

|  |  |
| --- | --- |
|  | UNIVERZITET U NIŠU ELEKTRONSKI FAKULTET |

**Implementacija sistema za steganografiju slika JPEG formata korišćenjem DCT-a**

Predmet: Digitalna forenzika

Studijski program: Računarstvo i informatika

Modul: Softversko inženjerstvo

|  |  |
| --- | --- |
| Student: | Profesor: |
| Nikola Mitić, br. ind. 1433 | dr Bratislav Predić |
|  |  |

Niš, septembar 2022. godina

Sadržaj

[1. Uvod 3](#_Toc114043986)

[2. Steganografija 4](#_Toc114043987)

[2.1. Steganografija slike i DCT 7](#_Toc114043988)

[2.2. Poboljšanje izgleda slike 9](#_Toc114043989)

[3. Steganoanaliza 11](#_Toc114043990)

[3.1. Napadi na steganografske sisteme 15](#_Toc114043991)

[3.2. Stegdetect - alat za detekciju steganografije 18](#_Toc114043992)

[4. JPEG Format slike 21](#_Toc114043993)

[5. Konkretna realizacija sistema 22](#_Toc114043994)

[6. Zaključak 25](#_Toc114043995)

[7. Literatura 26](#_Toc114043996)

# Uvod

Brzi razvoj informacionih tehnologija doveo je do toga da se računar danas koristi u svim aspektima, kako poslovnog sveta, tako i uobičajenog društvenog života. U ovakvim uslovima, prisutan je problem sigurnosti informacija, jer se informacije prenose putem raznih kanala i medijuma u digitalnom obliku i lako se mogu pronaći, videti i preuzeti.

Današnji svet interneta je pun kradljivaca podataka i hakera, te je samim tim sve veća potreba za sistemom koji može sigurno prenositi osetljive podatke preko interneta. Kriptografija može postići ovaj cilj. Ali, kriptografija samo transformiše osetljive podatke u drugi oblik koji ne mogu svi razumeti, tako da samo nameravani primaoci sa ključem mogu da otključaju podatke nazad u prvobitni oblik. Dakle, transformisani kriptovani podaci su vidljivi svima, i na taj način mogu izazvati radoznalost među sajber kriminalcima da provale u značenje kriptovanih podataka, iako to nije tako jednostavno.

Steganografija je još jedan moćan alat koji postiže cilj tajnog prenošenja osetljivih podataka putem interneta. Ova tehnika umesto da transformiše podatke u drugi oblik, sakriva osetljive podatke u drugim vrstama podataka, na takav način da niko nikada ne može posumnjati da su neki bajtovi podataka skriveni u tim podacima. Dakle, steganografija je umetnost i nauka pisanja skrivenih poruka na način da niko, osim pošiljaoca i nameravanog primaoca, ne posumnja u postojanje poruke.

# Steganografija

Steganografija je naučna disciplina koja obuhvata skup sredstava i metoda koji se koriste za formiranje skrivenog kanala prenosa informacija i najčešće se opisuje relacijom:

*Steganografski medijum= skrivena poruka + nosilac poruke + steganografski ključ*

Savremena steganografija zasnovana je na mogućnostima digitalne tehnologije, uglavnom je usmerena na skrivanje tajne poruke unutar sadržaja nekog multimedijalnog fajla npr. slike, audio ili video zapisa. Multimedijalni fajlovi u sebi sadrže veliki broj bitova od manjeg značaja koji se mogu iskoristiti i u njih smestiti određena tajna poruka.

Primena steganografije se najčešće bazira na sledećem principu: pošiljalac tajne poruke bira nasumično nosioca poruke; u izabrani nosilac poruke implementira se tajna poruka uz pomoć steganografskog ključa; primaocu se šalje steganografski medijum, a primaoc na drugoj strani obrnutim postupkom dolazi do sadržaja tajne poruke. Da tajna poruka ne bi bila vidljiva, bitno je da nosilac poruke sadrži dovoljno redundantnih bitova, koji mogu biti zamanjeni tajnom porukom. Važno je napomenuti da nisu svi digitalni formati pogodni za prenošenje tajnih poruka, jer se npr. promenom bitova u nekom izvršnom fajlu dovodi do toga da program ne radi ili javlja greške pri radu. Razmena sakrivene poruke je prikazana na Slici 1:

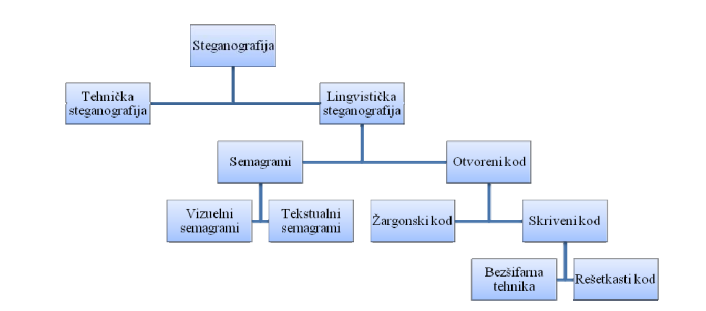


*Slika 1:Prikaz funkcionisanja razmene sakrivenih informacija*

Postoje dva tipa steganografije, a to su:

* Tehnička steganografija – ogleda se u korišćenju posebnih tehničkih sprava, uređaja, instrumenata i metoda za skrivanje poruke;
* Lingvistička steganografija – obuhvata steganografske metode koje skrivaju tajnu poruku u objekat nosilac nastojeći je prikazati kao bezazlen skup informacija. Deli se na:
  + Semagrame - skrivaju informacije korišćenjem različitih simbola i znakova, i mogu biti vizuelni (npr. specifično razmeštanje objekata na web stranici) i tekstualni (npr. dodavanje suvišnih razmaka u tekst)
  + Otvorene kodove - krije poruke u legitimne nosioce poruka na način koji nije očit nekom nesumnjičavom posmatraču. Ova kategorija je podeljena na žargonski kod i sakriveni kod.

Na Slici 2, u nastavku, data je podela prema tipu steganografije:



*Slika 2: Podela steganografije*

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

Kompjuterska steganografija je deo steganografije koja se bavi realizacijom stegosistema upotrebom kompjuterske tehnike. Savremene metode kompjuterske steganografije se razvijaju u dva pravca:

* Metodi zasnovani na korišćenju specijalnih svojstava kompjuterskih formata i
* Metodi zasnovani na statističkom preobilju informacija u audio i video digitalnim signalima.

Digitalni steganografski sistemi u svom funkcionisanju imaju tri veoma bitna aspekta a to su:

1. Kapacitet - količina informacija koja se može sakriti u stego medijumu za prikrivanje;
2. Bezbednost - nemogućnost prisluškivanja i otkrivanja skrivene informacije;
3. Robusnost – u odnosu na modifikacije koje stego medijum može da podnese pre nego što protivnik uništi skrivenu informaciju.

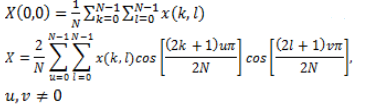
Steganografske tehnike se mogu podeliti u sledećih šest kategorija:

1. Tehnike supstitucije: Suvišni delovi nosioca poruke (medijuma) se iskorićavaju za ubacivanje tajne informacije. Najpoznatija tehnika ove kategorije je LSB (engl. Least Significant Bit) koja bitove najmanje važnosti koristi na način da postaju nosioci skrivene poruke;
2. Tehnike transformacije domena: Modifikacija se vrši u transformisanom domenu. Najčešće se koriste diskretna kosinusna transformacija i diskretna fourierova transformacija;
3. Tehnike rada u proširenom spektru: Signal tajne poruke sa definisanim propusnim opsegom se skriva unutar medijuma. Tajna poruka se modifikuje signalom šuma te se dodaje u medijum: isključivo poznavanjem ključa je moguće iz naizgled slučajnog signala šuma dobiti skrivenu poruku. Postoje dve metode proširenog spektra koje se koriste u digitalnoj steganografiji: metoda sa direktnom sekvencom i metoda frekvencijskog skakanja;
4. Statističke metode: Nosilac se podeli na onoliko blokova kolika je veličina poruke. Svaki blok služi za skrivanje jednog bita tajne poruke. Ukoliko je bit poruke jednak 1, blok se modifikuje tako da primalac može statističkim testiranjem hipoteze otkriti je li je taj blok promenjen. Ukoliko je bit poruke jednak 0, blok se ne menja;
5. Tehnike oblikovanja: Tajna poruka se ne skriva direktno u medijum, već se on oblikuje (menja mu se oblik), kako bi se prenela tajna poruka. Zahteva se da primalac poznaje originalnu verziju medijuma u kome je skrivena poruka, koji na neki način predstavlja ključ za otkrivanje skrivenog sadržaja;
6. Tehnike stvaranja medijuma skrivene informacije: Tajna poruka se ne skriva u medijum, već se na temelju nje stvara medijum koji joj odgovara.

## Steganografija slike i DCT

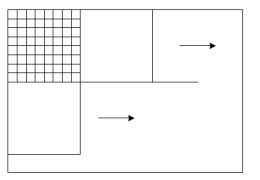
Sada kad smo se upoznali sa pojmom steganografije i šta on predstaljva možemo se detaljnije pozabaviti steganografijom slike. Za skrivanje informacija u slikama najčešće se koristi metod LSB. Najbolji format slike za sakrivanje informacija je 24-bitna BMP slika, kao najveći tip fajla, a samim tim i najkvalitetniji. Mnogo je lakše sakriti informacije u slici visokog kvaliteta i rezolucije. Međutim, najrasprostranjeniji format slike je ipak JPEG (Joint Photographic Experts Group). JPEG je standard koji se široko koristi za kompresiju slike. Pruža veoma dobar ili čak odličan kvalitet slike, kako crno bele, tako i u boji. Jednostavan je za implementaciju, a njegovi softverski algoritmi su prihvatljive računske složenosti. JPEG spada u klasu transformacionih tehnika kodiranja, što znači da se kompresija ne izvršava direktno na signalu, već nad njegovom transformacijom. Najčešće korišćena transformacija u obradi slike je diskretna kosinusna transformacija (DCT).

U JPEG formatu, slika je podeljena na 8x8 blokova za svaku odvojenu komponentu boje. Cilj je pronaći blok gde bi promena vrednosti piksela bila najmanja. Ako je vrednost prevelika, blok se deli na 8x8 podblokova, sve dok vrednost ne bude dovoljno niska. DCT se primenjuje na svaki blok, a dobijeni DCT koeficijenti ovih blokova su kvantizovani i kodirani. Slika za prikrivanje deli se na blokove od 8×8 piksela koji se ne preklapaju kako bi se izvela DCT i dobile kompresovane slike. Diskretna kosinusna transformacija slike dimenzija NxN , čija je funkcija osvetljaja x(m,n),0 < m,n < N – 1 može se odrediti iz jednačina prikazanih na Slici 3:



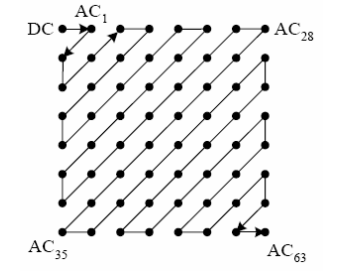
*Slika 3: Jednačine za određivanje DCT slike dimenzije NxN*

Koeficijent X(0,0) naziva se jednosmernom (DC) komponentom slike, dok se ostali koeficijenti nazivaju naizmeničnim (AC) komponentama. Prvi korak u diskretnoj kosinusnoj transformaciji ovakve slike je podela slike u matrice dimenzija 8 x 8. Ova veličina matrice odabrana je kao kompromis između složenosti i kvaliteta. Za svaku matricu se računa DCT. Tako se dobijaju po 64 DCT koeficijenta, počevši od X(0,0), pa do X(7,7). Ovaj proces ilustrovan je na Slici 4.



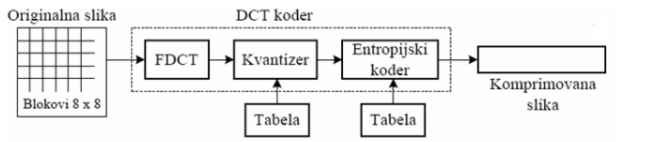
*Slika 4: Podela slike na blokove dimenzije 8x8*

Drugi korak jeste kvantizacija vrednosti u matrici bloka. Zbog svojstva kompresije podataka, DCT koeficijenti koji odgovaraju nižim učestanostima imaju značajne vrednosti. Pošto DC komponenta nosi najveći deo tajnih podataka i pošto postoji izražena korelacija između DC komponenata susednih matrica u slici, DC komponente se kvantizuju uniformnim diferencijalnim postupkom. AC komponente se uniformno kvantizuju, ali uz različite vrednosti koraka kvantizacije. Svi kvantizeri imaju jednak broj nivoa - 256. Vrednost koraka kvantizacije za svaki DCT koeficijent očitava se iz tabele od 64 elementa. Na izlazu kvantizera dobijaju se matrice koje imaju nenulte elemente u gornjem levom uglu, dok su ostali elementi po pravilu jednaki nulama. Kvantizovane vrednosti DCT koeficijenata uređuju se u vektor postupkom cik-cak očitavanja, kao što je prikazano na Slici 5:



*Slika 5: Cik-cak očitavanje DCT koeficijenta*

Prethodno opisanom kvantizacijom ostvaruje se kompresija sa gubicima. Nakon tog koraka, sledi entropijsko kodiranje, da bi se ostvarila kompresija kvantizovanih vrednosti bez gubitaka. Jedna od metoda koje se koriste u JPEG je Huffman-ovo kodovanje. Kodovane reči koje odgovaraju različitim amplitudama koeficijenata specificirane su tabelama. Pošto kvantizovane vrednosti koeficijenata imaju veliki broj nula, koristi se neki od postupaka kodiranja kojim se on smanjuje. JPEG koder sastoji se od tri bloka i to DCT, kvantizera i kodera, kao što je prikazano na Slici 6:



*Slika 6: JPEG koder*

Da bi stavili što veću količinu podataka u sliku, mi možemo pre ubacivanja podataka, da te iste podatke kompresujemo i tako smanjimo njihovu veličinu, a ujedno povećamo prostor za skladištenje podataka unutar slike. Postoje dve vrste kompresije. Obe vrste imaju isti cilj, ali ipak postoji jedna velika razlika.

1. Kompresija bez gubitaka (Lossless kompresija) smanjuje originalnu veličinu slike upotrebom različitih algoritama, a posle toga je moguće takvu sliku dekompresovati i vratiti u originalno stanje.
2. Kompresija sa gubicima (Lossy kompresija) takođe smanjuje originalnu veličinu slike, ali to radi na račun kvaliteta slike. Takvu sliku je nemoguće vratiti u originalno stanje jer su neki njeni delovi trajno uklonjeni. Pravi predstavnik lossy kompresije jeste sam JPEG. Za kompresiju podatka može se koristiti bilo koji algoritam.

## Poboljšanje izgleda slike

Može se desiti da se, i pored minimalnih promena boja, primeti mutnjikavost i šarenilo na slici, ili da se pojave „usamljene tačke“ na slici. Ovo se ipak može izbeći upotrebom različitih tehnika obrade slike, odnosno različitih filtera i efekata, ali pažljivo odabranih. Neki od njih su nabrojani u nastavku:

* Maskiranje i filtriranje - Ovo je jedna od najzastupljenijih tehnika u steganografiji. Postoji više načina na koje se može primeniti. Ako se primeti u nekom delu slike mutnjikavost posle ubacivanja skrivenih podataka, onda se original slike može malo potamniti i nakon toga ubaciti podaci u nju. Uspešnost ove tehnike se zasniva na činjenici da ljudsko oko slabije raspoznaje razlike među bojama slabije sjajnosti. Ali ne treba preterivati ni u tom polju jer onda stegoslika neće više ličiti na sliku.
* Dodavanje „šuma“ - Jedan od veoma efektnih metoda jeste i dodavanje šuma. Cela tehnika se zasniva na dodavanju belih tačaka ili izbeljivanju nekih tamnijih. Sve ovo krajnjem korisniku stvara utisak da je slika skenirana i da je slabijeg kvaliteta, i takvu sliku retko ko uzima u detaljno razmatranje. Pri dodavanju šuma, važno je da se ne menjaju bitovi koji nose skriveni podatak, već samo oni bitovi koji se ne koriste za skrivanje podataka.
* Korekcija boje piksela - Korekcija boje piksela je, dosad, najsavršenija tehnika. Funkcioniše tako što se skriveni podatak upisuje npr. u svaki drugi piksel, a pikseli koji ostanu slobodni, koriguju se prema bojama susednih piksela. Korekcija slobodnog piksela se vrši tako što se, pored njegove originalne boje, gledaju i one susedne (slika bolje izgleda ako se gleda nekoliko susednih), a potom se nađe srednja vrednost boje. Tako će slika izgledati skoro isto kao i original, odnosno približnije nego pre ugrađivanja podataka. Nedostatak ove tehnike jeste to što se, u stvari, koristi svaki drugi piksel za skrivanje podataka, što znači da ima duplo manje prostora za podatke. Velika prednost ovog načina poboljšanja izgleda slike je to što se šanse za otkrivanje tajnog sadržaja svode baš na minimum. Slika će još bolje izgledati ako se podaci sakrivaju u svakom trećem pikselu i tako dalje, ali, naravno, biće srazmerno manje mesta. Korekcija boje piksela može se nesmetano koristiti na slikama velikog formata u koje je potrebno staviti podatak relativno male dužine.

# Steganoanaliza

Steganoanaliza je veština detekcije poruke skrivene steganografskim metodama, a konačan cilj je otkrivanje poruke koja je skrivena unutar medijuma (nosioca skivene poruke). Relativno je mlada istraživačka disciplina o kojoj su se prvi članci pojavili 1990-tih godina. Zasniva se na:

* otkrivanju sakrivenih informacija posmatranjem nekog prenosa podataka, bez pretpostavke koji steganografski algoritam je korišćen;
* na izvlačenju skrivene poruke da se onemogući prijem poruke;
* na promeni tajne poruke radi dezinformacije primaoca

Ukratko steganonaliza treba da reši tri osnovna zadatka: detekciju, definisanje i dekodiranje skrivene poruke.

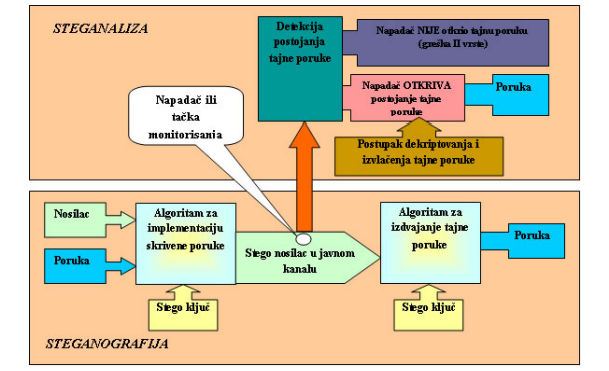
Detekcija steganografije se najčešće opisuje problemom zatvorenika. Problem uključuje dva zatvorenika, Alisa i Boba, koji su zaključani u odvojenim zatvorskim ćelijama i žele da prenesu neki tajni plan jedno drugom. Njima je dozvoljeno da razmenjuju poruke međusobno, ali Vilijam, stražar, može da čita sve poruke. Alis i Bob znaju da bi Vilijam, ukoliko otkrije tajni kanal, obustavio komunikaciju. Vilijam može da utiče na aktivan ili pasivan način. U pasivnom stražarskom modelu, on ispituje svaku poruku i odlučuje da li da prosledi poruku ili ne, bazirajući se na svojoj mogućnosti da detektuje skrivenu poruku. U aktivnom stražarskom modelu, može da promeni samu poruku ukoliko on to želi. Konzervativan ili zlonameran stražar je mogao da promeni svaku poruku u pokušaju da poremeti skriveni kanal tako da bi Alis i Bob morali da koriste veoma robustan (otporan na proboj) steganografski metod. Težina stražarevog zadatka najviše zavisi od kompleksnosti steganografskog algoritma i znanja koje poseduje. U čistom steganografskom modelu, Vilijam ne zna ništa o steganografskom modelu koji koriste Alis i Bob. Ovo je slaba pretpostavka za Alisa i Boba, pošto je zaštita sa skrivanjem retko uspešna, posebno kada se primenjuje kriptografija. Ovo je čest model koji se javlja kada digitalni forenzičari pretražuju web sajt ili hard disk na potencijalno prisustvo steganografije. Pri upotrebi tajnog steganografskog ključa pretpostavlja se da Vilijam zna steganografski algoritam, ali ne zna tajni steganografski/kriptografski ključ koji su koristili Alis i Bob. Ovo je u skladu sa pretpostavkom da korisnik kriptografije treba da napravi tajni ključ, prema Kirkofovom principu koji glasi: „Sigurnost kriptografske šeme je u upravljanju ključevima, ne u sigurnosti algoritma.“ Ovo je možda suviše zahtevna pretpostavka za praksu, ali da bi informacija bila kompletna trebalo bi uključiti i kontrolu pristupa nosiocu fajla.

Da bi steganoanaliza bila uspešna postoje različite tehnike kao što su napadi na steganografske algoritme. Ove tehnike se koriste i kao pomoć pri testiranju koliko je neki steganografski algoritam siguran. Tehnike steganalize mozemo podeliti na sledeće kategorije:

1. Tehnike nadziranog učenja – sistem sa kojim je moguće obaviti steganoanalizu gde su potrebne dve faze: učenje sistema i iskorišćavanje sistema;
2. Tehnike slepe identifikacije – iskorišćavaju se statistička svojstva nekog medijuma i poruke koja se prenosi. Naj taj način se prepoznaje steganografski sistem sakrivanja tajne poruke;
3. Tehnike statističke analize – postavlja se statistički model medijuma nosioca i stego medijuma i testira se mogućnost postojanja i prisustva tajnih podataka;
4. Hibridne tehnike – kombinacija prethodnih kategorija.

Steganoanaliza uglavnom startuje sa smanjivanjem skupa nekoliko sumnjivih informacionih tokova, podskup najverovatnije izmenjenih informacionih tokova, ali je neizvesno da li neki od njih sadrži skrivenu poruku. To se najčešće realizuje statističkom analizom korišćenjem napredne statističke tehnike. Najjednostavniji metod detekcije modifikovanih fajlova je njihovo upoređivanje sa originalima. Suština detektovanja informacije je kretanje kroz grafičke prikaze na Web sajtovima. Analitičar može sačuvati poznate čiste kopije tih materijala i uporediti ih sa aktuelnim sadržajima na sajtu. Razlike, pod pretpostavkom da je nosilac isti, će sačinjavati skrivenu tajnu informaciju.

Generalno, upotreba visokog nivoa kompresije čini steganografiju teškom za otkrivanje, ali ipak ne nemogućom. Dok postupak kompresije obezbeđuje dobro mesto za skrivanje podataka, visoka kompresija ipak smanjuje količinu podataka raspoloživih za skrivanje tajne poruke. Skrivanje informacija unutar jednog elektronskog nosioca podataka uzrokuje promene osobina nosioca koje mogu rezultirati nekim oblikom degradacije ili neuobičajenom karakteristikom. Odnos steganografije i steganalize prikazan je na Slici 7.



*Slika 7: Povezanost steganografije i steganoanalize*

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

Steganografski metodi za digitalne medije mogu se široko klasifikovati kao operateri u domenima slike i transformatorski domeni. Alati u domenima slike kriju poruku u nosiocu manipulacijom bitovima, poput zamene LSB. Alati za transformacijske domene manipulišu steganografskim algoritmima, poput DCT koeficijenata u JPEG slikama. Dakle, steganoanaliza prati način na koji funkcionišu steganografski algoritmi. Drugi pristup je traženje strukturalnih anomalija koje sugerišu manipulaciju. LSB u slikama baziranim na paletama najčešće su razlog velikog broja dupliranih boja, gde identične, ili najbliže identične, boje se dva puta pojavljuju i ne slažu se jedino u najmanje važnom bitu. Steganografski programi koji kriju informaciju jedino manipulacijom reda boja u paleti prouzrokuju strukturalne promene, koje često kreiraju potpis korišćenog steganografskog algoritma.

Statistička analiza se obično koristi za detekciju sakrivenih poruka, posebno kada se analiza radi na slepo. Steganografske tehnike menjaju statistiku nosioca i velike ili duge sakrivene poruke će više promeniti nosioca nego one manje. Statistička analiza slika i audio fajlova može pokazati da li su statističke osobine fajla deformisane u odnosu na očekivanu normu. Ova tzv., statistika prvog reda, varijacija, hi kvadrat test (Χ2), meri vrednost suvišnih informacija i/ili deformaciju u medijumu. Iako ova merenja mogu doprineti prognozi da li je sadržaj menjan ili je sumnjiv, ona nisu konačna. Statistička steganoanaliza je teško izvodljiva zato što se neki steganografski algoritmi muče da bi očuvali nosioca fajla statistike prvog reda kako bi izbegli ovu vrstu detekcije.

Šifrovanje tajne poruke takođe čini detekciju težom zato što šifrovani podaci imaju visok stepen slučajnosti, jedinice i nule se pojavljuju sa jednakim mogućnostima. Obnavljanje tajne poruke dodaje nov sloj kompleksnosti u poređenju sa jednostavnom detekcijom prisutnosti tajne poruke. Obnavljanje poruke zahteva poznavanje ili procenu dužine poruke i, ako je moguće, šifrovani ključ i poznavanje kripto algoritma. Specifičnost algoritma nosioca fajla može analizu učiniti jasnijom.

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

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

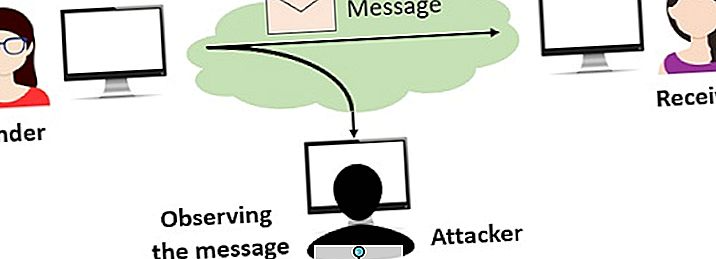
Opšti alati koji mogu detektovati i klasifikovati setganografiju su još uvek u razvoju, ali polako postaju dostupni u softverskim alatima.

## Napadi na steganografske sisteme

Stenografiju koriste napadači ne samo da bi sakrili podatke već da sakriju sam prenos podataka kroz mrežu. Takođe, ovaj koncept im je koristan radi zaobilaženja zaštitnih sistema koji koriste inspekciju sadržaja i druge napredne sisteme zaštite, što je uobičajeno za velike korporacije koje su najčešća meta napada. U praktičnoj primeni, korisnik tipično neće primetiti razliku između originalne datoteke i datoteke koja sadrži umetnutu poruku – kod.

Napadi i analize na skrivene informacije mogu imati nekoliko oblika: detekcija, izdvajanje ili uništavanje skrivene informacije. Pod pojmom "razbiti" steganografski sistem podrazumevaju se tri radnje: detekcija postojanja skrivene informacije, izvlačenje informacije iz nosioca i njeno dešifrovanje. Sistem je već postao nesiguran ako je napadač u stanju samo da dokaže postojanje tajne informacije. Polazna pretpostavka je da napadač poseduje neograničene računarske resurse i u stanju je da primeni raznovrsne algoritme napada. U slučaju da on ne može da potvrdi svoju hipotezu da je tajna poruka implementirana u nosioca, tada govorimo o teorijski sigurnom sistemu. Napadi na steganografske sisteme u odnosu na krajnji cilj napadača, mogu se teoretski podeliti na tri vrste: pasivne, aktivne i namerne.

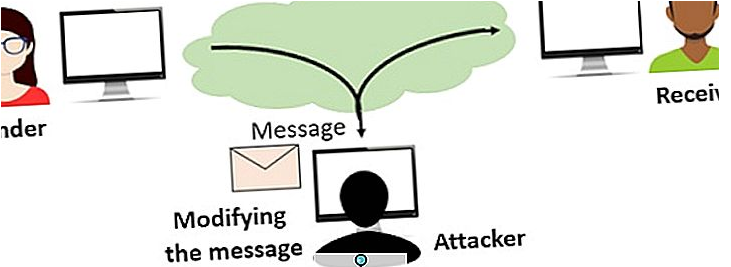
U pasivne napade spada ona grupa tehnika koje samo detektuju postojanje tajne poruke. Ovakav zadatak se formalno može predstaviti kao problem statističkog testiranja hipoteza. Napadač (prisluškivač), mora definisati test funkciju koja kao rezultat daje vrednost koju koristi da klasifikuje nosioce koji su emitovani javnim kanalom. Na Slici 8 demonstrirano je kako izgleda jedan pasivni napad.



*Slika 8: Pasivni napad na stegangrafski medijum*

Postoje dve mogućnosti greške u statističkom testiranju hipoteza. Greška I-vrste nastaje kada se detektuje postojanje tajne poruke u nosiocu, a ona stvarno ne postoji. Greška II-vrste nastaje kada se ne detektuje postojanje tajne poruke, a ona stvarno postoji. U praksi steganografski sistemi se trude da maksimizuju verovatnoću da napadač napravi grešku II-vrste. Prilikom projektovanja steganografskog sistema posebna pažnja se mora posvetiti aktivnim i namernim napadačima.

Aktivni napadači predstavljaju one napadače koji su u stanju da modifikuju stego nosioca u toku prenosa. Opšta pretpostavka je da aktivni napadači ne smeju previše modifikovati stego paket jer će u tom slučaju perceptulane i semantičke osobine biti narušene, već mogu vršiti samo manje izmene odnosno prepravke. Steganografski sistemi su često jako osetljivi na modifikacije stego paketa, kao što su digitalno procesuiranje, filtriranje, usrednjavanje, komprimovanje, prebacivanje iz formata u format. Čak i kompresije sa minimalnim gubicima mogu izazvati potpuni gubitak tajne informacije, jer one baš uklanjaju one neprimetne komponente signala u kojima se najčešće vrši utiskivanje tajne poruke. Aktivni napadač, koji često nije u stanju ni da detektuje postojanje tajne poruke, može dodati slučajan signal u stego nosiocu i uništiti tajnu informaciju. Na Slici 9 prikazano je kako izgleda aktivni napad na steganografski medijum.



*Slika 9: Aktivni napad na steganografski medijum*

Napadači mogu biti slučajni i namerni. Kao primer slučajnog napadača može se navesti slučajan šum koji se akumulira prilikom emitovanja signala nekim od spojnih puteva. Sve navedene tehnike mogu oštetiti ili onemogućiti tajnu komunikaciju. Zbog toga jedan od značajnih zahteva koje steganografski sistem mora da ispuni je robusnost.

Sistem se naziva robusnim ako se utisnuta tajna informacija ne može oštetiti bez drastičnih promena stego nosioca. Potrebno je naglasiti da postoji kompromis između sigurnosti, tj. tajnosti i robusnosti. Što je sistem robusniji na modifikaciju nosioca, to je on manje siguran. To se objašnjava na taj način što robusnost zahteva da se vrši implementacija redundantne informacije, koja će dosta narušiti statističke karakteristike nosioca i time prouzrokovati smanjenje verovatnoće greške II vrste. Jednostavno rečeno, sigurnost zahteva da tajnu informaciju sakrijete u oblasti koje su perceptulano neprimetne, dok robusnost zahteva baš suprotno da tajnu informaciju sakrijete u oblasti koje su perceptualno primetne jer će tako biti teže oštetiti informaciju bez velike degradacije kvaliteta nosioca.

Mnogi sistemi se dizajniraju tako da budu robustni na određene karakteristične tipove napada, kao što je kompresija, dekompresija, filtriranje, dodavanje šuma. Idealan sistem bi trebao da bude robustan na sve vidove napada - što bi bilo jako teško napraviti. Generalno postoje dva principa da se napravi robustan steganografski sistem. Kod prvog sistema vrši se predviđanje mogućih napada i zatim se projektuje takav postupak implementacije tajne poruke koji je robustan na tu vrstu modifikacija, tako da modifikacija ne uništi u potpunosti informaciju. Druga strategija je da se primene inverzne modifikacije, od onih koje su korišćene tokom napada, kako bi se rekonstruisala originalna tajna informacija.

U prisustvu namernih napadača robusnost nije dovoljna. Namerni napadači su svi oni napadači koji pokušavaju da falsifikuju poruku ili da startuju steganografski protokol lažno se predstavljajući kao komunikacioni partner. U slučajevima kada proces implementacije ne zavisi od neke tajne informacije koju poznaju samo pošiljalac i primalac, namerni napadač može falsifikovati poruku, s obzirom da primaoc nije u mogućnosti da verifikuje ispravnost identiteta pošiljaoca. Da bi se ovo predupredilo, algoritam za utiskivanje mora biti robustan i siguran.

Zbog svega navedenog se pred siguran steganografski sistem postavljaju četiri osnovna zahteva koje mora da ispuni i to:

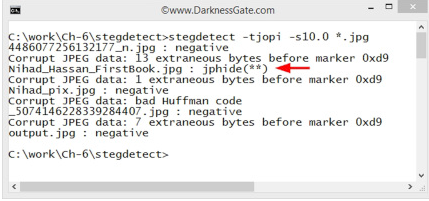
1. Poruke se moraju implementirati u nosioce korišćenjem javnih algoritama i tajnih ključeva, a tajni ključ mora jedinstveno identifikovati pošiljaoca.
2. Jedino vlasnik ispravnog ključa može detektovati, izdvojiti i dokazati postojanje tajne poruke. Niko drugi ne bi trebalo da bude u stanju da pronađe ikakav statistički dokaz da tajna poruka postoji.
3. Ako napadač uspe da selektuje sadržaj jedne skrivene poruke, ne sme biti u stanju da detektuje ostale.
4. Kompjuterski je neizvodljivo detektovati tajnu poruku.

## Stegdetect - alat za detekciju steganografije

Sa razvojem same oblasti steganografije razvijani su i alati za detekciju iste. Kako je steganografija sve više rasprostranjena iz godine u godinu tako se i sve više radi na pouzdanim alatima za njeno prepoznavanje. Jedan od značajnijih alata za detekiciju steganografije u JPEG slikama jeste Stegdetect.

*Stegdetect* je program razvijen od strane Niela Provos-a. Ovo je popularni automatizovani alat za detekciju steganografskog sadržaja u slikama. Niel Provos je autor i steganografskog programa OutGuess. Stegdetect je program za detekciju podataka skrivenih u JPEG slikama zasnovan na određenim steganografski baziranim aplikacijama. U stanju je da otkrije nekoliko različitih steganografskih metoda za ugradnju skrivenih informacija u JPEG slike. Omogućava detekciju JSteg, JPHide (unix i windows), Invisible Secrets, OutGuess 01.3b, F5 (analiza zaglavlja), AppendX i Camouflage. Stegdetect se kod Unixa koristi iz komandne linije dok za Windows ima svoj GUI.

Na Slici 10 prikazano je korišćenje Stegdetect-a kroz komandnu liniju.



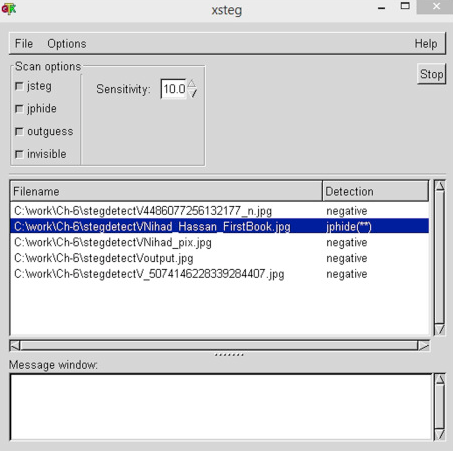
*Slika 10: Stegdetect kroz komandnu liniju*

Komande korišćene na Slici 10 u Stegdetectu su:

* *tjopi* sam znak t će postaviti tipove probnog rada na slici. j testovi za podatke sakrivene pomoću jsteg alata, o testovi za outguess alat, p testovi za jphide alat, i na kraju i testovi za podatke sakrivene korišćenjem programa nevidljive tajne.
* *-s 10.0* menja osetljivost algoritama detekcije; što je broj veći to će test postati osetljiviji. Podrazumevano je 1. U ovom slučaju je postavljen maksimum, koji je 10,0.
* *∗.jpg* pretražuje trenutni direktorijum za sve slike sa ekstenzijom .jpg.

Kada alat posumnja na postojanje skrivenih podataka unutar bilo koje slike, nacrtaće zvezde pored nje. Što je veći broj zvezda, veća je verovatnoća da unutar otkrivene slike postoje skriveni podaci. U našem slučaju na slici 10, Stegdetect ukazuje na mogućnost skrivenih podataka pomoću alatke za steganografiju jphide; nivo samopouzdanja je bio dve zvezdice.

Što se tiče Windowsa, njegovi korisnici mogu Stegdetect koristiti putem GUI verzije ovog alata koja se naziva Xsteg. Na Slici 11 je prikazan interfejs ovog alata:



*Slika 11: XSteg alat*

Na slici 11 možemo videti da smo za detekciju steganografije kroz Xsteg koristali istu postavku parametra kao i kod Slike 10 gde se radi o komandnoj liniji. Kao rezultat smo, takođe, dobili da postoji mogućnost skrivenih podataka pomoću alatke za steganografiju jphide, i nivo samopouzdanja je isto dve zvezdice na slici VNihad\_Hassan\_FirstBook.jpg.

# JPEG Format slike

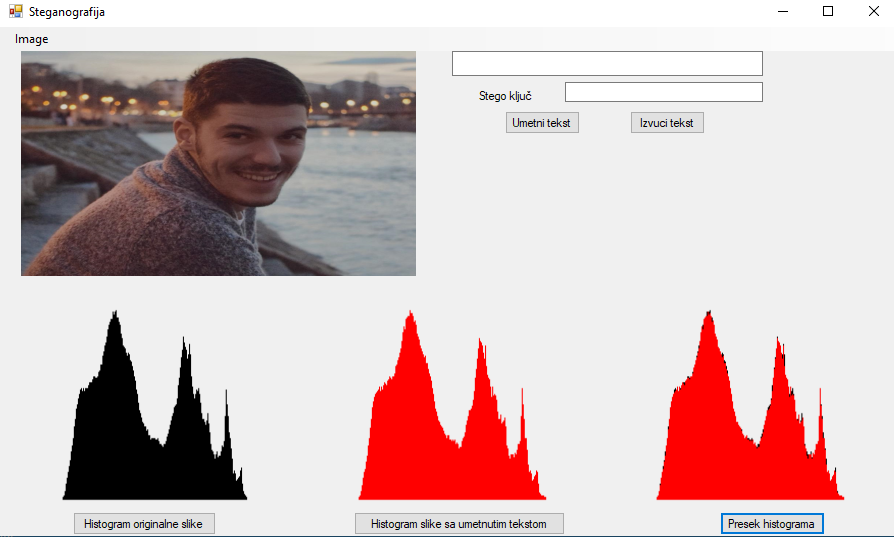
JPEG (ili skraćeno JPG) je možda najpoznatiji i najčešće korišćeni format slike. To je standard za slike koji se punim imenom naziva i Joint Photographic Ekperts Group, a to je format slike koji se najviše koristi za objavljivanje slika na Internetu na veb lokacijama koje zahtevaju najbolji mogući kvalitet slike. Koristi 3 bajta za svaku boju, ali kao osnovni elemenat nije jedan piksel nego grupa od 8\*8 piksela. Omogućava prikaz preko 16 miliona boja. Posebna pogodnost ovog formata je da omogućava kompresovanje veličine fajla, uz naravno ekvivalentan gubitak kvaliteta. Preporuka je da se ne kompresuje na više od 60%, da bi se zadržao kvalitet slike. Zavisno od primenjenog nivoa kompresije imamo različite nivoe kvaliteta slike i različite veličine fajlova.

JPEG spada među formate koji koriste kompresiju sa gubicima (lossy compression). Ova vrsta kompresije generalno ima za cilj uštedu memorije koju postiže preko algoritma za odbacivanja određene količine podataka. Upravo ta karakteristika JPEG formata jeste ujedno i njegova glavna prednost i razlog zašto je uspeo da postane tako popularan zamenivši nekad znatno popularniji BMP. Međutim, kada govorimo o različitim vrstama kompresija i formata treba da znamo da svaki od njih ima svoje prednosti i mane. Pitanje je samo u kojim okolnostima je poželjno koristiti jedan format, a u kojima pak neki drugi.

JPEG je format koji se veoma dobro pokazuje u slučaju fotografija koje su bogate detaljima, dok se prilično loše snalazi sa oštrim geometrijskim ivicama. U praksi, ako se radi o uobičajenim fotografijama koje prave fotoaparati ili mobilni telefoni, onda je JPEG zaista dobar izbor. S druge strane, ako imamo posla sa jednostavnijim slikama, ilustracijama na kojima se ističu oštre ivice, tanke linije i geometrijski oblici, onda kompresija koju koristi JPEG pokazuje sve svoje slabosti. Te slabosti se ogledaju u sitnim artefaktima koji se često (a naročito u slučaju slabijih rezolucija) mogu lako primetiti na ivicama različitih sadržaja na slici. Još jedna manjkavost JPG formata jeste to što ne podržava providnost (transparency), što u nekim situacijama može da predstavlja nepromostivu prepreku. To zapravo znači da, ukoliko neki deo slike ne poseduje boju (ma iz kog razloga) JPG će nešto što bismo očekivali da bude providno zameniti najčešće belom bojom. U slučaju, na primer, izrade logo-a mi često želimo da krajnji proizvod bude grafika koja nema pozadinu, odnosno čija pozadina ima dinamički aspekt, a to je za JPEG jednostavno nemoguć zadatak.

# Konkretna realizacija sistema

Kako smo do sada objasnili glavne pojmove ovog rada steganografiju i staganoanalizu sada ćemo malo govoriti o samoj aplikaciji u kojoj je prikazan način na koji se može videti da je određena slika kompromitovana, tačnije da ima umetnutu poruku u sebi. Naime, nije toliko truda uloženo u sam interfejs aplikacije, zato što ona služi samo da pokaže glavne karakteristike ovog rada. Interfejs aplikacije je prikazan na Slici 12.



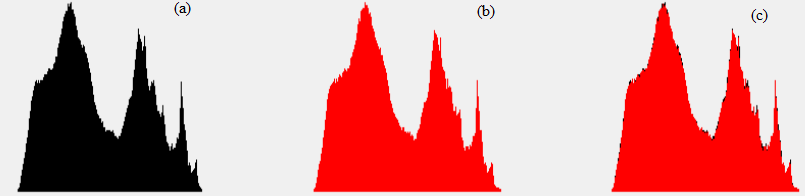
*Slika 12: Interfejs aplikacije*

Glavni cilj bio je prikazati odstupanje na histogramima kada se uporede dve naizgled identične slike, a ustvari jedna od njih ima sakriveni tekst u sebi. Histogram je alat koji pomaže da se brzo uoči tip raspodele za uzorke koji sadrže veliki broj podataka. Kako se slike sastoje od mnoštva bitova histogram je bio logični izbor za njihovo predstavljanje. Naravno, s obzirom da smo ranije govorili o JPEG formatu i u samoj aplikaciji su korišćene slike JPEG formata jer je na njemu najbolje primeniti neku od tehnika steganografije za umetanje teksta u sliku.

Kako ne bismo morali tražiti originalne slike i slike sa umetnutim tekstom, u aplikaciji je omogućeno da se putem DCT-a umetne tekst u sliku i da se ona kao takva sačuva radi kasnijeg poređenja sa originalom. Unosom teksta u polje predviđeno za to i unosom stego ključa, a zatim klikom na dugme „Umetni tekst“ vrši se umetanje poruke u sliku čime se obezeđuje da ona bude sakrivena od svih osim od osobe kojoj je namenjena.

Sada kada smo pokrili deo kreiranja slike sa umetnutim tekstom možemo se vratiti na našu analizu samih slika i kako zaključiti da li je neka slika promenjena, odnsono, da li u sebi ima neku poruku. Da bi se utvrdilo da li je na neku sliku primenjena steganografija, potrebno je izvršiti najpre vizuelnu analizu. Vrlo često ovom analizom se ne može doći do zaključka te se primenjuje neka konkretnija tehnika koja će prodreti u samu strukturu slika. Čak i recimo uvećavanjem (zumiranjem) slike ne može se golim okom videti da na njoj ima izmena. Ove izmene se najčešće ogledaju u promeni samog kvaliteta slike, ali ako je steganografija primenjena onako kako treba ovi nedostaci neće biti primetni našem oku.

Iz svih navedenih razloga do sada, ali i mnogih drugih, pribegava se drugim tehnikama anlize da bi se utvrdilo da li je na nekoj slici primenjena steganografija. U radu je data tehnika analize histograma gde se odluka donosi analiziranjem originalne slike i slike na kojoj je primenjen neki vid steganografije. U analizi histograma upoređivani su histogrami stegonosioca (a) i stego medijuma (b) histograma. Preklapanjem histograma uočavamo razliku koja je na Slici 13 prikazana pod slovom (c). Ovde se vidi da su određeni bitovi na originalnoj slici promenjeni.



*Slika 13: Histogrami stegonosioca (a), stegomedijuma (b) i razlika (c)*

Problem koji se javlja kod ove analize jeste da ju je nemoguće sprovesti ukoliko ne posedujemo originalnu sliku, odnosno, stegonosioca. Kao i kod većine metoda za detekciju setganografije. Međutim, ono što može rešiti ovakvu vrstu problema je da slika poseduje vodeni žig čime će se obezbediti sigurnost i autentičnost stegomedijuma. DVP je veština neprimetne izmene nekog rada. odnosno ugrađivanja poruke o tom istom radu. On je karakteristika koja identifikuje sliku, audio fajl, film ili bilo koji drugi digitalni format. Međutim, kako ovo nije tema rada neće biti dalje priče o njemu, jer postoji toliko toga što se može reći o vodenim pečatima da se bez problema može smestti u novi rad. Ovde je samo napomenut kao jedno od mogućih rešenja problema zaštite medijuma kroz koji je pokušan prenos tajne poruke.

# Zaključak

Steganografija raspolaže vrlo efikasnim i snažnim tehnikama koje ljudima omogućavaju bezbednu komunikaciju i razmenu podataka. Kombinovana sa kriptografijom, može biti dodatni sigurnosni stepen u zaštiti informacija. Steganografske tehnologije su vrlo jednostavne za upotrebu, a izrazito se teško otkrivaju i veoma su pouzdane. Glavni cilj steganografije je da prisustvo tajne poruke ostane neotkriveno. Tajnost poruke vezuje se za steganografski sistem (algoritam) i tajni ključ pod kojim je sakrivena tajna poruka.

Steganoanaliza je puno mlađa naučna disciplina od steganografije. Različite steganoanalitičke metode vrlo uspešno mogu otkriti i spečiti nedozvoljene radnje. Sa druge strane, steganografija ima značajnu primenu za legalne svrhe, kao što su digitalni vodeni pečati za utvrđivanje vlasništva i autorskih prava nad dokumentima ili sigurnije metode čuvanja važnih i poverljivih informacija

Na osnovu rezultata ovog istraživanja može se zaključiti da je sakrivanje tajne poruke u .jpeg formatu veoma delotvorno i ne tako lako za detektovanje.

Steganografija postaje sve popularnija kod kreatora malvera. Sigurnosni sistemi zaštite generalno ne mogu pomoći oko formata nosača malicioznog koda – jako je teško otkriti postojanje poruke spakovane u datoteke slike, zvuka ili nekog drugog tipa. Razvijaju se nova rešenja za zaštitu ali još uvek nisu dovoljno kvalitetna ili komercijalno primenljiva zbog značajnog usporavanja sistema i jako velikog broja grašaka u procesu otkrivanja.

# Literatura

[1] STEGANOGRAFIJA KAO ANTIFORENZIČKI ALAT, Manja Đuričkov

[2] DIGITALNA STEGANOGRAFIJA JPEG SLIKA PRIMENOM DCT TRANSFORMACIJE, Dejan Uljarević, Mladen Veinović

[3] SteganPEG Steganography + JPEG, V. Lokeswara Reddy , Dr. A. Subramanyam , Dr.P. Chenna Reddy

[4] STEGOTE - STEGANOGRAPHY TOOL FOR HIDING INFORMATION IN JPEG AND PNG IMAGES, Triinu Erik, TALLINN UNIVERSITY OF TECHNOLOGY

[5] Steganalysis

<http://io.acad.athabascau.ca/~grizzlie/Comp607/steganalysis.htm>

[6] A Novel Steganalysis Method Based on Histogram Analysis, Bismita Choudhury, Rig Das and Arup Baruah

<https://www.researchgate.net/publication/282889667_A_Novel_Steganalysis_Method_Based_on_Histogram_Analysis>

[7] The Simplest Classifier: Histogram Comparison

<https://mpatacchiola.github.io/blog/2016/11/12/the-simplest-classifier-histogram-intersection.html>

[8] An Analysis of LSB & DCT based Steganography, Dr. Ekta Walia a , Payal Jain

[9] Hiding data in images using DCT steganography techniques with compression algorithms, Osama F. AbdelWahab, Aziza I. Hussein, Hesham F. A. Hamed, Hamdy M. Kelash,

Ashraf A.M. Khalaf5, Hanafy M. Ali, Faculty of Engineering, Minia University, El Minia, Egypt

<https://www.researchgate.net/publication/330565811_Hiding_data_in_images_using_DCT_steganography_techniques_with_compression_algorithms>

[10] A DCT-Based Robust Methodology for Image Steganography, Stuti Goel, Arun Rana, Manpreet Kaur Dept. of E&C, Doon Valley Institute of Engg. & Technology, Karnal, Haryana, India

[11] A Review of Comparison Techniques of Image Steganography, Stuti Goel, Arun Rana & Manpreet Kaur Kurukshetra University

[12] Steganography Tool

<https://www.sciencedirect.com/topics/computer-science/steganography-tool>