U N I V E R Z I T E T U N I Š U

E L E K T R O N S K I F A K U L T E T

STEGANOGRAFIJA

IMPLEMENTACIJA DWT ALGORITMA ZA SKRIVANJE ZVUČNIH SNIMAKA U RASTERSKOJ SLICI

DIGITALNA FORENZIKA

Mentor:
Prof. dr Bratislav Predić

Student:
Milan Grujev 1137

SADRŽAJ

1. UVOD

Komunikacija je stara koliko i čovečanstvo. Istorija komunikacije datira još iz najranijih oblika života. Najraniji oblici komunikacije zasnivali su se na dimnim znakovima, crtežima u pećinama, itd. Tokom evolucije, sa razvojem čoveka, razvijali su se novi oblici komuniciranja. Pa se tako kroz istoriju javljaju usmena komunikacija, nakon toga nastaju prvi simboli i razvijaju se primitivni jezici. Sledeća etapa u razvoju komunikacije jeste pojava pisma. Kako je pismo postalo sredstvo komunikacije, pojavila se potreba da se neka pisma sačuvaju od tuđih pogleda. Pa su ljudi krenuli na razne načine da skrivaju ono što žele da prenesu porukom. Tako je kriptografija ugledala svetlost dana. Najpoznatiji primeri enkripcije podataka jeste komunikacija u vojne svrhe. Često su se poruke pre slanja šifrovale tako što su sva ili pojedina slova u poruci bila pomerena za nekoliko mesta u abecedi. Takvu poruku su mogli da dešifruju samo oni koji su poznavali pravila šifrovanja. Još jedan primer korišćenja šifrovanih poruka jeste *Enigma*, mašina koju su nacisti koristili za šifrovanje poruka tokom Drugog svetskog rata. Detaljnije o ovoj mašini i čoveku koji je uspeo da je odgonetne, Alanu Tjuringu, možete pogledati u filmu ”*The Imitation Game*“. Sa daljim napredovanjem tehnologije, nastao je internet i komunikacija kakvu danas poznajemo i koristimo. Osim prvobitnih pisama, tj. poruka, komunicira se slikama, zvučnim i video snimcima. Upotreba ovih medija za komuniciranje dovela je do naglog razvoja steganografije.

Steganografija je naučna disciplina koja se bavi prikrivenom razmenom informacija. Reč steganografija izvedena je od grčkih reči *steganos* i *graphein*, što u prevodu znači „skriveno pisanje“[8]. Osnovni princip steganografije počiva na prikrivanju samog postojanja informacije koja se prenosi unutar nekog naizgled bezazlenog medija ili skupa podataka. Činjenica da poruke ne privlače pažnju na sebe tj. da nisu na prvi pogled vidljive predstavlja osnovnu razliku i prednost u odnosu na kriptografiju. Ova prednost nam omogućava da steganografijom izbegnemo napad *man in the middle*, obzirom da napadač nije svestan postojanja komunikacije u nekom komunikacionom kanalu.

Najraniji primeri steganografije datiraju još iz perioda pre nove ere i njih je Herodot naveo u svom delu „Herodotova istorija“. Spomenuo je dva primera steganografije. Jedan primer je slanje poruke zapisivanjem na drveni kalup voštane ploče za pisanje, pre izlivanja voska, a drugi primer je priča o vernom robu iz grčko-persijskih ratova čiju su glavu obrijali i nakon toga ispisali poruku. Kada je robu kosa opet narasla, on je poruku neprimećeno preneo do druge strane. Drevni Kinezi su zapisivali poruke na tankim komadima svile, zatim su taj komad stavljali u voštanu kuglicu koji bi glasnik progutao[8]. Monah *Johannes Trithemius* je oko 1500. godine

napisao knjigu *Steganographia* u kojoj je opisao kako sakriti poruku unutar bezazlenog teksta. Tokom Drugog svetskog rata korišćena je nevidljiva tinta za prenos tajne poruke. Dobijanje tajne poruke zasnivalo se na nekom svojstvu tinte, kao što je vidljivost prilikom zagrevanja ili kontakta sa određenom hemijskom supstancom. Osim tinte, u ovom ratu korišćene su i mikrofotorafije.

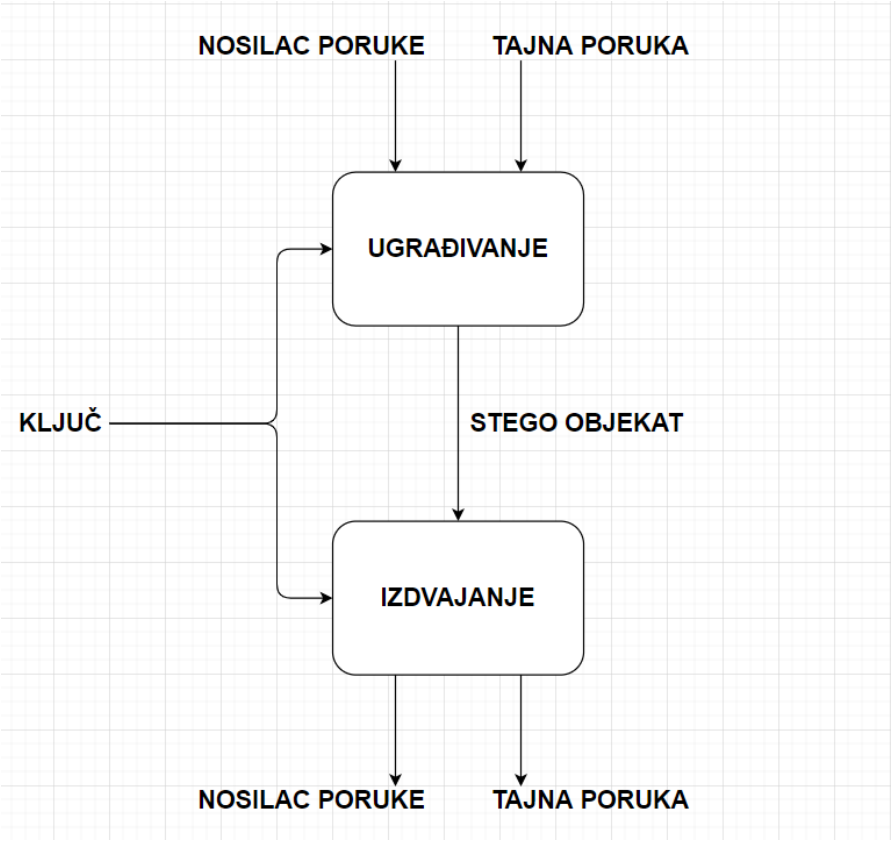
Slika 1.1 – Ilustracija steganografije

Moderna steganografija razvija se 1985. godine nastankom personalnih računara i sa primenom računara na do tada poznate steganografske tehnike. Početni razvoj je bio spor, ali vremenom razvile su se mnoge aplikacije za steganografiju. Najčešća upotreba steganografije danas je zaštita autorskih prava umetanjem žiga u medij.

U nastavku ovog rada videćemo šta je steganografija i koji sve tipovi steganografije postoje. Najveći fokus je na tehnikama digitalne steganografije, odnosno metodama koje koriste računare. U radu je opisana implementacija projekta koji demonstrira primenu DWT algoritma kod steganografije.

2. STEGANOGRAFIJA

Osnovni princip steganografije je tajna razmena informacija korišćenjem nekog medija tako da poruka ne privlači pažnju na sebe, odnosno nije vidljivo prisustvo poruke na prvi pogled. Steganografski proces prikazan je na sledećoj slici.



Slika 2.1 – prikaz steganografskog procesa

Neka osoba V želi da pošalje tajnu poruku osobi M. Pošiljalac, u ovom slučaju osoba V, postupkom skrivanja poruke umeće tajnu poruku (*secret message*) u objekat nosilac (*cover media*). Prilikom procesa ugrađivanja (*embedding*) poruke u medij moguće je koristiti dodatno šifrovanje upotrebom ključa (*key*). Ovim postupkom dobijamo stego objekat (*stego media*) koji se šalje kroz komunikacioni kanal. Na ovaj način obezbedili smo da tajna poruka nije vidljiva na prvi pogled, tj. samo njeno prisustvo nije lako uočljivo. Primalac, u ovom slučaju osoba M, mora da zna koji algoritam je iskorišćen prilikom ugrađivanja poruke da bi mogao izvršiti izdvajanje (*extraction*) poruke na prijemnoj strani. Ukoliko je u postupku ugrađivanja upotrebljen ključ, neophodno je i njegovo poznavanje[4].

Sam postupak skrivanja, odnosno izdvajanja poruke, može biti javni ili tajni. Obično se kod javnih postupaka koriste dodatni ključevi koji određuju tačan redosled poruke. Ti ključevi se razmenjuju sigurnim kanalom i time se izbegava da napadač jednostavno dođe do tajne poruke. Još jedna dodatna modifikacija koja postiže dodatnu sigurnost u očuvanju tajnosti poruke jeste upotreba nekog kriptografskog algoritma na samu poruku[4].

Pošto se prenos stego objekta vrši kanalom koji nije siguran javljaju se potencijalni napadači. Osnovni cilj napadača je detekcija tajne poruke, nije neophodno pročitati je. Ukoliko dođe do detekcija da postoji tajna poruka, napadač će pokušati da je otkrije, a ukoliko ne uspe nastojaće da naruši stego objekat tako da ona bude izgubljena. Pod pretpostavkom da potencijalni napadač ima pristup komunikacionim kanalu i mogućnost modifikacije stego objekta, razlikujemo tri vrste napadača:

- Pasivni napadač (napadač koji samo prisluškuje komunikacioni kanal)
- Aktivni napadač (napadač koji, pored prisluškivanja kanala, modifikuje stego objekat)
- Zlonamerni napadač (napadač koji šalje krivotvorene poruke)

Koliko je neki steganografski sistem siguran zavisi od toga koliko se dobro odupire pasivnim, aktivnim i zlonamernim napadima. Steganografski sistem je robustan ukoliko se tajna poruka može izmeniti tek „većim“ izmenama stego objekta. Siguran steganografski sistem ispunjava četiri uslova:

- Algoritam skrivanja je javan, ali koristi se tajni ključ
- Samo onaj ko poseduje tajni ključ može detektovati, izdvojiti i dokazati postojanost tajne poruke i niko drugi ne može otkriti nikakav trag o postojanju tajne poruke
- Ukoliko napadač otkrije sadržaj jedne poruke, mala je verovatnoća da će otkriti sadržaj preostalih poruka
- Detekcija tajne poruke mora biti veoma zahtevna operacija

Iako steganografski sistem koji ima javni algoritam skrivanja, a ne koristi tajni ključ, nije siguran, ponekad je i on zadovoljavajuć. To se odnosi na sisteme koji raspolažu ogromnom količinom informacija pa se ne mogu analizirati svi objekti koji su potencijalni nosioci tajnih poruka. U tom slučaju, nepostojanje ključa je olakšavajuća okolnost jer nije potreban siguran kanal za prenos ključa i postupak skrivanja/izdvajanja tajne poruke je jednostavniji[4].

Važno je napraviti razliku između steganografije i kriptografije. Kod kriptografije se tajnost postiže modifikacijom poruke, dok se kod steganografije tajnost poruke postiže njenim skrivanjem. Digitalni vodeni žig je dosta sličan steganografiji samo što je cilj vodenog žiga njegova vidljivost zbog obeležavanje digitalnog signala.

3. TIPOVI STEGANOGRAFIJE

Postoje tri osnovna tipa steganografije:

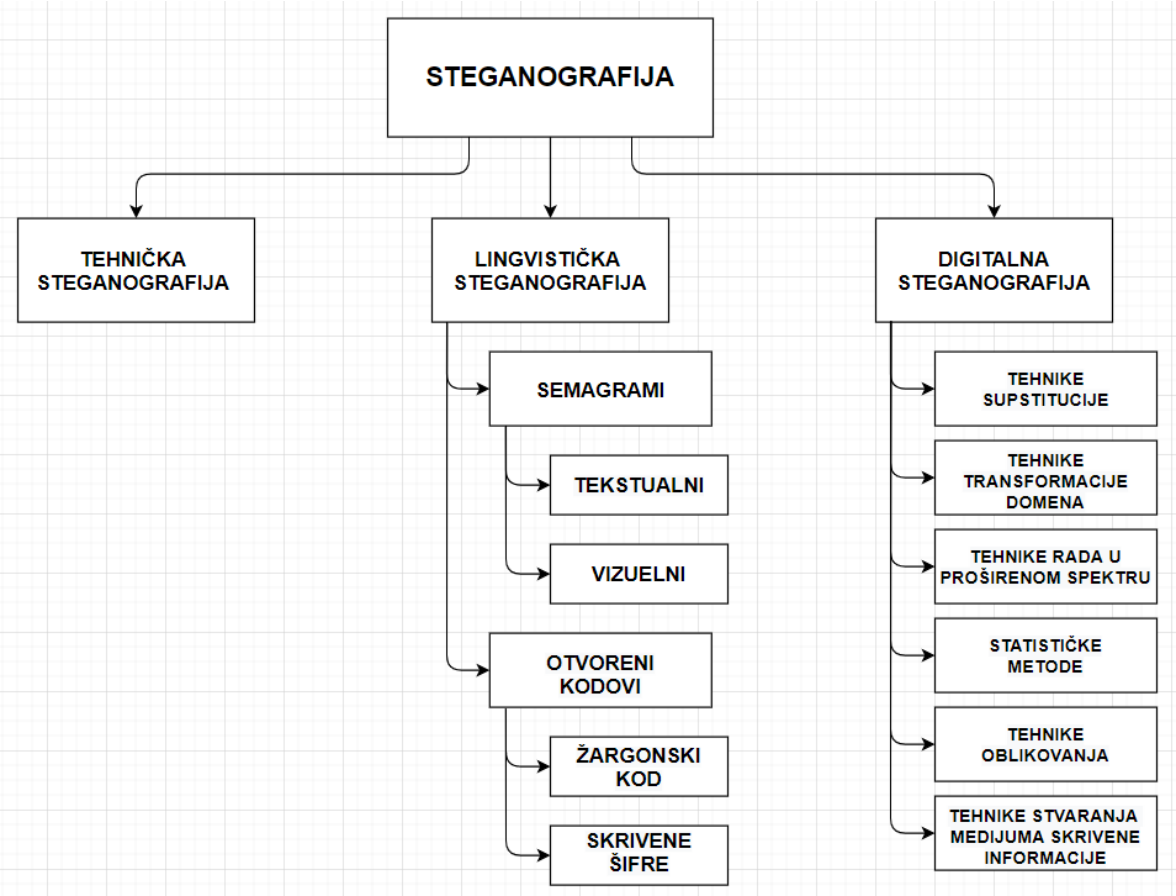
- Tehnička steganografija
- Lingvistička steganografija
- Digitalna steganografija

Tehnička steganografija obuhvata metode koje tajnu poruku skrivaju korišćenjem nekih hemikalija, uređaja ili alata. U ovu grupu steganografskih tehnika spadaju:

- Nevidljiva tinta – posebna bezbojna tinta koja ostaje nevidljiva dok ne dođe u kontakt sa određenom hemikalijom, toplotom ili posebnim izvorom svetlosti
- Korišćenje skrivenih mesta – npr. duplo dno, peta cipele, tetovaža ispod kose...
- Mikrofotografije – fotografije malih veličina, često ne veće od pola milimetra

Lingvistička steganografija obuhvata metode koje tajnu poruku skrivaju u bezazlen skup informacija. Dve osnovne metode lingvističke steganografije su korišćenje semagrama i otvorenih kodova. Semagrami skrivaju tajnu poruku upotrebom različitih simbola i znakova, a dele se na:

- Tekstualne semagrame – tajna poruka se skriva određenim promenama teksta (npr. dodavanje redundantnih praznih mesta, promena veličine slova, promena fonta...)
- Vizuelne semagrame – tajna poruka se skriva korišćenjem bezazlenih fizičkih objekata, odnosno njihovim specifičnim rasporedom (npr. raspored elemenata na web stranici ili predmeta na stolu...)



Slika 3.1 – Podela steganografije

Drugu grupu tehnika lingvističke steganografije čine otvoreni kodovi. Otvoreni kodovi za skrivanje tajne poruke koriste uobičajene poruke i tekstove iz svakodnevne komunikacije. Sadržaj tajne poruke sakriven je na određenim pozicijama u tekstu[4].

Otvoreni kodovi se dalje dele na:

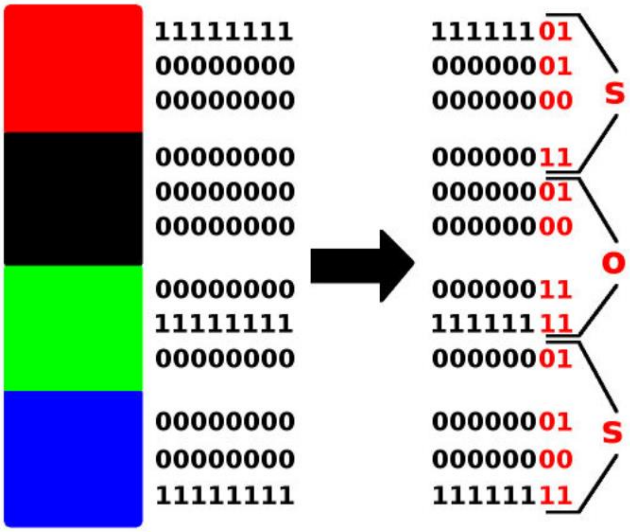
- Žargonske kodove – koristi se jezik koji je razumljiv samo određenoj grupi ljudi
- Skrivene šifre – tajnu poruku moguće je izdvojiti iz stego objekta samo ako se poznaje metoda kojom je poruka umetnuta
    - Rešetkaste šifre – preko teksta nosioca se postavi šablon sa otvorima, slova koja se pojave na otvorima predstavljaju sadržaj tajne poruke
    - Nulte šifre – skrivena poruka iz teksta se izdvaja primenom unapred dogovorenih pravila (npr. čitanje teksta dijagonalno, čitanje svakog n-tog slova...)

Digitalna steganografija zasniva se na korišćenju digitalnog medija (slika, audio snimak ili video zapis) kao nosiocu signala. Tajna poruka se raznim tehnikama umeće u digitalni medij i na taj način prenosi kroz komunikacioni kanal. Tehnike digitalne steganografije se mogu podeliti u sledećih šest kategorija:

- Tehnike supstitucije
- Tehnike transformacije domena
- Tehnike rada u proširenom spektru
- Statističke metode
- Tehnike oblikovanja
- Tehnike stvaranja medijuma skrivene informacije

3.1 TEHNIKE SUPSTITUCIJE

Kod ovih tehnika digitalne steganografije, suvišni delovi nosioca poruke se koriste za ubacivanje tajne informacije. Najpoznatija tehnika ove kategorije jeste LSB (engl. *Least Significant Bit*). Kod LSB tehnike bitovi najmanje težine nosioca poruke postaju nosioci skrivene poruke. Bitovi poruke se ugrađuju obično u bit najmanje težine i na taj način se postižu minimalne izmene medijuma koji služi za prenos poruke[6].



Slika 3.2 – LSB algoritam

3.2 TEHNIKE TRANSFORMACIJE DOMENA

Steganografske tehnike transformacije domena koriste matematičke funkcije za skrivanje podataka unutar medijuma (najčešće fotografije). Modifikacijom se prelazi u frekventni domen i onda se vrši ugrađivanje poruke. Najčešće korišćene transformacije jesu diskretna kosinusna transformacije (engl. *Discrete Cosine Transformation – DCT*), diskretna Furijeova transformacija (engl. *Discrete Fourier Transformation – DFT*) i diskretna talasna transformacija (engl. *Discrete Wavelet Transformation – DWT*).

Diskretna kosinusna transformacija (DCT) dekomponuje ulazni signal na signal posebne sekvence odmeraka i time transformiše energiju signala na pogodniji način za kodovanje manjim brojem bita po odmerku[7]. Diskretna kosinusna transformacija generiše konačan broj izlaznih sekvenci odmeraka signala kao sumu kosinusnih funkcija sa različitim frekvencijama. Ova transformacija je ključni deo mnogih segmenata nauke i inženjeringa, od audio kompresije sa gubicima (MP3 format) i slike (JPEG format), do spektralnih metoda za numeričko rešavanje parcijalnih diferencijalnih jednačina. Korišćenje kosinusne umesto sinusne funkcije u transformaciji je jako bitno pri kompresiji signala zato što je potrebno manje kosinusnih funkcija kako bi se aproksimirao signal. Dvodimenzionalna diskretna kosinusna transformacija najčešće korišćena za kompresiju slike podeljene na blokove, data je sledećom jednačinom:

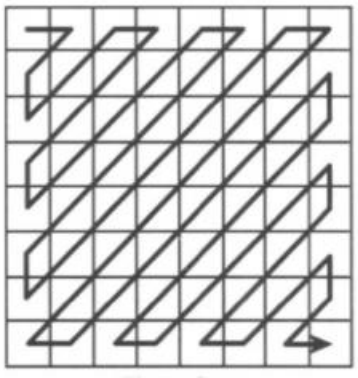
$$F(u,v) = 2 \cdot \frac{C(u) \cdot C(v)}{\sqrt{M \cdot N}} \left[\sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y) \cdot \cos\left(\frac{(2x+1)u\pi}{2M}\right) \cdot \cos\left(\frac{(2x+1)v\pi}{2N}\right) \right]$$

gde je M broj redova bloka, N broj kolona bloka, *f(x,y)* je diskretna vrednost pojedinačne tačke u bloku sa koordinatama *(x,y)*, a *C(u)* i *C(v)* su definisani izrazom:

$$C(u) = C(v) = \begin{cases} \frac{1}{\sqrt{2}}, za\ u, v = 0 \\ 1\ \ , za\ u, v\ \neq 0 \end{cases}$$

Prvi korak u DCT tehnici za steganografiju jeste podela slike u matrice dimenzija 8x8. Ukoliko dimenzije slike nisu deljive sa 8, vrši se ili smanjene dimenzija ili repliciranje nekih redova ili kolona u zavisnosti od dimenzija slike. Nakon generisanja ovih matrica, nad svakoj se primenjuje DCT algoritam. Tako se dobijaju po 64 koeficijenta. Koeficijenti u matrici sa

koordinatama (0,0) predstavljaju DC komponente, a ostali su AC komponente. DC komponente nose najviše informacija o samom bloku jer predstavljaju srednju vrednost elemenata bloka. AC komponente su one koje čuvaju informacije o promenama vrednosti elemenata bloka. Sada je potrebno urediti koeficijente tako što se oni obilaze u *zig – zag* obilasku.



Slika 3.3 – *Zig – zag* obilazak

Skeniranje po ovom obilasku i uređivanje elemenata u rastućem redosledu omogućava nam da nastavimo dalje sa algoritmom izdvajajući elemente sa manjom frekvencijom na početku. Nakon ovoga vrši se kvantizacija koeficijenata upotrebom kvantizacionih matrica. Na samom kraju koristi se LSB algoritam kako bi se bitovi tajne poruke ugradili u DCT koeficijente. Da bi se dobio stego objekat neophodno je sliku vratiti iz frekventnog u prostorni domen.

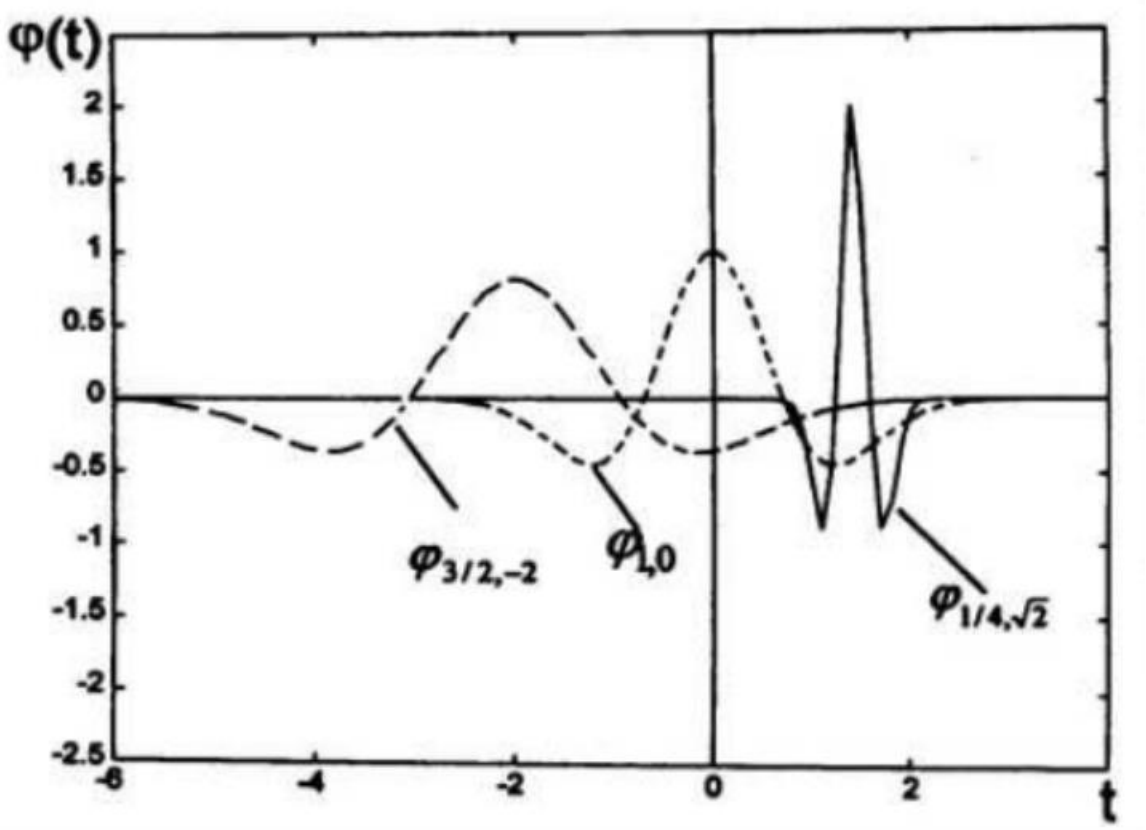
Diskretna talasna transformacija (DWT) predstavlja još jednu metodu koja se koristi za transformaciju signala u frekventni domen. Diskretna talasna transformacija se koristi u steganografiji zato što odlično razdvaja visokofrekventne i niskofrekventne delove. Govoreći o slikama, visokofrekventni delovi predstavljaju infomacije o ivicama, odnosno velikim promenama vrednosti piksela, dok su niskofrekventni delovi oni koji izdvajaju delove bez naglih promena. Upravo ova karakteristika DWT-a se koristi u steganografiji, jer je ljudsko oko manje osetljivo na promenama ivica[2].

Talasna transformacija obavlja dekompoziciju posmatranog signala preko jednostavnih talasnih oblika koji ne moraju biti isključivo prostoperiodični signali kao u slučaju Furijeove transformacije. Dakle, umesto da se dekompozicija posmatranog signala obavlja pomoću prostoperiodičnih signala, ona se vrši pomoću signala $\varphi(t)$ i njegovih transliranih i proširenih oblika. Drugim rečima, signal $\varphi(t)$ u talasnoj transformaciji ima ulogu prostoperiodičnog signala u Furijeovoj transformaciji[5].

U talasnoj transformaciji koristi se 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 sa φ(t) označena fiksna funkcija koja se naziva matrični ili osnovni talasić (engl. *mother wavelet*), a *a* i *b* su parametri transliranja i proširenja osnovnog talasića.

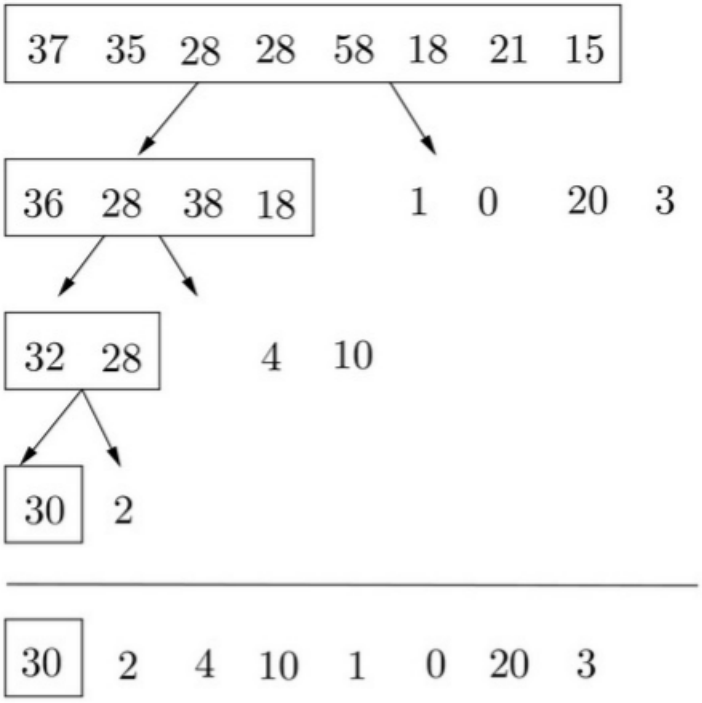


Slika 3.4 – Primeri osnovnog i izvedenih talasića

Najpoznatija transformacija iz ove porodice transformacija jeste Haarova transformacija. Neka je signal *f* zadat vrednostima *f* = { 37, 35, 28, 28, 58, 18, 21, 15 }. Kompresija signala primenom Haarove diskretne transformacije sa 3 nivoa prikazana je na slici 3.5. Radi jednostavnosti računa za filter koeficijente uzeti su $h_0 = ½$, $h_1 = ½$, i $g_0 = ½$, $g_1 = -½$. Cilj ove dekompozicije je formiranje znatno manjih koeficijenata, pomoću kojih rekonstruišemo polazni signal. Zbog pojašnjena ove transformacije, uzeto je da dižina ulaznog signala bude 2^N. U prvom koraku, vršeći transformaciju, dobijamo dva niza čije su dužine jednake polovini dužine polaznog niza[3]. Dakle, u svakom koraku polovimo dužinu niza iz prethodnog koraka, pa je ukupan broj

koeficijenata na kraju jednak dužini originalnog signala. Uokvireni deo na slici 3.5 predstavlja koeficijente skaliranja, odnosno prosečne vrednosti, a ostatak su talasni koeficijenti.

Konkretno, za ovaj primer, u prvom koraku dobijamo nizove {36,28,38,18} i {1,0,20,3} koji predstavljaju f^1 i d^1, redom. Zatim, u drugom koraku dobijamo nizove {32,28} i {4,10} koji predstavljaju f^2 i d^2. Konačno, u trećem koraku dobijamo aproksimaciju f^3 kojoj odgovara vrednost {30} i d^3 kojem odgovara vrednost {2}.

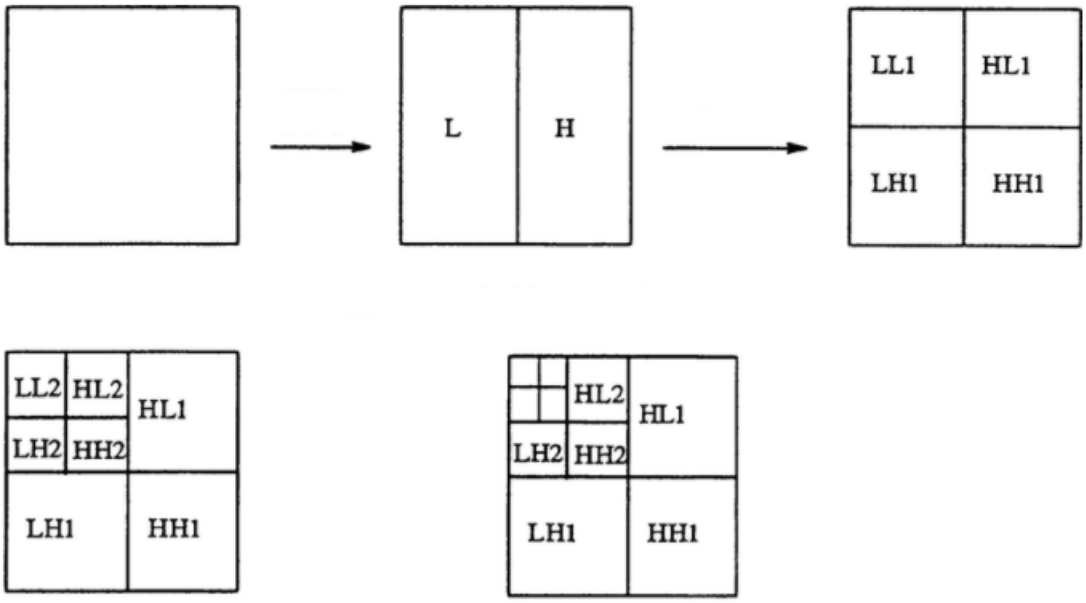


Slika 3.5 – Kompresija signala primenom Haarove transformacije

Ove transformacije veoma su zastupljene u računarstu. Konkretno, u ditigalnoj steganografiji ova transfromacija se koristi za komprimovanje nosioca poruke. Najpopularniji nosioci poruke u steganografiji jesu slike. Slike mogu biti slike u nijansama sive ili slike u boji. Slike u boji imaju mnogo više prostora za skrivanje informacija nego slike u nijansama sive boje. Slike u boji se mogu predstaviti u različitim formatima kao što su RGB (crvena – zelena – plava), HSV (nijansa – zasićenost – vrednost), CMYK, YcbCr, itd. Steganografija slike u boji može da radi u bilo kojem formatu boja. Kada se talasna transformacija primeni na sliku u boji, dobijaju se koeficijenti transformacije za svaki kanal u odgovarajućem predstavljanju.

Kada se na sliku primeni dvodimenzionalna diskretna talasna transformacija, ona se razlaže na četiri podopsega:

- LL – predstavlja aproksimaciju ulazne slike i sadrži najviše detalja sa ulazne slike i predstavlja niskofrekventni opseg
- LH – predstavlja visokofrekventni opseg koji sadrži horizontalne detalje slike
- HL – predstavlja visokofrekventni opseg koji sardži vertikalne detalje slike
- HH – predstavlja visokofrekventni opseg koji sadrži dijagonalne detalje slike



Slika 3.6 – Prikaz podopsega prilikom primene talasne transformacije nad slikom

Talasnu transformaciju je moguće primeniti nekoliko puta uzastopno, pri čemu se LL opseg iz prethodnog nivoa koristi kao ulazna slika za sledeći nivo. Da bi se tajna poruka sakrila unutar slike, nakon dekompozicije na opsege, vrši se ugrađivanje tajne poruke upotrebom LSB algoritma. Postoje varijante za odabir opsega u koji se vrši ugrađivanje, pa ugrađivanjem u LL opseg stego objekat činimo otpornijim na napade, ali možemo izazvati izobličenja u slici, dok kod ugrađivanja u ostale opsege imamo manje sigurni stego objekat, ali sa neprimetnim izobličenjima.

3.3 TEHNIKE RADA U PROŠIRENOM SPEKTRU

Kod tehnika koje se baziraju na proširenom spektru, tajna poruka se skriva unutar nosioca poruke. Tajna poruka se prvo modifikuje signalom šuma, pa onda se dodaje objekta nosioca poruke. Ova modifikacija dodatno štiti poruku tako da je ekstrakcija poruke moguća isključivo poznavanjem tajnog ključa pomoću koja je iz naizgled slučajnog signala šuma moguće dobiti skrivenu poruku. Postoje dve metode proširenog spektra koje se koriste u digitalnoj steganografiji:

- Metoda sa direktrom sekvencom (engl. *Direct Sequence Spread Spectrum – DSSS)*
- Metoda frekventnog skakanja (engl. *Frequency Hopping Spread Spectrum – FHSS*)

Navedene tehnike se karakteristično koriste za prenos podataka u bežičnim sistemima, povećavajući otpornost na smetnje i omogućavajući nesmetani rad više učesnika[1].

3.4 STATISTIČKE METODE

Statističke metode predstavljaju tehnike digitalne steganografije koje se fokusiraju na samom nosiocu poruke. Kod ovih metoda ne koristi se klasično ubacivanje tajne poruke u objekat koji nosi poruku. Nosilac poruke se podeli na onoliko blokova kolika je veličina poruke. Svaki blok tada služi za skrivanje jednog bita tajne poruke. Ukoliko je bit poruke jednak jedinici, blok se modifikuje tako da primalac može statističkim testiranjem hipoteze otkriti da li je taj blok promenjen. Ukoliko je bit poruke jednak nuli, taj blok se ne menja[1].

3.5 TEHNIKE OBLIKOVANJA

Tehnike oblikovanja su još jedna grupa tehnika koja ne primenjuje skrivanje poruke direktno u objekat koji nosi poruku. Ova grupa tehnika vrši modifikacije tj. oblikovanje (menjanje oblika objekta koji nosi poruku) kako bi se prenela tajna poruka. Pošto se „skrivanje“ poruke vrši na ovaj način, prijemnoj strani je neophodna originalna verzija objekta koji nosi poruku da bi mogla da otkrije tajnu poruku. Objekat u koji se krije poruka na neki način predstavlja ključ za otkrivanje sadržaja tajne poruke.

3.6 TEHNIKE STVARANJA MEDIJUMA SKRIVENE INFORMACIJE

Tehnike stvaranje medijuma skrivene informacije su grupa tehnika koja se fokurisa na tajnu poruku. Kod ove grupe tehnika digitalne steganografije ne koristi se slučajni nosilac poruke, već se on generiše na osnovu tajne poruke. Nema klasičnog skrivanja tajne poruke u neki medijum, već se na osnovu tajne poruke vrši generisanje medijuma koji će preneti tajnu poruku. Generisanje takvog medijuma nastoji da stvori medijum koji neće izazivati sumnju i privlačiti pažnju onih koji ne bi trebalo da prime tajnu poruku.

4. IMPLEMENTACIJA DWT ALGORITMA

U sklopu ovog rada izvršena je implementacija DWT algoritma za skrivanje audio-snimka unutar slike. U ovom primeru korišćene su 8-bitne RGB slike i audio-snimci u WAV formatu. Implementacije je odrađena u programskom jeziku *Python* uz primenu sledećih biblioteka:

- *NumPy* – biblioteka za rad sa nizovima i matematičkim proračunima
- *OpenCV* – biblioteka za rad sa slikama
- *Scipy* – biblioteka široke primene, ovde korišćena za rad sa WAV fajlovima
- *Wave* – biblioteka za rad za WAV fajlovima
- *Scikit-image* – biblioteka za obradu slika, ovde korišćena za evaluaciju algoritama

Tehnike digitalne steganografije koje koriste DWT algoritam baziraju se na upotrebi diskretne talasne transformacije u kombinacijom sa LSB algoritmom. Koraci u implementaciji ovog algoritma su sledeći:

1. Učitavanja slike i audio-snimka
2. Primena diskretne talasne transformacije nad slikom
3. Ugrađivanje audio-snimka u sliku primenom LSB algoritma
4. Primena inverzne diskretne talasne transformacije nad slikom sa ugrađenim snimkom

Za ekstrakciju tajne poruke, u ovom slučaju audio-snimka, neophodno je primeniti diskretnu talasnu transformaciju nad stego-objektom i izdvajanje bitova pomoću LSB algoritma.

U ovoj implementaciji korišćena je celobrojna talasna transformacija (engl. *Integer Wavelet Transform*). Ova verzija talasne transformacije odabrana je zbog prirode podataka sa kojima se radi jer slika predstavlja matricu celobrojnih vrednosti od 0 do 255.

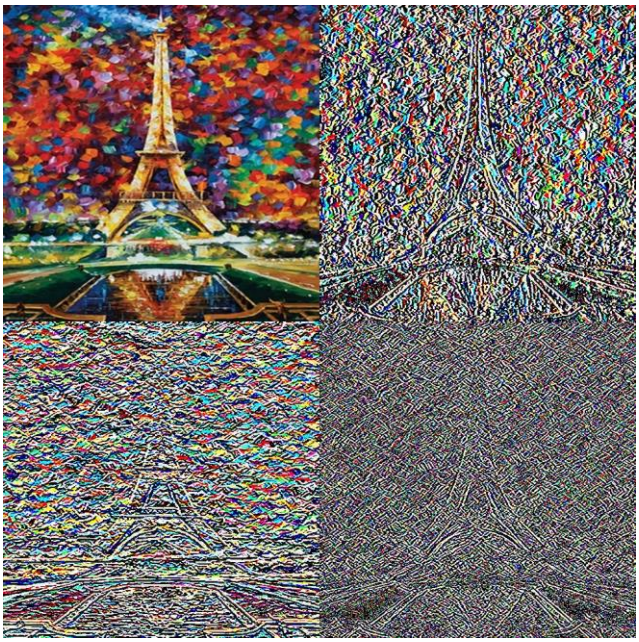
```
# region DISCRETE WAVELET TRANSFORM

def _IWT(array):
    output = np.zeros_like(array)
    nx, ny = array.shape
    x = nx // 2
    output[0:x, 0:ny] = (array[0::2, 0:ny] + array[1::2, 0:ny])//2
    output[x:nx, 0:ny] = array[0::2, 0:ny] - array[1::2, 0:ny]
    return output


def _IIWT(array):
    output = np.zeros_like(array)
    nx, ny = array.shape
    x = nx // 2
    output[0::2, 0:ny] = array[0:x, 0:ny] + (array[x:nx, 0:ny] + 1)//2
    output[1::2, 0:ny] = output[0::2, 0:ny] - array[x:nx, 0:ny]
    return output


def IWT2(array):
    return _IWT(_IWT(array.astype(int)).T).T


def IIWT2(array):
    return _IIWT(_IIWT(array.astype(int).T).T)


def applyImageTransform(red_plane, green_plane, blue_plane, inverse):
    if inverse:
        red_out = IIWT2(red_plane)
        green_out = IIWT2(green_plane)
        blue_out = IIWT2(blue_plane)
    else:
        red_out = IWT2(red_plane)
        green_out = IWT2(green_plane)
        blue_out = IWT2(blue_plane)
    return red_out, green_out, blue_out

# endregion
```

Slika 4.1 – Funkcije za implementiranje talasne transformacije i inverzne talasne transformacije nad slikom

Funkcije *_IWT* i *_IIWT* su funkcije za implementiranje jednodimenzionalne talasne i inverzne talasne transformacije. Funkcije *IWT2* i *IIWT2* implementiraju dvodimenzionalne talasne i inverzne talasne transformacije.

Slika 4.2 – Prikaz ulazne slike tj. objekta nosioca poruke

Na slici 4.2 možemo videli kako izgleda ulazna slika tj. slika koja će biti iskorišćena da se u njoj sakrije audio-snimak. Slika 4.3 prikazuje ovu sliku nakon primene talasne transformacije nad njom.



Slika 4.3 – Prikaz ulazne slike nakon primene talasne transformacije

Na slici 4.3 možemo uočiti 4 regiona koji se jasno izdvajaju nakon primene dvodimenzionalne talasne transformacije. Kao što smo već rekli, u gornjem levom uglu je LL region koji sadrži najviše detalja o slici. U donjem levom uglu je LH region koji prikazuje horizontalne detalje slike. Gornji desni ugao čini HL region koji sadrži vertikalne detalje slike i donji desni ugao je HH region sa dijagonalnim detaljima slike.

Postoje nekoliko varijanti ove tehnike steganografije u kojoj se primenjuje DWT algoritam. Naime, varijanta zavisi od regiona gde želimo da umetnemo tajnu poruku. Postoje varijante koje vrše skrivanje tajne poruke unutar visokofrekventnih regiona (LH, HL i HH) i tada je tajna poruka uočljivija, tj. lakše se može uočiti da slika sadrži neku tajnu poruku. Ali sa druge strane, izobličenja koja nastaju su minimalna, tj. ulazna slika i stego-slika su skoro identične. Ova varijanta može dodatno uključiti i piramidalnu dekompoziciju ulazne slike pomoću talasne transformacije. Algoritam piramidalne dekompozicije svodi se na primenu talasne transformacije nekoliko puta uzastopno pre neko što dođe do ugrađivanja tajne poruke unutar slike. U prvoj iteraciji talasna transformacija se primenjuje nad ulaznom slikom, dok svaki sledeći put talasna transformacija obrađuje LL region iz rezultata prethodne iteracije. Ovaj postupak je ilustrovan na slici 3.6. Druga varijanta ove steganografske tehnike, zasniva se na LL regionu. Tajna poruka se umeće u niskofrekventni LL region. Za razliku od visokofrekventnih regiona, umetanje poruke u ovaj region čini stego-sliku mnogo otpornijom i teže je uočiti da uopšte postoji skrivena komunikacija. Uglavnom svaka prednost vuče sa sobom i neku manu, pa kad se poruka umeće u LL region moguće je da se pojave izobličenja na slici koja su vidljiva golim oko. U ovom konkretnom slučaju, dodatna opcija je primena talasne transformacije nad audio-snimkom.

Slika 4.4 – Stego slika dobijena primenom DWT algoritma u kombinaciji sa LSB algoritmom

Veoma bitnu ulogu u tehnikama zasnovanim na transformacijama domena ima LSB algoritam. LSB algoritam je jedan od predstavnika tehnika supstitucije i on je dovoljan da sam kreira stego-objekat. Međutim, ovaj algoritam je veoma jednostavan i kao takav se koristi kao dodatni algoritam kod ostalih tehnika. U ovom projektu iskorišćen je da se unutar LL regiona dobijenim nakon primene dvodimenzionalne talasne transformacije u jednom prolazu, sakrije tajni audio-snimak. LSB je upotrebljen tako da se gornja četiri bita svakog kanala u LL regionu koriste za prenos objekta nosioca poruke, a donja četiri bita za prenos polovine jednog bajta tajne poruke. Ovaj način skrivanja tajne poruke omogućava da tajna poruka bude preneta uz minimalna odstupanja od originalne (moguća odstupanja predstavljaju devijaciju prilikom primene talasne transformacije).

```
for i in range(audio_height):
    for j in range(audio_length):
        bitRH = audio_r[j][i] >> 4
        bitRL = audio_r[j][i] & 15
        red_plane[i][j] = (red_plane[i][j] & 240) | bitRH
        red_plane[i+audio_height][j] = (red_plane[i+audio_height][j] & 240) | bitRL

        bitGH = audio_g[j][i] >> 4
        bitGL = audio_g[j][i] & 15
        green_plane[i][j] = (green_plane[i][j] & 240) | bitGH
        green_plane[i+audio_height][j] = (green_plane[i+audio_height][j] & 240) | bitGL

        bitBH = audio_b[j][i] >> 4
        bitBL = audio_b[j][i] & 15
        blue_plane[i][j] = (blue_plane[i][j] & 240) | bitBH
        blue_plane[i+audio_height][j] = (blue_plane[i+audio_height][j] & 240) | bitBL
```

Slika 4.5 – Prikaz dela koda koji vrši ugradnju tajne poruke u objekat nosilac primenom LSB-a

```
for i in range(audio_height):
    for j in range(audio_length):
        bitRH = (red_plane[i][j] & 15) << 4
        bitRL = red_plane[i+audio_height][j] & 15
        audio_r[j][i] = bitRH | bitRL

        bitGH = (green_plane[i][j] & 15) << 4
        bitGL = green_plane[i+audio_height][j] & 15
        audio_g[j][i] = bitGH | bitGL

        bitBH = (blue_plane[i][j] & 15) << 4
        bitBL = blue_plane[i+audio_height][j] & 15
        audio_b[j][i] = bitBH | bitBL
```

Slika 4.6 – Prikaz dela koda koji vrši ekstrakciju tajne poruke

Kao evaluacione mere za steganografske algoritme, u ovom projektu, korišćene su *PSNR* i *SSIM*. U pitanju su standardne mere koje se koriste ne samo za evaluaciju steganografskih algoritama, već i za bilo koje računarske algoritme i operacije koje se izvršavaju nad nekim signalom.

PSNR (engl. *Peak signal-to-noise ratio*) predstavlja odnos maksimalne moguće vrednosti (snage) signala i snage šuma koji utiče na kvalitet njegove reprezentaciije. Budući da mnogi signali imaju veoma širok dinamički opseg (odnos između najveće i najmanje moguće vrednosti), *PSNR* se izražava kroz logaritamsku skalu decibela. Poboljšanje vizuelnog kvaliteta digitalne slike može biti subjektivno. Izbor koja od ponuđenih metoda rezultuje kvalitetnijom slikom kada se te metode primene na istoj slici, uglavnom se razlikuje od osobe do osobe. Iz tog razloga nephodno je uspostaviti kvantitativne/empirijske mere za upoređivanje efekata algoritama za poboljšanje kvaliteta slike. Koristeći isti skup slika za testiranje, različiti algoritmi za poboljšanje slike mogu se sistematski upoređivati da bi se utvrdilo da li određeni algoritam daje bolje rezultate. Metrika koja se ispituje jeste odnos signal – šum. Ako možemo pokazati da algoritam ili skup algoritama mogu poboljšati degradiranu sliku kako bi bila što sličnija originalu, onda možemo zaključiti da je to bolji algoritam[10].

```
# region MEASUREMENT FUNCTIONS

def psnr(img1, img2):
    diff = img1 - img2
    mse = np.mean(np.square(diff))
    psnr_value = 10 * np.log10(255 * 255 / mse)
    print("PSRN:")
    print(psnr_value)
    return 0


def ssim(img1, img2):
    (grayScore, diff) = compare_ssim(img1, img2, full=True, multichannel=True)
    print("SSIM:")
    print(grayScore*100)
    return 0


def measurement_image(img1, img2):
    psnr(img1, img2)
    ssim(img1, img2)
    return 0

#endregion
```

Slika 4.7 – Prikaz dela koda koji implementira evaluaciju steganografskog algoritma

SSIM (engl. *Structural Similarity Index*) ili indeks strukturne sličnosti je perceptivna mera koja kvantifikuje degradaciju kvaliteta slike uzrokovanu obradom kao što je kompresija podataka ili gubicima u prenosu podataka. To je potpuno referentna mera koja zahteva dve slike istog kadra, referentnu sliku (original) i obrađenu sliku. *SSIM* zapravo meri perceptivnu razliku između dve slične slike. Ne može se proceniti koja je od te dve slike bolja, već se to mora zaključiti na osnovu saznanja šta je original, a šta je podvrgnuto obradi. Za razliku od *PSNR* mere, *SSIM* se zasniva na vidljivim strukturama na slici.

5. ZAKLJUČAK

Kao što se može videti iz ovog rada, steganografija je nešto što čoveka prati od samog početka. Ljudi su nastojali da sakriju informacije koje ne treba svako da čuje, već samo onaj kome su namenjene. Počevši od prvih oblika steganografije, do najmodernijih algoritama koji su nastali na osnovama modernog računarstva, vidimo da steganografija raspolaže vrlo efikasnim i snažnim tehnikama koje ljudima omogućavaju bezbednu komunikaciju i razmenu podataka. U kombinaciji sa kriptografijom, može biti dodatni sigurnosni stepen u zaštiti informacija. Steganografske tehnike su vrlo jednostavne za upotrebu, a vrlo teško se otkrivaju i veoma su pouzdane.

Glavni cilj steganografije je da prisustvo tajne poruke ostane neotkriveno. Tajnost poruke vezuje se za steganografski sistem (algoritam) i tajni ključ pod kojim je skrivena tajna poruka. Modifikacijom stego-medijuma za prikrivanje poruka, menjaju se njegova statistička svojstva tako da postoji mogućnost napada (otkrivanja postojanja tajne poruke u stego-medijumu) ali ne i njegovog sadržaja.

U ovom radu analizirane su steganografske tehnike koje se baziraju na transformaciji domema, tačnije obrađen je algoritam koji se temelji na diskretnoj talasnoj transformaciji. Postoje mnogo varijanti u DWT tehnici i sve one imaju svoje prednosti i mane. Koju ćemo odabrati, zavisi od konkretne primene. Ovde je za potrebe demonstacije implementirana varijanta koja je veoma pouzdana što se tiče otkrivanja i ekstrakcije tajna poruke od strane napadača. Ova prednost, donosi sa sobom i nedostatke koji se reprodukuju uočljivim izobličenjima na slici. DWT algoritam kombinovan je sa LSB algoritmom za umetanje tajne poruke u sliku, sa modifikacijom od 4 bita po bajtu (moguće je i smanjiti broj bitova, što će uzrokovati manje memorijskog prostora, za smeštanje tajne poruke). U ovom slučaju, tajna poruka je audio-snimak, dodatna opcija može biti i primena diskretne talasne transformacije nad tajnom porukom, što rezultira povećanjem pouzdanosti steganografskog sistema i dodatno otežava mogućnost ekstrakcije tajne poruke.

6. LITERATURA

1. Deepak Barua – *Steganographic Algorithms and Application of DNA*
   Kaunas University of Technology
2. Ahmed Shihab Ahmed Al-Naima – *Image Steganografy Based on DWT*
3. R. Punidha, M.Sivaram – *Integer wavelet transform based approach for high robustness of audio signal transmission*
4. Goran Radanović – *Steganografija i steganaliza digitalnih slika*
   Fakultet elektrotehnike i računarstva Zagreb
5. Dr. Branislav Todorović, Sandra Erić – *Talasna transformacija – novi metod za analizu signala*, Vojnotehnički institute VJ, Beograd
6. Marko Stanec – *Skrivanje informacija u objekt nositelj korišćenjem LSB algoritma* Fakultet prometnih znanosti, Zagreb
7. Dejan Uljarević, Mladen Veinović – *Digitalna steganografija JPEG slika primenom DCT steganografije*
8. Kristijan Klasan – *Steganografija i steganaliza*
   University of Pula
9. Ms. Asawari S. Shinde, Dr. Achana B. Patankar – *Image Steganography: Hiding Audio Signal in Image Using Discrete Wavelet Transform*
10. Aiswarya T, Mansi Shah, Aishwarya Talekar, Pallavi Raut – *Steganographic Technique for Hiding Secret Audio in an Image*