz steganografske datoteke.

Za razliku od kriptoanalize, gdje je očito da razmatrani kriptirani podaci sadrže poruku, steganaliza obično počinje s nekoliko sumnjivih skupova podataka od kojih nijedan sa sigurnošću ne sadrži tajnu poruku. Korištenjem različitih naprednih metoda statističke analize, steganalitičar reducira skup sumnjivih podataka dok ne pronađe pravu steganografsku datoteku.

Informacije mogu biti skrivene gotovo svugdje na Internetu pa stoga uvelike otežavaju proces stegoanalize. Npr. unutar web stranice, podatke je moguće sakriti na sljedećim mjestima:

- Tekst - može biti skriven unutar stranice ako je jednake boje kao i pozadina. Kako bi se pronašao, dovoljno je selektirati čitav sadržaj stranice, pri čemu će pozadina iza

teksta promijeniti boju. Male razlike u prostornom razmještaju riječi i redaka također mogu sadržavati tajnu informaciju. Takav slučaj može se otkriti pregledavanjem teksta unutar nekog tekstualnog procesora.

- Ne-tekstualni elementi - svaka slika, audio ili video datoteka na stranici može sadržavati skrivene linkove ili poruke.

- Linkovi - mogu biti skriveni tako da im se promijeni vizualni identitet, npr. da nisu podcrtani te da ne mijenjaju boju ili oblik kada se s mišem prelazi preko njih. Najlakši način lociranja skrivenih linkova na stranici je traženje znakovnog niza „HREF=“ unutar HTML koda *web* stranice. Pritiskom na tipku *tab* također se aktiviraju linkovi.

- Komentari - Pošto je sadržaj komentara vidljiv samo unutar HTML koda, to također može biti pogodno mjesto za skrivanje tajnih informacija.

- Strukturni elementi - mnogi web preglednici zanemaruju informacije u HTML kodu koje ne mogu interpretirati. Tako, na primjer, neobične opcije unutar HTML oznaka (engl. *tag*) mogu sadržavati tajne podatke.

- Okviri - informacije mogu biti skrivene unutar HTML koda svakog okvira web stranice. [3]

Tehnike steganalize predstavljaju napade na steganografske algoritme, odnosno metode analize steganografskih algoritama. Zbog toga se tim tehnikama testira koliko je steganografski sustav siguran, tj. koliku količinu informacija je moguće sakriti u objekt nositelj prije nego se detektira skrivena poruka. Tako su neke steganografske metode tek otporne na vizualne napade, dok su druge otporne i na statističke testove, ali količina informacija koje mogu sigurno sakriti je znatno manja.[2]

6.1.1. Oblici napada

Steganalitički napadi i analiza skrivenih podataka uključuju različite aktivnosti: detekciju, izdvajanje te onemogućavanje ili uništavanje skrivenih informacija. Vrsta napada ovisi isključivo o informacijama dostupnim steganalitičaru:

- Samo steganografska datoteka - dostupna je samo steganografska datoteka nad kojom se potom provode različite analize.
- Poznati nositelj - raspoloživi su i steganografska datoteka i steganografski nositelj, tj. izvorna datoteka unutar koje je tajna poruka skrivena.
- Poznata poruka - dostupna je tajna poruka.
- Odabrana steganografska tehnika - poznata je i steganografska datoteka i steganografski alat, odnosno algoritam korišten za umetanje tajne poruke.
- Odabrana poruka - poznata poruka i steganografski alat, odnosno algoritam koriste se za kreiranje steganografske datoteke koja se koristi za buduću analizu i usporedbe. Svrha ovog napada je utvrđivanje odgovarajućih uzoraka u steganografskoj datoteci koji mogu ukazati na korištenje određenog steganografskog alata i algoritma.
- Poznati nositelj i odabrana steganografska tehnika - raspoloživa je steganografska datoteka, steganografski nositelj te steganografski alat, odnosno algoritam korišten za umetanje tajne poruke. [3]

6.1.2. Osnovne tehnike steganalize

Skrivanje informacija unutar digitalnog medija uzrokuje izmjene karakteristika tog medija koje se mogu očitovati nekim oblikom degradacije ili neobičnim svojstvima. Slijedi pregled najpopularnijih tehnika steganalize. [3]

6.1.2.1. Neobični uzorci

Neobični uzorci unutar steganografskih datoteka impliciraju na potencijalno skrivenu poruku unutar istih. Upotrebom različitih alata i tehnika moguće je identificirati te uzorke. Npr. alatima za analizu diska moguće je filtriranjem pronaći skrivene informacije u nekorištenim particijama. Različiti filtri mogu poslužiti za identificiranje TCP/IP paketa koji sadrže skrivene ili neispravne podatke unutar svog zaglavlja. Pregledom teksta unutar nekog tekstualnog procesora moguće je pronaći male nepravilnosti kod razmještaja riječi i redaka ili suvišne razmake koji impliciraju na postojanje skrivene poruke. Slike mogu sadržavati izobličenja te varijacije u boji i luminanciji koje, nakon što se identificiraju nekim alatom, također upućuju na prisustvo skrivenih informacija. [3]

6.1.2.2. Vizualna detekcija

Analizom ponavljajućih uzoraka moguće je identificirati korišteni steganografski alat ili skrivenu informaciju. Ispitivanje uzoraka provodi se tako da se izvorni steganografski nositelj uspoređuje sa steganografskom datotekom koja sadrži skrivenu poruku. Takav napad naziva se napad s poznatim nositeljem. Usporedbom različitih steganografskih datoteka moguće je pronaći uzorke koji predstavljaju potpis specifičnog steganografskog alata. Ako izvorni steganografski nositelj nije dostupan, izvedeni potpisi dovoljni su za implikaciju postojanja skrivene poruke te identifikaciju steganografskog alata korištenog za umetanje tajne poruke. Detekcija takvih potpisa može se automatizirati korištenjem specijalnih alata za detekciju steganografije. Dotični alati obično koriste različite uzorke paleta i potpisa kako bi pronašli piksele koji odstupaju od neke standardne vrijednosti u određenom dijelu slike.

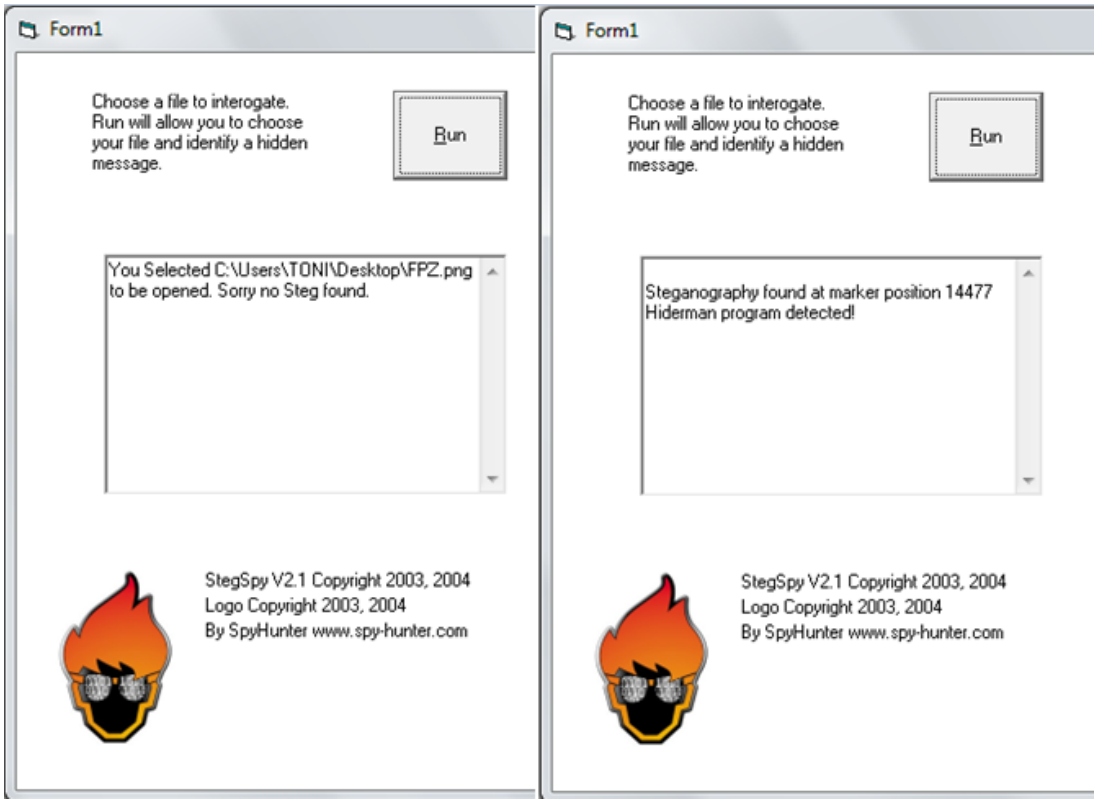
Dodatna indikacija postojanja skrivene informacije unutar slike je njeno nadopunjavanje ili rezanje. Naime, kod nekih steganografskih alata događa se da slika ne odgovara nekoj predefiniranoj fiksnoj veličini pa se mora odrezati ili nadopuniti crnim plohama. Nadalje, razlike u veličini između steganografskog nositelja i steganografske datoteke te neobično velik ili malen broj jedinstvenih boja unutra palete slike također upućuju na mogućnost postojanja umetnute poruke u slici. [3]

6.2. *StegSpy*

StegSpy (slika 5) je jednostavan steganografski programski alat dizajniran za detekciju prisutnih skrivenih podataka. Detektira steganografske promjene kreirane od sljedećih programskih alata:

- *Invisible Secrets* v.2,3 i 4
- *JP Hide and Seek* v.0.5
- *JpegX* v.1.00.6
- *Masker* v.7
- *Hiderman*

StegSpy provodi stegoanalizu locirajući određeni uzorak heksadecimalnog bajta unutar sumnjivih neobrađenih podataka na temelju kojih određuje sadrži li određena datoteka skrivene podatke, te daje pozitivan ili negativan rezultat.[12]



Slika 5.a) *StegSpy* nije detektirao stego sadržaj; b) *StegSpy* je detektirao stego sadržaj, [12]

Na prethodnoj slici prikazan je rezultat rada programskog alata *StegSpy*. Lijeva stana slike prikazuje kako *StegSpy* nije dektirao nikakvu promjenu u pikselima slike odnosno nije utvrdio stego sadržaj, dok je na desnoj stani slike utvrđen steganografski sadržaj.

6.3. *Digital Invisible Ink Toolkit*

DIIT[14] je JAVA[15]-in stenografski programski alat, koji može sakriti bilo koju datoteku unutar digitalne slike. Podržava Windows, Linux i MAC[16] operacijske sustave jer je napisan u JAVA-i te samim time neovisan o operacijskom sustavu. Prilikom unosa, radi sa formatima .PNG[17], .BMP i .JPG[18], dok se stego slike spremaju u formatima .PNG i .BMP. U alatu se nalaze prozori za kodiranje, dekodiranje, analizu i simulaciju, te šest vrlo prilagodljivih algoritama (*BattleSteg,BlindHide, DynamicBattleSteg, FilterFirst, DynamicFilterFirst i HideSeek*)**.**[13]

6.3.1. Kodiranje u DIIT-u

Da biste sakrili datoteku unutar slike, prvo se pokrene DIIT (slika 6) i otvori kratica *Encode*. Nakon toga pritisne se prozor *Get Message* i pojaviti će se novi prozor s opcijama da se izabere datoteka koju se želi sakriti. Slijedeći korak je da se pritisne prozor *Get Cover* koji omogućuje da se izabere slika unutar koje će se spremiti željena skrivena poruka. Zatim se dolazi do mogućnosti da se umetne željena zaporka, a u slučaju da se to ne želi onda se ostavi prazno polje. Pri izboru algoritama ponuđeni su: *BattleSteg***,** *BlindHide, DynamicBattleSteg, DynamicFilterFirst, FilterFirst i HideSeek.*

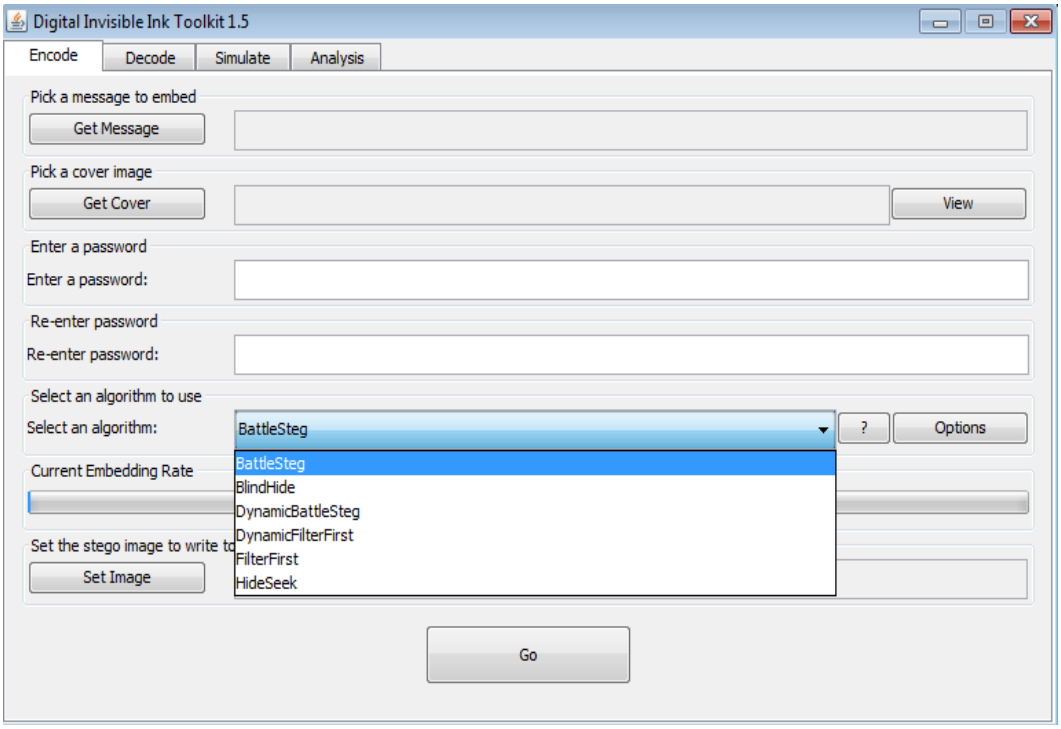
[14] DIIT - (engl. *Digital Invisible Ink Toolkit*) programski alat za stegnanografsku obradu podataka

[15] JAVA - programski jezik izričito dizajnirani za uporabu u distribuiranom okruženju Interneta

[16] MAC - (engl. *Media Access Control* ili skraćeno engl. *Macintosh*) osobna računala dizajnirana i razvijena od strane Apple Inc.

[17] PNG - (engl. *Portable Network Graphics*) otvoreni grafički format namjenjen pohrani nepokretnih slika

[18] JPG - (engl. *Joint photographic group*) format slike koji sažima sliku uz minimalne gubitke na kvaliteti, najčešće se koristi kod e-maila i web stranica

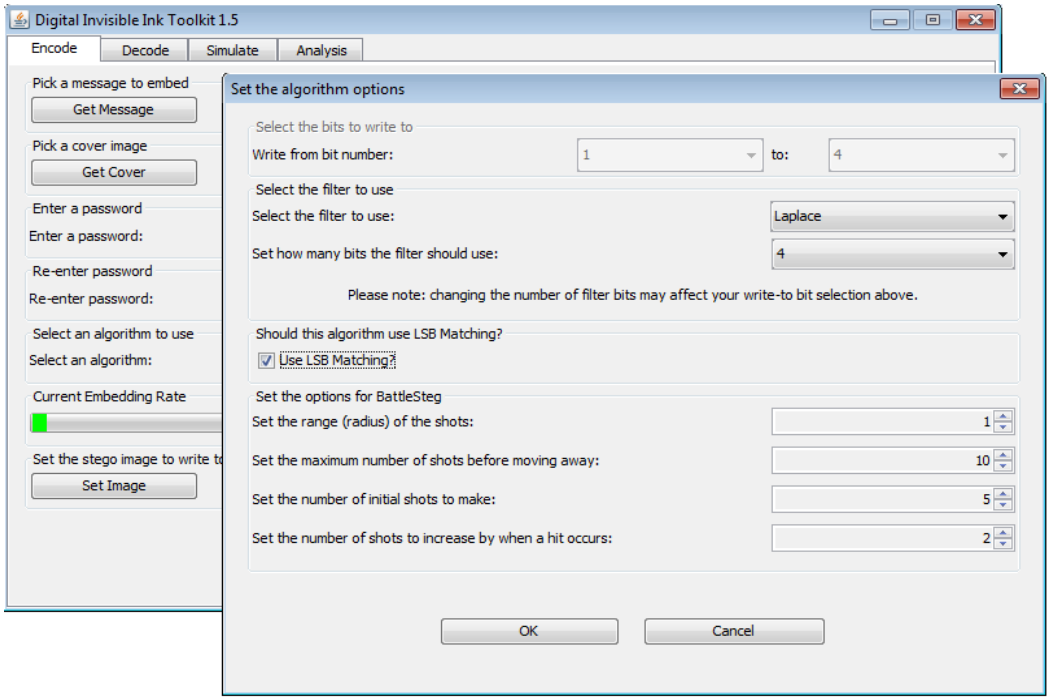


Slika 6. Radni prozor DIIT-a,
[13]

BattleSteg je najbolji od svih navedenih i zahtijeva lozinku. *BlindHide* je najjednostavniji način za skrivanje podataka u sliku. *DynamicBattleSteg* i *DynamicFilterFirst* – ova dva algoritma učinkovita su kao *BattleSteg i FilterFirst*, s time što se sakrivanje obavlja brže i s manje memorije. *HideSeek* algoritam nasumice distribuira poruke preko slike. *FilterFirst* algoritam filtrira sliku koristeći jedan od ugrađenih filtara i onda skriva u najvišem filtru vrijednosti koje stavlja na određeno mjesto, ne zahtijeva lozinku.[14]

Da bi se prilagodili algoritmi, klikne se na gumb *Options* te se otvori novi prozor. Najvažnija od ponuđenih opcija je *Number of bits to write to* koja zapravo prikazuje ako filtar koristi manji broj bitova, da se može u istu sliku spremiti veća količina informacija. Najveća količina informacija se može spremiti u odnosu 1 : 6. Bitovi su numerirani od LSB do MSB[19], tako da npr. ako se odabere 1 : 4, onda će četiri najmanje značajna bita od svake boje biti korištena za skrivanje (slika 7). [13]

[19] MSB - (engl. *Oracle Binary Message File*) algoritam koji umeće tajnu poruku u odabranu sliku



Slika 7. Radni prozor opcija algoritama,
[13]

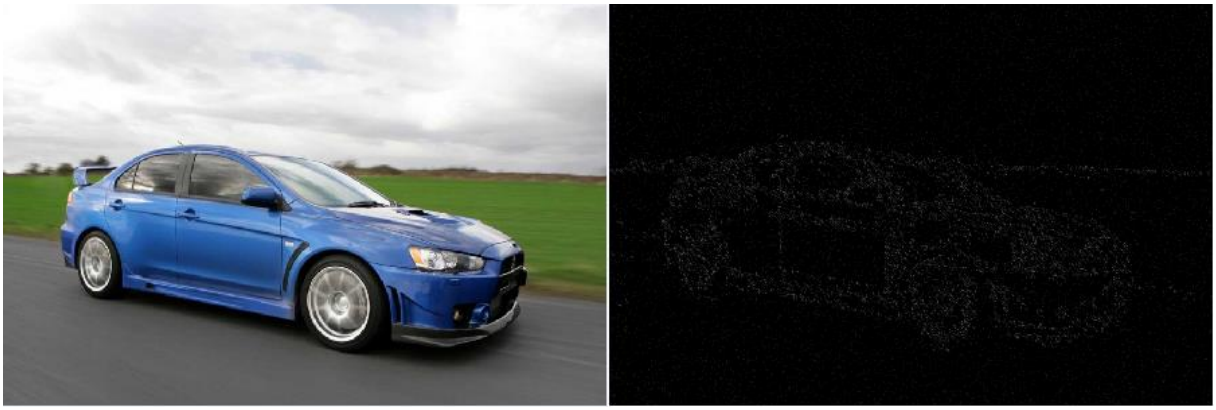
Posljednja opcija određuje gdje će se spremiti slika, te naziv slike i u kojem će se formatu spremiti. Treba paziti da slika bude dovoljne veličine da se u nju smjesti tekst. *Current Embeddin Rate* prikazuje slobodan postotak prostora (piksela) koji se mogu kodirati. Sve što je manje od 10% je dobra stopa.

6.3.2. Dekodiranje u DIIT-u

Kako bi se preuzela datoteka sa stego slike potrebno je učitati traženu stego sliku u prozoru *Get Image*, upisati zaporku (ukoliko je zapisana prilikom kodiranja), odabrati odgovarajući algoritam i postavke algoritma (istovjetan onome kojim je ta slika kodirana), te odabrati mjesto na koje se želi spremiti datoteka koja je kodirana u stego slici. U slučaju da je poznat format očekivanog teksta, može se upisati i kratica formata, npr. poruka.pdf, tada će operacijski sustav odmah prepoznati da se radi o PDF[20] datoteci. [13]

[20] PDF - (engl. *Portable Document Format*) format za zapis dvodimenzionalnih dokumenata neovisno o uređaju i rezoluciji ispisa

Na slici 8., 9., 10., 11., 12. i 13. prikazano je kodiranje ponuđenim algoritmima u DIIT-u.

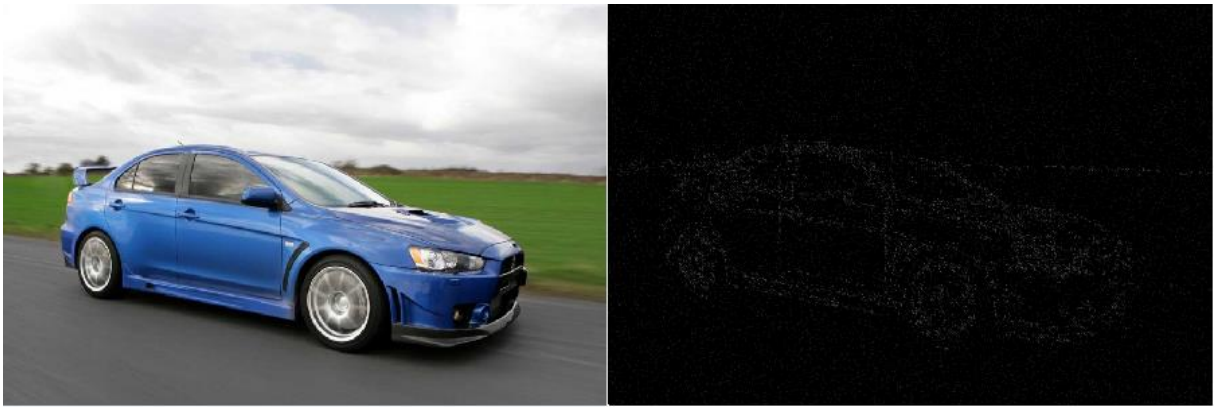


Slika 8. Kodiranje *BattleStage* algoritmom,

[13], [15]

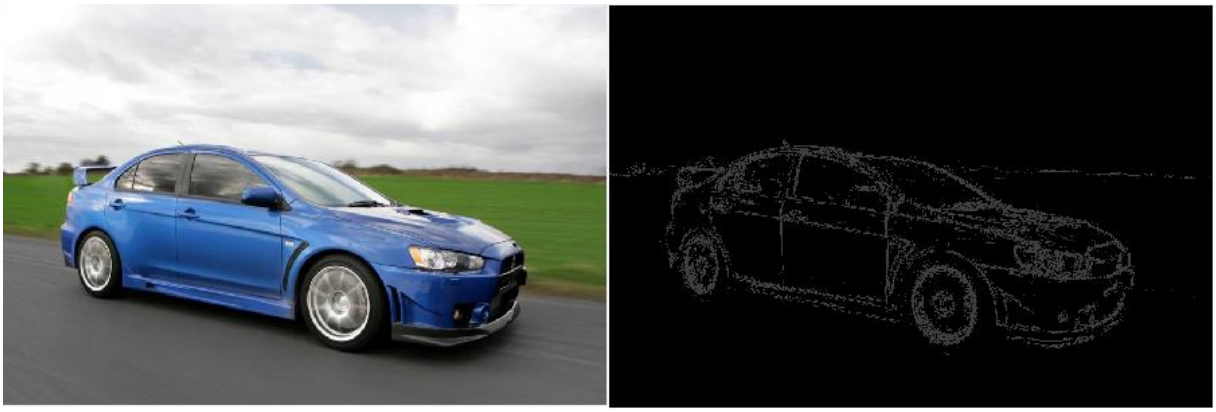
Slika 9. Kodiranje *BlindHide* algoritmom,

[13], [15]



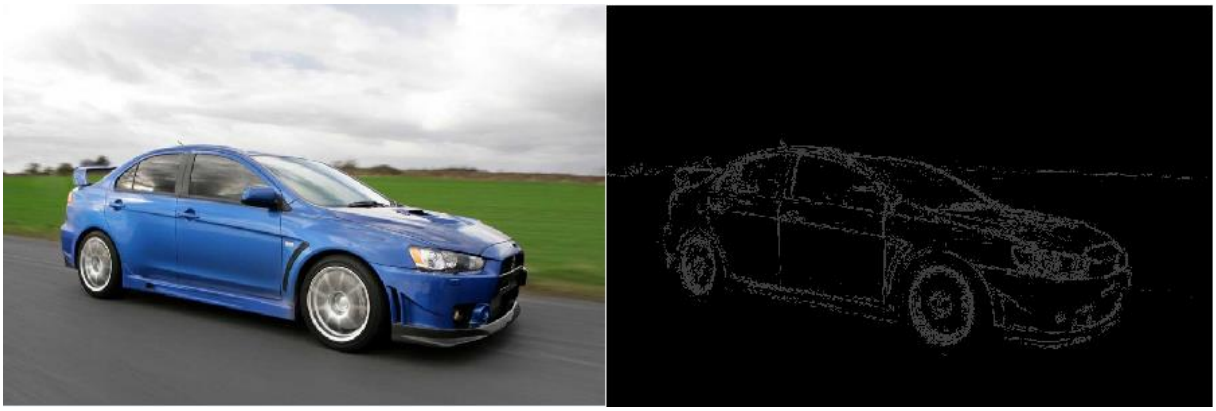
Slika 10. Kodiranje *DynamicBattleSteg* algoritmom,

[13], [15]



Slika 11. Kodiranje *DynamicFilterFirst* algoritmom,

[13], [15]



Slika 12. Kodiranje *FilterFirst* algoritmom,

[13], [15]

Slika 13. Kodiranje *HideSeek* algoritmom,

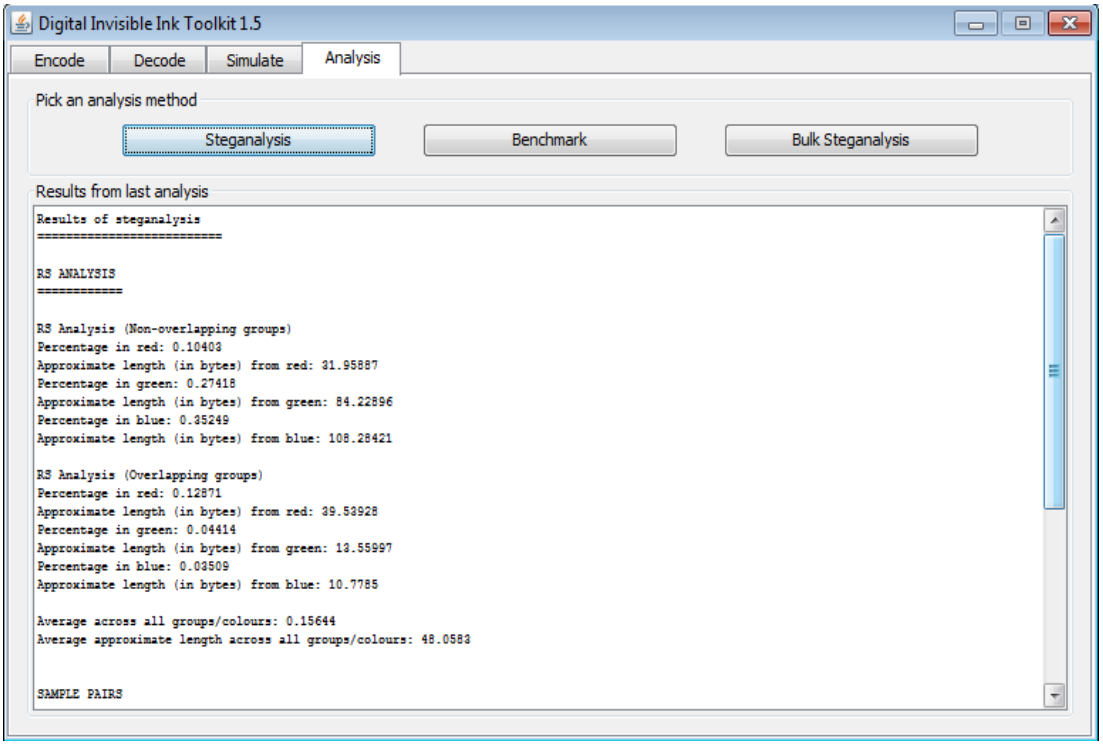
[13], [15]

Na prethodnim primjerima prikazani su načini načini kodiranja ponuđenim algoritmima u DIIT-u. Lijeve stane slika prikazuju stego sliku, dok se na desnoj stani slika vide bijele točkice na crnoj pozadini odnosno prikazana su mjesta na kojima se nalaze skrivene poruke.

6.3.3.Analiza u DIIT-u

Analizom se provjerava koliko je datoteka dobro sakrivena u slici. U steganografiji provjeravanje učinka nekih algoritama može se provjeriti steganalizom, budući da ima mogućnost detektiranja skrivenih informacija.

Za steganalizu prvo se klikne na *Steganalysis* (slika 14) i iz prozora koji se otvori klikne se *Pick Image*. Odabere se slika koja se želi analizirati (ne mora nužno biti stego slika), i klikne se gumb za otvaranje. Na kraju se odabere gdje se podaci žele spremiti.[13]



Slika 14. Radni prozor stegoanalize,

[13]

Slika 14 prikazuje rezultate stegoanalize. Rezultati se sastoje od dvije grupe – preklapajuće i nepreklapajuće, gdje se analiziraju tri osnovne boje – crvene, zelene i plave te se prikazuje razlika između grupa.

Za *RS Analysis*, što je broj manji, to je poruka bolje sakrivena (odnosi se na stego slike). Za originalne slike broj predstavlja prirodno stanje slike, odnosno ono će iznositi od 1-3 %.[13]

7. Zaključak

Voštane pločice i nevidljiva tinta samo su neke od steganografskih tehnika koje su se koristile još od grčkog doba kao način skrivenog prijenosa informacija. Dolaskom modernog doba i digitalne tehnologije,steganografija dobiva sasvim je novu dimenziju upotrebe. Razvijaju se efikasne tehnike i metode koje omogućuju pouzdan i siguran prijenos skrivenih informacija.

Svaka od navedenih metoda ima svoje prednosti i nedostatke. Tako je LSB metoda najčešće korištena metoda koja pruža prijenos velikog kapaciteta skrivenog sadržaja, no bilo kakva konverzija formata multimedijskog nositelja znači gubitak skrivene informacije. Bolje rezultate na konverziju multimedijskog nositelja daje metode transformacijske domene, jer one ne ovise o formatu slike tako da skrivena informacija ostaje sačuvana i nakon izvršene konverzije.

Steganografija predstavlja alternativu kriptografiji. Kriptirana informacija, koliko god dobro zaštićena bila, skreće pozornost napadača te uvijek postoji vjerojatnost njenog otkrivanja. S obzirom na veliku količinu multimedijskog sadržaja na mrežama, nemoguće je analizirati i detektirati zasebno svaki steganografski sadržaj. Međutim, treba voditi računa da slika bude visoke rezolucije i kontrasta te da skrivena poruka ne bude prevelika kako nebi došlo do deformacije nositelja. Ako se uzme u obzir da većina steganografskih programskih alata ima mogućnost kriptiranja sadržaja te da tajna poruka nije vidljiva napadaču, informacija je dobro zaštićena, čak ako napadač i izdvoji skriveni sadržaj on je i dalje kriptiran i nerazumljiv.

Upotrebom programskog alata *StegSpy* može se brzo i efikasno utvrditi posjeduje li određena multimedijska datoteka stego sadržaj. DIIT posjeduje puno više mogućnosti od *StegSpy*-a. Osim navedene stegoanalize, DIIT omogućava kodiranje, dekodiranje i simulaciju stego sadržaja, te kao dodatnu mjeru sigurnosti, uz sve navedeno, posjeduje mogućnost kriptiranja stego sadržaja.

Pored navedenih prednosti, steganografija ima i svoje nedostatke. Za prijenos skrivene poruke kanalom uvijek je potrebno koristiti nositelj koji sam po sebi nosi puno veću količinu podataka nego što nosi sama poruka. Nadalje, pojavljuju se problemi kao što su osjetljivost pri manipulaciji s podacima, kompresiji ili rotaciji slike i sl.. S obzirom da ju je jako teško detektirati, vrlo brzo je postala zanimljiva osobama koje se bave raznim ilegalnim i kriminalnim aktivnostima.

Bez obzira na brojne prednosti i mogućnosti primjene, ova tehnika zaštite podataka još uvijek nije u potpunosti iskorištena. U budućnosti se očekuje njen ubrzani razvoj te uz male modifikacije ima perspektivu postati jedna od najboljih sigurnosnih tehnika.

Literatura

[1] Zeljković, S.: Steganografija, Hrvatski matematički elektronski časopis, Broj 5, lipanj 2005. Dostupno na Internet-stranici: http://e.math.hr/old/stegano/index.html, učitano dana 3.9.2015.

[2] Radanović, G.: Steganografija i steganaliza digitalnih slika, Sveučilište u Zagrebu Fakultete elektronike i računarstva, diplomski rad br.58, Zagreb, lipanj 2010., Internet- stranica http://os2.zemris.fer.hr/ostalo/2010_radanovic/Stego.pdf, učitano dana 3.9.2015.

[3] Hrvatska akademska i istraživačka mreža: Steganografija, Zagreb: Steganografija; 2006.Internet-stranica:www.cert.hrsitesdefaultfilesCCERT-PUBDOC-2006-04-154.pdf, učitano dana 3.9.2015.

[4] Katzenbeisser, S.; Petitcolas, F. A. P.: Information hiding techniques for steganography and digital watermarking, Annales UMCS Informatica, Lubin-Polonia, 2006.I

[5] Kharrazi, M.; Sencar, H.T.; Memon, N.: Image steganography: Concepts and practice, WSPC / Lecture Notes, Polytechnic University, Brooklyn, New York, 2004.

[6] Cole, E.: Hiding in plain sight: Steganography and the art of covert communication, Wiley Publishing, Inc., Indianapolis, Indiana, 2003.

[7] Stančić A.: Steganografska integracija prikupljenih podataka unutar prometnog sustava, doktorska disertacija, Sveučilište u Zagrebu, Fakultet prometnih znanosti, Zagreb, 2013.

[8] Kipper G. Investigator's Guide to Steganography, London: Auerbach Publications; 2004.

[9] Ćajić, M.; Veinović, M.; Brkić, B.: Analiza steganografskih tehnika i metoda, Singipedia, 2010.,Internet-stranica:http://www.singipedia.com/content/1043-Analiza-steganografskih-tehnika-i-metoda, učitano dana 3.9.2015.

[10] Nosrati, M.; Karimi, R.; Hariri, M.: An introduction to steganography methods, World Applied Programming, Vol (1), No (3), 191-195, kolovoz 2011., Internet-stranica: http://citeseerx.ist.psu.edu/viewdoc/download?rep=rep1&type=pdf&doi=10.1.1.208.5195, učitano dana 3.9.2015.

[11] CyberScience Laboratory Functional Analysis of StegSpy, Version 2.1, Rome, New York 13441-4114, 315.838.7000, ožujak 2006., Internet-stranica: https://cyberfetch.org/sites/default/files/documents/csl_far_stegspy.pdf, učitano dana 3.9.2015.

[12] Rakhi, Suresh Gawande: A review on steganography methods, International Jurnal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 2, Broj 10, listopad 2013., Internet-stranica: http://www.ijareeie.com/upload/2013/october/8NAREVIEW.pdf, učitano dana 3.9.2015.

[13] Digital InvisibleInkToolkit, Internet stranica: http://diit.sourceforge.net/, učitano dana 3.9.2015.

[14] Kultan, R.: Usporedna analiza stenografskih alata, diplomski rad, Sveučilište u Zagrebu, Fakultet prometnih znanosti, Zagreb, 2012.

[15] Syahied: Custom Mitsubishi Lancer Evo X Mitsubishi Lancer Evo X Elegant In Color Photos Picture [slika sa Interneta]. 2014, Dostupno na Internet-stranici: http://autocarswallpaper.info/mitsubishi/custom-mitsubishi-lancer-evo-x.html, učitano dana 3.9.2015.

Popis kratica i akronima

AIFF	(*Audio Interchange File Format*)izmjenjeni audio format
ASCII	(*American Standard Code for Information Interchange*) standardni američki kod za razmjenu informacija
BMP	(*Bitmap image file*) format koji se koristi za pohranu bitmap digitalne slike, neovisno o zaslonu uređaja
CSV	(*Comma-Separated Values*)format koji pohranjuje tablične podatke (brojeve i tekst) u običan tekst oblik
CTCP	(*Covert Transmission Control Protocol*) verzija TCP protokola s tajnim komunikacijskim kanalima
DCT	(*Discrete Cosine Transform*) diskretna kosinusna transformacija
DIIT	(*Digital Invisible Ink Toolkit*) programski alat za stegnanografsku obradu podataka
DSSS	(*Direct Sequence Spread Spectrum*) tehnika raspršenog spektra direktnog slijeda
FHSS	(*Frequency Hopping SpreadSpectrum*) tehnika raspršenog spektra frekvencijskog skoka
GIF	(*Graphics Interchange Format*) bitmap grafički format, jedanpiksel prezentiran je jednimbajtom
HTML	(*Hyper Text Mark-Up Language*) programski jezik koji osim tekstualnog zapisa omogućuje postavljanje zvukovnog, slikovnog i trodimenzionalnoga zapisa na web stanice
JPEG	(*Joint Photographic Experts Group*) komprimiranislikovni formatsgubicima izveden izbitmape
LSB	(*Least Significant Bit substitution*) zamjena najmanje značajnog bita
MSB	(*Oracle Binary Message File*) algoritam koji umeće tajnu poruku u odabranu sliku
PDF	(*Portable Document Format*) format za zapis dvodimenzionalnih dokumenata neovisno o uređaju i rezoluciji ispisa
PNG	(*Portable Network Graphics*) otvoreni grafički format namjenjen pohrani nepokretnih slika
RGB	(*Red-Green-Blue*) sustav od tri osnovne boje, crvene, zelene i plave boje

WAV (*Waveform Audio File Format*) valni audio format

Popis slika i tablica

Slika 1. Shema steganografskog sustava 6
Slika 2. Shematski prikaz steganografskog sustava 7
Slika 3. Pregled steganografskih tehnika 10
Slika 4. RGB kocka 18
Slika 5. a) Stegspay nije detektirao stego sadržaj; b) Stegspay je detektirao stego sadržaj 28
Slika 6. Radni prozor DIIT-a 30
Slika 7. Radni prozor opcija algoritama 31
Slika 8. Kodiranje *Battlestage* algoritmom 32
Slika 9. Kodiranje *Blindhide* algoritmom 32
Slika 10. Kodiranje *DynamicBattlesteg* algoritmom 32
Slika 11. Kodiranje *DynamicFilterfirst* algoritmom 33
Slika 12. Kodiranje *Filterfirst* algoritmom 33
Slika 13. Kodiranje *Hideseek* algoritmom 33
Slika 14. Radni prozor stegoanalize 34

Sveučilište u Zagrebu
Fakultet prometnih znanosti
10000 Zagreb
Vukelićeva 4

METAPODACI

Naslov rada: Analiza metoda steganografske zaštite podataka

Autor: Toni Kuran, 0135212325
Mentor: dr. sc. Ivan Grgurević

Naslov na drugom jeziku (engleski):
Analysis of Steganographic Data Protection Methods

Povjerenstvo za obranu:

- prof. dr. sc. Zvonko Kavran, predsjednik
- dr. sc. Ivan Grgurević, mentor
- Siniša Husnjak, mag. ing. traff., član
- izv. prof. dr. sc. Dragan Peraković, zamjena

Ustanova koja je dodjelila akademski stupanj: Fakultet prometnih znanosti Sveučilišta u Zagrebu
Zavod: Zavod za informacijsko komunikacijski promet
Vrsta studija: sveučilišni
Naziv studijskog programa: Promet
Stupanj: preddiplomski
Akademski naziv: univ. bacc. ing. traff.
Datum obrane završnog rada: **15.9.2015.**

Sveučilište u Zagrebu
Fakultet prometnih znanosti
10000 Zagreb
Vukelićeva 4

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

Izjavljujem i svojim potpisom potvrđujem kako je ovaj završni rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu što pokazuju korištene bilješke i bibliografija.
Izjavljujem kako nijedan dio rada nije napisan na nedozvoljen način, niti je prepisan iz necitiranog rada, te nijedan dio rada ne krši bilo čija autorska prava.
Izjavljujem također, kako nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.
Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu završnog rada pod naslovom **Analiza metoda steganografske zaštite podataka**

na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

Student/ica:

U Zagrebu, 7.9.2015

(potpis)