Univerzitet u Nišu, Elektronski fakultet
Katedra za računarstvo

Steganografija u slikama

Digitalna forenzika

Seminarski rad

Mentor:

Prof. dr Bratislav Predić

Student:

Vladana Stojiljković 1135

Niš, 2021.

Sadržaj

1. Uvod

Komunikacija predstavlja važan aspekt kako u poslovanju, tako i u privatnom životu. U procesu komunikacije se između pošiljaoca i primaoca razmenjuju informacije. Informacije koje se prenose ne treba da budu dostupne svima, već samo željenom odredištu. Osnovno sredstvo za komunikaciju danas je računar i s razvojem računarskih mreža, razvile su se i informaciono-komunikacione tehnologije. Prilikom slanja kroz mrežu, poruka prolazi kroz više računara, pa podaci mogu da budu izloženi neautorizovanom pristupu. Zbog toga je potrebno zaštititi podatke tako da šanse za njihovu zloupotrebu budu minimalne. Jedno od rešenja jeste primena steganografije.

Steganografija je nauka koja se bavi zaštitom podataka tako što ih ugrađuje u druge, tj. omogućava sakrivanje poruke unutar neke datoteke. Od ključnog značaja je da prisustvo poruke bude neprimetno. U tu svrhu razvijene su različite tehnike. Detaljan opis steganografskih sistema i različitih tehnika dati su u poglavlju 2.

Digitalna steganografija podrazumeva sakrivanje poruke unutar nekog digitalnog formata (tekst, slika, audio, video). Često se kao medijum za sakrivanje poruka koristi slika. Pregled najkorišćenijih tehnika za steganografiju u slikama dat je u poglavlju 3.

Ugrađivanje poruke u sliku može da se vrši u prostornom ili u nekom drugom domenu. Najčešće se koristi diskretna kosinusna transformacija za prelazak u frekventni domen, nakon čega se poruke utiskuju u sliku. Za potrebe ovog rada implementirana je steganografija u slikama pomoću ovog algoritma i detalji implementacije prikazani su u poglavlju 4. Poglavlje 5 sadrži zaključak, a poglavlje 6 spisak korišćene literature.

2. Steganografija

Sa razvojem informacionih tehnologija i telekomunikacionih sistema, značajno se povećala količina informacija koja se njima prenosi, pa i mogućnost za njihovu zloupotrebu. Informacije se prenose u digitalnom obliku, pa se lako mogu pronaći i preuzeti. Zato je od ključnog značaja onemogućiti neovlašćen pristup poverljivim podacima. U tu svrhu koriste se dve tehnike: kriptografija, koja šifruje podatke i pretvara ih u oblik koji će biti čitljiv samo onome kome su podaci namenjeni, i steganografija, tehnika za sakrivanje podataka. Najbolji način za očuvanje bezbednosti podataka jeste kombinacija ove dve tehnike.

Steganografija je nauka koja se bavi sakrivanjem informacija u drugim podacima. Reč steganografija je kovanica od dve reči grčkog porekla, στεγανοσ (steganos) i γραφο (grafo), što u prevodu znači pisati skriveno [1]. Cilj steganografije je da prenese informacije od pošiljaoca do primaoca tako što podatak utisne u nosioca podatka, koji mora da bude čitljiv i razumljiv za odredište. Za razliku od kriptografije, gde je moguće presretanje poruka i narušavanje njenog integriteta, kod steganografije je samo postojanje poruke neprepoznatljivo.

Ideja o korišćenju steganografije nije nova, već se neki njen vid koristio još u doba Antičke Grčke. Pojam steganografije prvi put se konkretno pominje u 15. veku nove ere u knjizi Džona Tritemiusa "Steganografija: umetnost koja zahteva otkrivanje skrivenog pisanja misaonim aktivnostima čoveka". U srednjem veku steganografija je korišćena za sakrivanje sadržaja pisama koje su razmenjivali vladari, a prva konkretna tehnika razvijena je za vreme Drugog svetskog rata i zasniva se na korišćenju *mikrotačaka* [1]. Mikrotačke su delovi filma uvećani oko 200 puta unutar kojih su umetane informacije. Tada se koristila i bešifrarna tehnika koja podrazumeva umetanje jedne poruke u drugu na neki jednostavan način. Krajem 20. veka počeo je naučni razvoj steganografije i razvijeni su različiti algoritmi.

2.1. Steganografski sistem

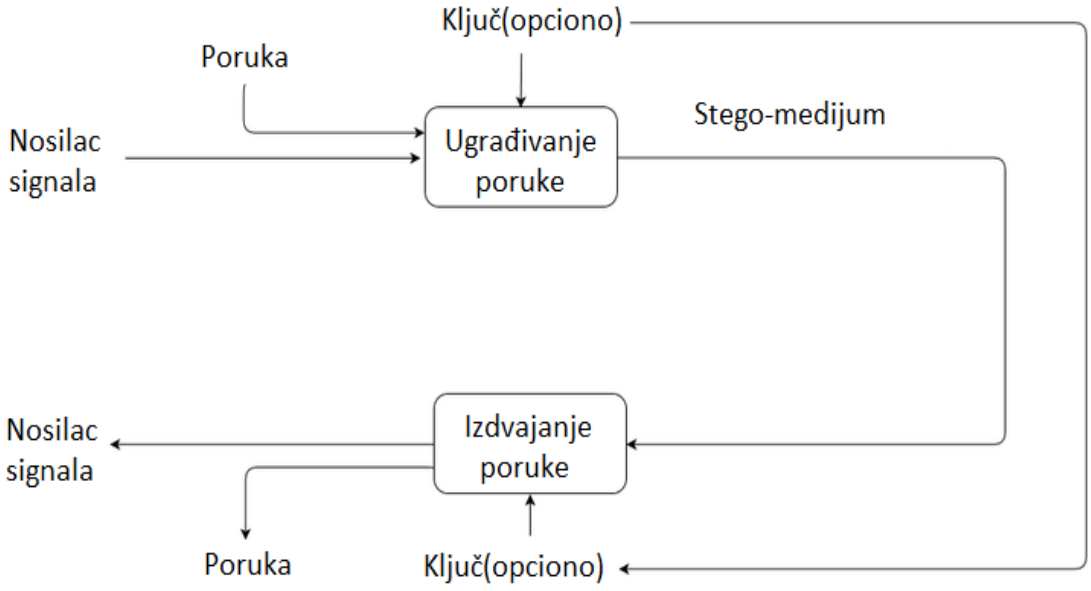
Funkcionisanje i performanse digitalnog steganografskog sistema opisuju se pomoću njegove tri važne karakteristike [2]:

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

Steganografija se bazira na prenosu informacija kroz skriveni kanal. Nosilac signala (eng. *carrier, cover media*) i poruka zajedno čine steganografski medijum. Steganografski medijum (eng. *steganography medium*) je posrednik koji sadrži ugrađenu poruku koja se prenosi, a

sama poruka se prenosi kroz steganografski kanal. Nosilac poruke može da bude bilo koja informacija u vidu teksta, slike, audio ili video formata. Poruka koju treba preneti se ugrađuje u nosioca (eng. *embedded message*). Prikaz steganografskog procesa dat je na slici 2.1.

Opciono može da se koristi i ključ (eng. *stego key*) za šifrovanje, kako bi se dodatno osigurala bezbednost podataka. Pomoću stego ključa se poruka šifruje, tako da i u slučaju da bude izdvojena iz nosioca poruke bude u nečitljivom formatu za primaoce koji nemaju ključ. Kao i kod kriptografije, ključ može da bude javni i tajni, a samim tim steganografski sistemi mogu biti simetrični (koriste samo tajni ključ) i asimetrični (koriste i tajni i javni ključ). 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.



Slika 2.1: Steganografski process

Pošiljalac bira nosioca poruke i primenom neke od tehnika u njega ugrađuje skrivenu poruku. Tako kreiran steganografski medijum se prenosi do primaoca koji, da bi pročitao poruku, treba da izvrši inverzan proces. Kako postojanje poruke u nosiocu ne bi bilo vidljivo, neophodno je da postoji dovoljan broj redundantnih bitova koji mogu da se iskoriste za njeno umetanje. Takođe, nephodno je da digitalni format nosioca poruke bude takav da promena redundantnih delove ne izaziva greške (što je slučaj sa npr. exe fajlovima).

2.2. Podela steganografije i steganografskih tehnika

Steganografija može da se podeli na *tehničku* i *lingvističku* steganografiju [1]. Tehnička steganografija odnosi se na ugrađivanje i ekstrakciju poruke iz pisanog teksta ili mikrofilma i u te svrhe koristi naučne metode poput metode mikrotačaka i drugih metoda koje redukuju veličinu tajne poruke. Lingvistička steganografija obuhvata tehnike skrivanja

podatka u datoteci tako da razlike između stego-datoteke i originalne datoteke budu neprimetne. Na taj način se kreiraju *semagrami* i *otvoreni kodovi*.

Semagrami koriste simbole i znakove za sakrivanje informacija i mogu biti vizuelni ili tekstualni. Kod vizuelnih semagrama se koriste svakodnevni fizički oblici za prenos poruka koji su naizgled bezopasni, poput detalja na nekom veb-sajtu. Tekstualni semagrami modifukuju tekst nosioca dodavanjem razmaka, promenom veličine ili boje fonta i sl.

Otvoreni kodovi koriste različite metode za neprimentno sakrivanje poruka. Dele se na *žargonski* i *skriveni* kod. Žargonski kodovi se baziraju na korišćenju predefinisanih fraza koje su poznate samo učesnicima komunikacije (unapred dogovoreni pojmovi i sl.). Kod skrivenih kodova se skrivena poruka može izdvojiti iz stego-datoteke samo u slučaju ako je poznata metoda kojom je skrivena informacija utisnuta u datoteku. U skrivene kodove se ubrajaju *rešetkasti* i *nulti* kodovi. Rešetkasti kodovi rade na principu šablona koji se koriste za skrivanje poruke u nosiocu, dok se kod nultog koda usvaja skup pravila za umetanje poruke u nosiocu podataka (izuzimanje neparnih redova, čitanje svake treće reči i sl.).

Savremena steganografija koristi mogućnosti digitalne tehnologije i 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 čija promena ne utiče značajno na sam fajl, pa je moguće iskoristiti ih za sakrivanje poruke.

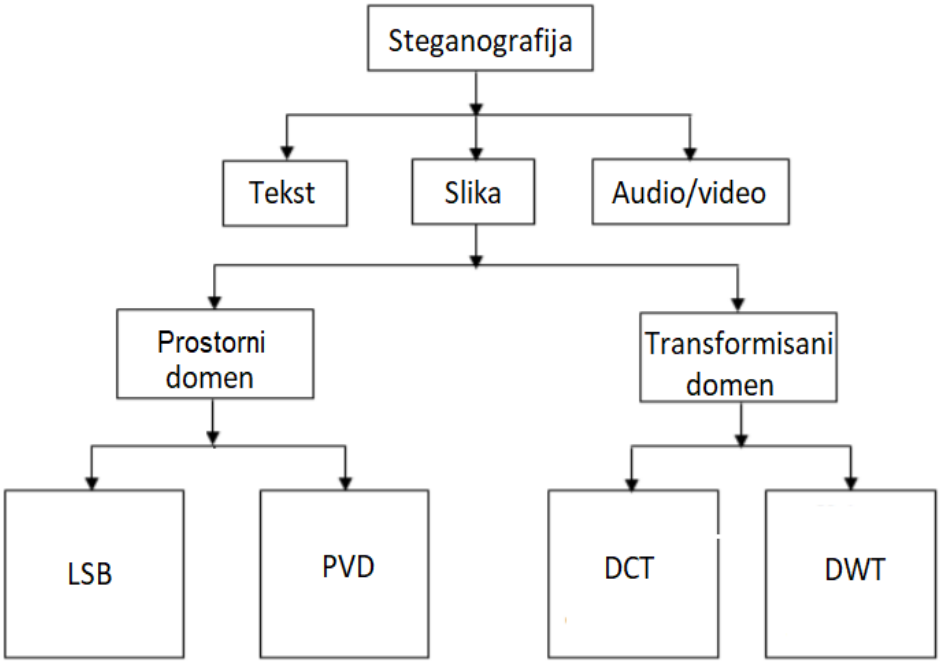
Vremenom su razvijene brojne steganografske tehnike i one mogu da se podele u sledeće grupe:

- *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, a pregled najčešće korišćenih tehnika u digitalnoj steganografiji prikazan je na slici 2.2.



Slika 2.2: Pregled najkorišćenijih tehnika

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

- *Ubacivanje* – 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.

3. Steganografija u slikama

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 [3]. 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.

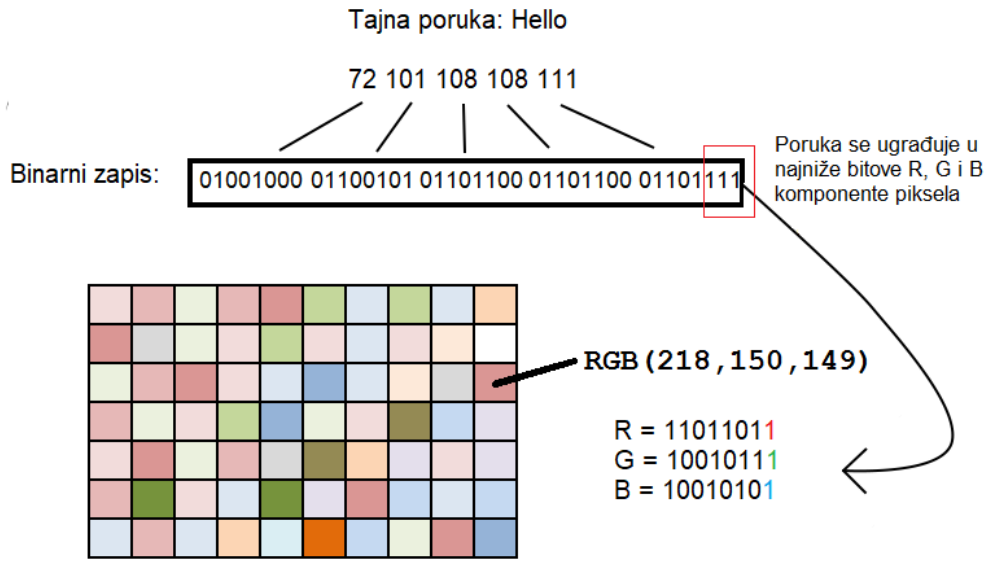
Ugrađivanje poruke u sliku može da se odvija kroz vrednosti piksela (prostorni domen) ili kroz vrednosti koeficijenata (frekventni domen). U fizičkom svetu, svaka veličina koja se meri vremenom u prostoru ili nekom drugom višom dimenzijom može se uzeti kao signal. Signal je matematička funkcija i on prenosi neke informacije i može biti jednodimenzionalni, dvodimenzionalni ili viši dimenzionalni. Jednodimenzionalni signal je signal koji se meri vremenom (npr. zvuk). Dvodimenzionalni signali su oni koji se mere preko nekih drugih fizičkih veličina. Digitalna slika nije ništa drugo do dvodimenzionalni signal. Definisana je matematičkom funkcijom $f(x, y)$ gde su x i y horizontalna i vertikalna koordinata. Vrednost f(x, y) u bilo kojoj tački je vrednost piksela u toj tački slike. Iz tog razloga, nad slikama mogu da se vrše transformacije za prelazak u frekventni domen (DCT, DWT). U nastavku će biti opisane različite tehnike koje su operativne u prostornom ili frekventnom domenu.

3.1. 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 and 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 [4]. 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.

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 3.1.



Slika 3.1: Tehnika zamene najnižeg bita kod 24-bitnih slika

U proseku, menja se otprilike polovina najnižih bitova, tako da se stego-slika ne razlikuje značajno od originalne slike. Ilustracija jednog takvog primera data je na slici 3.2.

Slika 3.2: Originalna i stego-slika nastala LSB metodom

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.

3.2. PVD

PVD ili metoda razlike vrednosti piksela (eng. *Pixel Value Difference*) je tehnika koja se koristi za sakrivanje poruka u slikama u prostornom domenu. Koristi sive slike kao nosioce signala, a stego-slike koje nastaju primenom ove tehnike odlikuje neuočljivost razlika u odnosu na originalnu sliku. Promene u glatkom region slike znatno su primetnije od promena u ivičnom region slike, pa se upravo u ivičnom regionu čuva veći deo tajne poruke [5].

Inicijalno, slika se deli u uzastopne, nepreklapajuće objekte veličine 1x2 rasterskim skeniranjem. Neka su dva uzastopna piksela u i-tom bloku označena sa P_i i P_{i+1}. Za svaki blok, vrednost d_i jednaka je apsolutnoj vrednosti razlike dva piksela u bloku $|P_i - P_{i+1}|$. Mala vrednosti d_i označava da se radi o glatkom regionu, a velika vrednost da je u pitanju ivični region. Pošto piksel može da ima vrednost između 0 i 255, razlika uzima vrednosti od -255 do 255, a njena apsolutna vrednost, tj. d_i, od 0 do 255. Vrednost d_i može da se kvantizuje u nekoliko opsega. Broj bitova koji može da se sakrije u dva uzastopna piksela zavisi od tabele kvantizacionog opesega. Ona se sastoji od n opsega iste dužine, čija je ukupna dužina 255. Ako je gornja granica opsega R_i jednaka $upper_i$, a donja granica $lower_i$, onda je širina opsega jednaka $(upper_i - lower_i + 1)$, tj. broj bitova poruke koji može da se smesti u okviru jednog bloka iznosi $t = \lfloor \log_2(upper_i - lower_i + 1) \rfloor$. Tabela kvantizacionih opsega prikazana je na slici 3.3.

R_1	R_2	R_3	R_4	R_5	R_6
8	8	16	32	64	128

0 7 8 15 16 31 32 63 64 127 128 255

Slika 3.3: Tabela kvantizacionih opsega za PVD[5]

Po izračunavanju parametra *t*, uzima se toliko bitova iz poruke i konvertuju se u decimalnu vrednost *b*, a onda se razlika između piksela ažurira na vrednost $d_i = b + lower_i$. Nova razlika treba da bude u istom opsegu kao stara. Nakon toga, računaju se nove vrednosti piksela po sledećoj formuli:

$$If\ (P_i \geq P_{i+1}\ and\ d_i' > d_i), (P_i', P_{i+1}') = (P_i + \left\lceil \frac{m}{2} \right\rceil, P_{i+1} - \left\lceil \frac{m}{2} \right\rceil)$$

$$If\ (P_i < P_{i+1}\ and\ d_i' > d_i), (P_i', P_{i+1}') = (P_i - \left\lceil \frac{m}{2} \right\rceil, P_{i+1} + \left\lceil \frac{m}{2} \right\rceil)$$

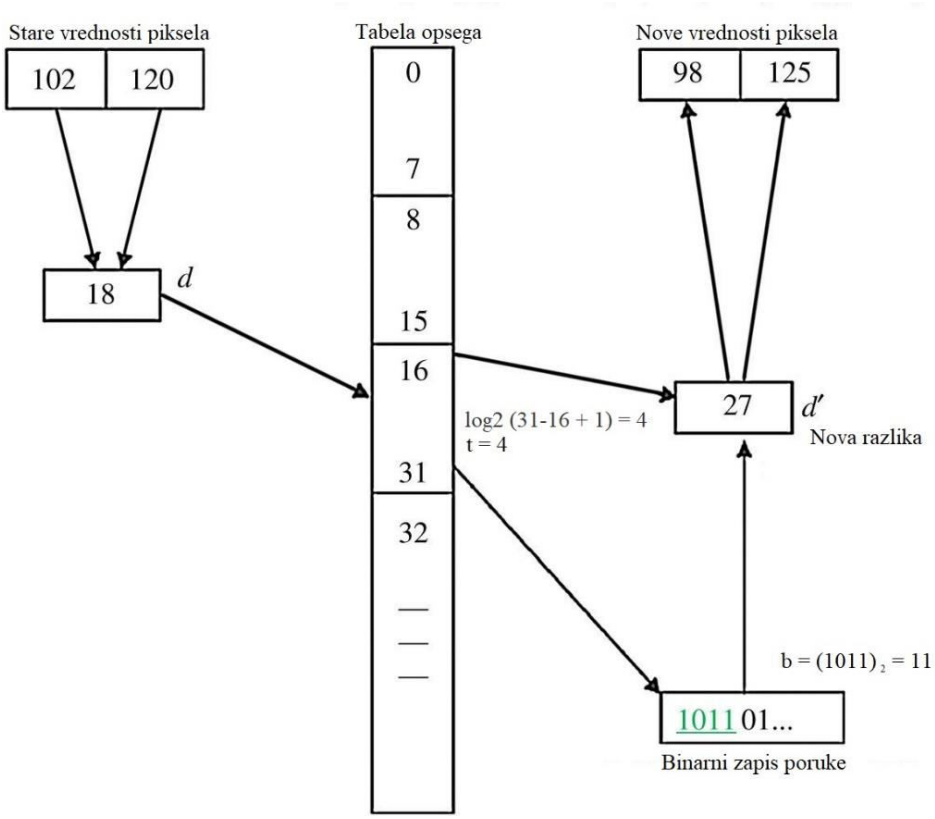
$$If\ (P_i \geq P_{i+1}\ and\ d_i' \leq d_i), (P_i', P_{i+1}') = (P_i - \left\lceil \frac{m}{2} \right\rceil, P_{i+1} + \left\lceil \frac{m}{2} \right\rceil)$$

$$If\ (P_i < P_{i+1}\ and\ d_i' \leq d_i), (P_i', P_{i+1}') = (P_i + \left\lceil \frac{m}{2} \right\rceil, P_{i+1} - \left\lceil \frac{m}{2} \right\rceil),$$

gde je $m = | d' - d |$.

Na prijemnoj strani poruka može da se izdvoji identičnim postupkom. Slika se ponovo deli na uzastopne, nepreklapajuće blokove od po 2 piksela. Za svaki blok se računa razlika piksela (d_i') i preko tabele kvantizaonih opsega određuje se broj bitova poruke koji je sakriven u tom bloku. Sami bitovi poruke dobijaju se konverzijom razlike $d_i - lower_i$ u binarnu vrednost.

Ilustracija rada ove tehnike na primeru prikazana je na slici 3.4. PVD metod može da se iskoristi i za RGB slike, s tim što se svaki RGB „blok“ deli na dva koja se preklapaju (jedan se sastoji od R i G, a drugi od G i B komponente) i onda se opisani postupak vrši nad njima.



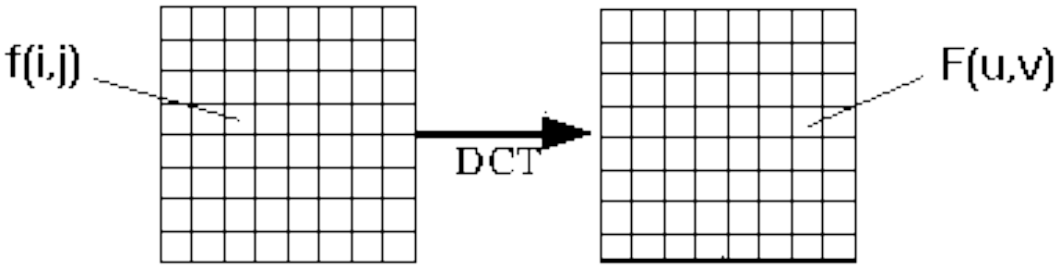
Slika 3.4: Primer rada PVD tehnike

3.3. 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 [6]. DCT je jedan vid Furijeove transformacije i često se naziva „realnim“ delom Furijeove transformacije. Matematički može da se predstavi sledećim formulama (ilustracija na slici 3.5.) :

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

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

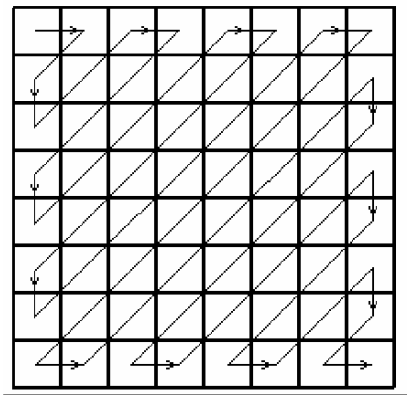


Slika 3.5 : Diskretna kosinusna transformacija

Ulazna slika se deli na blokove veličine 8x8 koji se ne preklapaju, a 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 :

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

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 [2] (slika 3.6.).



Slika 3.6 : Cik-cak obilazak matrice

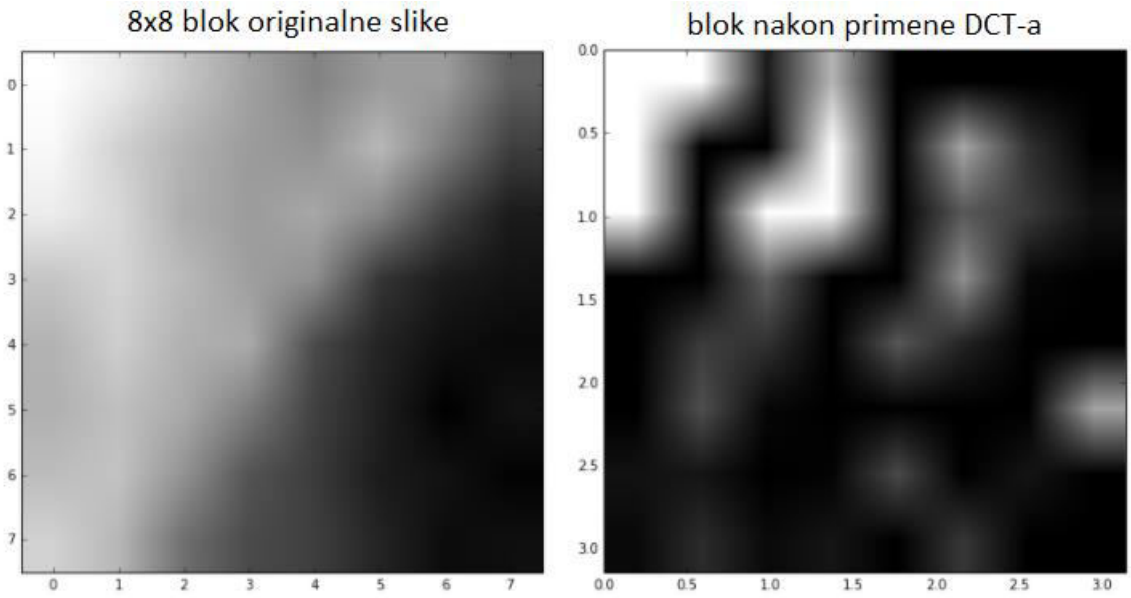
Korišćenjem cik-cak skeniranja koeficijenti se preraspoređuju tako da su na početku oni sa velikom količinom energije, tj. sa malom frekvencijom.

Kada se koeficijenti preurede po frekvenciji, primenje se kvantizacija [8]. 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 [2]. Kvantizaciona matrica prikazana je na slici 3.7:

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 3.7: Kvantizaciona matrica

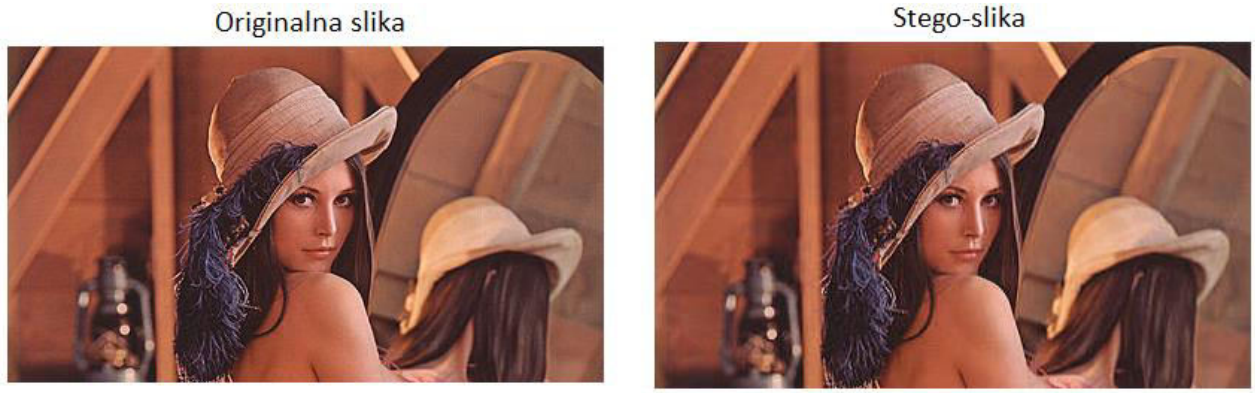
Na slici 3.8 prikazan je izgled bloka slike pre i posle primene diskretne kosinusne transformacije.



Slika 3.8: Primena DCT algoritma na 8x8 blok

Kad 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 [2]. 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.

Kad se poruka ugradi u sliku, slika se transformiše nazad u prostorni domen. Poruka se iz ovako kreirane stego-slike izdvaja inverznim postupkom. Na slici 3.9 prikazana je originalna slika i stego-slika u koju je poruka umetnuta na prethodno opisan način.



Slika 3.9: Originalna i stego-slika nastala primenom DCT algoritma

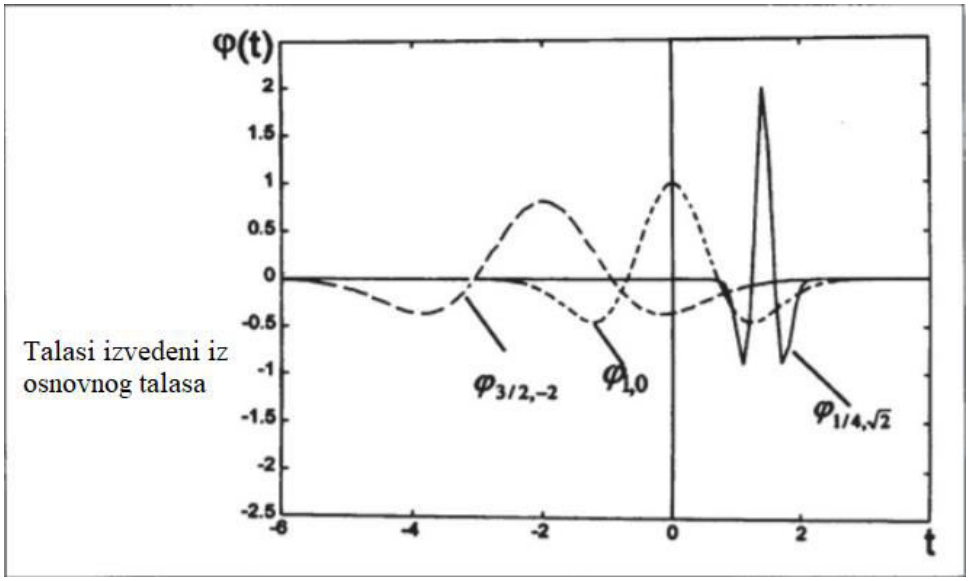
3.4. Diskretna talasna transformacija

DWT (eng. *Discrete Wavelet Transformation*) ili diskretna talasna transformacija konvertuje prostorni u frekventni domen. Koristi se u steganografiji zato što se ovom transformacijom jasno odvajaju visoke od niskih frekvencija [9]. Visoke frekvencije označavaju ivične komponente i one su pogodne za ugrađivanje poruke jer je ljudsko oko manje osetljivo na promene u ivicama.

Talasna transformacija obavlja dekompoziciju signala preko jednostavnih talasnih oblika. U transformaciji se koristi familija baznih funkcija:

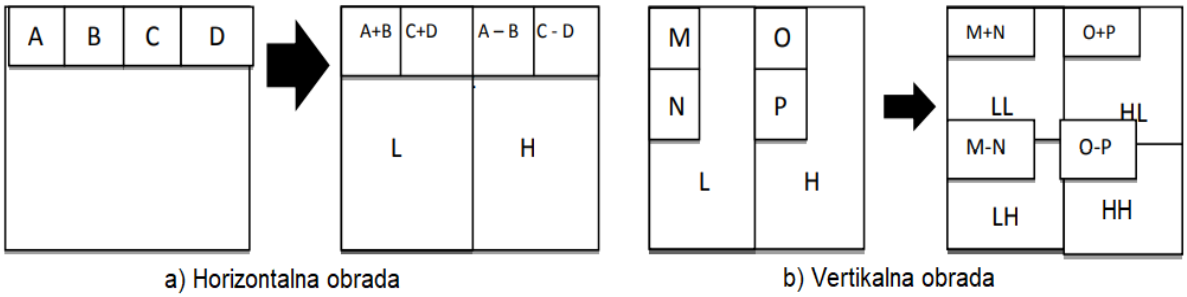
$$\varphi_{a,b}(t) = \frac{1}{\sqrt{a}}\varphi\left(\frac{t-b}{a}\right), a > 0, b \in R,$$

gde je φ(t) označena fiksna funkcija koja se naziva osnovni talas (eng. *mother wavelet*), a a i b su parametri transliranja i proširenja osnovnog talasa (slika 3.10.):



Slika 3.10 : Transliranje i proširenje osnovnog talasa

Najjednostavnija talasna transformacija je Haar talasna transformacija. Dvodimenzionalni Haar-DWT se sastoji od dve operacije, jedne horizontalne i jedne vertikalne [10]. Prvo se pikseli obilaze horizontalno, a onda se vrši sabiranje i oduzimanje susednih piksela. Suma piksela označava nisku frekvenciju i čuva se na levoj poziciji, a njihova razlika visoku i čuva se na desnoj poziciji. Ovaj proces se vrši dok se ne obrade sve vrste u matrici piksela. U drugom koraku, pikseli se obilaze vertikalno, tj. po kolonama, i ponov se vrši sabiranje i oduzimanje susednih piksela, s tim što se sada te vrednosti čuvaju na poziciji iznad i ispod. Postupak se ponavlja dok se ne obrade svi pikseli. Prilikom primene Haar-DWT-a, slika se razlaže na četiri podopsega: LL, LH, HL i HH (slika 3.11.).



Slika 3.11 : 2D Haar DWT [10]

Ovakva dekompozicija može da se vrši više puta uzastopno, pri čemu se LL podopseg iz prethodnog nivoa koristi kao ulaz u sledeći nivo. LL deo sadrži najvažnije detalje o slici. Ugrađivanje u LL deo čini stego-slika otporna na razne napade, ali može dovesti do izobličenja na stego-slici. Uprkos tome, korišćenje DWT tehnike u steganografiji ima svoje prednosti:

1. Dekompozicija signala u različite frekvencijske opsege pomoću DVT-a usko se podudara sa ljudskim vizuelnim sistemom (HVS) karakteristike i to omogućava nezavisno obrađivanje različitih frekvencijskih opsega.

2. Visokofrekventni podopsezi u DVT lociraju karakteristike slike poput ivica i područja teksture, koje su manje osetljivi na karakteristike HVS-a i stoga se mogu koristiti za ugrađivanje.

Kad se izvrši transformacija, bitove poruke mogu po LSB principu da se ugrade u dobijene DWT koeficijente. Nakon toga, vrši se inverzna 2D-Haar transformacija (na isti način). Za ekstrakciju poruke iz ovako dobijene stego-slike potrebno je izvršiti Haar, a onda očitati poruku iz najnižih bitova DWT koeficijenata.

3.5. Tehnike proširenog spektra

Tehnika proširenog spektra (eng. *Spread Spectrum*) radi na principu ubacivanja, a bazira se na proširenju frekvencijskog spektra signala u određenom domenu. u. 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.

Kad 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 [11]. 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 [11]. 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.

3.6. Statističke 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 [3]. 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.

3.7. 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 [3].

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.

3.8. 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.

3.9. Modifikacija elemenata slika

Neke steganografske tehnike ne pokušavaju da sakriju informacije koristeći stvarne elemente slika [3]. 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.

3.10. Tehnika zasnovana na paletama

Kod slika zasnovanim na paletama, broj boja se redukuje na 256, a onda se boja svakog piksela predstavlja jednim brojem. Ove slike se sastoje iz dva dela. Prvi deo je paleta koja dodeljuje N boja kao listu indeksiranih parova (i, c_i) gde je i indeks, a c_i vektor boja, i stvarnim podacima o slici, koji određuju indeks palete za svaki piksel, a ne samu vrednost boje [3]. Veličina datoteke dobijena ovim pristupom je manja kada se na slici koristi samo ograničeni broj vrednosti boja. Dva najpopularnija formata su format grafičke razmene (GIF) i bitmap format (BMP). U nekim slučajevima, sama paleta se može koristiti za sakrivanje tajnih podataka. Redosled boja u paleti obično nije bitan, pa može da se koristi za prenos informacija. U osnovi, skrivena poruka se može ugraditi koristeći razliku između dve boje u paleti (tj. jedan bit tajne poruke za svake dve boje u paleti). Palete boja se koriste da bi se smanjila količina informacija koje se koristi za predstavljanje boja. Budući da se poruka ugrađuje unutar bitova palete, dužina poruke ograničena je brojem boja u paleti.

3.11. Evaluacija tehnika

Kao mera performansi za distorziju slike koja nastaje usled ugrađivanja poruke koristi se odnos signal/šum PSNR (eng. *Peak Signal to Noise Ratio*) i računa se po formuli:

$$PSNR = 10 \log \frac{C_{max}^2}{MSE},$$

gde je MSE srednja kvadratna greška (eng. *Mean Squared Error*) i jednaka je:

$$MSE = \frac{1}{MN} \sum_{x=1}^{M} \sum_{y=1}^{N} (S_{xy} - C_{xy}).$$

Parametar C_{max} je najveća vrednost u slici (npr. 255 kod 8-bitnih slika), C_{xy} su pikseli originalne slike (nosioca), a S_{xy} pikseli stego-slike, dok su M i N dimenzije slike. PSNR se izražava u decibelima i vrednosti ispod 30 dB označavaju da se radi o lošijem kvalitetu stego-slike, dok vrednosti veće od 40 dB impliciraju visok kvalitet stego-slike.

Kao što je već pomenuto u prvom poglavlju, performanse steganografskog sistema određene su preko njegovih osobina (kapacitet, bezbednost, robusnost). LSB tehnika u prostornom domenu je praktičan način prikrivanja informacija, ali je osetljiv na male promene koje nastaju usled obrade slike ili kompresije sa gubicima. Iako se pomoću LSB tehnike mogu sakriti velike količine informacija, tj. LSB ima veliki kapacitet, ovako nastale stego-slike imaju često malu robusnost protiv statističkih napada i manipulacija slikom. Tehnike diskretne kosinusne i diskretne talasne transformacije nisu podložne napadima, pogotovo kad je poruka mala. To je posledica toga što se koeficijenti modifikuju u transformisanom domenu, pa je distorzija najmanja moguća. Kapacitet kod ovih tehnika je manji, ali je robusnost veća. Stego-slike nastale DCT tehnikom su otporne na statističke napade, dok je DWT tehnika robusnija na kompresiju. Tehnike proširenog spektra su uglavnom prilično robusne protiv statističkih napada, budući da skrivena poruka se „širi“ po celoj slici. Međutim, odlučni napadač je sposoban da kompromituje ugrađene podatke pomoću neke digitalne obrade, poput filtera za smanjenje šuma (slični onima koji se koriste u dekodiranju poruke). Ova tehnika je vrlo pogodna za steganografiju zbog prihvatljivih visokih vrednosti kapaciteta i robusnosti. Statističke metode su u većini slučajeva osetljive na odsecanje, rotiranje i skaliranje slike, dok kapacitet i bezbednost zavise od izabranog nosioca, tj. originalne slike. Za razliku od mnogih LSB tehnika, tehnike distorzije ne narušavaju nijedno statističko svojstvo slike. S druge strane, potreba da se stego-slika pošalje preko sigurnog kanala ograničava korisnost ove tehnike. Kao i u bilo kojoj steganografskoj tehnici, slika koja je nosilac ne bi trebalo da se koristi više puta. Ako napadač izvrši odsecanje stego-slike, njeno rotiranje ili skaliranje, to može lako da se detektuje na prijemnoj strani i invertuje ako je poruka kodirana sa informacijama o ispravljanju grešaka. Informacije za ispravljanje grešaka su značajne i ako je stego-slika filtrirana kroz šemu kompresije sa gubicima kao što je JPEG. Korišćenje ove tehnike ograničava kapacitet, jer se ugrađivanje poruke zasniva na dodavanju distorzije. Zbog toga se, pri sakrivanju dugačkih poruka, kao rezultat javlja vidljivo „oštećena“ slika.

4. Implementacija steganografije u slikama pomoću DCT tehnike

Za potrebe ovog rada implementirana je steganografija u slikama korišćenjem diskretne kosinusne transformacije u programskom jeziku *python*. Kao nosioci poruka koriste se 24-bitne RGB slike, dok su poruke u tekstualnom formatu. Slika u koju se ugrađuje poruka prolazi kroz nekoliko etapa:

1. priprema slike
2. izračunavanje DCT-a
3. ugrađivanje poruke
4. inverzni DCT

Pre primene diskretne kosinusne transformacije potrebno je pripremiti sliku. DCT se primenjuje nad blokovima veličine 8x8, pa se u slučaju da dimenzije slike nisu deljive sa 8, menja veličina slike da bi ova podela mogla da se izvrši. Pošto su slike u RGB formatu boja, potrebno je konvertovati ih u *YCbCr*. Komponenta Y se odnosi na osvetljenost, a komponente Cb i Cr se odnose na plavu i crvenu boju. Konverzija se vrši zato što su male promene u osvetljenosti manje vidljive od promena u nekoj od komponenti boja. Ako bi se DCT tehnika primenila nad RGB slikom, u zavisnosti od toga koji kanal je iskorišćen za sakrivanje poruke, stego-slika bi poprimila nijansu korišćenog kanala.

Nakon konverzije se na osnovu svakog kanala generišu 8x8 blokovi i nad njima se vrši DCT. Diskretna kosinusna transformacija predstavlja sliku kao sumu sinusoida različitih magnituda i frekvencija. Vrši se na sledeći način:

1. Za svaki element iz bloka se računa vrednost koeficijenta kao suma proizvoda stare vrednosti i kosinusne funkcije nad vrstom i kolonom u kojoj je element u bloku. U zavisnosti od toga da li se radi o DC ili AC koeficijentu (DC koeficijent je prvi element u prvoj vrsti), suma se množi odgovarajućim faktorom. Ova suma računa se po sledećoj formuli [12]:

$$Coeff_{pq} = c_u c_v \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} Img_{mn} cos \frac{\pi(2m+1)p}{2M} cos \frac{\pi(2n+1)q}{2N},$$

$$0 \le p < M, 0 \le q < N.$$

$$c_u = \begin{cases} {}^{1}/_{\sqrt{M}}, p = 0 \\ \sqrt{{}^{2}/_{M}}, 1 \le p < M \end{cases}, c_v = \begin{cases} {}^{1}/_{\sqrt{N}}, q = 0 \\ \sqrt{{}^{2}/_{N}}, 0 \le q < N \end{cases}.$$

2. Dobijene vrednosti koeficijenata se zaokružuju.

Nakon što se izračunaju koeficijenti, vrši se kvantizacija pomožu kvantizacione matrice, a onda se cik-cak skeniranjem koeficijenti uređuju u opadajući redosled. Ukoliko se radi o Y kanalu (eng. *luminance*), vrši se ugrađivanje poruke u koeficijente. Poruka se pretvara u niz bitova i ugrađuje u AC koeficijente po principu LSB metode. Koeficijenti se obilaze u

inverznom cik-cak smeru, kako bi se vratili u pređašnji redosled. Vrši se dekvantizacija, a onda i inverzna diskretna kosinusna transformacija (obrnutno od DCT-a). Sve ovo, sem promene AC koeficijenata, važi i za ostale komponente (Cb i Cr). Dobijeni blokovi se spajaju po kanalima u sliku, a onda se slika konvertuje nazad u RGB prostor boja.

Izdvajanje poruke se radi slično kao ugrađivanje, s tim što se obrađuje samo Y kanal jer je u njemu sakrivena informacija. On prolazi kroz DCT, dobijeni blokovi se kvantizuju, a onda se čitaju poslednji bitovi i spajaju kako bi se dobila poruka.

Testiranjem programa za različite dužine poruka i različite veličine slike dobijena prosečna vrednost za MSE je 103, što bi, da su korišćene 8-bitne slike predstavljalo veliku grešku, ali za 24-bitne nije značajno. Dobijena prosečna vrednost za PSNR je 35, što implicira da slike nisu mnogo izgubile na kvalitetu uzimajući u obzir da se pomoću DCT-a vrši kompresija. Sledeće slike ilustruju razlike između originalnih i dobijenih stego-slika (slike 4.1. i 4.2.).

Slika 4.1: Primer dobijene stego-slike

Slika 4.2: Primer dobijene stego-slike

5. Zaključak

Razvoj računarskih mreža, a kasnije i informacionih tehnologija zanačajno je unapredio i ubrzao komunikaciju. Istovremeno, informacije koje se prenose kroz mrežu postale su mnogo osetljivije na napade, pa je potrebno zaštiti ti ih od neovlašćenog pristupa. U tu svrhu se, osim kriptografije, koristi i steganografija. Steganografija je nauka koja se bavi sakrivanjem informacija u drugim podacima. Neki njen primitivni vid koristio se još u doba Antičke Grčke, a značajnu primenu imala je i tokom ratova. Naučni razvoj steganografije uznapredovao je krajem 20. veka. Vremenom su razvijene različite grane steganografije, kao i tehnike za njenu primenu.

Mrežom se prenose digitalni podaci, pa se digitalna steganografija upravo bazira na sakrivanju podataka u digitalne formate. Jedan od najčešćih tipova datoteka koje se koriste jesu slike. Najbolji kandidati za nosioce poruka su 24-bitne slike zbog svog kvaliteta jer se u njima deformacija najmanje vidi, ali se zbog njihove velike rezolucije često koriste i 8-bitne slike. 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.

Implementiran je stego-sistem za sakrivanje tekstualne poruke u slikama korišćenjem diskretne kosinusne transformacije. RGB slike se konvertuju u YCbCr model, jer su promene u Y kanalu (osvetljenost) najmanje primetne ljudskom oku. Slike se dele u blokove nad kojima se primenjuje DCT, vrši se kvantizacija, a poruka se ugrađuje u koeficijente Y kanala po LSB principu. Stego-slike nastale ovom metodom u poređenju sa originalnom slikom daju MSE od 100, što je poprilično dobra vrednost za 24-bitne slike i PSNR od 35, što znači da je slika zadovoljavajućeg kvaliteta.

6. Literatura

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

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

[3] 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

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

[5] A. Sahu, M. Sahu, *DIGITAL IMAGE STEGANOGRAPHY TECHNIQUES IN SPATIAL DOMAIN*, https://www.researchgate.net/publication/312826532_Digital_image_steganography_techniques_in_spatial_domain_A_study

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

[7] O. Foaud, H. Hamed, *Hiding data in images using DCT steganography techinuque with compression algorithms*, (2019), https://www.researchgate.net/publication/330565811_Hiding_data_in_images_using_DCT_steganography_techniques_with_compression_algorithms

[8] H. Sheisi, J. Mesgerian, M. Rahmani, *Steganography: Dct Coefficient Replacement Method and Compare With JSteg Algorithm*, (2012), http://www.ijcee.org/papers/533-P0025.pdf

[9] S. Zagade, *S. Boshale, Secret Data Hiding in Images by using DWT Technique*, (2014), https://www.ijeat.org/wp-content/uploads/papers/v3i5/E3215063514.pdf

[10] M. Tushara, K. Navas, *Image Steganography Using Discrete Wavelet Transform – A Review*, (2016), https://ijireeice.com/wp-content/uploads/2016/07/nCORETech-38.pdf

[11] C. Boncelet, *Spread Spectrum Image Steganography*, (1999), University of Delaware

[12] *Discrete Cosine* Transform, (januar 2021), https://www.mathworks.com/help/images/discrete-cosine-transform.html