Univerzitet u Nišu, Elektronski fakultet

Katedra za računarstvo

Video steganografija

Digitalna forenzika

Seminarski rad

Mentor:

Prof. dr Bratislav Predić

Student:

Milica Trifunović, 1234

Niš, 2023.

Sadržaj

Uvod

Informaciono-komunikacione tehnologije razvile su se usled razvoja računarskih mreža i nametnule širu upotrebu računara u skoro svim sferama društvenog života. Danas, u svim aspektima ljudskog delovanja računar igra značajnu ulogu, pa tako i u komunikaciji, odnosno prenosu informacija između pošiljaoca i primaoca, pri čemu informacije koje se prenose treba da budu dostupne samo željenom primaocu. U ovakvim uslovima, pojavio se problem sigurnosti informacionih sistema, jer se informacije prenose putem raznih medija u digitalnom obliku i lako se može doći u njihov posed. Zbog toga je potrebna zaštita ovakavih informacija. Najčešće se koriste metode kao što su kriptografija, kodiranje, ali i steganografija. Svaka od ovih metoda ima svoje prednosti i nedostake. U radu se opisuje stegonografija jer je u posljednjih nekoliko godina ova metoda postala veoma raširena. Prvo poglavlje govori o pojavi i istoriji steganografije, dok je u drugom poglavlju predstavljen sam pojam steganografije, steganografskih sistema.

Digitalna steganografija podrazumeva sakrivanje poruke unutar nekog digitalnog formata (tekst, slika, audio, video). Često se kao medijum za sakrivanje poruka koristi video, koji predstavlja skup slika (*frejmova*). Pregled najkorišćenijih tehnika za steganografiju u slikama dat je u četvrtom poglavlju.

Steganografija i kriptografija se neretko poistovećuju, međutim, ove dve metode se značajno razlikuju. Kod upotrebe kriptografije je vidljivo da se komunikacija odvija kroz kriptovan kanal, odnosno da postoji poruka unutar kriptovanog faja. Kada je u pitanju steganografija ne vidi se postojanje komunikacije i skrivene datoteke jer je ona obično "*umetnuta*" i skrivena u drugu datoteku. Zbog ovoga, mogućnosti primene steganografije su, pored legalnog korištenja kod zaštite vlasništva (eng. *watermarking*) uvideli zlonamerni korisnici na Internetu. Njihovo svakodnevno korištenje ove tehnike zadaje probleme kako stručnjacima zaduženim za sigurnost, tako i kompjuterskim forenzičarima, ali i sudskim veštacima prilikom istraga kriminalnih dela. U nastavku rada naglasak će se, pored pojma i načina funkcioniranja steganografije, staviti i na moguće zloupotrebe steganografije, kao i načine njenog otkrivanja i stegoanalizu.

Za potrebe ovog rada implementirana je steganografija videa pomoću LSB (Least Significant Bit) tehnike i Knight Tour algoritma za odabir piksela. Detalji implementacije prikazani su u poglavlju 4.

Steganografija kroz istoriju

Upotreba steganografije potiče od davnina (440god. pre n. e.), iako ne u obliku u kakvom nam je danas poznata. Herodot je naveo dva primera steganografije u svom delu „*Herodotova istorija*". U delu je navedeno kako je Demaratus poslao upozorenje o predstojećem napadu na Grčku zapisivanjem poruke na drveni kalup voštane ploče za pisanje, pre izlivanja voska. Drugi drevni primer upotrebe steganografije je priča o Histaeusu i njegovom vernom robu na čiju glavu je Histiaeus ispisao poruku i sačekao da mu kosa izraste. Kasnije je rob tu poruku neprimećeno preneo kako bi pokrenuo ustanak protiv Persijanaca.

Poznat je i primer steganografije u Peruu. Na suvoj ravni je izgrebano više od 80 km linije između dva grada Naska i Palpe, od kojih su mnoge vidljive tek iz vazduha. Tragovi steganografije mogu se pronaći u delima Džon Tritemius (1462-1516) *(„Steganografija: umetnost koja zahteva otkrivanje skrivenog pisanja misaonim aktivnostima čoveka2*"). Kraljica Marija od Škotske je koristila kombinaciju kriptografije i steganografije da sakrije pisma.

U novijoj istoriji, neke od steganografskih metoda korišćene su tokom Drugog svetskog rata. Mikrotačke razvijene od strane nacista su delovi mikrofilma, napravljene pod velikim uveličanjem, najčešće preko 200 puta. Ove tačke mogu sadržavati stranice informacija, slika itd. [6]

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

Savremena steganografija

Reč steganografija je kovanica od dve reči grčkog porekla, **στεγανοσ** (steganos) i **γραφο** (grafo), što u prevodu znači "skriveno pisanje". [1]. Danas se situacija nije promenila u pogledu bitnosti prenosa informacija, i dalje se informacije prenose, ali na drugačiji način. Snaga Interneta se ogleda u tome da se u kratkom roku mogu preneti ogromne količine informacija sa jednog na drugi kraj sveta.

Steganografija je disciplina koja se bavi prikrivenom razmenom informacija. Osnovni princip steganografije počiva na prikrivanju samog postojanja informacije koja se prenosi unutar nekog naizgled bezazlenog medija ili skupa podataka. Moderna steganografija, koja koristi prednosti digitalne tehnologije, najčešće podrazumijeva skrivanje tajne poruke unutar multimedijalne datoteke. Multimedijalne datoteke sadrže prostore podataka koje različite steganografske tehnike popunjavaju tajnim informacijama.

Pomoću steganografije informacije je moguće sakriti unutar:

- Slike - fotografije (.bmp, .gif, .jpeg i sl.)
- Video fajla (.avi, .mpg, .vob i sl.)
- Audio fajla (.mp3, .midi, .wav, .wma i sl.)
- Datoteke (.doc, .xls, .ppt, .txt i sl.)
- ali i bilo kog binarnog fajla

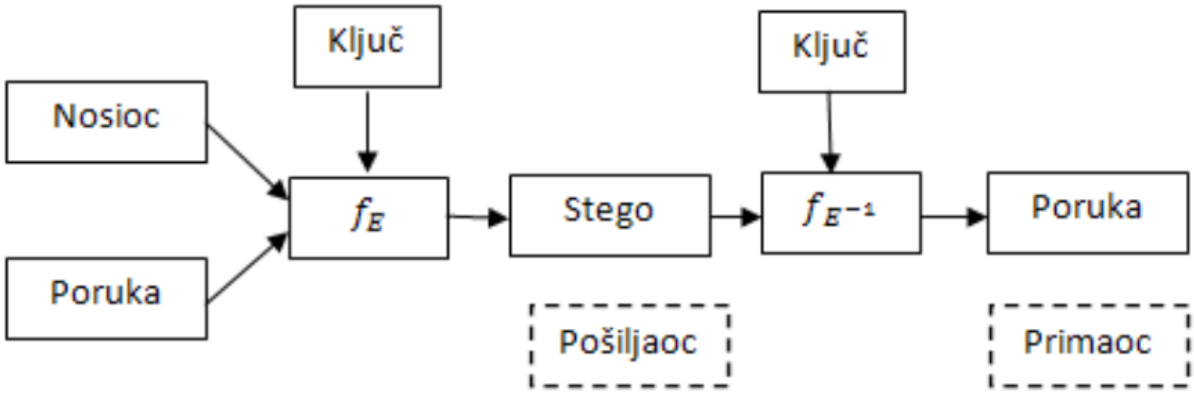
Proces steganografije

Osnova steganografije je prenos informacija kroz skriveni komunikacioni kanal (stego kanal). Proces steganografije počinje umetanjem poruke u transportni posrednik, koji se zove nosilac. Skrivena poruka i nosilac zajedno formiraju steganografski medijum. Nakon toga se, opciono, dodaje steganograski ključ kako bi se fajl dodatno kriptovao i osigurala bezbednost podataka. Poruka šifrovana na ovaj način, biće nečitljiva za primaoce koji ne poseduju ključ i u slučaju da bude izdvojena iz nosioca poruke. U stego sistemu može postojati jedan ili više stego ključeva, a po analogiji sa kriptografijom, razlikujemo stego sisteme sa tajnim i javnim ključem, pa samim tim postoje simetrični (samo tajni ključ) i asimetrični (i tajni i javni ključ) steganografski sistemi. Kod simetričnih sistema isti ključ se koristi i za šifrovanje i za dešifrovanje, dok se kod asimetričnih sistema javni ključ koristi za šifrovanje, a tajni za dešifrovanje poruke.

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

Steganografski medijum = skrivena poruka + nosilac poruke + steganografski ključ

Proces se može pokazati kao:



Slika 1 Opšti proces steganografije

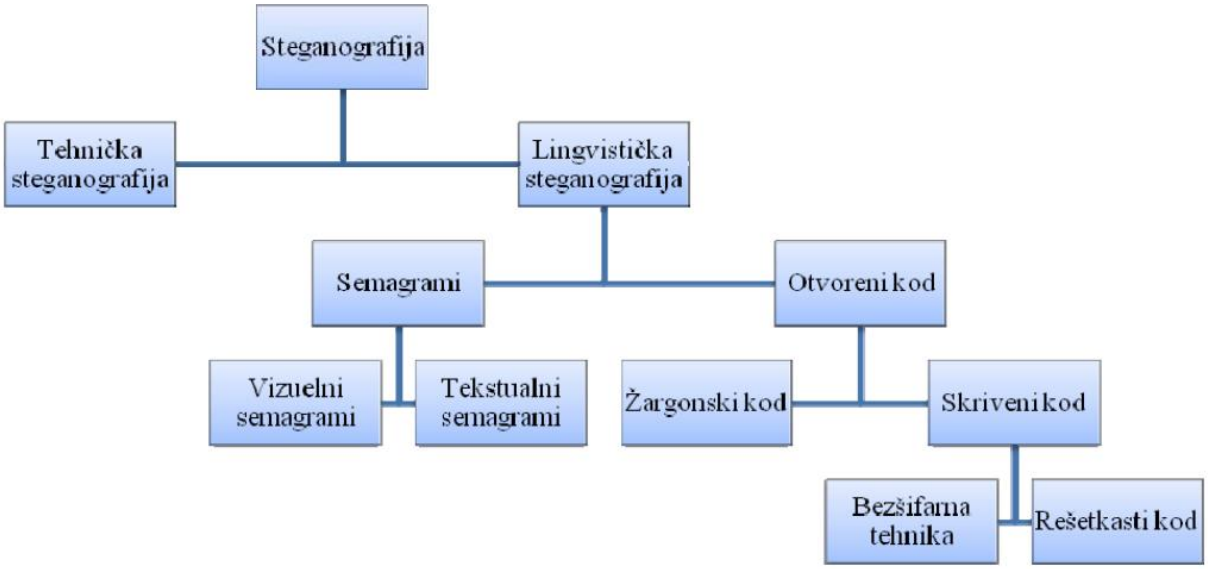
Na slici 1 prikazan je način funkcioniranja steganografskog sistema, gde je:

- Nosioc - medijum unutar kojeg se sakriva tajna poruka (eng. *carrier, cover medium*)
- Poruka - tajna poruka koja treba biti sakrivena (eng. *payload, embedded message*)
- Ključ - steganografski ključ; parametar funkcije fE
- fE - steganografska funkcija "ugrađivanje"
- Stego - steganografski fajl (eng. *package, steganography medium*)
- fE^{-1} : steganografska funkcija "izdvajanje"

Primena steganografije se najčešće bazira na sledećem principu: pošiljalac tajne poruke bira nasumično nosioca poruke. U izabrani nosilac poruke implementira se tajna poruka uz pomoć stego ključa primenom neke od tehnika. Primaocu se šalje steganografski medijum, a primaoc na drugoj strani inverznim 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 zamenjeni tajnom porukom. Takođe, nephodno je da digitalni format nosioca poruke bude takav da promena redundantnih delove ne izaziva greške (što je slučaj sa npr. exe fajlovima).

Klasifikacija steganografskih tehnika

Podela steganografskih tehnika predstavljena je na slici 2:



Slika 2 Klasifikacija steganografskih tehnika

Popis steganogafskih tehnika:

• **Tehnička steganografija** (eng*. technical steganography*) koristi naučne metode za skrivanje poruka, kao što su upotreba nevidljivog mastila, mikrotačaka i ostale tehnike smanjivanja veličine tajne poruke.

• **Lingvistička steganografija** (eng. *linguistic steganography*) obuhvata sve tehnike koje skrivaju tajnu poruku unutar nosioca na način da deluje kao bezazleni skup informacija. Ova grana steganografije dalje se kategoriše na semagrame i otvorene kodove.

• **Semagrami** (eng. *semagrams*) skrivaju informacije upotrebom različitih simbola i znakova. Postoje vizualni i tekstualni semagrami.

• **Vizualni semagrami** (eng. *visual semagrams*) baziraju se na principu skrivanja poruke upotrebom bezazlenih i svakodnevnih fizičkih objekata, npr. specifičnim rezmeštanjem detalja na desktop-u ili objekata na Web stranici.

• **Tekstualni semagrami** (eng. *text semagrams*) skrivaju informacije različitim modifikacijama izgleda nosioca teksta, npr. suptilna promena veličine ili tipa fonta, dodavanje dodatnih razmaka, ulepšavanje slova ili dodavanje ručno pisnaog teksta.

• **Otvoreni kodovi** (eng*. open codes*) uključuju sve tipove prenosa tajne poruke u kojima se koristi legitiman nosilac poruke na način koji nije očigledan nekom nesumnjičavm posmatraču. Otvoreni kodovi se dele na žargonski kod i skrivene šifre.

• **Žargonski kod** (eng*. jargon code*) podrazumijeva korišćenje jezika koji razume ograničena grupa ljudi, a koji je beznačajan ostalima, npr. specifična terminologija određene grupe ljudi ili simboli za indikaciju postojanja i tipa bežičnog mrežnog signala ili terminologije. Podskup žargonskog koda je i znakovni kod u kome se izvesnim preuređenjem fraze menja značenje.

• **Skriveni kod** (eng*. covered code*) predstavlja steganografsku tehniku kod koje je umetnutu tajnu poruku moguće izdvojiti iz steganografskog medija samo ako je poznata tačna metoda korišćenja za njeno umetanje u nosiocu. Skrivene šifre uključuju rešetkaste i nulte šifre.

• **Rešetkasti kod** (eng*. grille code*) pri otkrivanju koristi šablon koji je korišćen za prikrivanje u nosiocu poruke. Reči koje se pojave pri otvaranju šablona je sakrivena poruka.

• **Nulta šifra** (eng. *null cipher*) ili **bezšifarna tehnika** koristi se za skrivanje informacija tako što se definiše neki set pravila, npr. „čitaj svaku petu reč" ili „čitaj svaki treći znak u svakoj reči". Ova metoda omogućava skrivanje tajnih poruka u svakodnevnim porukama bez uporabe komplikovanih algoritama ili alata. Primeri umetanja tajnog teksta unutar datoteka su: ispod slike u PowerPoint datoteci, u Properties delu Word datoteke, unutar komentara na Web stranicama, unutar bilo kojeg dokumenta tako da boja teksta odgovara boji pozadine.

Primer: Jedan od najjednostavnijih i najpoznatijih primera primene nulte šifre je poruka koju je jedan nemački špijun slao za vreme Drugog svetskog rata:

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

Uzimanjem 2. slova iz svake reči, dobija se sledeća tajna poruka:

„PERSHING SAILS FROM N.Y. JUNE 1"

Podela steganografije na osnovu medija

Savremena steganografija koristi skrivanje tajne poruke unutar sadržaja nekog multimedijalnog fajla. Multimedijalni fajlovi u sebi sadrže veliki broj bitova od manjeg značaja. Promena ovih bitova ne utiče značajno na sam fajl, pa je moguće iskoristiti ih za sakrivanje poruke.

Seganografija se na osnovu tipa medija u koji se ugrađuje tajna poruka deli na:

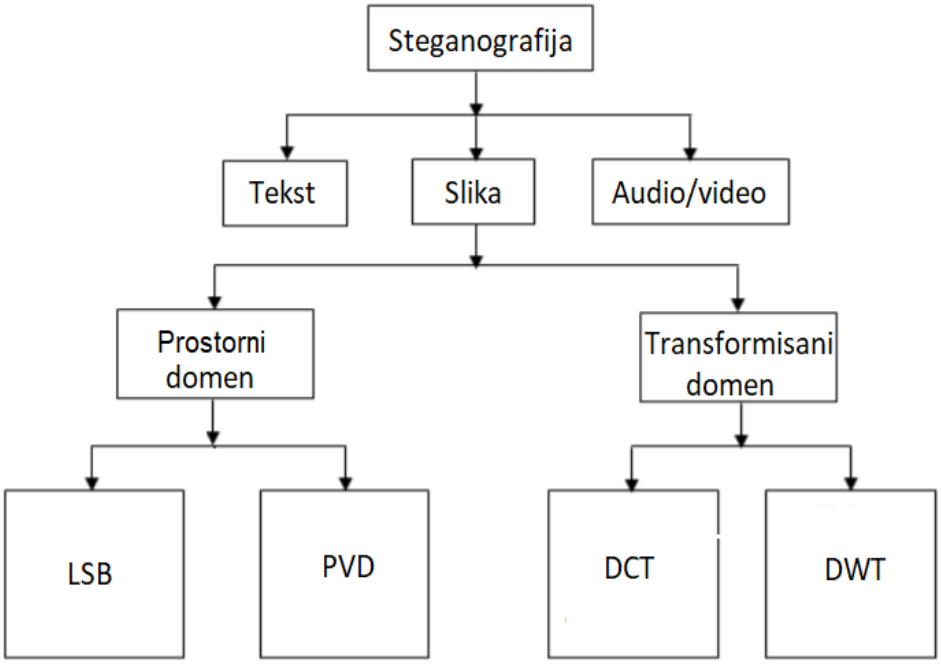
- Steganografiju teksta
- Steganografiju slika i video snimaka
- Steganografiju audio snimaka

Steganografske tehnike se mogu podeliti u sledeće grupe:

- *Tehnike supstitucije* – Delovi nosioca poruke koji nisu od velike važnosti koriste se za sakrivanje poruke. Primer ovakve tehnike je LSB (*Least Significant Bit*). Kod ove tehnike, delovi poruke smeštaju se u najniže bitove nosioca poruke jer njihova promena najmanje dovodi do vidljive promene.
- *Tehnike transformacije domena* – Kod ovih tehnika, pre sakrivanja poruke vrši se transformacija domena, a onda se u novom, transformisanom domenu vrši sakrivanje. Ovde se ubraja diskretna kosinusna tranformacija (eng. *Discrete Cosine Transform*), diskretna Furijeova transformacija (eng. *Discrete Fourier Transform*) i diskretna talasna transformacija (eng. *Discrete Wavelet Transform*).
- *Tehnike proširenog spektra* – Poruka koja se prenosi se modifikuje signalom šuma, tako da i sama izgleda kao slučajan šum, a ne informacija. Ove tehnike se obično koriste u bežičnim sistemima jer povećavaju otpornost na smetnje i omogućavaju nesmetanu komunikaciju između više učesnika. Najčešće korišćene tehnike ovog tipa su proširenje spektra metodom direktne sekvence (eng. *Direct Sequence Spread Spectrum*) i proširenje spektra metodom frekvencijskog skakanja (eng. *Frequency Hopping Spread Spectrum*).
- *Statističke tehnike* – Poruka koju treba sakriti se deli na bitove, a nosilac poruke na onoliko delova koliko bitova poruke ima. Ako je bit poruke 1, odgovarajući blok se menja tako da primalac može statističkim testiranjem da otkrije da li je blok promenjen, u suprotnom blok se ne menja.

- *Tehnike distorzije* – Umesto da se poruka sakriva direktno u medijum, sam medijum menja oblik kako bi mogao da sakrije i prenese poruku. Da bi poruka mogla da se ekstrahuje na prijemnoj strani, neophodno je da bude poznat originalni oblik medijuma.
- *Tehnike stvaranja medijuma pomoću skrivene poruke* – Kod ovog metoda se na osnovu poruke formira medijum.

Steganografija se primenjuje u prostornom ili transformisanom domenu. Na slici 3 su prikazane najčešće korišćene tehnike u digitalnoj steganografiji.



Slika 3 . Najčešće tehnike u digitalnoj steganografiji

Sve pomenute tehnike, nakon što izvrše neophodne transformacije, ugrađuju poruku u medijum koristeći jedan od sledeća tri principa:

- *Ubacivanje* se koristi za sakrivanje podataka u delovima medijuma koji su od manjeg značaja za potencijalnog napadača. Zasniva se na dodavanju bitova u datoteke tako da površinski deo medijuma ostane savršeno čist. Umetanjem određenog broja dodatnih bezopasnih bitova u medijum njegova struktura se ne menja značajno, tako da krajnji korisnik ne može da detektuje prisustvo skrivenog podatka u medijumu. Mana ovog pristupa je što u zavisnosti od veličine poruke koja se ugrađuje raste i veličina medijuma, tj. datoteke koja se prenosi. U slučaju da je poruka velika, veličina medijuma može da naraste tako da izazove sumnju kod potencijalnih napadača.

- *Supstitucija* ili zamena podrazumeva zamenu najmanje značajnih (najnižih) bitova datoteke, tako da promene datoteke budu što manje vidljive. Prednost ovog pristupa je što se ne menja veličina datoteke, a mane to što ipak dolazi do degradacije datoteke i što je veličina poruke koja može da se ugradi u datoteku ograničena brojem najmanje značajnih bitova datoteke.
- Generisanje ne zahteva originalnog nosioca poruke, već se nosilac poruke, tj. datoteka generiše na osnovu poruke koja se šalje. Rezultat generisanja je originalna datoteka, imuna na komparaciju sa drugim datotekama. To je glavna prednost generisanja u odnosu na ubacivanje i supstituciju, kod kojih je moguće uočiti promene u datoteci upoređivanjem sa originalom.

Steganografija slika i videa

Kada se kao medijum za prenos sakrivene poruke koristi slika, obično se unutar nje smešta tekst ili neka druga slika. Poruku je potrebno sakriti tako da u originalnoj slici ne dođe do većih distorzija i promena. Sa stanovišta računara, slika je matrica piksela od kojih je svaki predstavljen određenim brojem bitova koji određuju boju i intenzitet svetlosti. Broj bitova kojim je predstavljena boja piksel je dubina bita i minimalna vrednost za nju je 1, što je slučaj kod binarnih ili monohromatskih slika. Pomoću 8 bitova može da se prikaže 256 različitih boja ili nijansi sive. Digitalne slike mogu da se pamte tako da dubina bita iznosi 24, što znači da je za svaku komponentu boju iskorišćeno po 8 bitova, čime se postiže najveći kvalitet slike. Takve slike su pogodni kandidati za sakrivanje informacija zbog njihove visoke rezolucije [2]. Razlog je što one sadrže veliku količinu informacija, pa promene koje nastaju sakrivanjem poruke ne utiču značajno na kvalitet slike. Ipak, ako je poruka koju treba sakriti veoma velika, može doći do deformacija slike.

Digitalni video predstavlja skup okvira (slika) koji se reprodukuju sa fiksnom brzinom kadrova na osnovu video standarda. Kvalitet digitalnog video zapisa zavisi od kombinacije parametara poput fps (broj frejmova u sekundi), broja piksela u kadru i veličine kadra. Svaka slika u video zapisu naziva se frejm koji sadrži broj piksela koji imaju tri ili četiri kombinacije boja poput RGB (crvena, zelena, plava) ili CMIK (cijan, magenta, žuta, crna). Preostale boje sastoje se od mešavine ovih osnovnih boja. Digitalne slike se koriste za steganografiju zbog slabosti HVS-a (ljudskog vizuelnog sistema) koji ima malu osetljivost kod slučajnih promena obrazaca. Zbog ove slabosti tajna poruka može se sakriti u video ili sliku i da pritom ne bude primećena.

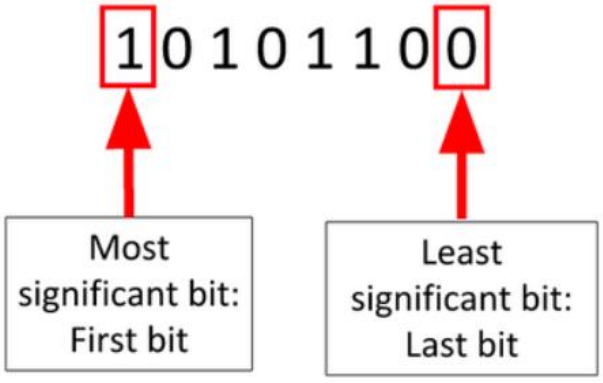
Postoje razne tehnike ugrađivanja koje nam omogućavaju da sakrijemo tajnu poruku u datom objektu koje će biti opisane u nastavku.

LSB

LSB ili bit najmanje težine je najjednostavnija i najkorišćenija steganografska tehnika. Najniži bitovi slike koja se koristi kao medijum služe za prenos skrivene poruke. Slika obično sadrži određen broj bitova koji ne nosi značajne informacije, tj. ne utiču mnogo na njen izgled. U ovoj tehnici se upravo ti bitovi modifikuju tako da predstavljaju bitove tajne poruke. LSB metoda je najpogodnija za slikovne datoteke koje imaju visoku rezoluciju uz upotrebu različitih boja.

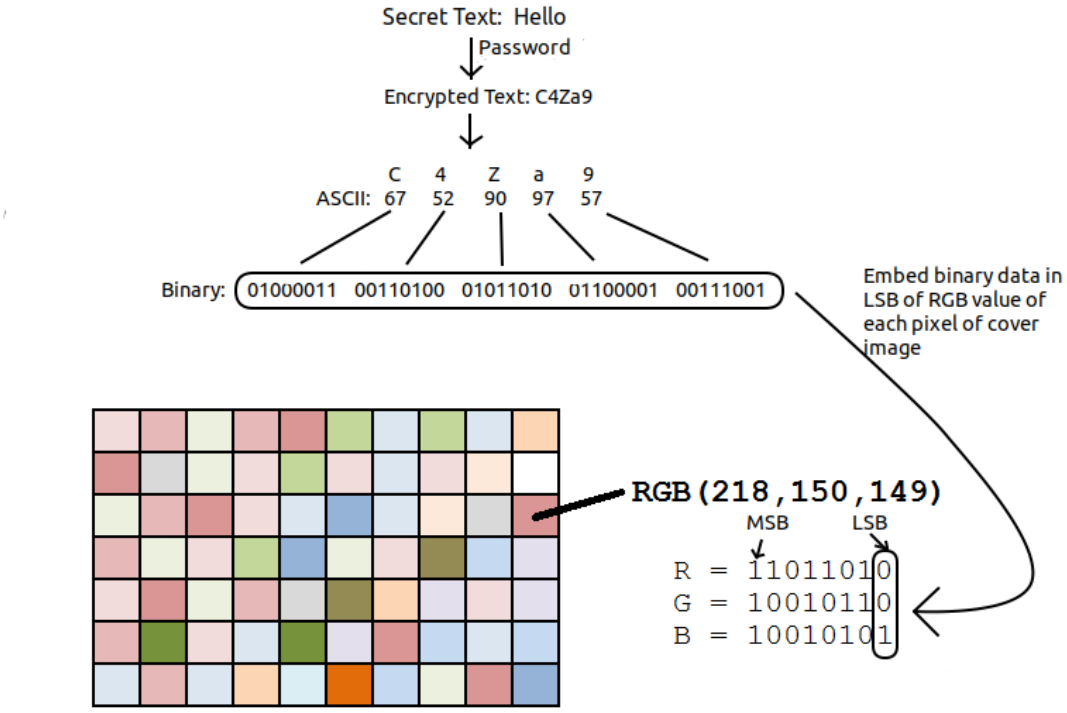
Primenom ove metode ne povećava se veličina datoteke, ali zavisno od veličine informacije koja se skriva, može doći do primetnih distorzija. Zato su najbolji kandidati za ovu metodu 24-bitne slike, zbog njihove veličine. Međutim, na mreži se uglavnom razmenjuju slike u 8-bitnom format, pa je LSB moguće primeniti i nad njima, samo je veličina poruke koja u njih može da se smesti manja. Bitna karakteristika ovog metoda je da se konverzijom slike u drugi format gubi skrivena informacija. LSB metod može da se koristi za sve digitalne formate, a kad su u pitanju slike, može da se primenjuje i nad kvantizovanim DCT koeficijentima.

Postoje dve varijante ovog metoda: zamena najnižeg bita i poklapanje najnižeg bita [3]. Obe koristi big-endian binarnu reprezentaciju piksela ili koeficijenta u kojoj je bit na poslednjoj poziciji bit najmanje težine. Ti bitovi služe za ugrađivanje poruke koja je, takođe, u binarnoj reprezentaciji.



Slika 4 Big-endian binarna reprezentacija piksela

Zamena najnižeg bita (eng. *LSB substitution*, *LSB flipping*) se zasniva na upoređivanju bitova poruke i najnižih bitova slike. Ukoliko su isti, najniži bit ostaje isti, u suprotnom se najniži bit komplementira (1 postaje 0, a 0 postaje 1). Na taj način, svaki poslednji bit u bajtu postaje jednak odgovarajućem bitu poruke. Ilustracija ovog metoda prikazana je na slici 5.



Slika 5: Zamena najnižeg bita

Mana ovog metoda je njegova "asimetričnost". To znači da se parne vrednosti piskela nikad ne smanjuju, a neparne vrednosti ne povećavaju, pa je moguće detektovati primenu ove tehnike. Ona može da se unapredi ako se obilazak piksela, umesto redom, obavi po nekom uvrđenom pravilu koje mora biti poznato i pošiljaocu i primaocu, da bi mogao da izdvoji poruku iz slike, a poboljšanje je i varijanta LSB-a sa poklapanjem.

Poklapanje najnižeg bita (eng. *LSB matching, ±1 embedding*) takođe menja najniži bit u bajtu, ali ne tako da se on poklapa sa bitom poruke koja se prenosi. Umesto toga se vrednost najnižeg bita nasumično povećava ili smanjuje, što može da dovede do promena i ostalih bitova u bajtu. U ekstremnom slučaju, mogu da se promene svi bitovi. Naime, ako je binarna reprezentacija piksela $(0111111)_2$, a najniži bit se poveća, piksel postaje $(10000000)_2$. U praksi, ovaj algoritam nije tako jednostavan jer zavisi od slike koja je nosilac poruke i zahteva dodatne provere za granične slučajeve. Kada se poruka ugrađuje u piksele, vrednost 255 može samo da se smanjuje, a vrednost 0 samo povećava, a ako se poruka ugrađuje u DCT koeficijente, koeficijent s vrednošću 1 može samo da se poveća, a koeficijent s vrednošću 2 samo smanji (ne sme da postane 0).

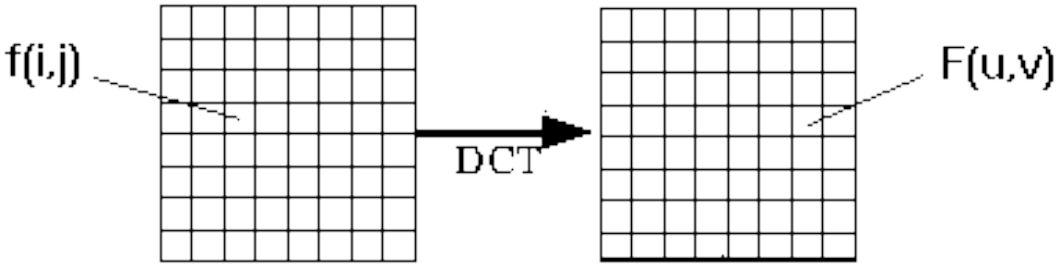
Dekodiranje poruka u obe varijante LSB tehnike svodi se na prikupljanje najnižih bitova koji formiraju poruku.

Diskretna kosinusna transformacija

Kad se podaci sakrivaju u prostornom domenu, gubici mogu da budu vidljivi ako se slika iseče i sl. Zbog toga je bolje pre promene slike preći u frekventni domen, za šta se koristi DCT algoritam. Ovom transformacijom izdvajaju se komponente visoke, srednje i niske frekvencije. Nakon primene algoritma poruka se sakriva po LSB metodi, ali se umesto realnih vrednosti piksela koriste dobijeni DCT koeficijenti. Ovaj algoritam ima svojstvo da je za tipičnu sliku većina vizuelno značajnih informacija o slici koncentrisana u samo nekoliko koeficijenata DCT-a. Iz tog razloga, DCT se često koristi u aplikacijama za kompresiju slike [4]. DCT je jedan vid Furijeove transformacije i često se naziva „realnim“ delom Furijeove transformacije. Matematički može da se predstavi sledećim formulama (slika 6.1) :

$$F(u,v) = \frac{1}{4}C(u)C(v)$$

$$\sum_{x=0}^{7}\sum_{y=0}^{7}\left[f(x,y)\cos\left(\frac{(2x+1)u\pi}{16}\right)\cos\left(\frac{(2y+1)v\pi}{16}\right)\right]$$

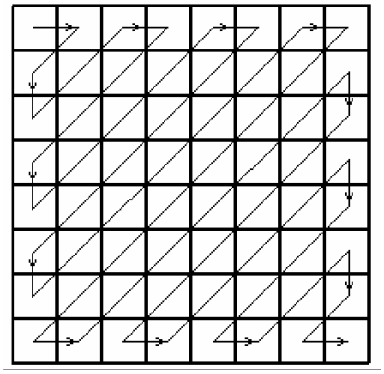


Slika 6.1: Diskretna kosinusna transformacija

Ulazna slika se deli na blokove veličine 8x8 koji se ne preklapaju, a na osnovu njih se generiše 64 DCT koeficijenta. Ova veličina blokova odabrana je kao kompromis između kvaliteta i složenosti. Za neke druge algoritme, veličina bloka može da bude 4x4 ili 16x16. Ukoliko broj vrsta ili kolona nije umnožak broja 8, poslednja vrsta ili kolona se repliciraju kako bi se ispunio uslov (eng. *padding*). Replicirane vrste ili kolone se uklanjaju u inverznom procesu. Vrednosti piksela su u rangu od 0 do 255, a da bi se centrirali oko nule, pre primena DCT-a im se vrednost umanjuje za 128, tako da im je vrednost u rangu [-128, 127]. Kada se izgenerišu ovi blokovi, vrši se njihova kvantizacija po formuli :

$$F(u,v) = Round\left(\frac{F(u,v)}{Q(u,v)}\right),$$

gde je *Q(u, v)* odgovarajući element kvantizacione matrice. U svakom bloku veličine 8x8 ima 64 koeficijenata, od kojih se prvi koeficijent naziva direktnom komponentom slike (DC), dok preostali koeficijenti predstavljaju naizmenične (AC) komponente. DC koeficijent je prvi koeficijent u matrici, na poziciji (0, 0), i on predstavlja procenu detalja u celom 8x8 bloku, tj. jednak je srednjoj vrednosti uzorka u bloku [7]. Visoke frekvencije koeficijenata uglavnom odgovaraju velikim vrednostima, dok niske frekvencije odgovaraju malim vrednostima. DC koeficijent predstavlja srednju vrednost bloka, pa bi njegova promena dovela do vidljivih distorzija u rezultujućoj slici. Zbog toga je potrebno izbegavati ove koeficijente, kao i AC koeficijente visokih frekvencija čija je vrednost bliska nuli ili jedinici. Da bi se odredili AC koeficijenti u bloku, potrebno je transformisati blok pomoću *cik-cak* šablona (slika 6.2).



Slika 6.2: Cik-cak obilazak matrice

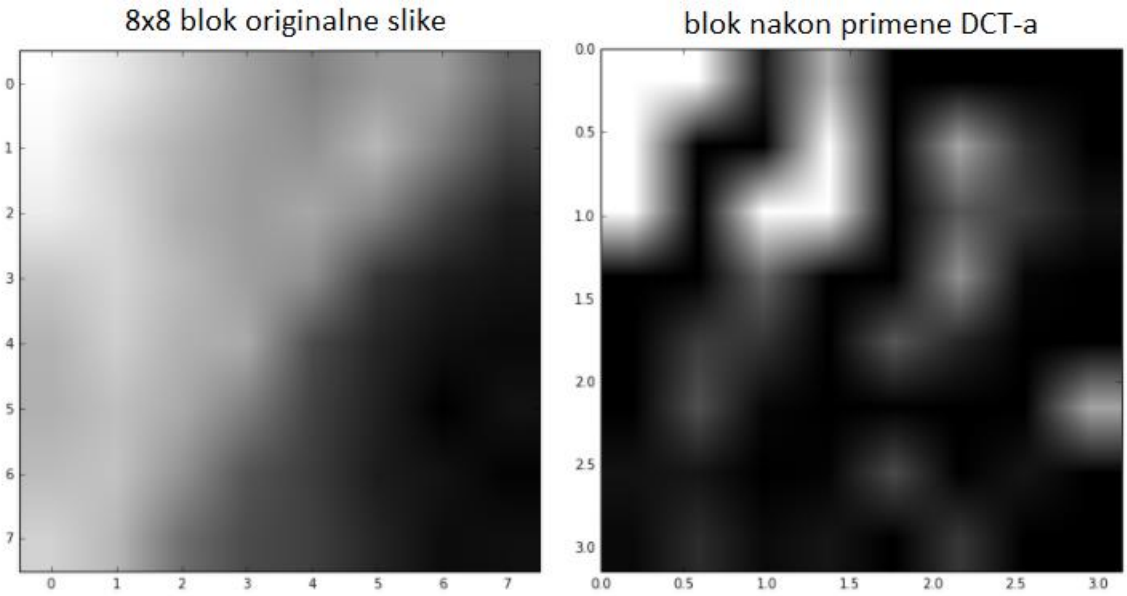
Korišćenjem cik-cak skeniranja koeficijenti se preraspoređuju tako da su na početku oni sa velikom količinom energije, tj. sa malom frekvencijom.

Kada se koeficijenti preurede po frekvenciji, primenje se kvantizacija. Kvantizacija se vrši nad svakim elementom DCT bloka pomoću standardne kvantizacione matrice, a rezultat se zaokružuje na najbližu celobrojnu vrednost. Kvantizacijom se blokovi kompresuju, a nakon toga je moguće korišćenjem prethodno opisane LSB tehnike sakriti poruku u okviru DCT koeficijenata [5]. Kvantizaciona matrica prikazana je na slici 6.3:

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

Slika 6.3: Kvantizaciona matrica

Na slici 6.3 prikazan je izgled bloka slike pre i posle primene diskretne kosinusne transformacije.



Slika 6.3: Primena DCT algoritma na 8x8 blok

Kada je izvršena kvantizacija, binarna reprezentacija poruke može da se ugradi u DCT koeficijente. Kao što je već rečeno, DC koeficijent je prosečna vrednost čitavog bloka, pa njegova promena dovodi do vidljivih distorzija. Da bi distorzija bila manje primetna, u obzir se uzimaju karakteristike ljudskog vizuelnog sistema (eng. *Human Visual System*). On je osetljiv na signale niže frekvencije, pa nije pogodno ugrađivati poruku u koeficijente sa nižom frekvencijom. Iz tog razloga, zaobilaze se DC koeficijenti, a poruka se smešta u AC koeficijente [5]. Promene mogu da se dalje ublaže odabirom samo pozitivnih AC koeficijenata. To je posledica veće osetljivosti negativnih koeficijenata na promenu, što može da rezultuje distorzijom stego-slike.

Kada se poruka ugradi u sliku, slika se transformiše nazad u prostorni domen. Poruka se iz ovako kreirane stego-slike izdvaja inverznim postupkom.

Tehnike proširenog spektra

Tehnika proširenog spektra (eng. *Spread Spectrum*) radi na principu ubacivanja, a bazira se na proširenju frekvencijskog spektra signala u određenom domenu. Koristi slabosti koje imaju ljudska čula. Ima primenu u kontroli bezbednosti komunikacionog kanala, povećanju otpornosti na prirodne smetnje i u ograničavanju snage određenih prenosnih linkova. Funkcioniše tako što dodaje šumove u slučajne odabrane signale. Informacije se kriju unutar nosioca i šire se preko frekvencijskog spektra. Šum može da bude sam nosilac poruke, tj. slika, ili neki pseudo-šum.

Kada se slika koristi kao šum, onda se može preneti jedna vrednost ispod nivoa šuma. Praktično, na taj način može da se prenese samo 1 bit [1]. Da bi se prenelo više, potrebno je sliku podeliti na manje delove. Varijanta sa dodavanjem pseudo-šuma je mnogo teža za detekciju zato što se poruka prenosi kroz nosioca, tj. sliku.

Tehnika proširenog spektra ugrađuje poruku u sliku u vidu Gausovog šuma [6]. Na nižim nivoima energije šuma, degradacija slike nije primetna ljudskom oku, dok se na višim nivoima manifestuje u vidu „pega“. Poruka koja treba da se prenese se konvertuje u binarni zapis i generiše se pseudo-slučajna sekvenca šuma. Vrši se modulacija pseudo-šuma pomoću poruke čime se dobija šum koji će da se kombinuje sa nosiocem poruke, tj. sa slikom.

Za inverzni proces nije neophodna originalna slika. Nad stego-slikom se primenjuju filteri za izdvajanje šuma, što rezultuje slikom koja je aproksimacija originalne slike [6]. Što su filteri bolji, to je aproksimacija verodostojnija, pa će manje grešaka biti u izdvojenoj poruci. Međutim, da bi poruka mogla da se izdvoji, neophodno je da odredišnoj strani bude poznata pseudo-slučajna sekvenca šuma. Vrši se demodulacija izdvojenog šuma upoređivanjem sa pseudo-šumom, čime se dobija sakrivena poruka.

Statičke metode

Statističke metode, poznate kao tehnike zasnovane na modelu (eng. *Model based techniques*), moduliraju ili modifikuju statistička svojstva slike pored njihovog očuvanja u procesu ugrađivanja [1]. Ta modifikacija je obično mala i na taj način je u stanju da iskoristi ljudsku slabost u detekciji promene osvetljenosti. Ovaj postupak se vrši jednostavnim modifikovanjem slike koja je nosilac poruke pravljenjem neke značajne promene u statističkim karakteristikama ako se prenosi „1“, a u suprotnom ne dolazi do promena. Da bi se poslalo više bitova, slika se deli na manje, od kojih će svaka da prenese 1 bit poruke.

Pored ove, koristi se i tehnika koja se naziva maskiranje podataka [2]. Prema ovoj tehnici, signal poruke se obrađuje u odnosu svojstva proizvoljnog signala nosioca. Slika se transformiše u frekventni domen, a onda se koeficijenti dele na dva dela kako bi signal poruke mogao zameniti perceptivno beznačajan deo. Stoga se menja statistika kvantizovanih nenultih AC (DCT) koeficijenata uzimajući u obzir funkciju parametarske gustine. Ovaj postupak zahteva histogram male preciznosti svakog frekvencijskog kanala uz poredjenje modela sa svakim histogramom da bi se izabrali odgovarajućim parmetri modela. Međutim, statističke steganografske metode u njihovom najjednostavnijem obliku, za koje su delovi slike (eng. *sub-images*) jednostavno pravougaonici originalne slike, osetljivi su na odsecanje, rotiranje i skaliranje, zajedno sa napadima koji rade protiv tehnike vodenog žiga. Da bi se to izbeglo, sliku treba deliti na „pod-slike“ (eng. sub-images) na osnovu elemenata slike (npr. lica u gužvi) uz korišćenje koda za ispravljanje grešaka u poruci.

Tehnike distorzije

Tehnike distorzije zahtevaju poznavanje originalne slike tokom procesa dekodiranja, gde dekoder proverava razlike između originalne slike i stego-slike kako bi se izdvojila tajna poruka. Poruka se ugrađuje tako što se originalna slika modifikuje sekvencom funkcija, tako da poruku u stvari krije distorzija signala. Modifikacije se biraju tako da se poklapaju sa tajnom porukom koja se prenosi [2].

Poruka se smešta u pseudo-slučajno izabranim pikselima. Ako se stego-slika razlikuje od originalne slike na određenom pikselu, onda je bit poruke 1. U suprotnom, bit poruke je 0. Modifikacije mogu da se izvrše tako da se statističke karakteristike slike ne menjaju. Prednost ove tehnike je što, ukoliko dođe do napada i napadač izvrši odsecanje, skaliranje ili rotaciju slike, primalac to može lako da detektuje. U nekim slučajevima, ako se poruka kodira sa informacijom za ispravljanje grešaka, modifikacije napadača mogu da se invertuju i da se izdvoji cela poruka bez grešaka.

Tehnika generisanja slike

Umesto da se poruka ugradi u sliku, od nje može da se izgeneriše slika. Poruka se konvertuje u elemente slike, a onda se oni spajaju i formiraju stego-sliku [1]. Ova tehnika ne može da se razbije skaliranjem ili rotiranjem slike, a ni kompresijom sa gubicima. Čak i ako se primeni odsecanje i izgube se neki delovi slike, ukoliko je poruka kodirana sa informacijom za ispravljanje grešaka, ona može da se izdvoji cela. U opštem slučaju, ova tehnika koristi pseudo-slučajne slike iz razloga što prenos više slučajnih slika koje se prenose kroz mrežu može da izazove sumnju da se u njima krije neka informacija, pa “napadači“ to mogu da iskoriste i blokiraju prenos.

Modifikacija elemenata

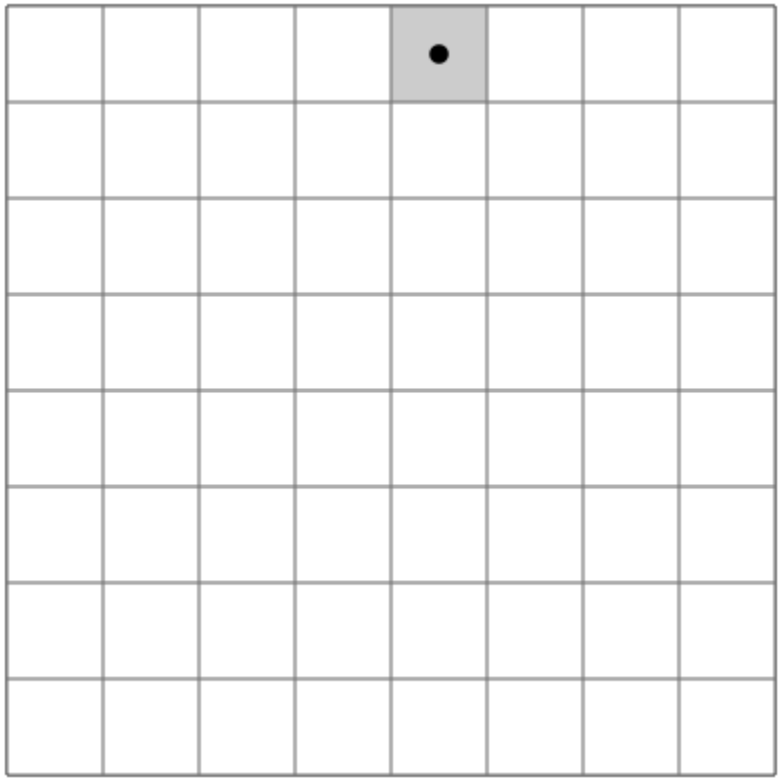
Neke steganografske tehnike ne pokušavaju da sakriju informacije koristeći stvarne elemente slika [2]. Umesto toga, one prilagođavaju elemente slike na načine koji nisu primetni, na primer, modifikovanjem boje očiju ili boje kose neke osobe na fotografiji. Ove modifikacije mogu da se koriste za prenos skrivenih informacija. Pored toga, ove informacije su otporne na rotaciju, skaliranje i kompresiju sa gubicima. Kod korišćenja ovog metoda treba imati na umu da istog nosioca (sliku) ne bi trebalo koristiti više puta, jer će korišćeni elementi postati vidljivi. Ova tehnika može da se izvede ručno bilo kojim softverom za uređivanje fotografija, a znatno je olakšana razvojem računarskog vida.

Implementacija steganografije videa pomoću LSB tehnike korišćenjem Knight Tour algoritma

Knight Tour algoritam

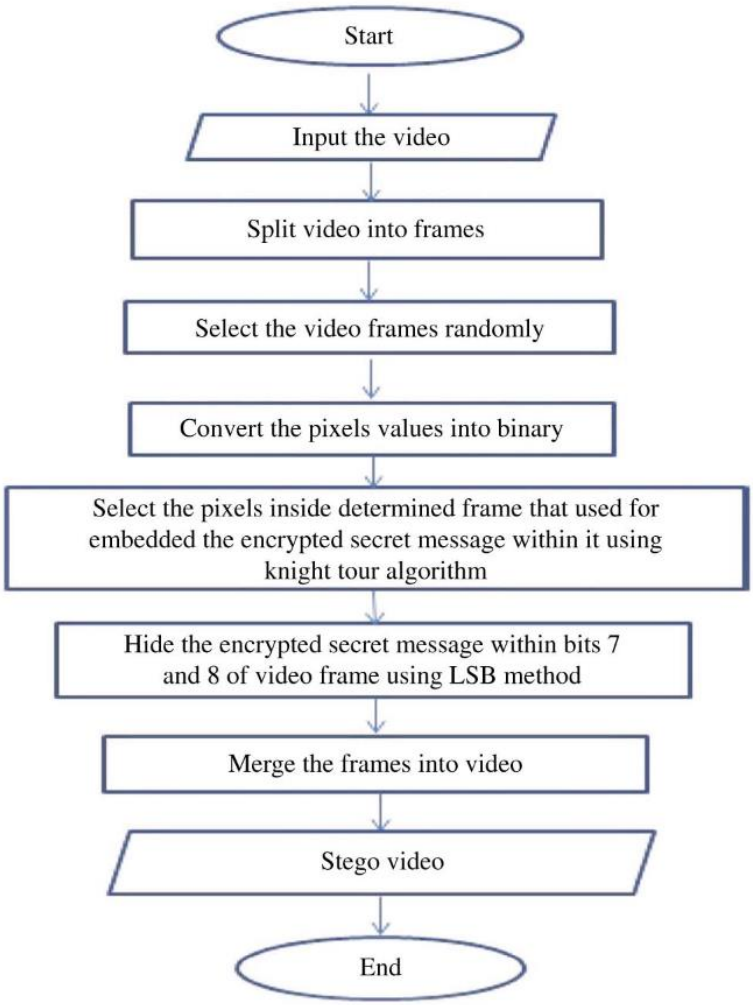
Jedan od nedostataka LSB metode je serijski odabir piksela. Iz tog razloga, važno je pronaći metode koje koriste slučajni odabir. Jedna od ovih metoda je algoritam viteške turneje. To je niz poteza viteza na šahovskoj tabli do te mere da vitez obiđe svako polje samo jednom. Nakon razdvajanja video snimka u frejmove, prema ovoj metodi, izabrani okvir se predstavlja kao šahovska tabla i prema kretanju viteza na šahovskoj tabli, a to je jedan red i dve kolone ili dva reda i jedna kolona na nasumične načine – latinično slovo (L), da izaberete piksele koji se koriste za ugrađivanje podataka.

Ovaj proces se koristi da bi se povećala robusnost predložene metode i da bi se nadomestio nedostatak LSB metode koja primenjuje serijski izbor piksela i nedostatak protiv elektronskih napada. [7]



Ilustracija 1 Primer Knight Tour algoritma na tabli 8x8

Proces ugradnje slike u video



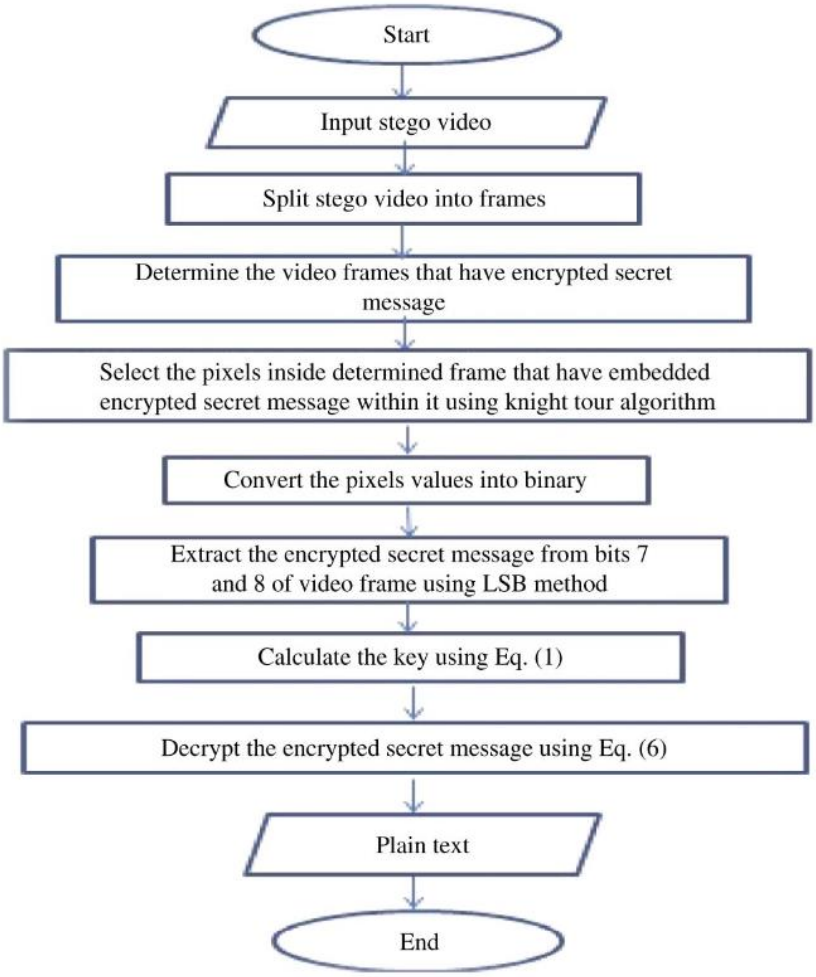
Slika 7: Algoritam ugradnje slike u video[7]

Kodirana tajna poruka je ugrađena u odabrane video frejmove korišćenjem algoritma viteškog obilaska i LSB metode. Video je podeljen u frejmove i konvertovan u skup slika. Nakon toga, odabrani su frejmovi koji će skrivati poruku. Zatim, pikseli unutar izabranog frejma koji se koriste za skrivanje podataka u njemu se biraju nasumično koristeći algoritam viteškog obilaska. LSB metoda se koristi za skrivanje šifrovane tajne poruke unutar izabranih piksela. Ovaj proces je primenjen na skup slika sve dok nije urađena cela tajna poruka. Zatim je skup slika konvertovan u frejmove. Konačno, video frejmovi se spajaju da bi se dobio stego video.

Koraci procesa ugradnje su:

- Ulaz: Početni video.
- Korak 1: podela video datoteke u frejmove.
- Korak 2: pretvaranje video frejmova u slike.
- Korak 3: odabir slika koje se koriste kao nosioci poruke.
- Korak 4: određivanje piksele unutar slike koji se koristi za ugrađivanje tajne poruke nasumično koristeći algoritam viteškog obilaska.
- Korak 5: LSB metoda se koristi za skrivanje šifrovane tajne poruke unutar bitova (7 i 8).
- Korak 6: pretvaranje sliku u frejm.
- Korak 7: spojanje video frejmova.
- Izlaz: stego video.

Proces ekstrakcije slike iz videa



Slika 8: Algoritam ekstrakcije slike iz videa [7]

Koraci procesa ekstrakcije su:

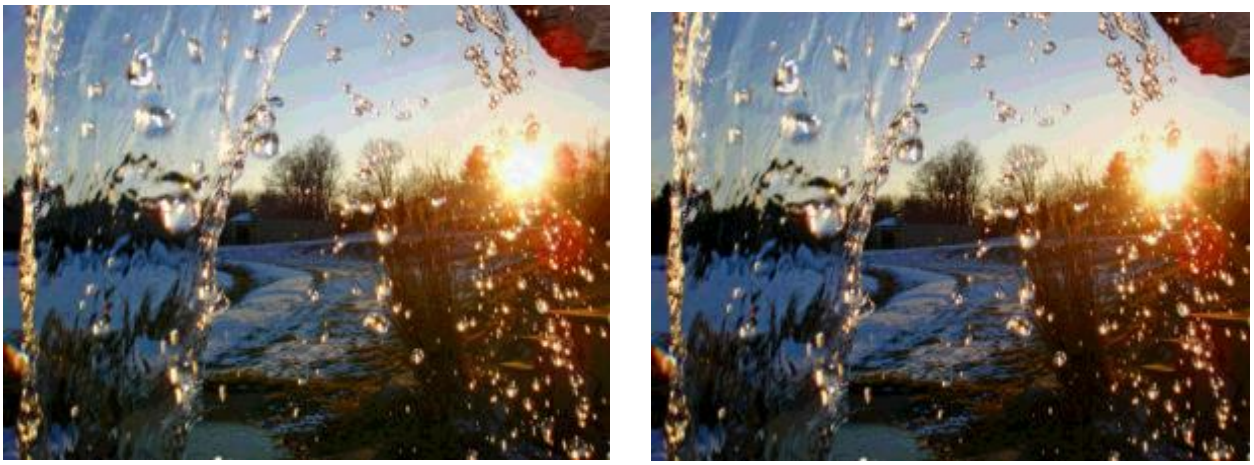
- Ulaz: stego video.
- Korak 1: otvaranje stego videa i podela na frejmove.
- Korak 2: pretvaranje video frejmova u slike.
- Korak 3: određivanje slika koje se koriste kao nosioci poruke.
- Korak 4: određivanje piksele unutar slike koji se koristi za ugrađivanje tajne poruke nasumično koristeći algoritam viteškog obilaska.
- Korak 5: LSB metoda koja se koristi za oporavak šifrovane tajne poruke iz bitova (7 i 8).
- Korak 6: dešifrovanje tajne poruke metodom oduzimanja.
- Izlaz: slika.

Rezultat implementacije

Primer jednog frejma pre i nakon umetanja poruke prikazan je na slikama ispod:

Slika 9: Originalan frejm (levo) i stego frejm (desno)

Primer početne slike i slike nakon ekstrakcije iz videa prikazan je ispod:



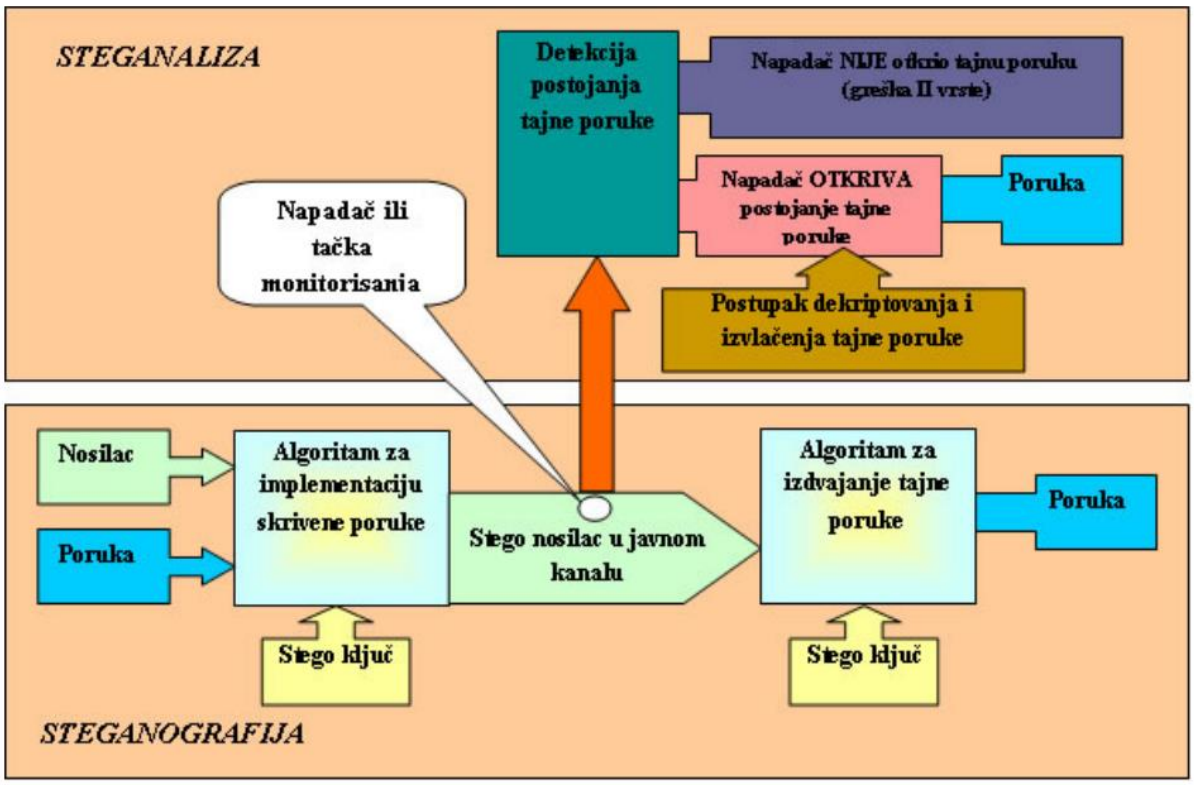
Slika 10: Početna slika(levo) i slika nakon ekstrakcije(desno)

Detekcija steganografije – steganoanaliza

Steganoanaliza, detekcija steganografije, 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, ili na izvlačenju skrivene poruke da se onemogući prijem poruke, ili na promeni tajne poruke radi dezinformacije primaoca. Uništavanje i/ili zamena tajne poruke može, takođe, biti pravno legitimna tokom istrage aktivnosti kriminalne ili terorističke grupe. U suštini steganonaliza treba da reši tri osnovna zadatka: detekciju, definisanje i dekodiranje skrivene poruke.

Za razliku od kriptoanalize, gde je evidentno da dobijeni šifrovani sadržaj sadrži tajnu poruku, steganoanaliza uglavnom počinje 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 11.



Slika 11: Odnos steganografije I steganalize

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

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

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

steganografski medijum je jedina stavka dostupna za analizu,

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

Tipovi napada na steganografske sisteme

Napadi na skrivene informacije mogu imati nekoliko oblika: detekcija, izdvajanje i/ili uništavanje i/ili dešifrovanje skrivene informacije. Sistem je već postao nesiguran ako je napadač u stanju samo da dokaže postojanje tajne informacije. Polazna pretpostavka je da napadač poseduje neograničene računarske resurse i u stanju je da primeni raznovrsne algoritme napada.

Napadi na steganografske sisteme u odnosu na krajnji cilj napadača, mogu se teoretski podeliti na tri vrste: pasivne, aktivne i namerne. U pasivne napade spadaju tehnike koje samo detektuju postojanje tajne poruke, npr., statističko testiranje hipoteze u kojoj postoje dve mogućnosti greške: greška I-vrste nastaje kada se detektuje postojanje tajne poruke u nosiocu, a ona stvarno ne postoji, a greška II-vrste nastaje kada se ne detektuje postojanje tajne poruke, a ona stvarno postoji. Steganografski sistemi maksimizuju verovatnoću da napadač napravi grešku II-vrste. Aktivni napadači su u stanju da modifikuju stego nosioca u toku prenosa, ali ne previše, jer će u tom slučaju perceptulane i semantičke osobine biti narušene. Steganografski sistemi su često jako osetljivi na modifikacije stego-paketa (npr., digitalno procesiranje, filtriranje, usrednjavanje, komprimovanje, prebacivanje iz formata u format), pa čak i kompresiju sa minimalnim gubicima, koje mogu izazvati potpuni gubitak tajne informacije, jer uklanjaju baš one neprimetne komponente signala u kojima se najčešće vrši utiskivanje tajne poruke. Aktivni napadač, koji često nije u stanju ni da detektuje postojanje tajne poruke, može dodati slučajan signal u stego nosioc i uništiti tajnu informaciju.

Napači mogu biti slučajni i namerni. Kao primer slučajnog napadača može se navesti slučajan šum koji se akumulira prilikom emitovanja signala nekim od spojnih puteva. Zbog toga jedan od značajnih zahteva koje steganografski sistem mora da ispuni je robusnost, tj., da se utisnuta tajna informacija ne može oštetiti bez drastičnih promena stego nosioca. Potrebno je naglasiti da postoji kompromis između sigurnosti (tajnosti) i robusnosti. Sigurnost zahteva da tajnu informaciju sakrijete u oblasti koje su perceptulano neprimetne, dok robusnost zahteva da tajnu informaciju sakrijete u oblasti koje su perceptualno primetne jer će tako biti teže oštetiti informaciju bez velike degradacije kvaliteta nosioca. Mnogi sistemi se dizajniraju tako da budu robustni na određene karakteristične tipove napada (kompresija, dekompresija, filtriranje, dodavanje belog šuma), a idealan sistem bi trebao da bude robustan na sve vidove napada. Generalno postoje dva principa da se napravi robustan steganografski sistem. Kod prvog sistema vrši se predviđanje mogućih napada i zatim se projektuje takav postupak implementacije tajne poruke koji je robustan na tu vrstu modifikacija, tako da modifikacija ne uništi u potpunosti informaciju. Druga strategija je da se primene inverzne modifikacije, od onih koje su korišćene tokom napada, kako bi se rekonstruisala originalna tajna informacija.

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

1. Poruke se moraju implementirati u nosioce korišćenjem javnih algoritama i tajnih ključeva,

2. Jedino vlasnik ispravnog ključa može detektovati, izdvojiti i dokazati postojanje tajne poruke.
3. Iako napadač uspe da selektuje sadržaj jedne skrivene poruke, ne može da detektuje ostale i
4. Kompjuterski je neizvodljivo detektovati tajnu poruku

Zaključak

Informacije koje se prenose kroz mrežu postale su mnogo osetljivije na napade sa razvojem informacionih sistema i mreža koji je doveo do unapređenja komunikacije. Ove informacije je neophodno zaštititi od neovlašćenog pristupa. Pored kriptografije, za zaštitu informacija, koristi se i steganografija. Steganografija raspolaže vrlo efikasnim i snažnim tehnikama koje ljudima omogućavaju zaštićenu i skrivenu komunikaciju. Kombinovana sa kriptografijom, predstavlja dodatni sigurnosni sloj u zaštiti informacija. Posljednjih godina, steganografija je bila tema mnogih diskusija vezanih za njenu zloupotrebu, naročito u terorističkim aktivnostima. Tako u mnogim zakonskim telima raste zabrinutost oko upotrebe steganografije za razmenu ilegalnih materijala preko multimedijalnih datoteka na web stranicama. Sa druge strane, postoji veliki broj prednosti korištenja steganografije u legalnom kontekstu, kao što su digitalni vodeni pečati za utvrđivanje vlasništva i autorskih prava ili sigurnije metode prenosa važnih i poverljivih informacija, stoga se u budućnosti očekuje još intenzivniji razvoj ove tehnologije, te široka mogućnost primjene.

Digitalna steganografija se bavi sakrivanjem podataka u digitalne formate kao što su tekst, slika, video itd. Video steganografija zasniva se na deljenju video snimka na frejmove i primenu steganografije nad slikom. Ugrađivanje poruke u sliku može da se odvija u prostornom domenu, kroz vrednosti piksela, ili u frekventnom domenu, kroz vrednosti koeficijenata. Tehnike prostornog domena koje se često koriste su LSB, PVD i tehnike distorzije. U frekventnom domenu najviše se koriste diskretna kosinusna i diskretna talasna transformacija. Originalna slika se deformiše ugrađivanjem poruka, a suština jeste iskoristiti tehniku kod koje će promene da budu najmanje vidljive. Svaka od ovih tehnika ima prednosti i mane, a one se ogledaju kroz njihov kapacitet, bezbednost i robusnost, što su 3 glavne karakteristike steganografskog sistema:

- Kapacitet - količina informacija koja se može sakriti u stego medijumu.
- Bezbednost - zaštita podataka od neautorizovanog pristupa, tj. nemogućnost presretanja podataka i otkrivanja poruke.
- Robusnost – sposobnost steganografskog sistema da se odupre izdvajanju poruke, tj. otpornost medijuma kojim se poruka prenosi na napade.

Literatura

[1] M. Ćajić, B. Brkić, M. Veinović, Analiza steganografskih tehnika, (2010), https://www.researchgate.net/publication/265003223_ANALIZA_STEGANOGRAFSKIH_TEHNIKA_I_METODA

[2] N. Hamid, A. Yahua, R. Ahmad, O. Al-Qershi, Image Steganography Techniques: An Overview, (2012), https://www.cscjournals.org/manuscript/Journals/IJCSS/Volume6/Issue3/IJCSS-670.pdf

[3] T. Eriik, STEGOTE - STEGANOGRAPHY TOOL FOR HIDING INFORMATION IN JPEG AND PNG IMAGES, (2019), Tallin

[4] S. Goel, A. Rana, m. Kaur, A DCT-Based Robust Methodology for Image Steganography, (2013), Karnal: Doon Valley Institute of Engg. & Technology

[5] D. Veljarević, M. Veinović, DIGITALNA STEGANOGRAFIJA JPEG SLIKA PRIMENOM DCT TRANSFORMACIJE

[6] C. Boncelet, Spread Spectrum Image Steganography, (1999), University of Delawar

[7] Z. Safaa Younus, G. Thanoon Younus, Video Steganography Using Knight Tour Algorithm and LSB Method for Encrypted Data, (2019), https://www.degruyter.com/document/doi/10.1515/jisys-2018-0225/html#j_jisys-2018-0225_eq_006

[8] Ms. Pooja Vilas Shinde , Dr.Tasneem Bano Rehman , A Survey : Video Steganography techniques, https://www.researchgate.net/publication/329572494_A_Survey_of_Video_Steganography_Techniques