HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Steganografija

CCERT-PUBDOC-2006-04-154

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Steganografija je znanstvena disciplina koja se bavi prikrivenom razmjenom informacija. Riječ steganografija izvedena je od grčkih riječi *steganos* i *graphein*, što u doslovnom prijevodu znači "skriveno pisanje".

Osnovni princip steganografije počiva na prikrivanju samog postojanja informacije koja se prenosi unutar nekog naizgled bezazlenog medija ili skupa podataka. Moderna steganografija, koja koristi prednosti digitalne tehnologije, najčešće podrazumijeva skrivanje tajne poruke unutar neke multimedijske datoteke, npr. slike, audio ili video datoteke. Multimedijske datoteke u pravilu sadrže neupotrijebljene ili nevažne podatkovne prostore koje različite steganografske tehnike koriste tako da ih popune s tajnim informacijama. Takve datoteke se potom mogu razmjenjivati bez da itko bude svjestan prave svrhe dotične komunikacije.

Steganografija ima vrlo široke mogućnosti primjene - od prikrivene razmjene podataka u privatne i poslovne svrhe pa sve do zaštite autorskih prava u obliku vodenog pečata. No, zbog svog temeljnog principa "nevidljivosti" informacija, često se koristi i tijekom ilegalnih aktivnosti.

Ovaj dokument opisuje osnovne steganografske principe i tehnike te moguću primjenu steganografije. Premda je u dokumentu dan i povijesni pregled steganografije, sve navedene teme obrađene su u kontekstu digitalnih aplikacija, s naglaskom na skrivanje informacija unutar slika i zvučnih zapisa.

Slika 1: Slika koja se javno prijenosi i služi kao nositelj

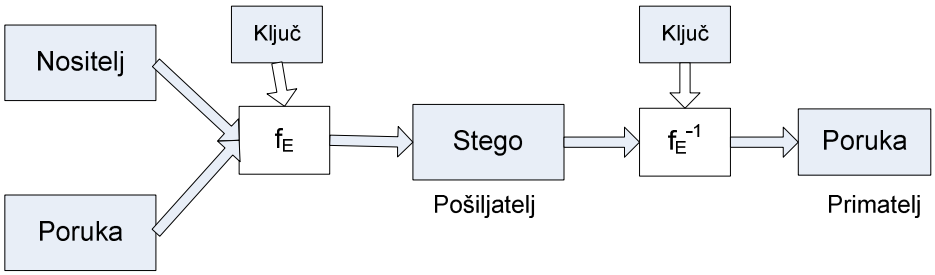
Slika 2: Tajna slika koja se prenosi skrivena

Slika 3: Stego - tajna slika skrivena unutar slike nositelja

2. Steganografija

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 uobičajene svakodnevne komunikacije te kao takav ne privlači posebnu pozornost na sebe, npr. tekst, slika, audio ili video zapis. Cjelina sačinjena od tajne poruke i nositelja unutar kojeg je ta poruka ugniježđena, naziva se **steganografski medij** ili **stego**. U svrhu dodatne zaštite, moguća je i uporaba **steganografskog ključa** kojim se tajna poruka kriptira prije umetanja u nositelj. Steganografski medij se stoga može prikazati u sljedećem obliku:

steganografski_medij = tajna_poruka + nositelj + steganografski_ključ



Slika 4: Steganografski sustav

Pojašnjenje pojmova s prethodne slike koji čine dio steganografskog sustava:

- $\mathbf{f_E}$: steganografska funkcija "ugrađivanje"
- $\mathbf{f_E^{-1}}$: 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

2.1. Povijest steganografije

Premda je pojam steganografija formiran tek krajem 15. stoljeća, različite steganografske tehnike koriste se već nekoliko tisućljeća. Slijedi pregled najpoznatijih primjena steganografije kroz povijest:

- Voštane pločice - u staroj 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 kompliciranо 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 (eng. *null cipher*) - 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.

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. Razvijen je velik broj različitih steganografskih alata koji omogućavaju skrivanje bilo kakve binarne datoteke unutar druge binarne datoteke. Slike i zvučni zapisi ipak su najuobičajeniji nositelji u kontekstu steganografije.

2.2. Primjena steganografije

Kao i mnoge druge sigurnosne metode i alati, steganografija se može koristiti u različitim područjima i aktivnostima, kako legalnim tako i ilegalnim. Legalnu primjenu najvećim dijelom sačinjava korištenje digitalnog vodenog pečata u svrhu zaštite autorskih prava i vlasništva nad multimedijskim datotekama. Steganografija se također koristi kao supstitut za generiranje jednosmjerne *hash* vrijednosti, tj. sažetka. Na taj način se nakon obrade varijabilne veličine informacija kao rezultat dobiva izlazni skup podataka fiksne veličine kojim se potom može utvrditi ukoliko su izvršene ikakve promjene nad izvornim skupom podataka. Nadalje, steganografijom je moguće dodati različite bilješke multimedijskim datotekama tako da se njihov format ne mijenja, čime se ne stvara potreba za korištenjem posebnih preglednika. Naposljetku, daleko najlogičnija primjena steganografije je upravo očuvanje povjerljivosti i tajnosti važnih informacija te njihova zaštita od potencijalne sabotaže, krađe ili neovlaštenog pristupa.

Zbog svoje posebnosti kao sredstva tajne komunikacije, steganografija često nalazi mjesto i u ilegalnim aktivnostima pošto omogućava skrivanje dokaza o istima. Ilegalna primjena steganografskih tehnika najčešće se veže uz krađu povjerljivih informacija (npr. u industriji i poslovnom sektoru), financijsku pronevjeru, razmjenu dječju pornografije, krađu identiteta, kockanje, krijumčarenje, hakiranje i terorizam. Tako je npr. nakon terorističkog napada 11.09.2001., napisano mnogo članaka u kojima je predstavljena teorija o komunikaciji između članova terorističke organizacije pomoću steganografskih medija u kojima je kao nositelj korištena pornografija.

2.2.1. Vodeni pečat

Digitalni vodeni pečat temelji se na umetanju dodatnih informacija u izvornu datoteku (nositelj) na način da se kvaliteta nositelja ne promijeni u tolikoj mjeri da dodavanje pečata postane primjetno. U današnje vrijeme vodeni pečat koristi se u sljedeće svrhe:

- zaštita autorskih prava - onemogućavanje krađe vlasništva nad digitalnim multimedijskim datotekama pri čemu je bitno je da se pečat ne može neautorizirano ukloniti te da je otporan na razne modifikacije signala nositelja,
- zaštita od kopiranja – kontroliranje uređaja za kopiranje podataka i prevencija kopiranja zaštićenih multimedijskih sadržaja,
- provjera autentičnosti – provjeravanje autentičnosti multimedijskih sadržaja pri čemu se pečat dodaje po cijelom signalu nositelja tako da se kasnije može detektirati lokacija na kojoj isti nedostaje i
- pohrana dodatnih informacija – dodavanje veće količine podataka koji mogu služiti kao bilješke o multimedijskoj datoteci. Koriste se posebne metode dodavanja pečata koje podržavaju pohranu većeg skupa podataka, a pri kojima se zadržava kompatibilnost sa starijim preglednicima dotičnih multimedijskih sadržaja.

Vodeni pečat umeće se izravno u datoteku i to obično primjenom neznatnih varijacija u svjetlini piksela (eng. *pixel*). Te varijacije su iznimno suptilne i ne mogu se uočiti ljudskim okom. Uzorci se višestruko ponavljaju što omogućava obnovu vodenog pečata i u slučaju uklanjanja nekih dijelova multimedijske datoteke. Neki vodeni pečati također mogu opstati i nakon ograničenog broja uređivanja multimedijske datoteke koje uključuje promjenu kontrasta i filtriranje.
U svrhu testiranja i unapređivanja tehnika umetanja vodenog pečata, razvijeno je nekoliko metoda napada ili razbijanja istog: uništavanje vodenog pečata (eng. *robustness attacks*), onemogućavanje detekcije vodenog pečata (eng. *presentation attacks*), krivotvorenje vodenog pečata (eng. *interpretation attacks*), iskorištavanje manjkavosti zakona (eng. *legal attacks*):

1) Uništavanje vodenog pečata
Metoda uništavanja vodenog pečata bazira se na pokušaju uklanjanja prisustva vodenog pečata bez oštećivanja multimedijske datoteke. Ovakvi napadi mogu biti klasificirani u dvije skupine: napadi procesiranjem signala te analitički i algoritamski napadi. Prva skupina uključuje uobičajene operacije procesiranja multimedijske datoteke kao što su kompresija, filtriranje, promjena veličine, ispis i skeniranje. Druga pak skupina bazira se na uklanjanju ili slabljenju vodenog pečata korištenjem specifičnih metoda umetanje i detekcije vodenog pečata. Primjer takvog napada je generiranje nove multimedijske datoteke kombiniranjem različitih inačica iste datoteke s vodenim pečatom. Na taj način reducira se jakost vodenog pečata.

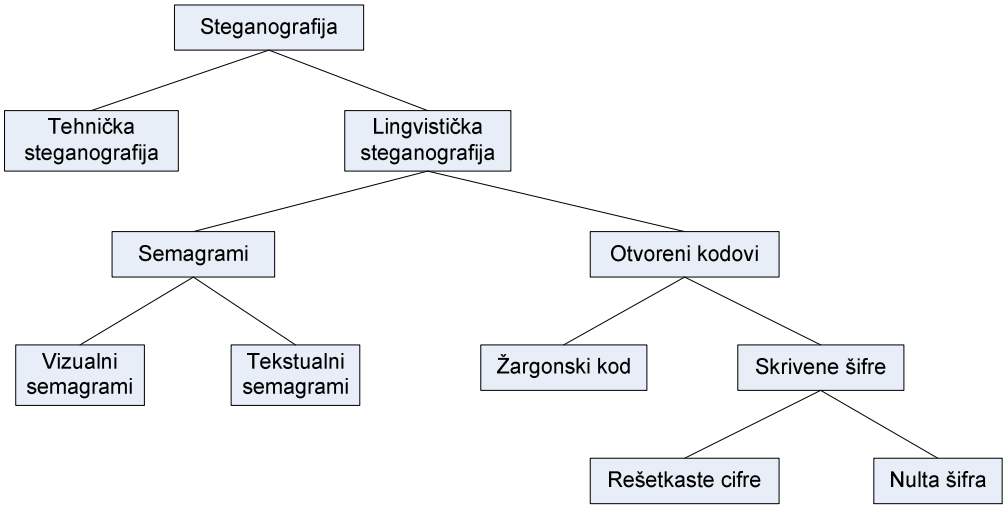
2) Onemogućavanje detekcije vodenog pečata
Da bi strana koja pokušava detektirati vodeni pečat bila onemogućena u tome, koriste se različite tehnike manipulacije sadržajem u kojem se nalazi pečat, ali na način da se pečat ne uklanja niti da mu se smanjuje jakost. Primjeri takvih napada su promjena lokacije vodenog pečata unutar multimedijske datoteke, njegova rotacija ili promjena veličine.

3) Krivotvorenje vodenog pečata
Napadi krivotvorenjem baziraju se na neispravnim ili višestrukim interpretacijama vodenog pečata. Npr. napadač može pokušati umetnuti dodatni vodeni pečat u ciljnu multimedijsku datoteku i to tako da bude jednake jakosti kao i izvorni vodeni pečat. Na taj način onemogućava se jednoznačno i ispravno utvrđivanje vlasništva te datoteke.

4) Iskorištavanje manjkavosti zakona
Ovakvim napadima moguće je osporiti vodeni pečat iskorištavanjem potencijalnih manjkavosti u sljedećim komponentama: zakonske legislative vezane uz zaštitu autorskih prava i vlasništva nad digitalnim informacijama, kredibilitet vlasnika i napadača, financijska potkovanost vlasnika i napadača, stručni svjedoci i kompetentnost odvjetnika.

3. Tehnike steganografije

Na slici *Slika 5: **Pregled steganografskih tehnika*** prikazana je taksonomija steganografskih tehnika (Bauer 2002):



Slika 5: Pregled steganografskih tehnika

Popis steganogafskih tehnika:

- **Tehnička steganografija** (eng. *technical steganography*) koristi znanstvene metode za skrivanje poruka, kao što su uporaba nevidljive tinte, mikrofotografija i ostale tehnike smanjivanja veličine tajne poruke.
- **Lingvistička steganografija** (eng. *linguistic steganography*) 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** (eng. *semagrams*) skrivaju informacije uporabom različitih simbola i znakova. Postoje vizualni i tekstualni semagrami.
- **Vizualni semagrami** (eng. *visual semagrams*) 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** (eng. *text semagrams*) skrivaju informacije različitim modifikacijama teksta nositelja, npr. suptilna promjena veličine ili tipa fonta, dodavanje suvišnih razmaka ili korištenje različitih ukrasa u rukopisu.
- **Otvoreni kodovi** (eng. *open codes*) 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** (eng. *jargon code*) 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** (eng. *covered ciphers*) 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** (eng. *grille ciphers*) 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** (eng. *null cipher*) 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.

Jedan od najjednostavnijih i najpoznatijih primjera primjene nulte šifre je poruka koju je jedan njemački špijun slao za vrijeme 2. svjetskog rata:

„APPARENTLY NEUTRAL'S PROTEST IS THOROUGHLY DISCOUNTED AND IGNORED. ISMAN HARD HIT. BLOCKADE ISSUE AFFECTS PRETEXT FOR EMBARGO ON BYPRODUCTS, EJECTING SUETS AND VEGETABLE OILS.“

Uzimanjem 2. slova iz svake riječi, dobiva se sljedeća tajna poruka:

„PERSHING SAILS FROM N.Y. JUNE 1“

U drugom primjeru tajna poruka iz prvog primjera zamaskirana je unutar lažiranog PGP ključa generiranog na web stranici https://www.spammimic.com/. Kreirani steganografski medij, tj. PGP ključ sa skrivenom tajnom porukom izgleda ovako:

```
-----BEGIN PGP MESSAGE-----
Charset: ISO-8859-1
Version: GnuPG v1.2.5 (MingW32)
Comment: Using GnuPG with Thunderbird - http://enigmail.mozdev.org

UEVSU0hJTkcgU0FJTFMgRlJPTSBOLlkuIEpVTkUgMQ==
-----END PGP MESSAGE-----
```

Također korištenjem nulte šifre, na ovaj se način dobiva stego u obliku PGP ključa koji obično ne privlači posebnu pozornost na sebe u svakodnevnoj komunikaciji. Tajnu poruku moguće je izdvojiti kopiranjem cijelog lažiranog PGP ključa u tekstualno polje na web stranici https://www.spammimic.com/decodepgp.shtml i pritiskom na gumb *Decode*.

3.1. Digitalne steganografske 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.

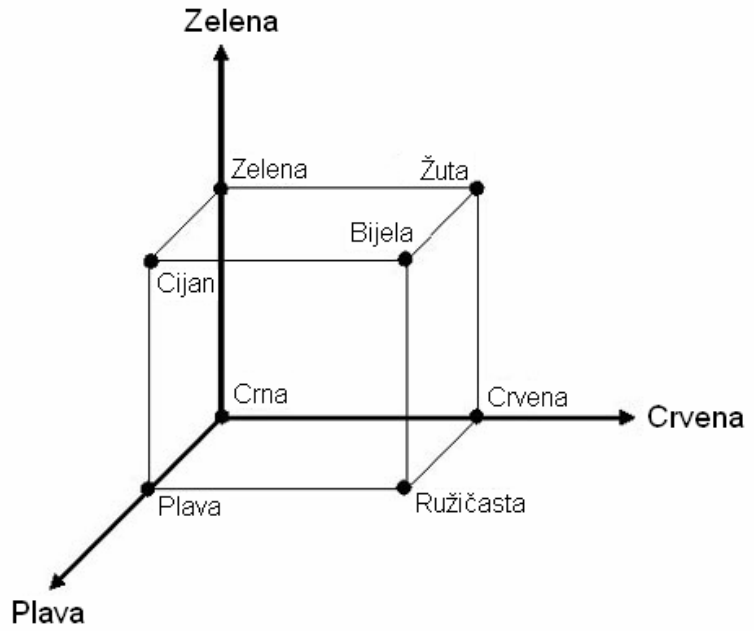
Mrežni protokoli također mogu igrati ulogu digitalnih nositelja. Tako npr. CTCP protokol (eng. *Covert Transmission Control Protocol*) osmišljen od strane Craiga Rowlanda, formira tajne komunikacijske kanale korištenjem identifikacijskog polja u IP paketima ili polja s brojem sekvence u TCP paketima.

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. Najpopularnije od njih opisane su u ostatku ovog poglavlja s naglaskom na korištenje digitalne slike kao nositelja.

3.1.1. Sustavi bazirani na supstituciji

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 RGB (eng. *Red-Green-Blue*) sustava.

Unutar RGB sustava, svaka boja se prikazuje pomoću relativnog intenziteta svake od 3 postojeće komponente – crvene, zelene i plave. Nedostatak svih komponenti rezultira pojavom crne, dok prisustvo svih komponenti rezultira dobivanjem bijele boje.



Slika 6: RGB kocka

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 u slici. Svaki piksel kodiran je s 8 bitova, gdje dotična vrijednost označava indeks zapisa željene boje u paleti. Stoga ova metoda ograničava broj korištenih boja u slici na 256, zbog 8-bitnog prikaza indeksa boje u paleti. 8-bitna shema tipična je za GIF (eng. *Graphics Interchange Format*) formate slika koji se generalno smatraju kompresijom slike bez gubitaka.

3.1.1.1. Supstitucija bita najmanje važnosti

Supstitucija bita najmanje važnosti (eng. *least significant bit substitution; LSB substitution*) 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 (128_{10}), a bit najmanje važnosti onaj s najmanjom aritmetičkom vrijednošću (1_{10}). 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 primijećivanje takvih promjena u boji.
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
```

Slovo *'G'* se prema ASCII *(eng. American Standard Code for Information Interchange)* standardu zapisuje kao binarni niz 01000111. Ovih 8 bitova zapisuje se na mjesto bitova najmanje važnosti u izvornom skupu okteta:

```
10010100 00001101 11001000 10010110
00001110 11001011 10011111 00010001
```

U navedenom primjeru zapravo je promijenjeno samo pola bitova najmanje važnosti.
LSB supstitucija je jednostavna steganografska tehnika, no njena primjena često i nije tako jednostavna. Naime, ako se skup okteta u koje se umeće po bit tajne poruke odabere na jednostavan način, npr. niz susjednih okteta na početku datoteke, vrlo je vjerojatno da će taj dio slike imati drugačije statistike od ostatka slike te će kao takav privući pozornost na sebe i kompromitirati tajnost skrivene poruke. Stoga se skup ciljnih okteta najčešće definira nekom metodom nasumičnog odabira što je jedan od faktora koji detekciju steganografskih poruka čine izrazito kompliciranom.
Primjer jednostavne LSB supstitucije dan je na slici *Slika 7**: 4-bitna LSB supstitucija***. Na lijevoj strani slike prikazane su izvorne slike – gornja lijeva predstavlja nositelja, a donja lijeva tajnu poruku. Obje slike iste su veličine. 4 bita najmanje važnosti unutar slike nositelja zamjenjuje se s 4 odgovarajuća bita najveće važnosti iz tajne slike. Na desnoj strani slike prikazane su modificirane slike – gornja desna predstavlja stego, tj. poruku skrivenu unutar nositelja, a donja desna naposljetku izdvojenu tajnu sliku.

Slika 7: 4-bitna LSB supstitucija

LSB supstitucija pokazuje dobre rezultate i u radu s crno-bijelim slikama. Ako se podaci sakriju unutar 2 bita najmanje važnosti, ljudsko oko još uvijek ne vidi razliku.
Nažalost, LSB supstitucija osjetljiva je i na najmanje operacije nad slikom, kao što su kompresija ili uklanjanje nekih dijelova slike. Npr. konvertiranje GIF ili BMP steganografske datoteke u JPEG format te konvertiranje natrag u izvorni format može dovesti do uništavanja informacija u bitovima najmanje važnosti.

3.1.1.2. Sortiranje paleta

Kao što je već rečeno, mnoge slike koriste palete boja korištene unutar slike. Palete, naravno, sadrže samo podskup cjelovitog prostora boja unutar 24-bitnog prikaza te je svaka 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 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.

3.1.2. Transformacije domena

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 format slike koristi diskretnu kosinusnu transformaciju (eng. *discrete cosine transform* - DCT) 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.

3.1.3. Maskiranje i filtriranje

Tehnike maskiranja i filtriranja obično se koriste samo na 24-bitnim i crno-bijelim slikama i najčešće se primjenjuju za umetanje digitalnog vodenog pečata. Umetnuta poruka sofisticiranije je integrirana u nositelj i dodaje određenu redundanciju skrivenoj informaciji. Zato je u radu s JPEG slikama ova tehnika prikladnija od LSB supstitucije. Također može pridonijeti zaštiti od gubljenja umetnute informacije tijekom procesiranja slike.

3.1.4. Modeli proširenog spektra

Modeli proširenog spektra kao steganografski nositelj koriste signal širokog spektra, dok je poruka koja se umeće signal uskog spektra. Tajni podaci prostiru se preko dijelova nositelja koji imaju najveću važnost (obično su to najveći DCT koeficijenti),te tako otežavaju svoje otkrivanje i ometanje. Ovakvi modeli polaze od činjenice da se male distorzije na slici ili zvučnom zapisu najteže otkrivaju u dijelovima nositelja koji nose najvišu energiju. Ovo je vrlo popularna tehnika u području digitalnog vodenog pečata.

3.1.5. Kvantizacija

U svakom kvantizacijskom koraku javlja se kvantizacijska greška. Za visoko korelirane signale dotični signal razlike, tj. pogreške, biti će blizu nule pa se za njih može efikasno koristiti entropijski koder. Za potrebe steganografije, kvantizacijska pogreška u predvidljivoj shemi kodiranja može se iskoristiti tako da signal razlike prenosi veću količinu informacija.

3.1.6. Binarne slike

Binarne slike (npr. podaci dobiveni faksom) sadrže određenu količinu redundancije u distribuciji crnih i bijelih piksela. Jednostavne LSB supstitucije ne daju dobre rezultate u radu s ovakvim slikama, ali moguće je iskoristiti njihovu redundantnost i umetnuti tajne informacije korištenjem broja crnih piksela u specifičnom dijelu slike.

4. Steganaliza

Steganaliza je proces detektiranja steganografskih datoteka koji se temelji na proučavanju varijacija uzoraka bitova i neobično velikih datoteka. Ciljevi steganalize 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 i
- 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 steganalize. 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 (eng. *tag*) mogu sadržavati tajne podatke.
- Okviri - informacije mogu biti skrivene unutar HTML koda svakog okvira web stranice.

4.1. Oblici napada (otkrivanja steganografije)

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 (eng. *Steganography-only attack*) - dostupna je samo steganografska datoteka nad kojom se potom provode različite analize.
- Poznati nositelj (eng. *Known-carrier attack*) - raspoloživi su i steganografska datoteka i steganografski nositelj, tj. izvorna datoteka unutar koje je tajna poruka skrivena.
- Poznata poruka (eng. *Known-message attack*) - dostupna je tajna poruka.
- Odabrana steganografska tehnika (eng. *Chosen-steganography attack*). poznata je i steganografska datoteka i steganografski alat, odnosno algoritam korišten za umetanje tajne poruke.
- Odabrana poruka (eng. *Chosen-message attack*) - 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 (eng. *Known-steganography attack*) - raspoloživa je steganografska datoteka, steganografski nositelj te steganografski alat, odnosno algoritam korišten za umetanje tajne poruke.

4.2. 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.

4.2.1. 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.

4.2.2. 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.

5. Zaključak

Steganografija raspolaže vrlo efikasnim i snažnim tehnikama koje ljudima omogućavaju zaštićenu i skrivenu komunikaciju. Kombinirana s kriptografijom, predstavlja dodatni sigurnosni sloj u zaštiti informacija. Steganografska tehnologija vrlo je jednostavna za upotrebu, a izrazito se teško detektira.
U posljednjih nekoliko godina, steganografija je bila tema mnogih diskusija vezanih uz njenu zloupotrebu, naročito u terorističkim aktivnostima. Tako u mnogim zakonskim tijelima raste zabrinutost oko upotrebe steganografije za razmjenu ilegalnih materijala preko multimedijalnih datoteka na web stranicama. Steganaliza je puno mlađa znanstvena disciplina od steganografije, no, već danas postoje različite steganalitičke metode pomoću kojih se vrlo uspješno mogu detektirati i spriječiti takve kriminalne aktivnosti.
S druge strane, postoji velik broj prednosti korištenja steganografije u legalnom kontekstu, kao što su digitalni vodeni pečati za utvrđivanje vlasništva i autorskih prava ili sigurnije metode pohrane važnih i povjerljivih informacija, stoga se u budućnosti očekuje još intenzivniji razvoj ove tehnologije te široka mogućnost primjene.

6. Reference

[1] Steganography Revealed, Kristy Westphal, http://www.securityfocus.com/infocus/1684
[2] Steganography & Digital Watermarking, http://www.jjtc.com/Steganography
[3] StegoArchive.Com, http://www.stegoarchive.com/
[4] Steganography, Neil F. Johnson, George Mason University, http://www.jjtc.com/stegdoc
[5] Wikipedija, http://en.wikipedia.org/wiki/Steganography
[6] An Overview of Steganography for the Computer Forensics Examiner, Gary C. Kessler, http://www.fbi.gov/hq/lab/fsc/backissu/july2004/research/2004_03_research01.htm
[7] A brief history of steganography, Matteo Fortini, http://www.lia.deis.unibo.it/Courses/RetiDiCalcolatori/Progetti98/Fortini/history.html
[8] Introduction to Steganography, http://www.infosyssec.com/infosyssec/Steganography/menu.htm