Elektronski fakultet u Nišu

Univerzitet u Nišu

Katedra za računarsvo

Detekcija steganografije

Digitalna forenzika

Anđelija Đorđević 1033

Sadržaj

Uvod

Ovaj seminarski rad daje prikaz i objašnjenja metoda koje se koriste za detekciju steganografije. Na početku rada data je definicija steganografije i opšte podele. Steganografija predstavlja način sakrivanja podataka u nekom drugom skupu podataka. O korišćenju steganografije postoje zapisi još iz perioda pre nove ere. Od tada, sve do današnjice, steganografija je u upotrebi, a jedino se njene forme menjaju, shodno vremenu. Od najranijeg vremena vladari su imali različite ideje za sakrivanje informacija, poput tetovaža na obrijanoj glavi roba ili nevidljivog mastila, dok se danas zbog gotovo neizbežne upotrebe interneta sve više steganografije nalazi u digitalnim medijima. Pre mnogo vremena se steganografija često koristila u junačke svrhe, međutim danas sve češće nailazi na zloupotrebu. U mnogim radovima se navodi da je upravo steganografija sredstvo komunikacije među teroristima. Za sada nema dokaza za navedene teorije, ali u ovakvim situacijama je neophodno uraditi sve kako bi se nemili događaji sprečili.

Često je nemoguće otkriti sakrivenu poruku u nekom digitalnom mediju, često su te poruke kodirane i sam tekst se može otkriti jedino ključem koji je poznat samo stranama koje komuniciraju. Međutim, postoje načini kojima se može detektovati postojanje sakrivene poruke, što u određenoj meri predstavlja napredak u otkrivanju zlonamernog sadržaja. Poruke se mogu sakriti u bilo kom digitalnom medijumu, ali se možda najčešće steganografija pronalazi u slikama. Zbog svega navedenog ovaj rad istražuje načine za detekciju postojanja sakrivenih poruka u slikama.

Sakrivanje informacija

Sakrivanje informacija je oblast računarskih nauka koja se bavi prikrivanjem postojanja informacija. Povezana je sa kriptografijom, ali za razliku od kriptografije kod koje se zna da postoji poruka koja se prenosi, ali je sadržaj poruke sakriven, kod tehnike sakrivanja informacija poruka se nalazi tamo gde se ne očekuje. Celokupan sadržaj je sakriven.

U sakrivanje informacija spadaju:

1. Steganografija
2. Watermarking
3. Sakriveni kanali

Watermarking (Vodeni žig)

Osnovna ideja kod vodenog žiga jeste da se on ne može ukloniti bez oštećenja osnovnih podataka. Watermarking se zbog ove osobine najčešće koristi za zaštitu autorskih prava.

Postoji nekoliko vrsti vodenih žigova. Jedna podela je:

1. Nevidljivi vodeni žigovi
2. Vidljivi vodeni žigovi.

U prvom slučaju, kod nevidljivih vodenih žigova, podacima se dodaje nevidljivi identifikator. Ovakve tehnike se koriste za skoro sve tipove digitalnih medija ili softvera. Može se koristiti za utvrđivanje vlasništva ili pronalaženja piratskih verzija medija.

Vidljivi vodeni žigovi postoje kako bi se poštovali, u vidu posebnih napomena na dokumentima. Većina savremenih valuta sadrži vidljive vodene žigove. Često je vodeni žig na novčanicama napravljen tako da se vidi samo kada se drži okrenut prema svetlosti. Novčanice sadrže vodene žigove kako bi se falsifikovanje znatno otežalo. Čak i sa posebnim papirom, znatno je teže umnožiti ovakvu novčanicu, dok se vrlo jednostavno može proveriti ispravnost iste.

Postoji još jedna kategorizacija vodenih žigova:

1. Robusni vodeni žigovi
2. Fragile vodeni žigovi.

Robusni vodeni žigovi bi trebalo ostati čitljivi čak i nakon napada. Dok su *fragile* vodeni žigovi dizajnirani tako se unište ili oštete u slučaju pokušaja zloupotrebe. Ukoliko je vodeni žig nečitljiv, primalac zna da je došlo do neovlašćenog pristupa. Ovakav tip watermarking-a je od suštinskog značaja za oblik provere integriteta [1].

Skriveni kanali

Tehnike prikrivenih kanala koriste komunikacione kanale za prenos poruka na način na koji nisu predviđeni. Određeni broj zvona telefonskog poziva može imati posebno značenje. Nekorišćeni, tačnije rezervisani bitovi u zaglavljima paketa računarskih mreža takođe mogu nositi tajne informacije. Steganografija se može smatrati prikrivenim kanalom [2].

Steganografija

Reč steganografija potiče od dve grčke reči, “steganos” koja ima značenje sakriven ili tajna i “graphy” koja znači pisanje ili crtanje. U bukvalnom prevodu, steganografija označava skriveno pisanje.

Steganografija predstavlja umetnost i nauku sakrivanja komunikacije [3]. Poruka koja se prenosi sakrivena je u drugom skupu podataka tako da se sakriveni podaci ne mogu detektovati. Razmena poruka ne mora biti tajna, ali je neophodno obezbediti da se poruke razmenjuju javno, ali neopaženo, bez saznanja šta je u njima sakriveno. Postoji veliki broj razloga zbog kojih se koristi steganografija i često su u bitanju značajne oblasti. Može se koristi za komunikaciju sa potpunom slobodom čak i u situacijama kada je komunikacija cenzurisana ili posmatrana. Takođe se može koristiti kao zaštita privatnih komunikacija gde korišćenje kriptografije nije dozvoljeno ili bi proizvelo sumnju koja bi zahtevala neki vid provere samih poruka [4]. U prošlosti, ljudi su koristili sakrivene tetovaže i nevidljiva mastila, dok danas računari i računarske mreže omogućuju jednostavne komunikacione kanale za primenu steganografije. Najčešće se primenjuje na rasterskim slikama, na audio, video i tekstualnim podacima ili izvršnim datotekama.

Oko 440. godine pre nove ere, grčki general je obrijao glavu roba i na njoj napisao tajnu poruku radi upozorenja na persijsku invaziju koja je predstojila. Kada je kosa roba izrasla dovoljno da prekrije poruku, rob je poslat kroz neprijateljske linije kako bi isporučio skrivenu poruku. Ovo je jedan od prvih primera steganografije.

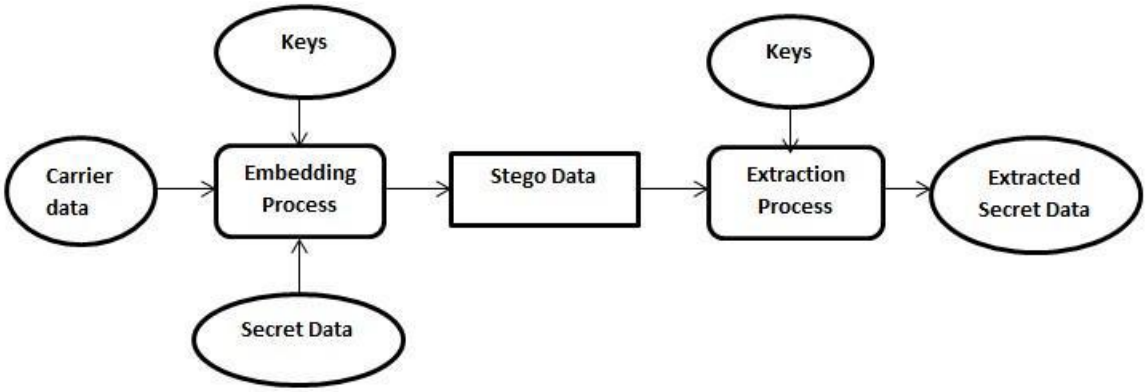
Pored primarnog cilja steganografije koji je sakrivanje podataka u drugom skupu podataka, postoje i sekundarni ciljevi. Neophodno je sprečiti ekstrakciju sakrivenih podataka bez uništenja podataka koji ih sakrivaju. Takođe, potrebno je sprečiti i uništenje sakrivenih podataka bez uništenja podataka koji ih sakrivaju.

Podaci u kojima se sakriva poruka ne smeju biti vidljivo promenjeni nakon dodavanja tajne poruke. Međutim, kako bi ovo bilo zadovoljeno postoji ograničenje kapaciteta tajne poruke u zavisnosti od samog tipa podatka koji se koristi za sakrivanje. Postoji pravilo 15% koje govori da se u nekoj datoteci može sakriti do 15% originalne količine podataka bez izobličenja.

Sistem steganografije se sastoji od tri komponente:

1. *Cover* objekta koji sakriva tajnu poruku
2. Tajne poruke
3. Stego-objekta koji predstavlja *cover* objekat sa sakrivenom porukom.

Često se pre slanja stego-objekta poruka koja se krije kodira pomoću odgovarajućeg ključa. Na prijemnoj strani, primalac sadrži ključ sa kojim dekodira prenetu poruku. Čak i uspešnom detekcijom steganografije, niko ne može saznati tačan sadržaj skrivene poruke, ukoliko ne zna ključ za dekodiranje [19]. Na slici 1 da je prikaz procesa steganografije.



Slika 1. Proces steganografije.

Mere uspešnosti steganografije

Efikasnost tehnika steganografije određuje se poređenjem naslovne slike (cover-slike) sa stego slikom. Faktori kojima se meri uspešnost su sledeći:

Robustnost

Robustnost se odnosi na sposobnost ugrađenih podataka da ostanu nepromenjene ukoliko dođe do transformacija stego objekta. U slučaju steganografije slika transformacije mogu biti linearno ili nelinearno filtriranje, izoštrenje ili zamućenje fotografije, dodavanje šuma, rotacija, skaliranje, sečenje ili kompresija.

Neprimetnost

Neprimetnost označava nevidljivost algoritma steganografije. Ovo je prvi i najvažniji zahtev steganografije, obzirom da jačina steganografije leži upravo u karakteristici da je steganografija nevidljiva za ljudsko oko.

Mean Square Error

Mean Square Error se izračunava poređenjem bajta po bajt za slike. Distorzija slike se može meriti korišćenjem Mean Square Error. Neka je I naslovna slika (cover slika), a neka je K stego slika. Proizvod m*n predstavlja ukupan broj piksela. Tada se MSE može izračunati na sledeći način:

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

Tehnike steganografije

Postoje različite tehnike steganografije, to su:

1. Sistemi substitucije
2. Tehnike u domenu transformacije
3. Tehnike širokog sprektra
4. Statističke metode
5. Tehnike distorzije
6. Tehnike kreiranja podataka koji sakrivaju.

Kod sistema substitucije sakrivanje podataka se vrši u redundantnim delovima ili delovima sa šumom. Tehnike u domenu transformacije sakrivanje vrše u prostoru transformacije. Kod tehnika širokog spektra sakrivanje se vrši širom sprektra koji koriste podaci koji sakrivaju. Statističke metode vrše izmenu nekih statističkih karakteristika. Tehnike distorzije vrše blagu izmenu karakteristika podataka koji kriju dok tehnike kreiranja podataka koji sakrivaju vrše kodiranje tajne poruke prilikom kreiranja podataka koji kriju.

Steganografija u slikama

U digitalnom dobu veliki deo komunikacije se obavlja putem digitalnih medija. Posledica ovoga jeste da se i steganografija sve više koristi u digitalnom formatu korišćenjem digitalnih medija. Zbog sve veće upotrebe interneta u komunikaciji, postao je vodeći prenosnik digitalne steganografije [8].

Bilo koji digitalni format može se koristiti za steganografiju, slike, audio, video, tekstualni podacima i slično, ali najpogodniji i najrasprostranjeniji mediji u steganografiji su slike. Na slici 2 dat je prikaz steganografije u slikama.

Slika 2. Steganografija slike.

Steganografija u slikama se najčešće deli na:

1. *Least significant bit* (LSB) metod dodavanja
2. Maskiranje i filtriranje
3. Algoritmi i transformacije

Least significant bit metod dodavanja

Least significant bit metod dodavanja je metod koji se najčešće koristi. Podaci koji se sakrivaju dodaju se na mesto najmanje značajnog bita u pikselima. U digitalnom formatu slike se predstavljaju numeričkim vrednostima za svaki piksel, gde numerička vrednost predstavlja boju i intenzitet. U nastavku će se razmatrati dva formata slika, 24-bitna i 8-bitna slika.

24-bitne slike imaju 24 bita vrednosti za svaki piksel, gde se u svakih 8 bitova vrednost odnosi na boje *crvena, plava* i *zelena.* U svakom pikselu mogu se uneti 3 bita koja bi predstavljala deo sakrivene poruke, tako što se upisuju u svakoj LSB poziciji ove tri 8-bitne vrednosti koje predstavljaju boje u 24-bitnom formatu slika.

U svakom pikselu 8-bitnih slika može se sakriti 1 bit informacije. Kako se u 8-bitnom formatu slika boja predstavlja sa 8 bitova, ukupno ima 256 boja. Dodavanjem sakrivene informacije menja se LSB, a samim tim i boja, te se u korišćenju steganografije kod 8-bitnih slika mora biti posebno oprezan. Kod 8-bitnog formata boja najbolje je koristiti sliku sa paletom sivih boja, kako bi razlika između boja sa susednim vrednostima bila što manja.

Prednosti ovakvog modela steganografije ogledaju se u neznatnim promenama originalne slike, manja je šansa uništenja iste. Takođe, na ovaj način se veliki broj informacija može sakriti, kapacitet sakrivanja je veliki.

Mane ovog metoda ogledaju se u nedostatku robustnosti. Sakriveni podaci mogu biti izgubljeni ukoliko se izvši modifikacija slike. Još jedna mana ovog pristupa jeste što se sakriveni podaci mogu lako uništiti jednostavnim napadom.

Maskiranje i filtriranje

Maskiranje se odnosi na prekrivanje jednog signala drugim signalom. Ovakav pristup bazira se na činjenici da ljudsko oko ne može da detektuje sitne promene. Maskiranje se često koristi kod tehnika vodenog žiga (watermarking). Ova tehnika ne predstavlja čistu tehniku steganografije jer se u ovom slučaju proširuju informacije slike, kao i ostali atributi slike.

Kako je većina podataka integrisana u samoj slici, podaci neće biti izgubljeni čak i kada se izvrši transformacija slike potput kompresije, sečenja i slično.

Algoritmi i transformacije

Tehnika algoritmi i transformacije u sliku koja će biti nosilac sakrivenih informacija, ugrađuje podatke menjajući koeficijente transformacija slike, poput *discrete cosine transform coefficients.* Ukoliko se sakrivene informacije ugrađuju u sliku u prostornom domenu može doći do gubitka informacije ukoliko se vrši neka modifikacija slike (kompresija, sečenje…). Kako bi se sprečio ovaj problem, informacije se sakrivaju u frekventnom domenu. Kako bi se analizirali podaci slike, neophodno je prvo izvršiti transformaciju iste. Sakriveni podaci se ugrađuju menjanjem vrednosti koeficijenata transformacija na taj način.

Najbitnije tri tehnike koje se koriste kao tehnike transformacije su:

1. *Fast Fourier transformation technique (FFT)*
2. *Discrete cosine transformation technique (DCT)*
3. *Discrete Wavelet transformation technique (DWT)*

Discrete Fourier Transform (DFT)

Diskretna Furijeova transformacija je transformacija koja je čisto diskretna, diskretni vremenski signali se pretvaraju u diskretni broj frekvencija. DFT pretvara konačnu listu jednako raspoređenih uzoraka funkcije u listu koeficijenata konačne kombinacije složenih sinusoida poređanih po njihovim frekvencijama. Može se reći da konvertuje funkciju iz njenog izvornog domena koji je često vreme ili položaj duž linije frekventnog domena. *Discrete Time Fourier* transformacija koristi diskretno vreme, ali se pretvara u neprekidnu frekvenciju. Algoritam za računanje DFT je veoma brz na savremenim računarima. Ovaj algoritam je poznat kao Fast Fourier Transform, tj. FFT i proizvodi isti rezultat kao i kod DFT-a korišćenjem *Inverse Discrete Fourier Transform.*

Discrete Cosine Transform (DCT)

Ovo metoda je slična diskretnoj Fourierovoj transformaciji. DCT transformišite signal ili sliku iz prostornog domena u frekventni domen. Matematičke transformacije vrše izmene piksela na takav način da daju efekat "širenja" lokacije vrednosti piksela na deo slike. DCT se koristi u steganografiji kao da se slika razbija u blokove od 8 × 8 piksela i transformiše ove blokove piksela u 64 DCT. Krećući se od leva na desno, odozgo na dole, DCT se primenjuje na svaki blok. Kroz tablicu kvantizacije se svaki blok kompresuje skalirajući koeficijente DCT i tajna poruka se ugrađuje u DCT koeficijente. Niz kompresovanih blokova koji sačinjavaju sliku, zauzimaju drastično manju količinu prostora. Po potrebi slika se rekonstruiše dekompresijom, procesom koji koristi *Inverse discrete cosine transform*, tj. IDCT.

Discrete Wavalet Transform (DWT)

Discrete Wavalet Transform se koristi za transformisanje slike iz prostornog domena u frekvencijski domen. U procesu steganografije DWT identifikuje visoku i nisku frekvenciju informacije svakog piksela slike. Ovo je matematički alat za hijerarhijsku dekompoziciju slike. Uglavnom se koristi za obradu nestacionarnih signala. The talasna transformacija se zasniva na malim talasima, poznatim kao *wavelet*, različite frekvencije i ograničenog trajanja. Što omogućava i frekvencijski i prostorni opis slika. *Wavelet*-i su stvoreni translacijama i dilatacijama fiksne funkcije, poznate kao matični talas (*mother wavelet*). DWT se izvodi u dvodimenzionalnoj ravni. DWT je tačniji model od DFT ili DCT. Kompresija slike JPEG se zasniva na wavelet transformacijama.

Steganaliza (steganalysis)

Steganalysis je tehnika suprotna steganografiji. Steganaliza pokušava da detektuje postojanje steganografije, odnosno postojanje skrivenih poruka, ili čak da otkrije sadržaj poruke. Pored detekcije i otkrivanja sadržaja sakrivene poruke, u steganalizu spadaju i sve ostale vrste napada na steganografiju, poput uništavanja ili izmene sakrivenih podataka u stego objektima.

Motivacija

Steganografija i steganalysis su veoma aktuelni, posebno sa pravnog stanovišta. Kako je kriptografija u mnogim zemljama ograničena, u sajber kriminalu, a čak i u terorizmu, sve se više koristi komunikacija u vidu steganografije. Korišćenjem steganografije izbegavaju se optužnice sa dekodiranim kriminalnim materijalom kao dokazom. Razumevanje načina na koji

poruke mogu biti ugrađene u digitalne medijume, najčešće slike, kao i metoda detektovanja sakrivenih informacija predstavlja osnovu za razotkrivanje ovakvih kriminalnih aktivnosti [5].

Tipovi detekcije steganografije bazirani na dostupnim podacima

Stego-only attack

Jedini dostupan objekat za analizu jeste objekat u kome je sakrivena poruka (stego-objekat).

Known cover attack

Za obavljanje analize postoji objekat koji sadrži sakrivenu poruku i orginalni objekat bez sakrivene poruke. Porede se dva navedena objekta i pronalazi se razlika.

Known message attack

Known message attack je analiza moguće poruke koja odgovara sakrivenoj informaciji. Ovakav pristup može pomoći detekciji steganografije i u budućnosti. Međutim, čak i sa porukom ovakav pristup je veoma težak i može se posmatrati kao *stego-only attack.*

Chosen stego attack

Za razotkrivanje steganografije poznat je stego-objekat, odnosno objekat koji sadrži sakrivenu poruku, ali i alat ili algoritam uz pomoć kog je urađena steganografija.

Chosen message attack

Steganaliza generiše stego-objekat uz pomoć određenog alata ili algoritma za steganografiju odabrane poruke. Cilj je odrediti šablon u stego-objektu koji će možda ukazati na korišćenje konkretnog alata ili algoritma.

Known stego attack

Poznat je alat za kreiranje steganografije, kao i originalni i stego objekat.

Često korišćene steganografije i njihova detekcija

Prazni delovi diska se mogu iskoristiti za sakrivanje informacija. Postoji veliki broj alata poput EnCase [6] i ILook Investigator [7] koji mogu prijaviti i filtrirati sakrivene informacije na neiskorišćenim delovima klastera ili particija na uređajima.

TCP/IP paketi sadrže sakrivene ili nevalidne informacije u zaglavljima, kao i neiskorišćene delove. TCP paket ima 6 rezervisanih (neiskorišćenih) bitova, dok IP paket ima 2 rezervisana bita. Informacije mogu biti sakrivene i u neiskorišćenim Type of Service (TOS) poljima. Druge opcije za sakrivanje informacija u TCP/IP paketima jesu opciona polja u IP zaglavljima, Timestamp i Time to Live (TTL). Ove tehnike se mogu primenjivati i u drugim protokolima. Hiljade paketa se šalje u svakom komunikacionom kanalu, što obezbeđuje odličan način tajnih komunikacija. Međutim, ovakav način korišćenja steganografije nije pouzdan jer može doći do prepisivanja informacija u toku procesa rutiranja paketa jer rezervisani bitovi mogu biti promenjeni. U tom slučaju bi se izgubile informacije koje su se tajno prenosile.

Za prevenciju ovakvih steganografija može se koristiti firewall. Podešavanjem određenih filtera proverava se sadržaj rezervisanih bitova u paketima, te se takvi paketi mogu izdvojiti ili odbaciti.

Različiti pristupi stegoanalize

Vizuelna detekcija

Posmatranjem šablona koji se ponavljaju može se detektovati sakrivena informacija u slikama koje sadrže steganografiju. Ponavljajući šabloni mogu otkriti “potpis” alata za kreiranje steganografije ili samu sakrivenu informaciju. Čak i mala razlika može otkriti postojanje sakrivenih informacija.

Takođe, posmatranjem slika ponekad se mogu uočiti razlike ili “greške” koje mogu biti put do otkrivanja steganografije.

Strukturni napad

Struktura podatka se često može promeniti sa dodavanjem skrivenih poruka. Identifikovanjem karakterističnih strukturnih promena može se detektovati postojanje skrivene poruke. Primer ovoga je korišćenje steganografije koje se bazira na slikama paleta. Paleta slike se menja pre unošenja tajnih podataka kako bi se redukovao broj boja i kako bi razlika boja između susednih piksela bila što manja. Na ovaj način se dobija da grupa piksela u paleti ima istu vrednost što nije slučaj u normalnoj slici.

Palette Image

Slika paleta (palette image) redukuje memorijski prostor koji je potreban za čuvanje slika. Memorijski prostor se redukuje tako što se prvo redukuje broj boja koji se koristi u slici na najviše 256, a zatim se uzima jedan broj po pikselu kako bi se indeksirala boja o kojoj je reč. Svaki broj koji predstavlja boju odgovara jednoj boji u paleti od 256 boja. Svaka boja u paleti predstavlja jednu RGB boju, iz opsega od milion boja [20].

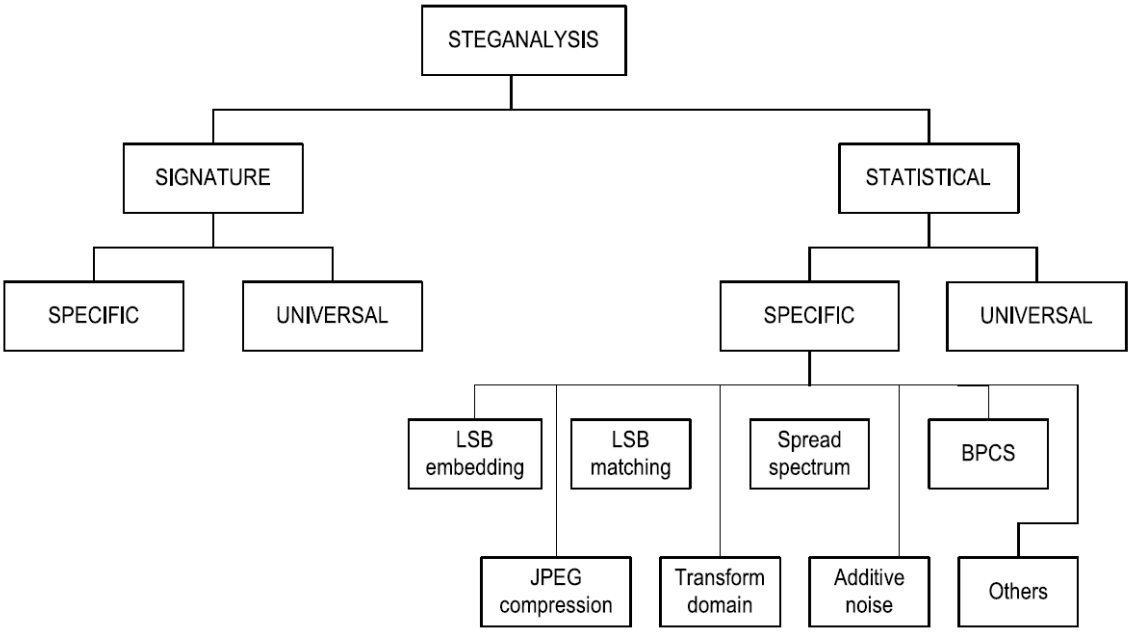
Statistički napad

U statističkim napadima vrši se statistička analiza slika u vidu izračunavanja posebnih matematičkih formula, na osnovu dobijenih rezultata obavlja se detekcija skrivenih podataka. Skrivena poruka je “slučajnije” generisana od originalnih podataka na slici. Korišćenjem odgovarajućih formula može se utvrditi postojanje sakrivene poruke.

Klasifikacija tehnika steganalize

U radu [9] steganaliza je podeljena u dve klase - steganalizu potpisa (u prethodnoj podeli strukturni napad) i statističku steganalizu. Klasifikacija se zasniva na tome da li se koristi potpis tehnike steganografije ili statistika slike kako bi se otkrilo prisustvo skrivenih poruka u slikama ugrađenim pomoću steganografije.

U svakoj klasi navedene tehnike su dalje podele na specifične i univerzalne pristupe. Ovakva podela se zasniva na tome da li se tehnika steganalize odnosi na specifičnu steganografsku metodu ili može rešavati većinu steganografskih tehnika. Čitava hijerarhija podela je prikazana na slici 2.



Slika 2. Klasifikacija steganalize.

Steganaliza potpisa

Metode steganografije skrivaju tajne podatke i manipulišu slikama i drugim digitalnim medijima na način koji ostaje neprimetan za ljudsko oko. Međutim, sakrivanje informacija unutar bilo kog elektronskog medija pomoću steganografije zahteva izmene svojstva medija koja mogu uvesti neki oblik degradacije ili neobične karakteristike i obrasce. Ovi obrasci i karakteristike mogu delovati kao potpisi koji emituju postojanje ugrađene poruke. Dakle, jedna metoda otkrivanja postojanja skrivene poruke u sumnjivoj slici je traženje ovih očiglednih i ponavljajućih obrazaca-potpisa alata za steganografiju. U početnim fazama steganalize, koristili su se potpisi alata za kreiranje steganografije kao mogući način za detekciju i otkrivanje sakrivenih informacija. Ovi specifični potpisi automatski otkrivaju koji se alat koristio za ugrađivanje poruke u digitalni medij. Takve metode uglavnom posmatraju tablice paleta u GIF slikama i anomalije koje su u njima izazvane korišćenjem uobičajenih alata steganografije. Ovi napadi se posebno mogu primenjivati na palete slika za LSB ugrađivanje u indekse u paleti. Takvi napadi su jednostavni, daju obećavajuće rezultate kada se poruka ugrađuje sekvencijalno, ali ih je teško automatizovati i često nisu veoma pouzdani.

Specifična steganaliza potpisa

Hide and Seek [10], softver za steganografiju iz domena slika, stvara slike steganografije sa različitim svojstvima u zavisnosti od korišćene verzije. Verzije 4.1 i 5.0 softvera *Hide and Seek* dele zajedničku karakteristiku u stavkama paleta slika sa steganografijom. Istraživanjem paleta slika sa 256 boja ili pregledavanjem histograma, dokazuje se da su svi ulazi paleta deljivi

sa četiri za sve vrednosti bita. Ovo je vrlo neobična pojava. Slike u formatu *grey-scale* obrađene u verzijama 4.1 i 5.0 imaju 256 tripleta kao što se očekivalo, ali raspon u skupovima od četiri vrednosti ide od 0 do 252, sa inkrementalnim koracima od 4 (tj. 0, 4, 8, …, 248, 252). Ključno za otkrivanje ovoga kada se slike pogledaju je to da su "najsvetije" vrednosti na slici (252, 252, 252). Ovakav potpis je jedinstven za *Hide and Seek*.

Vrlo često se napadi zasnovani na potpisu koriste kako bi se detektovalo prisustvo skrivenih poruka. Kod korišćenja *Jpegx*, alata steganografije za umetanje podataka, tajna poruka se dodaje na kraj JPEG datoteke i dodaje se konstantni potpis programa pre sadržaja tajne poruke. Potpis je sledeći heksa kod: 5B 3B 31 53 00. Prisustvo ovog potpisa automatski implicira da slika sadrži tajnu poruku ugrađenu u osnovi koristeći *Jpegx*.

Razmotrićemo još jedan specifični napad na steganografiju, zasnovan na potpisu specifičnom za BPCS (*Bit Plane Complexity Segmentation*). U BPCS-steganografiji tajni podaci su ugrađeni zamenom blokova koji izgledaju kao šum u ravni bitova. Dakle, blokovi u ravni bitova su kategorisani kao "region šuma" ili "informativni region" pomoću funkcije binarne slike koja se naziva složenost. Mera složenosti predstavlja gustinu crno-belog uzorka. Kroz nekoliko eksperimenata potvrđeno je da histogram složenosti ima neobičan oblik, u obliku doline, kada se radi o slikama steganografije, formiranim pomoću BPCS-steganografije. Ova pojava nije slučaj kod originalnih slika. Opisana "dolina" predstavlja potpis BPCS-steganografije i može se iskoristiti za steganalizu.

Univerzalni potpis steganalize

Slike koje se koriste za sakrivanje poruka, slike steganografije, koje su u JPEG formatu predstavljaju vrlo loš izbor za steganografske metode koje deluju u prostornom domenu. To je zato što kvantizacija, koja je uvedena u JPEG kompresiji, služi kao jedinstveni identifikator koji se može koristiti za detekciju veoma malih modifikacija slike. Modifikacije se mogu uočiti jednostavnom proverom kompatibilnosti slike za koju se sumnja da sadrži tajni podatak sa JPEG formatom.

U ovoj tehnici se slika koja se proverava prvo deli na 8 × 8 blokova, a matrica kvantizacije se dobija analizom vrednosti DCT koeficijenata u svim 8 × 8 blokova. Tabela kvantizacije se upoređuje sa standardnom JPEG tablicom kvantizacije za kompatibilnost. Ukoliko je bilo koji blok nekompatibilan, slika za koju je vršena provera jeste slika steganografije. Navedena tehnika je veoma pouzdana da čak i najsitnije promene poput zamene LSB jednog piksela mogu pouzdano biti detektovane. Međutim, određenim modifikacijama slika može doći do gubljenja JPEG potpisa.

Statistička steganaliza

Razmatrana steganografija ugrađuje tajne poruke u slike. Statistika slike tada prolazi kroz izmene zbog informacija koje sakriva. Statistička steganaliza, kao što i ime implicira, analizira statistiku slike kako bi se detektovale tajne umetnute informacije. Statistička steganaliza smatra se pouzdanijom od steganalize potpisa, jer su matematičke tehnike osetljivije od vizuelne percepcije.

Specifična statistička stegoanaliza

Specifična statistička steganaliza uključuje tehnike statističke steganalize koje traže podatke ugrađene određenom tehnikom steganografije uz malu varijaciju. Ove vrste tehnika su razvijene analizom načina umetanja podataka i određivanjem statistike slike koja će se promeniti nakon procesa ugradnje. Za dizajniranje takvih tehnika neophodno je detaljno znanje o procesu ugradnje. Ove tehnike daju vrlo precizne rezultate kada se koriste protiv steganografskih tehnika. U ovom radu je specifična statistička steganaliza dalje grupisana na osnovu tipa ciljne steganografije.

Least significant bit (LSB) metod dodavanja – stegoanaliza

Ubedljivo najpopularniji i najkorišćeniji metod steganografije jeste Least significant bit (LSB) metod dodavanja. LSB metod dodavanja funkcioniše tako što se bitovi poruke koja se sakriva umetaju u bitove najmanje težine sekvencijalnih ili slučajno odabranih piksela. Selekcija bitova zavisi od tajnog stego ključa koji je određen od strane osoba koje komuniciraju. Popularnost ovog metoda je u njegovoj jednostavnosti. Veliki broj softvera koji koristi ovu tehniku se može naći na internetu.

Kada se poruka koja se ugrađuje kodira, kodirani tekst je veoma sličan slučajnom tekstu. U tom slučaju bi prosečna vrednost LSB u blokovima slike bila oko 0.5, gotovo za sve blokove. Ovo se retko dešava kada su u pitanju originalne slike bez steganografije. Tako da se merenjem prosečnih vrednsti LSB u blokovima slika može ustanoviti da li slika sadrži steganografiju.

Jedan od načina za detekciju LSB ugrađene steganografije u 24-bitne slike u boji jeste Raw Quick Pair (RQP). Metod je predložen u [11]. Metoda se zasniva na analizi bliskih parova boja stvorenih LSB ugradnjom. Pokazano je da se odnos broja sličnih boja sa ukupnim brojem jedinstvenih boja znatno povećava kada je poruka odabrane dužine ugrađena u originalnu sliku. Upravo ta razlika omogućava razlikovanje originalne slike od slike sa ugrađenom LSB steganografijom. Metoda je pouzdana sve dok je broj jedinstvenih boja na originalnoj slici manji od 30% broja piksela. Ova metoda se ne može primeniti na slike u sivim tonovima.

Sofisticiranija tehnika predstavljena je u [12] za detekciju ugradnje LSB u slikama u boji i u sivim tonovima (RS steganaliza). Ova tehnika koristi osetljive dvostruke statistike izvedene iz prostornih korelacija u slikama. Slika je podeljena u odvojene grupe fiksnog oblika. Unutar svake grupe meri se šum kao srednja apsolutna vrednost razlike između susednih piksela. Svaka grupa je klasifikovana kao "regular" ili "singular", zavisno od toga da li se šum piksela unutar grupe povećava ili smanjuje nakon prevrtanja LSB-ova fiksnog skupa piksela unutar svake grupe koristeći "masku". Klasifikacija se ponavlja za dvostruki tip okretanja. Teorijska analiza i eksperimenti pokazali su da udeo "regular" i "singular" grupa formira kvadratne krive u količini poruke koju ugrađuje LSB metod. Poruke za koje je potrebno manje od 0,005 bita po pikselu nije moguće prepoznati korišćenjem RS steganalize.

Tehnika koju su predložili Avcibas i dr. [13] je specifična za algoritme za LSB ugradnju. Ova tehnika posmatra sedmu i osmu bitsku ravan slike i izračunava nekoliko binarnih mera sličnosti. Pristup se zasniva na činjenici da se odnos između kontinualnih bitskih ravni kao i karakteristike binarne teksture unutar bitskih ravni nakon što je poruka ugrađena u sliku, menja. Kako bi se zabeležio efekat stvoren ugradnjom poruke, postoji nekoliko karakteristika koje se izračunavaju. Na osnovu tih karakteristika steganalizator je opremljen merama sličnosti binarnih slika i multivarijantna regresija se koristi za klasifikaciju date slike kao čiste slike ili sa stego sadržajem.

Specifična LSB metoda steganalize data je u [14]. Ovde je istraženo da je statistika uzorka parova signala vrlo osetljiva na LSB ugradnju. Tehnika je zasnovana na konačnim automatima stanja čija su stanja odabrani multisetovi uzorka parova nazvanih *multisets trace*. Ponašanje *multisets trace* sa operacijama LSB ugradnje predstavljeno je konačnim automatom. Struktura ovakvih konačnih automata stanja se koristi za uspostavljanje kvadratnih jednačina na osnovu kojih se procenjuje dužina ugrađenih poruka u zavisnosti od kardinalnosti *multisets trace*. Tehnika precizno meri dužinu ugrađene poruke, čak i kada je skrivena poruka vrlo kratka u odnosu na veličinu slike.

Gradient Energy-Flipping Rate Detection (GEFR) predložen je u [15]. Odnos između dužine ugrađene poruke i gradijenta energije čini osnovu za ovaj metod detekcije. U ovoj tehnici izračunava se gradijentna energija naslovne slike. Nakon izračunavanja gradijentne energije, urađeno je ugrađivanje LSB s različitim brzinama okretanja (kako je diskutovano u radu) i izračunava se dobijena gradijentna energija slike nakon svakog ugrađivanja. Zatim se kriva gradijentne energije procenjuje pravom linijom za procenu dužine poruke. Kada je stopa ugradnje veća od 0,05 bita po pikselu, tehnika pouzdano otkriva prisustvo tajne poruke.

U radu [16] predložena je steganalitička tehnika specifična za LSB steganografiju sivih slika. Tehnika koristi histogram razlike slike kao alat za statističku analizu. Koeficijenti translacije između razlike histograma slike su definisani kao mera slabe korelacije između LSB i ostalih ravni. Navedeni koeficijenti translacije se koriste za kreiranje klasifikatora koji razlikuju stego slike od čistih slika. Ovaj algoritam može otkriti postojanje skrivenih poruka ugrađenih korišćenjem sekvencijalne ili slučajne LSB zamene u slikama, a takođe može i tačno proceniti količinu skrivenih poruka.

Steganalitički metod za slike palete poznat kao *Pairs Analysis* predložen je u [17]. Pristup idealno odgovara 8-bitnim GIF slikama gde su bitovi poruke ugrađeni u LSB u indekse uređene palete. *Pairs Analysis* prvo podeli sliku na delove boja skeniranjem slike i odabirom samo onih piksela koji padaju u svaki par vrednosti (0, 1), (2, 3), i tako dalje. Delovi boja su spojeni u jedan tok i meri se homogenost LSB-ova. Homogenost se ponovo procenjuje za alternativne parove vrednosti (255, 0), (1, 2), (3, 4), . . . Dokazano je da dobijena homogenost predstavlja kvadratnu funkciju dužine tajne poruke, a samim tim se obavlja i procena dužine nepoznate poruke sa stego slike.

U radu [18] dat je način detekcije za poruke koje su nasumično raspoređene u bitove najmanjih težina obojenih slika i slika u nijansama sive. Ova metoda se zasniva na prikupljanju i proveri skupa *feature-a* slike iz grupe piksela stego slika. *Feature-i* su dobijeni merenjem korelacija i sličnosti između grupa piksela u operacijama prevrtanja. Ovi *feature-i* se menjaju sa različitim odnosima LSB ugradnje. Za razlikovanje između stego slika i čistih slika koristi se *support vector regression*. Ovaj pristup otkriva postojanje skrivenih poruka, ali i njihovu veličinu.

Least significant bit (LSB) metod poklapanja – stegoanaliza

LSB *matching* predstavlja metod sličan LSB *embedding-u*, ali je kompleksniji i teže ga je detektovati, u odnosu na običnu LSB zamenu. Kod standardne LSB zamene i kod LSB *matching* bira se podskup piksela, pseudorandomno, korišćenjem tajnog ključa koji je poznat stranama komunikacije. Kod LSB zamene, bit najmanje težine svakog selektovanog piksela se menja vrednošću bita poruke koja se krije. Tada parne vrednosti piksela ili ostaju nepromenjene ili se povećaju za jedan, dok se neparne vrednosti povećavaju za jedan ili ostaju iste. U proseku se samo polovina selektovanih bitova stvarno promeni dok preostala polovina ostaje ista kao pre ugradnje poruke. Ova osobina se ponekad koristi za detekciju same poruke. Zbog ovoga je uvedena steganografija LSB *matching* koja je teža za detektovanje, sa statistične perspektive. U ovoj tehnici, kada je potrebno promeniti vrednost bita izvršava se operacija ±1 nad vrednošću piksela. Vrednost + ili – bira se slučajno i nema nikakvog efekta na bit koji se krije [21].

U radu [24] predložena je tehnika steganalize za LSB *matching*. Tehnika deluje za slike u sivim tonovima. HCF (Histogram Characteristic Function) tehnika za slike u boji se ovde koristi za detekciju u sivim slikama. Uvedena su dva nova načina primene HCF: (a) Kalibracioni centar mase (COM) korišćenjem slike uzoraka i (b) računanje histograma susedstva umesto uobičajenog histograma. U ovom radu primećeno je da operacija *downsampling-a* utiče na centar mase HCF stego slike i ta varijacija je korišćena kao diskriminator. Ova dva načina dovode do pouzdanih detektora za LSB *matching* u sive slike. Međutim, dokazano je da dužina ugrađene poruke izuzetno utiče na rezultate.

Još jedna šema za steganalizu LSB *matching* steganografije data je u [25]. Zasniva se na *feature extraction* i *pattern recognition* tehnikama. Navedene tehnike se koriste kako bi se

trenirali i klasifikovali skupovi feature-a. Rezultati pokazuju da je ova šema vrlo efikasna za slike u boji i zadovoljavajuće efikasna za slike u sivim tonovima.

Spread-sprectrum steganaliza

Steganografija slike raširenog spektra skriva podatke u Gausovom stego šumu koji je dodat naslovnoj slici. Ova vrsta steganografije je robusnija i ima malu verovatnoću otkrivanja. I pored poteškoća u njegovom otkrivanju tokom mnogih godina predstavljen je veliki broj metoda steganalize.

Harmsen i Pearlman [26] dali su prikaz steganalitičke metode steganografije širokog spektra za slike u boji. Ova metoda koristi svojstva centra mase HCF-a gde je centar mase moment prvog reda, a HCF Fourierova transformacija histograma slike. Razvijen je framework za sakrivanje informacija dodavanjem šuma koji dozvoljava analiziranje efekata sakrivanja podataka na histogramu signala. HCF centar mase se koristi kao jednostavna metrika koja se smanjuje dodavanjem šuma. Kreiran je jednostavni klasifikator, Bajesov multivarijantni klasifikator [27], pomoću navedenog framework-a. Eksperimentalni rezultati pokazuju da je tehnika pouzdana.

Chandramouli i Subbalakshmi [28] predložili su još dve šeme steganalize specifične za steganografiju širokog spektra. Prva šema je jednostavan algoritam koji ne koristi statistiku višeg reda. Procena razlike naslovne slike od stego slike vrši se tehnikama standardnih regresija poput Steins Unbiased Risk Estimator (SURE) [29]. Procenjena vrednost oduzima se od stego slike kako bi se dobila procena tajne poruke. U drugoj šemi se pokušava slepo invertovanje stego funkcija koričćenjem statistike višeg reda. Eksperimenti pokazuju da u poređenju sa jednostavnom šemom procene, korišćenje statistike višeg reda poboljšava performanse steganalize.

BPCS-steganografija steganaliza

U [30] predložen je metod specifičan za BPCS-steganografiju. Ovaj pristup otkriva postojanje skrivenih poruka u prostornom i transformacionom domenu. Primećeno je da se statistička karakteristika koja se naziva izotropija menja nakon ugradnje pomoću BPCS-steganografije u prostornu domenu. Ova promena koristi se za steganalizu. Otkrivanje tajne poruke vrši se korišćenjem Hi-kvadratnog testa. U domenu transformacije uočeno je da se histogram kvantiziranih koeficijenata pod-opsega prirodnih slika simetrično distribuira oko nule. Ugrađivanje pomoću BPCS-steganografije uzrokuje promenu histograma što se može koristiti za steganalizu. Otkrivanje se vrši Hi-kvadrat testom. Eksperimentalni rezultati pokazuju da je navedena metoda efikasna. C. Kiml i dr. [31] su predložili još jednu tehniku za otkrivanje BPCS-steganografije u prostornom domenu. Ova metoda takođe koristi Hi-kvadrat napad koji se inače često koristi u LSB steganalizi.

Hi-kvadrat test

Hi-kvadrat test, takođe napisan kao χ2 test, jeste test statističke hipoteze gde je distribucija uzorka testirane statistike hi-kvadratna distribucija kad je nulta hipoteza istinita. Hi-kvadratni test se često koristi kao zamena za Pirsonov Hi-kvadrat test [22]. Hi-kvadrat test se koristi kada je potrebno utvrditi da li neke dobijene (opažene) frekvencije odstupaju od frekvencija koje bi se očekivale pod određenom hipotezom. Gotovo u svim slučajevima se hi-kvadrat izračunava na isti način uz ograničenje da ponekad treba uneti neke dodatne korekcije. U pitanju je formula:

$$\chi^2 = \sum \frac{(f_o - f_t)^2}{f_t}$$

Pri čemu f_0 označava zapažene frekvencije, a f_t očekivane (teoretske) frekvencije, odnosno frekvencije koje bi se očekivale pod određenom hipotezom [23].

JPEG-kompresija

JPEG slike su u širokoj upotrebi na internetu i zato su idealan ciljni format za steganografiju. JSteg [32] je verovatno prvi steganografski alat za ugrađivanje u JPEG slike. Određene steganalitičke metode mogu da otkriju sekvencijalni JSteg poput ugradnje u većinu formata slike, uključujući JPEG. Zhang i Ping [33] su predložili napad na sekvencijalni JSteg i slučajni JSteg za JPEG slike. Tehnika je zasnovana na statističkom modelu DCT koeficijenata. Primećeno je da se kvantizovani DCT koeficijenti JPEG slike distribuiraju simetrično oko nule u čistim slikama bez steganografije. Ove distribucije se menjaju zbog ugrađivanja poruke bilo da se one ugrađuju sekvencijalno ili nasumično. Hi-kvadrat statistika stego slike se izračunava i koristi se nejednakost za procenu prisutnosti skrivene poruke. Koeficijent ugradnje se takođe izračunava. Tehnika je jednostavna i veoma efikasna.

Da bi se sprečio navedeni napad, uveden je algoritam F5 [34]. Steganalitički napad na F5 steganografski algoritam je predstavljen u [35]. Ovaj napad procenjuje veličinu i otkriva poruku skrivenu u JPEG slikama pomoću F5 algoritma. Napad se zasniva na proceni histograma naslovne slike sa stego slike. Ovo se postiže dekompresijom stego slike, obrezujući je za četiri piksela u oba smera kako bi se uklonila kvantizacija u frekventnom domenu, a zatim se ponovo kompresuje koristeći matricu za kvantizaciju stego slike.

U radu [36] predložen je metod steganalize specifičan za JSteg steganografiju u JPEG formatu. Ovom tehnikom se najpre kreira statistička raspodela kvantizovanih DCT koeficijenata korišćenjem generalizovane Cauchy distribucije. Histogram naslovne slike DCT koeficijenata procenjuje se iz histograma stego slike. Na osnovu rezultata ova dva histograma detekcija se vrši pomoću Hi-kvadrat testa, a dužina poruke se takođe procenjuje.

Fridrich [37] predlaže feature-based steganalitičku metodu koja je kombinovana sa konceptom kalibracije za JPEG slike. Feature-i prvog i drugog reda se analiziraju kako u DCT tako i u prostornom domenu poput histograma globalnog DCT koeficijenta, dualnog histograma, blockiness, matrica ko-pojava. Linearni diskriminatorni klasifikator se obučava na vektorima feature-a koji odgovaraju naslovnoj i stego slici. F5, OutGuess, MB1 i MB2 [38] koriste se za dobijanje stego slika. Iz eksperimenata je primećeno da se mogućnost detekcije smanjuje redom: OutGuess, F5, MB1, MB2. U [39] je navedeno da steganografija zasnovana na modelu JPEG može biti otkrivena samo korišćenjem statistike prvog reda.

Metoda data u [40] specifična za steganografiju u JPEG slikama opisuje algoritam koji koristi hiperdimenzionalne geometrijske metode za modeliranje čistih JPEG slika. Geometrijski model je kreiran pomoću konveksnih polipota, hiper-sfera i hiper-elipsoida u prostoru atributa. Model prepoznaje JPEG stego sliku kao anomaliju kada se ne podudara sa čistim modelom datoteke. Kao što je rečeno, ovaj geometrijski model pruža superiornu detekciju anomalije.

Metoda steganalize razmatrana je u [41] kako bi se efikasno „napale“ napredne JPEG steganografske šeme. Ova metoda koristi Markov empirijske prelazne matrice za hvatanje i intra-blok i inter-blok zavisnosti između blokova DCT koeficijenana u JPEG slikama. Skrivene poruke su nekada nezavisne od podataka na naslovoj slici i proces ugradnje poruke često smanjuje zavisnosti koje postoje u originalnim podacima naslovne slike. Takve promene su zabeležene statistikama drugog reda pošto statistike drugog reda uzimaju u obzir vrednosti dva ili više zapažanja kao i njihov međusobni položaj u skupu podataka. Feature-i se dobijaju iz empirijskih matrica tranzicije tehnikom praga. Feature-i se procenjuju pomoću SVM i tada se SVM koristi kao klasifikator.

Steganaliza u domenu transformacija

Steganaliza na osnovu neuronskih mreža data je u [42]. Digitalne slike, čiste kao i stego, analiziraju se u DFT, DCT, i DWT domenu transformacija pomoću neuronskih mreža. Neuronska mreža izračunava statističke karakteristike slika na koje značajno utiče skrivanje podataka. Neuronska mreža se trenira korišćenjem statistika čistih slika i slika sa skrivenim porukama. Rezultati pokazuju da je metoda obećavajuća.

Steganaliza steganografije dodavanja šuma

Metoda predložena u [43] rešava problem steganalize u tri faze. U prvoj fazi stego slika se transformiše u domen transformisanja. Histogrami sub-band koeficijenata modeliraju se upotrebom nestacionarne Generalizovane Gaussove distribucije. Parametri modela naslovne slike se procenjuju MAP estimatorom [44]. U drugoj fazi, stego poruka se procenjuje korišćenjem MAP estimatora, dok se u trećoj fazi, dužina poruke, lokacija i znak procenjuju deljenjem stego slike u regione sa različitim SNR-om koristeći metode segmentacije zasnovane

na lokalnoj varijaciji datoj u [45] i ekstrapoliranju rezultate cele slike. Predložena metoda deluje i na slike u boji i u sivim tonovima.

Tehnika steganalize binarnih slika koje su ugrađene okretanjem piksela duž granica data je u [46]. Predložena tehnika se zasniva na odnosu između ocene kompresije i ocene ugradnje podataka. Ova metoda vrši steganografsko umetanje kao dodavanje šuma kako bi se iskoristila činjenica da se ocena kompresije bita date slike povećava kada se povećava ocena ugradnje podataka. Tako se koristi stopa kompresije za razlikovanje stego slika od naslovnih slika.

M. Jiang i dr. [47] predlaže drugu metodu steganalize. Ova metoda takođe modelira steganografski sistem kao proces aditivnog šuma za korišćenje činjenice da su srednja vrednost i varijansa stego signala rastuće funkcije stope ugradnje. Ova statistika razlikovanja koristi se za procenu stope umetanja bez znanja o naslovnom objektu. Formula je izvedena tako da je u direktnoj vezi sa srednjom vrednošću i varijansom stego signala. Obe statističke mere se koriste za procenu stopa ugradnje.

U radu [90] data je tehnika steganalize specifična za graničnu steganografiju u binarnim dokumentima. Podaci steganografije zasnovani na granicama skrivaju se duž granica karaktera i simbola u dokumentu mešanjem malih poremećaja piksela sa kvantizacijskim i digitalizacijskim šumom. U datoj metodi steganalize granice karaktera i simbola u dokumentu se modeluju polinom trećeg stepena i samim tim se modeluju kao autoregresivni proces. Eksperimentalni rezultati pokazuju veoma tačne rezultate.

Univerzalna statistička steganaliza

Univerzalna statistička steganaliza uključuje tehnike statističke steganalize koje nisu prilagođene nijednoj specifičnoj tehnici ugradnje. Univerzalna statistička steganaliza je metoda meta-detekcije u smislu da se može prilagođavati, nakon treniranja na čistim i stego slikama, kako bi se detektovala bilo koja steganografska metoda, bez obzira na domen ugradnje. Trik je u pronalaženju odgovarajućih osetljivih karakteristika sa mogućnošću njihovih razlikovanja. Neuronske mreže, *clustering* algoritmi i drugi računarski alati se tada koriste za detekciju modela eksperimentalnih podataka. Ove tehnike ne zavise od ponašanja algoritama ugradnje.

Zaključak

U seminarskom radu date su definicije i tehnike steganografije i steganalize. Centralni deo posvećen je steganografiji i detekciji steganografije u slikama. Kako se steganografija u digitalnim medijima sve češće zloupotrebljava od velike je značajnosti detektovati sakrivene poruke koje se prenose. Otkrivanje same poruke često nije moguće, ali je u većini slučajeva moguća detekcija postojanja poruke. Postoji puno načina za detekciju steganografije, ali često sama tehnika detekcije zavisi upravo od metode kojom je poruka sakrivena. U ovom seminarskom radu navedene su podele detekcija steganografije u slici i ukratko objašnjenje mnogobrojne metode koje se koriste, a zavise od algoritma kojim je poruka ugrađena. Tehnike se temelje na teoriji iz različitih oblasti nauke, matematici, statistici, računarskog vida, mašinskog učenja, neuronskih mreža i slično, te je u zavisnosti od konkrentne problematike i teorijskog znanja pojedinih oblasi moguće izvršiti implementaciju nekih od navedenih algoritama.

Literatura

[1] Vučković V, Rajković P: "Zaštita informacija"
[2] Digitalna forenzika, Elektronski fakultet Univerziteta u Nišu
[3] Provos N, Honeyman P: "Hide and Seek: An Introduction to Steganography"
[4] Richer P: "Steganalysis: Detecting hidden information with computer forensic analysis"
[5] Karampidis K, Kavallieratou E, Papadourakis G: "A review of image steganalysis techniques for digital forensics", dostupno na: https://www.sciencedirect.com/science/article/abs/pii/S2214212617300777 (pristupljeno juna 2020)
[6] Guidance Software, Inc, dostupno na: http://www.encase.com/products/software/encaseforensic.shtm (pristupljeno juna 2020)
[7] IRS Criminal Investigation Electronic Crimes Program ILook Investigator ©Elliot Spencer, dostupno na: http://www.ilook-forensics.org/ (pristupljeno juna 2020)
[8] Reddy S: "Steganalysis Techniques: A Comparative Study"
[9] Nissar A, Mir A: "Classification of steganalysis techniques: A study"
[10] Johnson N, Jajodia S: "Steganalysis of images created using current steganography software"
[11] Fridrich J, Du R, Meng L: "Steganalysis of LSB encoding in color images"
[12] Fridrich J, Goljan M, Du R: "Detecting LSB steganography in color and gray-scale images"
[13] Avcibas I, Memon N, Sankur B: "Image steganalysis with binary similarity measures"
[14] Dumitrescu S, Wu X, Wang Z: "Detection of LSB steganography via sample pair analysis"
[15] Zhi L, Fen S, Xian Y: "A LSB steganography detection algorithm"
[16] Zhang T, Ping X: "Reliable detection of LSB steganography based on difference image histogram"
[17] Fridrich J, Goljan M, Soukal D: "Higher-order statistical steganalysis of palette images"
[18] Lin E, Woertz E, Kam M: "LSB steganalysis using support vector regression"
[19] Kaur H, Rani J: "A Survey on different techiques of steganography"
[20] Manifold: "Palette Images" dostupno na: http://www.manifold.net/doc/mfd9/palette_images.htm (pristupljeno juna 2020)
[21] Science Alert: „A Review on Detection of LSB Matching Steganography" dostupno na: https://scialert.net/fulltext/?doi=itj.2010.1725.1738 (pristupljeno juna 2020)
[22] Wikipedia: „Hi-kvadratni test" dostupno na: https://sr.wikipedia.org/wiki/Hi-kvadratni_test (pristupljeno juna 2020)
[23] „Hi-kvadrat test" dostupno na: http://zaf.biol.pmf.unizg.hr/behaviour/Hi%20kvadrat%20test.pdf (pristupljeno juna 2020)

[24] Ker A: “Steganalysis of LSB matching in grayscale images”
[25] Liu Q, Sung A, Xu J, Ribeiro B: “Image complexity and feature extraction for steganalysis of LSB matching steganography”
[26] J.J. Harmsen, W.A. Pearlman, Steganalysis of additive noise modelable information hiding
[27] R.O. Duda, P.E. Hart, H.G. Stork, Pattern Classification
[28] R. Chandramouli, K.P. Subbalakshmi, Active steganalysis of spread spectrum image steganography
[29] D.L. Donoho, I.M. Johnstone, Adapting to unknown smoothness via wavelet shrinkage
[30] X. Yu, T. Tan, Y. Wang, Reliable detection of BPCS-steganography in natural images
[31] C. Kiml, S. Chul, S. Lee, W. Yang, H. Lee, Steganalysis on BPCS steganography
[32] JPEG-JSteg-V4, http://www.funet.fi/pub/crypt/steganography/jpeg-jsteg-v4.diff.gz
[33] T. Zhang, X. Ping, A fast and effective steganalytic technique against JSteg-like algorithms
[34] A. Westfeld, F5 – A steganographic algorithm. High capacity despite better steganalysis
[35] J. Fridrich, M. Goljan, D. Hogea, Steganalysis of JPEG images: Breaking the F5 algorithm
[36] X. Yu, Y. Wang, T. Tan, On estimation of secret message length in JSteg-like steganography
[37] J. Fridrich, Feature-based steganalysis for JPEG images and its implications for future design of steganographic schemes
[38] P. Sallee, Model-based steganography, in: T. Kalker, et al. (Eds.), International Workshop on Digital Watermarking,
[39] R. Bohme, A. Westfeld, Breaking Cauchy model-based JPEG steganography with first order statistics
[40] B.T. McBride, G.L. Peterson, S.C. Gustafson, A new blind method for detecting novel steganography
[41] Fu Dongdong, Yun Q. Shi, Dekun Zuo, Guorong Xuan, JPEG steganalysis using empirical transition matrix in block DCT domain
[42] Shaohui Liu, Yao Hongnun, Wen Goa, Neural network based steganalysis in still images
[43] T. Holotyak, J. Fridrich, D. Soukal, Stochastic approach to secret message length estimation in ±k embedding steganography
[44] S. Voloshynovskiy, O. Koval, T. Pun, Wavelet-based denoising using non-stationary stochastic geometrical image priors
[45] P. Felzenszwawalb, D. Huttenlocher, Image segmentation using local variation
[46] M. Jiang, X. Wu, E.K. Wong, N. Memon, Quantitative steganalysis of binary images
[47] P. Howard, F. Kossentini, et al., The emerging JBIG2 standard

[48] M. Jiang, X. Wu, E.K. Wong, N. Memon, Steganalysis of boundary-based steganography using autoregressive model of digital boundaries