UNIVERZITET U NIŠU

ELEKTRONSKI FAKULTET

Predmet:DIGITALNA FORENZIKA

Primena diskretne talasne transformacije (DWT) u steganografiji zasnovanom na slici

Seminarski rad

Student: Teodora Pantić

Mentor: Bratislav Predić

Niš, Decembar 2024

SADRŽAJ

1. Uvod

Definicija i značaj teme

Diskretna talasna transformacija (DWT) je matematička tehnika koja se koristi za analizu i obradu signala, posebno u kontekstu digitalne obrade slike. DWT razlaže signal na različite frekventne komponente koje se analiziraju pojedinačno. Za razliku od Fourierove transformacije, koja pruža informacije samo o frekvencijama, DWT omogućava i vremensku lokalizaciju informacija. Ova tehnika se pokazala kao veoma korisna u različitim aplikacijama obrade slike, uključujući kompresiju, uklanjanje šuma i ekstrakciju karakteristika.

Talasna transformacija koristi posebne funkcije poznate kao talasi (wavelets), koje su lokalizovane u vremenu i frekvenciji. To znači da talasna transformacija može istovremeno pružiti informacije o "kada" i "kojoj frekvenciji" se određeni događaji u signalu pojavljuju. Diskretna talasna transformacija, konkretno, primenjuje ove talase na diskretizovane signale, što je idealno za digitalne slike koje su već diskretizovane u pikselskoj mreži. To znači da se signal ili slika, koji su inicijalno u kontinuiranom obliku, pretvaraju u niz diskretnih vrednosti ili uzoraka. Na primer, digitalne slike su već diskretizovane jer su predstavljene kao mreža piksela, gde svaki piksel ima određenu boju i intenzitet. DWT koristi ove diskretne vrednosti piksela za dalju obradu.

Diskretna talasna transformacija funkcioniše tako što koristi specifične matematičke funkcije, talase, za analizu različitih frekvencijskih komponenti slike. DWT razdvaja sliku na niz podslika koje predstavljaju različite detalje slike na različitim skalama. Na ovaj način, možemo analizirati i obraditi detalje slike na različitim nivoima rezolucije, što je veoma korisno za različite primene kao što su kompresija, uklanjanje šuma, ekstrakcija karakteristika i steganografija.

U kontekstu digitalne obrade slike, DWT omogućava:

Razdvajanje detalja slike: DWT razdvaja sliku na različite komponente, omogućavajući analizu finih i grubih detalja odvojeno. Ovo je korisno za identifikaciju i obradu specifičnih karakteristika slike.

Smanjenje podataka: Primena DWT omogućava smanjenje količine podataka potrebnih za prikaz slike, što je korisno za kompresiju slike bez gubitka važnih informacija.

Poboljšanje kvaliteta slike: DWT može pomoći u uklanjanju šuma iz slike, čime se poboljšava kvalitet i jasnoća slike.

Efikasno skrivanje informacija: U steganografiji, DWT omogućava umetanje skrivenih informacija u frekvencijske komponente slike, čime se postiže bolja otpornost na otkrivanje i manipulaciju.

Na ovaj način, DWT koristi diskretizovane vrednosti piksela digitalne slike za dalju analizu i obradu, pružajući moćan alat za razne primene u digitalnoj obradi slike.

Steganografija je tehnika skrivanja informacija unutar drugih, naizgled bezopasnih, podataka. Reč "steganografija" dolazi od grčkih reči "steganos" (što znači skriven) i "graphein" (što znači pisati), što u osnovi znači "skriveno pisanje". Za razliku od kriptografije, koja je usmerena na zaštitu sadržaja informacije tako što ga čini nečitljivim bez odgovarajućeg ključa, steganografija teži da sakrije samu činjenicu da informacija postoji. Dok kriptografija koristi šifrovanje da bi osigurala da samo ovlašćene osobe mogu čitati informacije, steganografija se fokusira na to da informacije budu skrivene u običnom tekstu, slikama ili drugim medijima, tako da niko osim pošiljaoca i primaoca ne zna da informacija uopšte postoji. Oba pristupa imaju za cilj zaštitu informacija, ali koriste različite metode i strategije za postizanje tog cilja.

U kontekstu digitalne obrade, steganografija se može primeniti na različite medije, uključujući tekst, audio, video i slike. Steganografija zasnovana na slici (image-based steganography) koristi digitalne slike kao nosioce skrivene informacije. Informacija koja se sakriva može biti bilo kojeg tipa, uključujući tekstualne poruke, binarne fajlove ili druge slike. Glavni cilj steganografije zasnovane na slici je da sakrije podatke na takav način da promene na slici budu neprimetne ljudskom oku.

Diskretna talasna transformacija (DWT) igra ključnu ulogu u steganografiji zasnovanoj na slici. Korišćenjem DWT, slika se može dekomponovati u različite frekventne komponente, što omogućava umetanje skrivenih informacija u određene frekventne opsege slike. Ova tehnika ima prednosti u odnosu na tradicionalne metode skrivanja informacija, kao što je manipulacija najmanje značajnog bita (Least Significant Bit, LSB), jer pruža veću otpornost na napade i modifikacije slike, kao i bolju zaštitu skrivenih informacija.

Cilj seminarskog rada

Cilj ovog seminarskog rada je da istraži i objasni kako se diskretna talasna transformacija (DWT) koristi u steganografiji zasnovanoj na slici. Fokus je na razumevanju osnovnih principa DWT-a i načina na koji ova metoda omogućava efikasno sakrivanje informacija u digitalnim slikama. Rad takođe upoređuje prednosti i izazove ove tehnike u poređenju s drugim pristupima, kako bi se pokazalo zašto je DWT važan alat u ovoj oblasti.

Kroz rad će biti obrađene sledeće teme:

- Osnovni principi DWT-a i njegova primena u obradi digitalnih slika.
- Ključni koncepti steganografije i njen značaj za zaštitu informacija.
- Detaljan prikaz procesa skrivanja informacija u slikama korišćenjem DWT-a.
- Prednosti koje DWT pruža u odnosu na druge metode steganografije.
- Tehnički i sigurnosni izazovi povezani s primenom DWT-a.

Primena DWT-a u steganografiji predstavlja važan korak napred u zaštiti informacija. Cilj rada je da ne samo objasni kako DWT funkcioniše, već i da pruži konkretne primere i mogućnosti primene u praksi. Na taj način, rad ima za cilj da čitaocima približi ovu tehnologiju, ističući njen potencijal za unapređenje sigurnosti i otpornosti digitalnih podataka na različite pretnje.

2. Teorijska pozadina

Osnove diskretne talasne transformacije (DWT)

Diskretna talasna transformacija (DWT) je matematički alat koji se koristi za analizu signala, kao što su zvuk, slike ili vremenske serije, istovremeno u vremenskom i frekventnom domenu. Ova tehnika je posebno korisna jer omogućava da se signal posmatra i u pogledu vremena i u pogledu frekvencije, što nije moguće sa nekim drugim metodama, poput Fourierove transformacije.

Ključne razlike između DWT i Fourierove transformacije

Fourierova transformacija pretvara signal u zbir sinusoida, dajući informacije o tome koje frekvencije postoje u signalu. Problem je što ona pretpostavlja da su te frekvencije konstantne tokom celog trajanja signala, što nije tačno za realne, nestacionarne signale. Nestacionarni signali su oni kod kojih frekvencije i njihov intenzitet variraju tokom vremena (npr. govor ili EEG signali).

S druge strane, DWT koristi talasne (wavelet) funkcije koje su lokalizovane u vremenu i frekvenciji. To znači da ona može da pokaže ne samo koje frekvencije postoje, već i kada se one pojavljuju tokom trajanja signala.

Kako funkcioniše DWT?

Kada primenimo DWT na signal, dobijamo skup koeficijenata koji predstavljaju signal na različitim nivoima rezolucije. Ti nivoi su organizovani hijerarhijski:

1. **Najviši nivo detalja (npr. d1):** Ovaj nivo sadrži informacije o signalima sa najvišim frekvencijama i najfinijom vremenskom rezolucijom. To znači da možemo tačno da odredimo kada se promene u visokim frekvencijama dešavaju.
2. **Niži nivoi detalja (npr. d2, d3, ...):** Kako idemo niz hijerarhiju, vremenska rezolucija opada, ali frekventna rezolucija raste. To znači da možemo bolje da analiziramo niže frekvencije, iako sa manje preciznim vremenskim informacijama.
3. **Aproksimacija:** Ovo je najniži nivo koji sadrži opštu sliku ili osnovni oblik signala. Ona uključuje najniže frekvencije signala.

Ova hijerarhijska struktura omogućava analizu signala na različitim skalama. Na primer, možemo istovremeno posmatrati sitne detalje (visoke frekvencije) i opštu strukturu (niske frekvencije) signala.

Talasne funkcije (Wavelets)

Talasne funkcije su osnovni elementi koji se koriste u DWT. One se skaliraju i pomeraju kako bi se analizirale različiti delovi signala na različitim nivoima rezolucije. Postoji mnogo različitih talasnih funkcija, a izbor odgovarajuće zavisi od vrste signala koji analiziramo i šta želimo da postignemo.

Daubechies talasne funkcije

Jedan od najčešće korišćenih setova talasnih funkcija su **Daubechies talasi**. Oni su dobili ime po matematičarki Ingrid Daubechies, koja ih je razvila. Ovi talasi imaju različite verzije, kao što su Daubechies-4, Daubechies-6, Daubechies-8, itd. Broj (npr. 4, 6, 8) označava broj nultih momenata talasa, što utiče na preciznost i lokalizaciju u vremenu i frekvenciji.

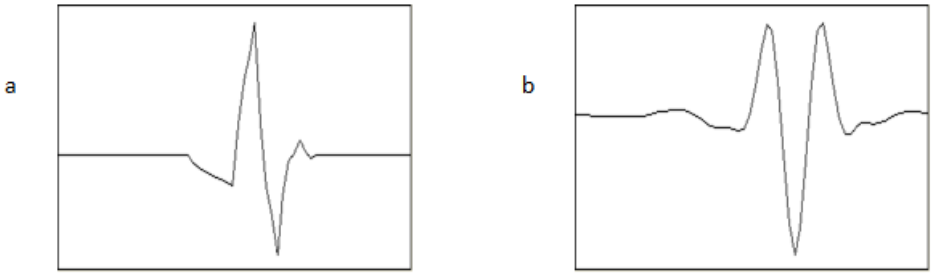
- **Daubechies-4 talasna funkcija** ima četiri nulta momenta, što omogućava preciznu analizu signala i njegovu kompaktnu reprezentaciju. Ova funkcija je naročito pogodna za obradu signala gde je potrebna dobra ravnoteža između vremenske i frekventne rezolucije.
- Promenom talasne funkcije, kao što je prelazak sa Daubechies-4 na Daubechies-6 ili Daubechies-8, menja se način na koji se signal razlaže, jer različite funkcije imaju različite osobine lokalizacije

Daubechies talasne funkcije su idealne za obradu podataka gde je potrebna detaljna vremensko-frekventna analiza. Ove talasne funkcije su poznate po svojoj kompaktnoj podršci i ortogonalnosti, što ih čini idealnim za analizu i rekonstrukciju signala.

Ostale talasne funkcije

Pored Daubechies funkcija, postoje i druge talasne funkcije, kao što su Coiflets i Symlets. **Coiflet talasne funkcije** imaju dodatna svojstva glatkoće i simetričnosti, što ih čini pogodnim za analizu signala gde je potrebna velika preciznost.

- **Coiflet-30 talasna funkcija** pruža viši nivo glatkoće, što može biti korisno za specifične primene, poput analize slike.



Slika1:a)Daubechies-4 talasna funkcija; b)Coiflet-30 talasna funkcija [1]

[1] https://www.st-andrews.ac.uk/~wjh/dataview/tutorials/dwt.html

Prednosti DWT

- **Analiza nestacionarnih signala:** DWT je idealna za signale koji se menjaju tokom vremena.
- **Vremensko-frekventna lokalizacija:** Omogućava preciznu identifikaciju promena u signalu u oba domena.
- **Kompresija podataka:** Koeficijenti DWT se mogu koristiti za uklanjanje redundantnih informacija, što je korisno u kompresiji slike (npr. JPEG2000).
- **Eliminacija šuma:** DWT može da pomogne u uklanjanju šuma iz signala dok zadržava važne informacije.

Diskretna talasna transformacija je moćan alat za analizu signala, jer pruža vremensko-frekventne informacije koje nisu dostupne putem tradicionalnih metoda kao što je Fourierova transformacija. Njena sposobnost da različite frekvencije posmatra u vremenskom kontekstu čini je nezamenjivom u oblastima kao što su obrada zvuka, analiza slike i obrada biomedicinskih podataka. Pažljiv izbor talasne funkcije, poput Daubechies-4 ili Coiflet-30, i nivoa rezolucije je ključan za uspešnu primenu ove metode.

DWT u obradi slika

Diskretna talasna transformacija (DWT) je tehnika koja omogućava dekompoziciju slike na različite frekvencijske komponente, čime se omogućava analiza slike u prostorno-frekventnom domenu.Tokom transformacije, signal se deli na delove visoke i niske frekvencije. Komponenta visoke frekvencije sadrži informacije o ivičnim detaljima slike, dok se komponenta niske frekvencije dalje razlaže na svoje visoke i niske frekvencije. Za potrebe steganografije, najčešće se koriste visoke frekvencije, jer su promene u ovim delovima manje primetne ljudskom oku, posebno u oblastima sa naglim prelazima i ivicama slike.

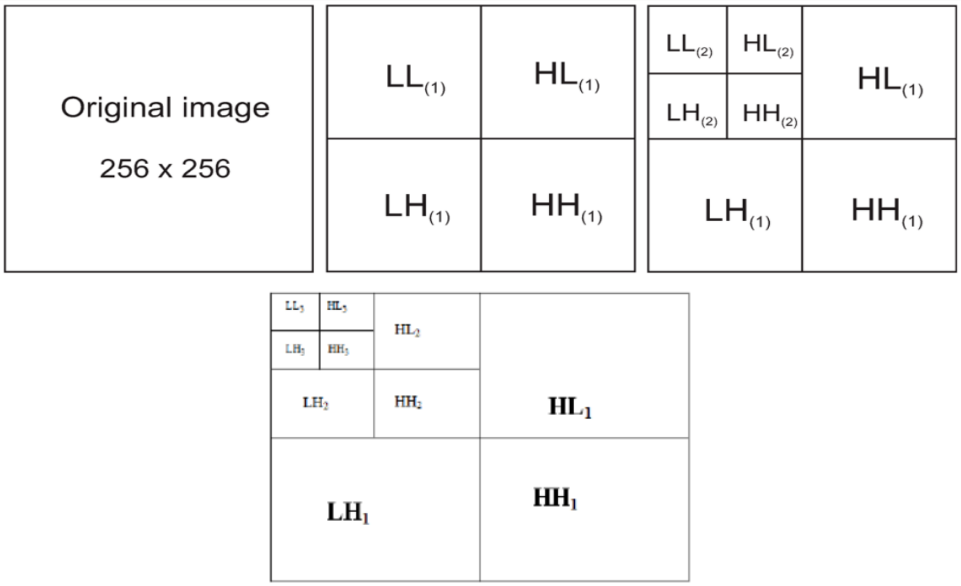
Ova metoda je posebno značajna u obradi slika zbog svoje sposobnosti da odvoji osnovne informacije o slici od njenih detalja, što je korisno u oblastima poput kompresije slike, uklanjanja šuma i steganografije.

U dvodimenzionalnim aplikacijama, DWT se primenjuje u dva koraka: prvo u vertikalnom, a zatim u horizontalnom pravcu. Ovaj proces dekompozicije na prvom nivou deli sliku na četiri podopsega: LL1, LH1, HL1 i HH1.

- **LL (Low-Low)**: Ovaj podopseg sadrži niske frekvencije u oba pravca – horizontalnom i vertikalnom. Predstavlja grubu aproksimaciju originalne slike sa smanjenom rezolucijom i sadrži osnovne informacije o slici koje su manje osetljive na šum i promene.
- **LH (Low-High)**: Sadrži niske frekvencije u horizontalnom pravcu i visoke frekvencije u vertikalnom pravcu. Ovaj podopseg obuhvata informacije o horizontalnim detaljima slike, poput ivica i tekstura.

- **HL (High-Low)**: Obuhvata visoke frekvencije u horizontalnom pravcu i niske frekvencije u vertikalnom pravcu. Ovaj podopseg sadrži informacije o vertikalnim detaljima slike.
- **HH (High-High)**: Ovaj podopseg uključuje visoke frekvencije u oba pravca. Sadrži informacije o dijagonalnim detaljima, poput ivica i tekstura koje su karakteristične za sliku.

Na svakom sledećem nivou dekompozicije, LL podopseg iz prethodnog nivoa koristi se kao ulaz za dalje razlaganje. Na primer, za drugi nivo dekompozicije, DWT se primenjuje na LL1 podopseg, razlažući ga na četiri nova podopsega: LL2, LH2, HL2 i HH2. Ovaj proces se može nastaviti kroz više nivoa, pri čemu se svaki put postiže još finija analiza slike.



Slika2: Prikazuje trofaznu dekompoziciju slike primenom DWT-a.

Na digitalnim slikama diskretna talasna transformacija (DWT) omogućava njihovu dekompoziciju na četiri podopsega: LL, LH, HL i HH. Podopseg LL sadrži ključne informacije o slici, pa njegovo korišćenje za ugrađivanje podataka može povećati otpornost stego slike na različite vrste napada. Međutim, ovaj pristup nosi rizik od vizuelnih distorzija u stego slici.

Tehnike steganografije zasnovane na DWT-u sve su popularnije u poređenju s drugim transformacionim metodama, zahvaljujući sledećim karakteristikama:

- Dekompozicija slike na frekvencijske pojaseve u skladu je s funkcionisanjem ljudskog vizuelnog sistema (HVS). Ovo omogućava selektivnu obradu različitih pojaseva bez značajnog narušavanja vizuelne percepcije slike.

- Visokofrekventni podopsezi (LH, HL, HH) precizno identifikuju detalje poput ivica i tekstura, koje su manje primetne ljudskom oku. Zbog toga su ovi podopsezi pogodni za ugrađivanje podataka, jer ne izazivaju lako uočljive promene na slici.

Ove osobine omogućavaju efikasnije i sigurnije ugrađivanje podataka, uz očuvanje kvaliteta slike i otpornost na različite napade.

Osnove steganografije

Steganografija predstavlja tehniku skrivanja informacija unutar pokrivnog medija, koji može biti tekst, slika, audio ili video zapis. Kada se kao pokrivni medij koristi slika, rezultat nakon skrivanja podataka naziva se *stego slika*. Poreklo termina "steganografija" vodi se iz grčkog jezika, gde reč *stegano* znači "pokriveno", dok *graf* označava "pisanje".

U domenu tajne komunikacije, steganografija i kriptografija predstavljaju dve komplementarne tehnike. Dok se kriptografija fokusira na zaštitu sadržaja poruke kroz enkripciju, steganografija se bavi prikrivanjem same egzistencije poruke unutar pokrivnog medija. Kada se ove dve metode kombinuju, postiže se viši nivo sigurnosti, jer je poruka istovremeno zaštićena i skrivene prirode, čime se povećava otpornost na potencijalne napade.

Steganografski sistemi karakterišu tri ključna aspekta:

1. **Kapacitet**: Predstavlja maksimalnu količinu podataka koji se mogu sakriti unutar pokrivnog medija bez značajnog uticaja na njegov vizuelni kvalitet.
2. **Neprimetnost**: Proces ugrađivanja podataka mora osigurati da se vizuelne ili perceptivne promene na pokrivnoj slici ne mogu lako detektovati.
3. **Bezbednost**: Skriveni podaci treba da budu zaštićeni od otkrivanja pomoću steganalizatora ili drugih metoda analize.

Tehnike steganografije dele se u dve osnovne kategorije:

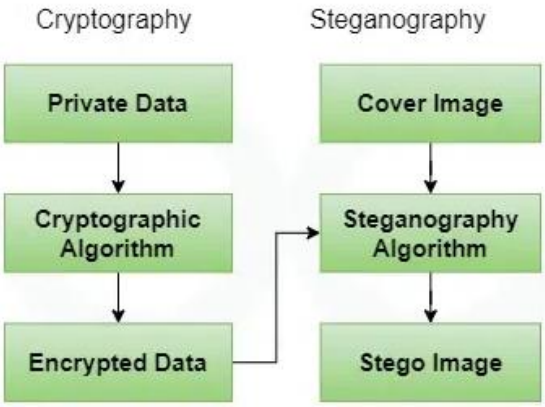
- **Tehnike prostornog domena**: Podaci se direktno ugrađuju u vrednosti piksela slike. Ove metode su jednostavnije i brže, ali su manje otporne na napade.
- **Tehnike transformacionog domena**: Slika se prvo transformiše u frekvencijski domen, gde se podaci ugrađuju u koeficijente transformacije. Transformacije koje se koriste uključuju **DCT** (diskretna kosinusna transformacija), **DFT** (diskretna Fourierova transformacija) i **DWT** (diskretna talasna transformacija). Ove tehnike su otpornije na analize, ali su računski zahtevnije.

Steganografski sistem sastoji se od tri osnovna elementa:

- **Nosilac (cover medium)**: Digitalni medijum koji služi kao pokrivni sloj za skrivene podatke, poput slike, audio ili video zapisa.
- **Skrivena informacija (payload)**: Podaci koji se ubacuju u nosilac, poput tekstualne poruke, binarnih fajlova ili slika.
- **Steganografski algoritam**: Metodologija koja definiše kako će podaci biti umetnuti u nosilac na način koji očuva neprimetnost i bezbednost sistema.

Ovakav pristup pruža sveobuhvatno razumevanje ključnih aspekata i elemenata steganografskih sistema.

Razlika između steganografije i kriptografije



Slika 3: Razlika između stenografije i kriptografije[2]

Kriptografija i steganografija su dve komplementarne tehnike koje se koriste za zaštitu informacija, ali se razlikuju po svojoj osnovnoj svrsi i metodologiji. Kriptografija ima za cilj zaštitu sadržaja informacije tako što je čini nečitljivom bez odgovarajućeg ključa. Koristeći tehnike kao što su enkripcija i dekripcija, kriptografija se fokusira na skrivanje značenja informacije. Na taj način, čak i ako treća strana presretne komunikaciju, bez ključa neće moći da razume stvarni sadržaj.

S druge strane, steganografija se bavi skrivanjem postojanja same informacije. Umesto da šifrira podatke, steganografija teži da informacija bude neprimetna unutar nosioca, bilo da je to digitalna slika, audio zapis ili drugi medij. Na taj način, osnovni cilj steganografije je da se sakrije činjenica da bilo kakva tajna informacija uopšte postoji, čineći je teškom za otkrivanje.

Dok kriptografija osigurava da je poruka nečitljiva bez odgovarajućeg ključa, steganografija osigurava da poruka ostane skrivena unutar običnog podatka. Kombinovanjem ovih tehnika može se postići dvostruka zaštita informacija, i od otkrivanja postojanja i od čitanja sadržaja bez dozvole.

Kriptografija i steganografija mogu se koristiti zajedno za dodatni nivo sigurnosti. Na primer, poruka može prvo biti šifrovana kriptografskim algoritmom, a zatim umetnuta u nosilac steganografskim algoritmom. Na taj način, čak i ako se otkrije postojanje skrivene informacije, sadržaj poruke ostaje zaštićen.

[2] https://media.geeksforgeeks.org/wp-content/uploads/20240404170623/Cryptography-and-steganography.webp

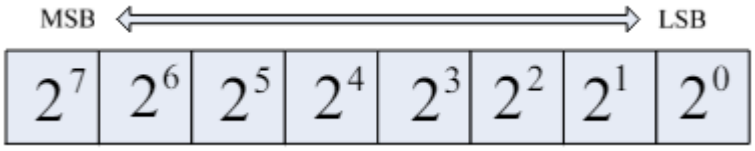
Osnovni koncepti skrivanja informacija u slikama

Skrivanje informacija u slikama može se izvesti na različite načine, od kojih su najpopularniji:

Manipulacija najmanje značajnog bita (LSB) predstavlja osnovnu tehniku steganografije koja omogućava skrivanje informacija unutar digitalnih medija, poput slika, audio zapisa ili tekstualnih datoteka. Suština ove metode leži u izmeni najmanje značajnih bitova piksela, zvučnih uzoraka ili tekstualnih karaktera, pri čemu su te izmene statistički neprimetne ljudskom oku ili uhu.

Osnovni princip ove tehnike je da male promene u najmanje značajnim bitovima ne uzrokuju primetne razlike u vizuelnom ili auditivnom kvalitetu medija, što je čini pogodnom za efikasno sakrivanje podataka. Međutim, metoda je ranjiva na steganalizu, jer algoritmi mogu otkriti statističke obrasce izazvane promenama u LSB-ovima, čak i kada te promene nisu uočljive čoveku.

Zbog ovih ograničenja, LSB tehnika se često kombinuje s dodatnim merama, poput enkripcije, ili se koristi zajedno s naprednijim tehnikama, kao što su transformacione metode (npr. DWT). Ove kombinacije pružaju veću sigurnost, otpornost na analizu i bolju neprimetnost prilikom skrivanja informacija.

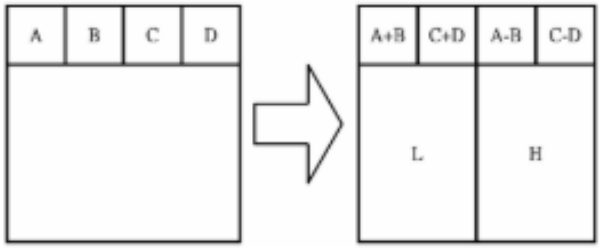


Slika 4: Ponderisanje 8-bitnog piksela.[3]

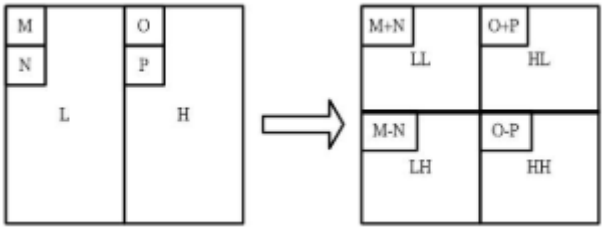
Transformacioni domeni obuhvataju tehnike koje manipulišu frekventnim komponentama slike, za razliku od metoda koje direktno menjaju piksele u prostornom domenu. Ključne metode u ovom pristupu su diskretna kosinusna transformacija (DCT) i diskretna talasna transformacija (DWT), poznate po efikasnosti u sakrivanju informacija i otpornosti na analize i napade**.**

Jedna od popularnih transformacionih tehnika je **Haar-DWT**, koja se često koristi u steganografiji. Dvodimenzionalni Haar-DWT uključuje dve osnovne operacije: horizontalnu i vertikalnu

[3] https://gigvvy.com/journals/ijase/articles/ijase-200612-4-3-275.pdf



Slika 5:Horizontalna operacija na prvom redu.[4]



Slika 6:Vertikalna operacija[5]

Ključne karakteristike ovih transformacionih domena:

 Frekventne komponente: Ove tehnike razlažu sliku na frekventne komponente umesto da rade direktno s pikselima. Na primer, **DCT** razbija sliku na komponente koje predstavljaju različite frekvencije kosinusnih talasa, dok **DWT** deli sliku na različite frekvencijske podopsege, pružajući višestruke nivoe analize.

 Neprimetnost: Informacije se skrivaju u manje vidljivim delovima slike, poput visokofrekventnih oblasti koje ljudsko oko teško primeti. Ovo omogućava da ugrađeni podaci ostanu skriveni bez narušavanja vizuelnog kvaliteta slike.

 Otpornost na napade: Transformacione tehnike su otpornije na napade poput kompresije, filtriranja i manipulacije slikom. To je zato što se podaci ne nalaze direktno u prostornom domenu, već u frekventnim komponentama, čime se otežava njihovo otkrivanje.

 Kompleksnost: Ove tehnike, poput DCT i DWT, zahtevaju složene proračune za prelazak iz prostornog u frekventni domen i obrnuto. Iako to može povećati vreme obrade, moderni algoritmi i hardverska ubrzanja omogućavaju njihovu efikasnu primenu.

Prostorni domeni koriste metode koje direktno menjaju vrednosti piksela slike. To uključuje tehnike poput razbacivanja piksela i prilagođavanja histograma boja. Iako su ove metode složenije, pružaju veću sigurnost prilikom skrivanja informacija u slikama.

[4] https://gigvvy.com/journals/ijase/articles/ijase-200612-4-3-275.pdf

[5] https://gigvvy.com/journals/ijase/articles/ijase-200612-4-3-275.pdf

Steganografske tehnike zasnivane na DWT-u

Steganografija slike visokog kapaciteta koristeći talasnu transformaciju i genetski algoritam

Ghasemi i saradnici [1] predstavili su tehniku steganografije koja koristi talasnu transformaciju i genetski algoritam. Funkcija mapiranja zasnovana na genetskom algoritmu koristi se za ugrađivanje podataka u koeficijente diskretne talasne transformacije (DWT) u blokovima veličine 4x4 na pokrivačkoj slici. Optimalni proces prilagođavanja piksela primenjuje se nakon ugrađivanja poruke. Obrada u frekvencijskom domenu poboljšava otpornost steganografije. Upotreba genetskog algoritma i procesa optimalnog prilagođavanja piksela (OPAP) rezultira optimalnom funkcijom mapiranja koja smanjuje razliku greške između pokrivačke slike i stego slike, poboljšavajući kapacitet skrivanja uz minimalne distorzije. Predložena metoda ugrađuje poruku u koeficijente diskretne talasne transformacije zasnovane na genetskom algoritmu i algoritmu OPAP, a zatim se primenjuje na dobijenu ugrađenu sliku.

Haar diskretna talasna transformacija: DWT analiza deli signal na dve klase (tj. aproksimaciju i detalje) pomoću dekompozicije signala za različite frekventne opsege i skale. DWT koristi dva seta funkcija: skaliranje i talasne, koje su povezane sa niskopropusnim i visokopropusnim filterima. Ovakav način dekompozicije prepolovljuje vremensku odvojivost. Drugim rečima, samo polovina uzoraka u signalu je dovoljna da predstavlja ceo signal, udvostručujući frekventnu odvojivost.

Haar talasna funkcija operiše na podacima računajući zbirove i razlike susednih elemenata. Ova talasna funkcija prvo operiše na susednim horizontalnim elementima, a zatim na susednim vertikalnim elementima. Jedna od lepih karakteristika Haar talasne transformacije je da je transformacija jednaka svojoj inverzi. Svaka transformacija računa energiju podataka koja se relocira u gornji levi ugao. Nakon svake transformacije, veličina kvadrata koji sadrži najvažnije informacije se smanjuje za faktor 4.

Genetski algoritam: Genetski algoritam je tehnika koja oponaša genetsku evoluciju kao svoj model za rešavanje problema. Dati problem se smatra ulazom, a rešenja su kodirana prema određenom obrascu. Funkcija fitnesa procenjuje svako rešenje kandidata, većina kojih je izabrana nasumično. Evolucija počinje od potpuno nasumičnog skupa entiteta i ponavlja se u narednim generacijama. Najprikladniji, a ne najbolji, se biraju u svakoj generaciji. Upotreba genetskog algoritma ima za cilj poboljšanje kvaliteta slike.

Algoritam za ugrađivanje:

1. Podeliti pokrivačku sliku na blokove veličine 4×4.
2. Pronaći predstavu u frekvencijskom domenu blokova pomoću 2D Haar diskretne talasne transformacije i dobiti četiri podpojasa: LL1, HL1, LH1 i HH1.
3. Generisati 16 gena koji sadrže brojeve piksela svakog 4×4 bloka kao funkciju mapiranja.
4. Ugraditi bitove poruke u k-najmanje značajne bitove (LSBs) DWT koeficijenata svakog piksela prema funkciji mapiranja. Za odabir vrednosti k, slike se procenjuju za k=3 do 6. K jednako 1 ili 2 pruža nizak kapacitet skrivanja uz visok vizuelni kvalitet stego slike, dok k jednako 7 ili 8 pruža nizak vizuelni kvalitet uz visok kapacitet skrivanja.
5. Izvršiti evaluaciju fitnesa kako bi se izabrala najbolja funkcija mapiranja.
6. Primeniti proces optimalnog prilagođavanja piksela na sliku.
7. Izračunati inverznu 2D-HDWT na svakom 4×4 bloku.

Algoritam ekstrakcije:

1. Podeliti pokrivačku sliku na blokove veličine 4×4.
2. Ekstrahovati koeficijente u transformacionom domenu pomoću 2D HDWT za svaki 4×4 blok.
3. Koristiti funkciju mapiranja dobijenu u fazi ugrađivanja i pronaći sekvence piksela za ekstrakciju.
4. Ekstrahovati k-najmanje značajne bitove (LSBs) u svakom pikselu.

Ova tehnika povećava kapacitet i neprimetnost slike nakon ugrađivanja. Upotreba GA očuva lokalne osobine slike. OPAP se koristi za povećanje kapaciteta skrivanja algoritma u poređenju sa drugim sistemima. Međutim, ovom metodom se povećava računarska složenost. Kapacitet i neprimetnost slike se istovremeno povećavaju. Takođe, može se izabrati najbolja veličina bloka kako bi se smanjili troškovi obrade i povećao PSNR koristeći optimizacione algoritme poput genetskog algoritma.

Steganografija EKG signala zasnovana na talasima

Ibaida i saradnici [2] predstavili su tehniku steganografije zasnovanu na talasnoj transformaciji koja kombinuje enkripciju i tehniku šifrovanja kako bi zaštitila poverljive podatke pacijenata. Ova metoda omogućava EKG signalu da sakrije odgovarajuće poverljive podatke pacijenta i druge fiziološke informacije, čime se garantuje integracija između EKG-a i ostalih podataka.

Glavne karakteristike metode:

- Ova tehnika je hibrid između dve postojeće kategorije:
    1. Koristi steganografske tehnike za sakrivanje poverljivih informacija pacijenata unutar njihovog biomedicinskog signala.
    2. Uključuje model baziran na enkripciji kako bi omogućio samo ovlašćenim osobama da izvuku skrivene podatke.
- **EKG signal** se koristi kao glavni (host) signal za prenos poverljivih informacija pacijenta, kao i očitanja sa drugih senzora, poput temperature, nivoa glukoze, položaja i krvnog pritiska.
    1. EKG signal je odabran jer većina zdravstvenih sistema prikuplja ove informacije, a veličina EKG signala je znatno veća u poređenju sa veličinom drugih informacija.

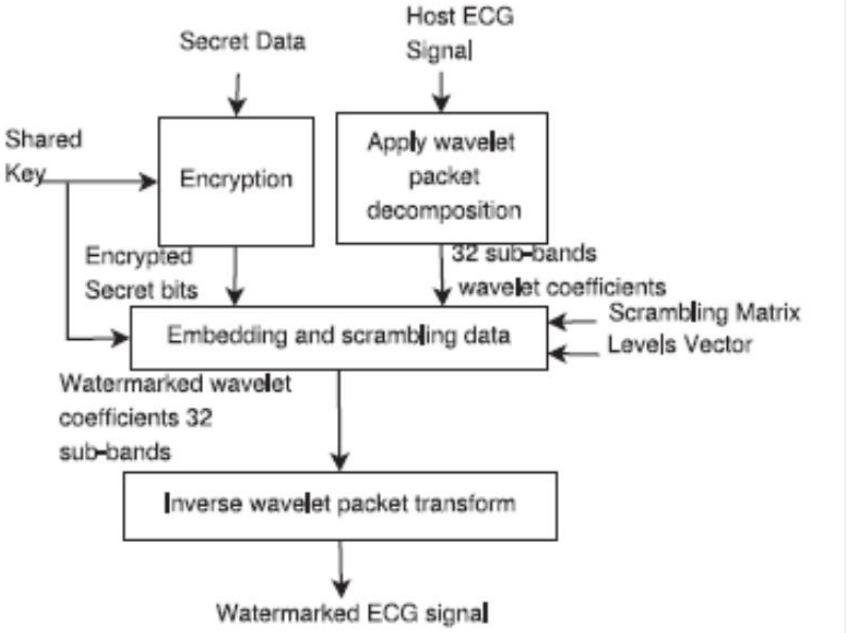
Proces:

1. **Prikupljanje podataka:**
   Telesni senzori beleže podatke o EKG-u, nivou glukoze, temperaturi, položaju i krvnom pritisku. Senzori šalju očitavanja pacijentovom PDA uređaju putem Bluetooth-a.
2. **Primena steganografije:**
   U PDA uređaju se primenjuje steganografska tehnika kojom se poverljivi podaci pacijenta i fiziološka očitavanja ugrađuju u EKG signal.
3. **Prenos podataka:**
   Vodeni žig (watermarked) EKG signal, koji sada sadrži skrivene informacije, šalje se na serverski sistem bolnice putem interneta.

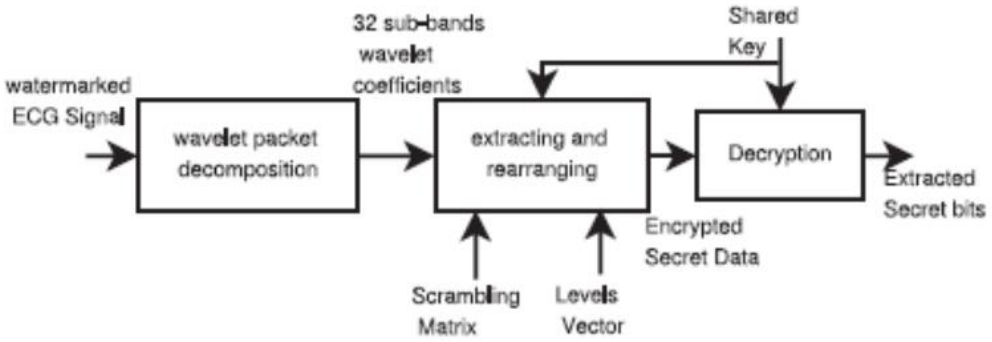
Prednosti:

- **Bez dodatnog povećanja veličine podataka:** Stvarna veličina prenesenih podataka ostaje ista kao veličina EKG signala, jer su ostale informacije skrivene unutar njega bez povećanja njegove veličine.

  Slika 7 prikazuje sistem za ugrađivanje.



Slika 7 : Blok dijagram steganografskog sistema pošiljaoca [6]



Slika 8: Blok šema steganografskog sistema prijemnika[7]

[6] https://ijireeice.com/wp-content/uploads/2016/07/nCORETech-38.pdf

[7] https://ijireeice.com/wp-content/uploads/2016/07/nCORETech-38.pdf

Na serverskom sistemu bolnice biće sačuvan EKG signal i skrivene informacije. Bilo koji lekar može videti EKG signal sa vodenim žigom, dok samo ovlašćeni lekari i određeno administrativno osoblje mogu izdvojiti skrivene informacije i pristupiti poverljivim podacima pacijenta, kao i drugim očitavanjima koja su sačuvana u glavnom EKG signalu. Slika 8 prikazuje proces izdvajanja.

Ova metoda garantuje minimalnu prihvatljivu distorziju EKG signala i obezbeđuje visok nivo sigurnosti. Tehnika blago utiče na kvalitet EKG signala, ali vodeni žig u EKG signalu i dalje omogućava njegovu upotrebu u dijagnostičke svrhe.

Optimizovana steganografija slike korišćenjem diskretne talasne transformacije

Parul i saradnici [3] predstavili su metodu steganografije slike zasnovanu na DWT (Diskretna Talasna Transformacija), u kojoj se pokrivačka slika deli na podopsege viših i nižih frekvencija, a podaci se ugrađuju u podopsege viših frekvencija. Arnoldova transformacija koristi se za povećanje sigurnosti.

U ovom pristupu DWT se koristi za dekompoziciju slike na podopsege viših i nižih frekvencija. Tajni podaci se transformišu koristeći Arnoldovu transformaciju. Tajna slika se deli na RGB komponente, koje se zatim ugrađuju u HL podopseg RGB komponenti pokrivačke slike.

Proces ugrađivanja:

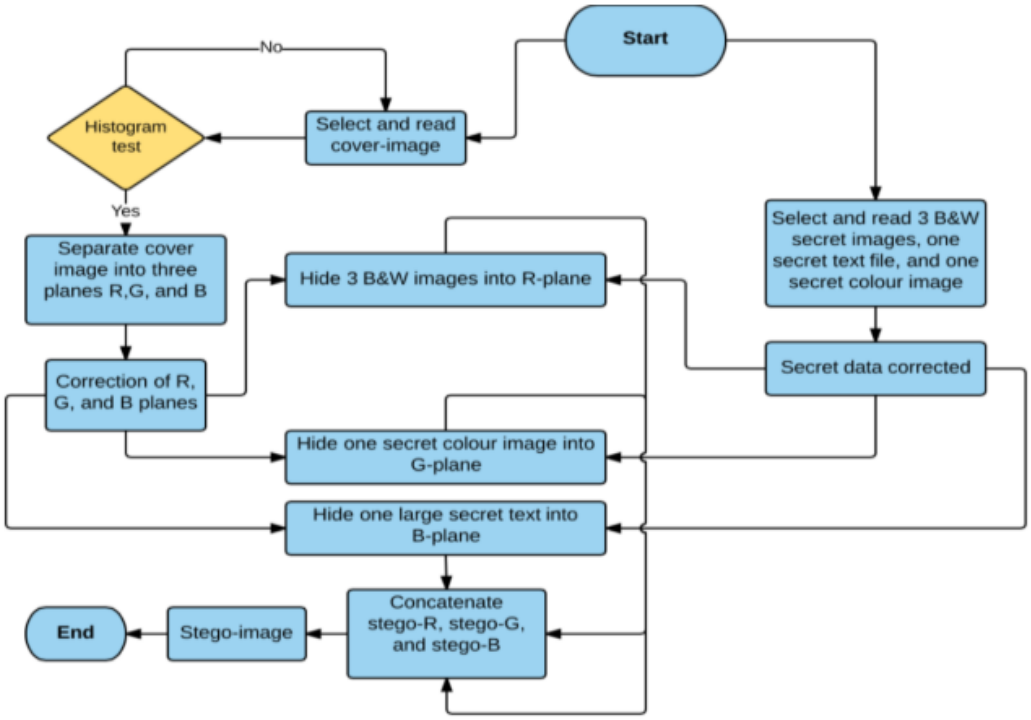
1. **Pokrivačka slika:**
   - Podeli se na RGB komponente.
   - Na svaku komponentu se primenjuje DWT, čime se dobijaju podopsezi (LL, HL, LH, HH).
2. **Tajna slika:**
   - Transformiše se pomoću Arnoldove transformacije.
   - Svaka boja tajne slike (R, G, B) se razdvaja.
3. **Ugradnja:**
   - Komponente tajne slike se ugrađuju u podopsege HL, HH i LH RGB komponenata pokrivačke slike.
4. **Obnavljanje stego slike:**
   - Primeni se inverzna DWT (IDWT) na pokrivačku sliku kako bi se dobila stego slika.

Postupak izdvajanja je obrnut procesu ugrađivanja.

Ova metoda steganografije pruža nekoliko ključnih prednosti. Prvo, postiže visok PSNR (odnos signal-šum), što znači da je vizuelni kvalitet stego slike bolji u poređenju sa drugim tehnikama. Pored toga, metoda omogućava visok kapacitet ugrađivanja, što znači da se veća količina tajnih podataka može sakriti unutar slike bez značajnog narušavanja njenog kvaliteta. Konačno, sigurnost podataka je dodatno povećana korišćenjem Arnoldove transformacije, koja komplikuje rekonstrukciju tajnih informacija za neovlašćene korisnike.

Steganografija slike visokog kapaciteta zasnovana na Haar DWT-u za skrivanje raznovrsnih podataka

Hamad A. A. i saradnici [4] su predložili tehniku steganografije visokog kapaciteta i efikasnosti, gde se binarne slike, slike u boji i veliki tekstualni fajlovi mogu svi sakriti unutar jedne nosilac slike istovremeno koristeći Haar talasnu transformaciju.

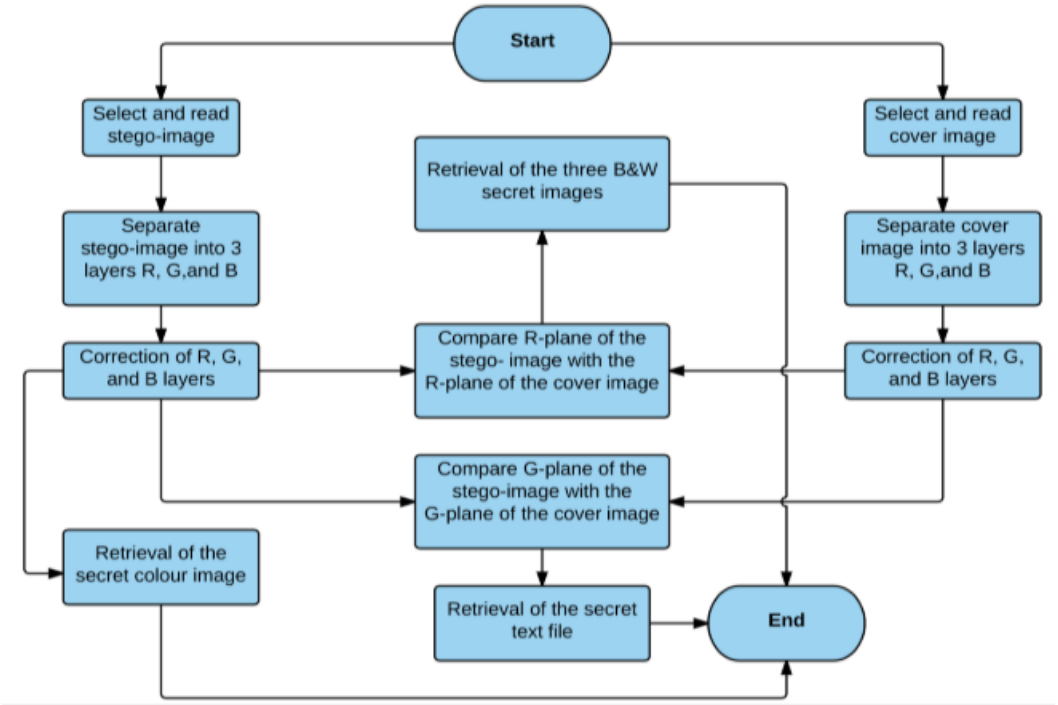


Slika 9: Proces enkripcije[8]

Proces enkripcije (Slika 9):

U ovoj tehnici koristi se Haar DWT za pretvaranje pokrivačke slike u četiri podopsega: aproksimativni (LL), vertikalni (HL), horizontalni (LH) i dijagonalni (HH) koeficijenti, koji predstavljaju niske i visoke frekvencije u različitim pravcima. Tajni podaci se koriguju i skrivaju u koeficijentima osim u aproksimativnim (LL) pomoću tehnike najmanje značajnog bita (LSB) i pseudo-slučajnog broja. Tehnika pseudo-slučajnog broja implementirana je za sakrivanje crno-belih slika, kao i tajnih tekstualnih fajlova. Kada se proces ugrađivanja završi, primenjuje se inverzna Haar DWT kako bi se formirala stego slika.

[8] https://ijireeice.com/wp-content/uploads/2016/07/nCORETech-38.pdf



Slika 10: Proces dekripcije[9]

Proces dekripcije (Slika 10):
Predložena tehnika steganografije omogućava visok kapacitet skrivanja podataka. Kapacitet je visok osim kod sakrivanja crno-belih slika, jer aproksimativni koeficijenti (LL), koji predstavljaju niske frekvencije u talasnoj transformaciji, nisu korišćeni za proces skrivanja. Međutim, kako kapacitet raste, PSNR opada, a MSE (srednja kvadratna greška) se povećava.

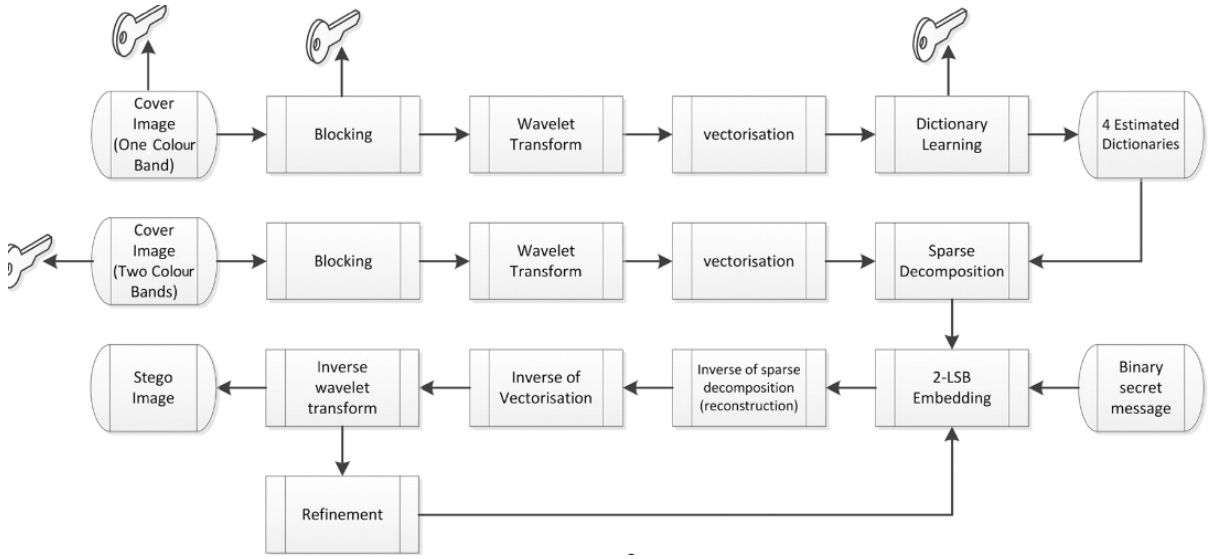
Metoda steganografije slike u boji zasnovana na retkoj reprezentaciji

Ahani i saradnici su predložili inovativan metod za sigurno skrivanje poruka unutar slika koristeći talasne transformacije. Ova tehnika temelji se na upotrebi retke reprezentacije u talasnom domenu, gde se podaci uklapaju u posebne, nepreklapajuće blokove dvodimenzionalne talasne transformacije u okviru boja. Metod koristi sve četiri podslike (grupe informacija) u okviru dvodimenzionalne talasne transformacije koje su povezane sa dve kolor trake, omogućavajući ugrađivanje podataka bez značajnog uticaja na vizuelni izgled slike.

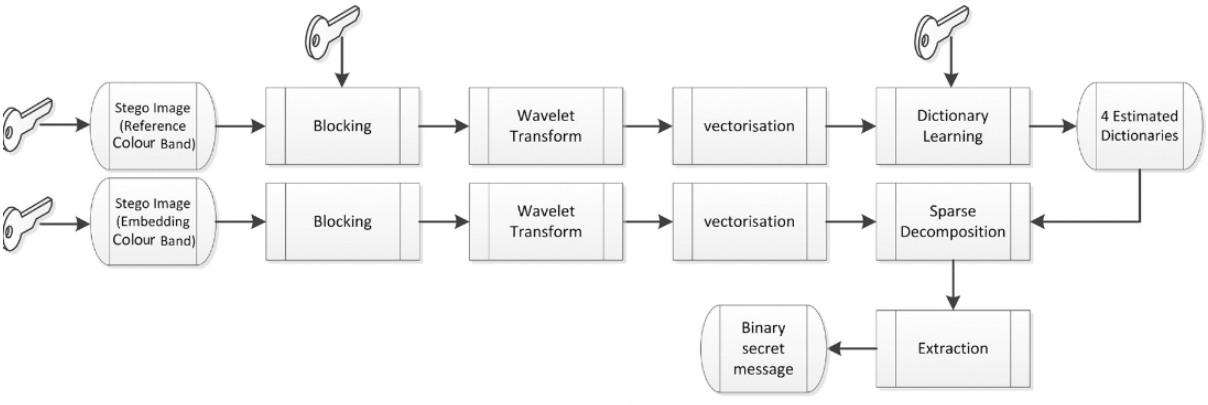
Da bi se smanjila verovatnost grešaka kod ekstrakcije ovih skrivenih podataka, predložena je nova procedura rafiniranja koja uklanja greške koje mogu nastati zbog različitih faktora kao što su zaokruživanje vrednosti, prelivanja i priroda aproksimacije u retkoj dekompoziciji. Ova procedura osigurava da skriveni podaci mogu biti ekstraktovani bez grešaka, čak i kod kompleksnih operacija u steganografiji.

[9] https://ijireeice.com/wp-content/uploads/2016/07/nCORETech-38.pdf

Ovaj metod je pokazao bolje performanse u poređenju sa mnogim drugim postojećim metodama steganografije koje se oslanjaju na transformacione tehnike. Konkretno, algoritam je uspeo da postigne viši prosečni PSNR (Peak Signal-to-Noise Ratio) kod stego slika, pri čemu su podaci skrivani uz istu stopu ugradnje. PSNR je važan pokazatelj jer meri kvalitet slike; viša vrednost znači da se kvalitet slike očuva uz minimalne promene.Osim toga, testirano je da li bi ovaj metod mogao biti otkriven od strane postojećih i moćnih steganografskih analiza. Rezultati su pokazali da je predloženi metod otporan na ove analize, tj. da ga nije moguće otkriti pomoću postojećih steganografskih tehnika. Ova otporna karakteristika čini metod sigurnijim i pouzdanijim za skrivanje podataka, posebno u aplikacijama gde je diskretnost ključna.



Slika 11: Blok dijagram procesa ugradnje[10]



Slika 12: Blok dijagram procesa ekstrakcije[11]

[10] https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/iet-ipr.2014.0351

[11] https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/iet-ipr.2014.0351

3. Primena DWT u steganografiji zasnovanoj na slici

Diskretna talasna transformacija (DWT) je popularna i efikasna metoda koja se koristi u steganografiji za umetanje skrivenih informacija unutar digitalnih slika. DWT omogućava da se tajni podaci implementiraju u oblasti frekvencije, čineći izmene manje vidljivim ljudskom oku i povećavajući otpornost na razne oblike napada i manipulacija.

U nastavku je prikazan proces implementacije DWT u steganografiji, uključujući ključne korake i prednosti ove tehnike:

Koraci u implementaciji DWT za steganografiju:

1. **Priprema slike i podataka:**

Na početku se priprema originalna (pokrivačka) slika i tajni podaci. Pokrivačka slika može biti siva ili u boji, ali se radi jednostavnosti često koristi sivotonska (grayscale) verzija. Tajni podaci mogu biti bilo kog tipa—tekst, binarni podaci ili druga slika.

Pre umetanja, tajni podaci se konvertuju u niz bitova. Za tekst, svaki karakter se pretvara u ASCII kod i dalje u binarni oblik. Za sliku, svaki piksel (0–255) se konvertuje u 8-bitnu binarnu reprezentaciju. Time se dobija jedinstven, linearan niz bitova koji treba ugraditi u koeficijente DWT.

2. **Primena DWT na originalnu sliku**:

Na pokrivačku sliku primenjuje se DWT, čime se slika dekomponuje na četiri podkomponente (LL, LH, HL, HH). LL sadrži niskofrekventne informacije i glavnu strukturu slike, dok LH, HL i HH predstavljaju detalje (horizontalne, vertikalne i dijagonalne visoke frekvencije).
Za steganografiju se uglavnom koriste LH, HL i HH komponente za umetanje podataka, jer su izmene u njima manje uočljive ljudskom oku. Transformacija u frekvencijsku oblast omogućava da se izmene „razliju“ preko finih detalja slike, umesto da direktno menjaju osnovne, lako vidljive strukture.

3. **Umetanje skrivene informacije**:

Kada su dobijeni DWT koeficijenti, tajni bitovi se umeću u jednu ili više visokofrekventnih podkomponenti. U konkretnom pristupu, umesto direktnog manipulisanja binarnim vrednostima (npr. brisanjem ili postavljanjem LSB-a prostim binarnim operacijama), pristupa se maloj numeričkoj izmeni koeficijenata.

Postupak je sledeći:

- DWT koeficijenti, koji su realne vrednosti, prvo se zaokružuju na najbliže celobrojne vrednosti.
- Svakom koeficijentu se posmatra najmanje značajan bit (LSB). Ako taj bit ne odgovara željenom tajnom bitu koji treba ugraditi, vrednost koeficijenta se neznatno promeni (poveća ili smanji za 1) tako da mu se LSB uskladi sa tajnim bitom.

Ovaj pristup menja koeficijent za najviše 1, što je izuzetno mala promena i neće dovesti do vidljivih razlika u rezultujućoj slici. Na ovaj način, tajni bitovi se „raspoređuju“ po koeficijentima, a minimalne izmene koeficijenata obezbeđuju da se vizuelna svojstva slike praktično ne menjaju.

4. **Inverzna DWT (IDWT)**:

Nakon umetanja svih tajnih bitova u odabrane podopsege, primenjuje se inverzna DWT. Ovim postupkom se koeficijenti ponovo spajaju i prevode nazad u prostornu oblast slike. Rezultat je stego slika koja izgleda gotovo identično originalnoj, a ipak sadrži tajne podatke skriveno raspoređene u DWT koeficijentima.

5. **Distribucija i detekcija**:

Stego slika se može sačuvati, poslati ili na drugi način distribuirati kao i svaka druga digitalna slika. Primalac koji zna metod (a možda i ključ, ako je primenjena neka vrsta šifrovanja) može ponovo primeniti DWT na primljenu sliku, dobiti slične podopsege koeficijenata, i odatle ekstrakcijom LSB bitova (i po potrebi dodatnim koracima) rekonstruisati skrivene informacije.

Prednosti korišćenja DWT u steganografiji:

Robusnost:DWT je veoma robustan, što znači da skrivena informacija ostaje zaštićena od gubitaka ili oštećenja tokom obrade slike. Ova robusnost dolazi od činjenice da se podaci ugrađuju u frekventne komponente slike, koje su otpornije na operacije poput kompresije, rezanja ili filtriranja.

Otpornost na kompresiju: Podaci skriveni u DWT koeficijentima su manje podložni gubitku tokom kompresije slike, kao što je JPEG kompresija, koja prvenstveno utiče na visoke frekvencije. Korišćenjem viših frekvencijskih komponenti za umetanje podataka, steganografski sistem može sačuvati skrivene informacije čak i nakon kompresije.

Otpornost na šum: Skriveni podaci često ostaju nepromenjeni ili minimalno promenjeni u slučaju šuma ili drugih oštećenja slike, zahvaljujući prirodi talasne transformacije.

Neprimetnost: Jedan od ključnih ciljeva steganografije je da informacije ostanu neprimetne. Korišćenjem viših frekventnih komponenti za umetanje podataka, DWT omogućava visoku vizuelnu kvalitetu slike, jer ljudsko oko nije osetljivo na promene u visokim frekvencijama. Promene u niskim frekvencijskim komponentama (LL) su lakše uočljive, dok promene u LH, HL i HH komponentama imaju manji uticaj na izgled slike.

Fleksibilnost: DWT omogućava fleksibilnost u umetanju informacija na različitim nivoima dekompozicije, što pruža veći kapacitet za skrivanje podataka i prilagodljivost specifičnim zahtevima aplikacije. Takođe, može se kombinovati sa drugim tehnikama, poput kriptografije i kvantisanja, čime se poboljšava sigurnost sistema.

Kapacitet: DWT omogućava veći kapacitet za umetanje podataka u poređenju sa nekim drugim metodama, poput LSB (Least Significant Bit) metode. Dekompozicija slike na više

frekventnih komponenti omogućava bolje iskorišćavanje prostora za umetanje skrivenih informacija, što povećava kapacitet sistema. Takođe, redundantne informacije mogu biti umetnute kako bi se povećala otpornost na gubitak podataka.

Sigurnost: DWT pruža složenost transformacije koja otežava otkrivanje skrivenih podataka bez odgovarajuće dekodirajuće procedure. Takođe, može se koristiti u kombinaciji sa kriptografijom, gde se podaci prvo šifruju pre nego što se umetnu u DWT koeficijente. Ovo dodaje dodatni sloj zaštite, jer čak i ako napadač otkrije skrivene podatke, njihova sadržina ostaje zaštić

Složenost transformacije i sigurnost
Proces primene diskretne talasne transformacije (DWT) i umetanja podataka u različite frekvencijske komponente slike dodaje složenost u detekciji skrivenih informacija. Zbog ove složenosti, otkrivanje skrivenih podataka postaje znatno teže bez tačne dekodirajuće procedure. Ovo povećava sigurnost, jer napadač mora imati precizno znanje o tome kako su podaci umetnuti i kako ih izvući.

Kombinacija sa kriptografijom
DWT može biti efikasno kombinovan sa kriptografskim tehnikama. U ovom slučaju, podaci se prvo šifruju pre nego što se umetnu u DWT koeficijente. Ova kombinacija osigurava da, čak i ako napadač otkrije da su podaci skriveni, sadržaj tih podataka ostaje zaštićen zahvaljujući šifrovanju. Ovakva dvostruka zaštita povećva sigurnost sistema i čini ga otpornijim na napade.

4. Metodologija

U ovoj metodologiji detaljno će biti opisan pristup steganografiji zasnovan na diskretnoj talasnoj transformaciji (DWT), kao i implementacioni detalji korišćenih biblioteka i koda. Prikazani kod služi za skrivanje tajnih informacija (teksta ili slike) unutar druge, tzv. „cover“ slike, uz što manju vidljivost umetnutih podataka. Primena DWT omogućava da se umetanje podataka vrši u frekvencijskoj (transformacionoj) domeni, čime se smanjuje verovatnoća da će ljudsko oko primetiti razliku između originalne i stego slike.

U izloženom algoritmu i kodu primenjuju se standardne Python biblioteke: **pywt** za diskretnu talasnu transformaciju, **Pillow (PIL)** za obradu slika, i **numpy** za manipulaciju nizovima. Cilj je da, nakon transformacije slike u talasnu oblast, sakrijemo tajne bitove u određeni podopseg koeficijenata, a zatim izvršimo inverznu transformaciju i dobijemo konačnu stego sliku.

Biblioteke i okruženje

1. **PyWT (Python Wavelet Transforms)**:
   Biblioteka `pywt` omogućava jednostavnu primenu talasne transformacije i inverzne talasne transformacije na slike. Korišćenjem `pywt.dwt2` možemo dobiti talasne koeficijente slike, a pomoću `pywt.idwt2` rekonstruisati sliku iz tih koeficijenata. Primeri:

```
import pywt
coeffs2 = pywt.dwt2(cover_arr, 'haar')
# coeffs2 -> (LL, (LH, HL, HH))
stego_arr = pywt.idwt2(new_coeffs, 'haar')
```

Slika 13: a) Originalna slika b) Slika nakon 2d-haar-dwt

Izbor 'haar' talasa je zbog njegove jednostavnosti i dobre lokalizacije u vremenu i frekvenciji

2. **Pillow (PIL)**:
   `Pillow` je standardna biblioteka za rad sa slikama u Python-u. Omogućava:

   - Učitavanje slika raznih formata (PNG, JPEG, BMP...).
   - Prevođenje u različite modove (npr. `.convert('L')` za grayscale).
   - Spremanje rezultujuće slike u fajl.

   Na primer:

```
from PIL import Image
cover = Image.open(cover_image_path).convert('L')
# Učitava i konvertuje cover sliku u grayscale
stego_img = Image.fromarray(stego_arr)
stego_img.save(stego_image_path)
```

3. **Numpy**:
   `numpy` je ključna biblioteka za naučno računarstvo u Python-u, pruža efikasno rukovanje višedimenzionalnim nizovima. Slike se pretvaraju u numpy nizove radi lakše obrade piksela i koeficijenata. Primer:

   ```
   import numpy as np
   arr = np.array(img, dtype=np.uint8)
   ```

   Na ovaj način lako manipulišemo pikselima i koeficijentima.

Opis algoritma i koda

Postoje dve glavne verzije koda:

- Jedna za skrivanje tekstualne poruke u sliku.
- Druga za skrivanje jedne slike unutar druge slike.

Princip je veoma sličan: tajni sadržaj se konvertuje u binarni oblik (niz bitova), a zatim se ovi bitovi ugrađuju u koeficijente DWT podopsega slike-nosioca.

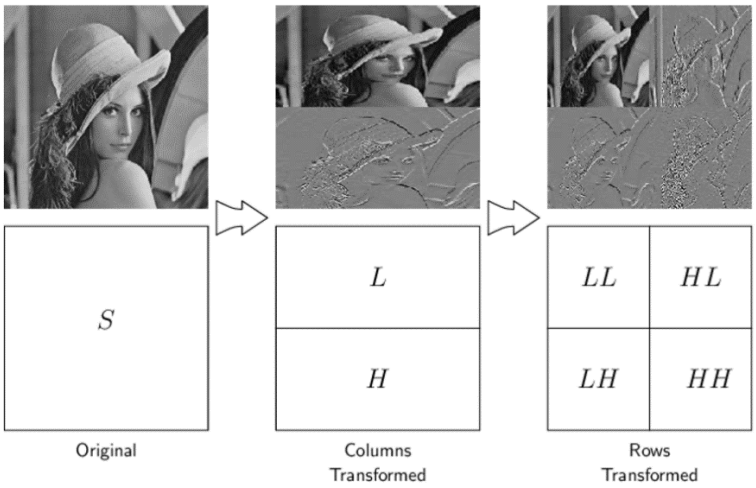
Glavni koraci su:

1. **Učitavanje i priprema cover slike**:
   Cover slika je osnovna slika u koju se ubacuju tajni podaci. Ona se učitava i konvertuje u grayscale mod. Grayscale pojednostavljuje obradu i uklanja potrebu za radom sa više kanala (kao što su R, G, B).

   ```
   cover = Image.open(cover_image_path).convert('L')
   cover_arr = np.array(cover, dtype=np.float32)
   ```

2. **Primena DWT-a na cover sliku**:
   Koristeći `pywt.dwt2`, slika se transformiše u talasnu oblast i dobijamo četiri podniza koeficijenata (LL, LH, HL, HH):

   ```
   coeffs2 = pywt.dwt2(cover_arr, 'haar')
   LL, (LH, HL, HH) = coeffs2
   ```



Slika14: Primena dwt na cover-sliku

3. **Priprema tajne poruke ili tajne slike u bitove**:

   Za tekst:
   Svaki karakter se pretvara u ASCII vrednost, zatim u binarni niz od 8 bitova. Cela poruka tako postaje dugi niz bitova.

   Za sliku:
   Tajna slika se takođe konvertuje u grayscale i pretvori u numpy niz. Za svaki piksel (0 do 255) dobija se 8-bitna reprezentacija. Osim pikselnih podataka, pre umetanja se u bitove kodiraju i širina i visina tajne slike (npr. 16 bita za širinu i 16 bita za visinu), kako bi se pri ekstrakciji znalo koliko podataka treba pročitati.

   Na primer, za tajnu sliku:

```
w, h, secret_bits = image_to_bits(secret_image_path)
width_bits = int_to_bits(w, 16)
height_bits = int_to_bits(h, 16)
all_bits = width_bits + height_bits + secret_bits
```

4. **Umetanje bitova u DWT koeficijente**:
   Nakon što imamo niz bitova tajnih podataka, ti bitovi se ubacuju u podopseg koeficijenata (npr. LH). Svaki koeficijent se malo prilagodi tako da njegov LSB (least significant bit) odgovara željenom bitu tajnih podataka.

   Funkcija `embed_bits_in_coefficients` radi sledeće:

   - Spljoštava koeficijente u jednodimenzioni niz.
   - Za svaki bit iz tajnog niza upoređuje LSB koeficijenta. Ako se ne poklapa, vrednost koeficijenta se poveća ili smanji za 1 da bi se LSB promenio.
   - Nakon ovog postupka, koeficijenti imaju ugrađene tajne bitove.

Na primer:

```
def embed_bits_in_coefficients(coeffs, bits):
    flat = coeffs.flatten()
    for i, bit in enumerate(bits):
        val = flat[i]
        if (val % 2) != bit:
            val = val - 1 if (val % 2 == 1) else val + 1
        flat[i] = val
    return flat.reshape(coeffs.shape)
```

5. **Inverzna DWT i rekonstrukcija stego slike**:
   Nakon umetanja tajnih bitova, novi koeficijenti se vraćaju u strukturu (LL, (LH_modified, HL, HH)) i primenjuje se inverzna DWT:

   ```
   stego_arr = pywt.idwt2(new_coeffs, 'haar')
   stego_arr = np.clip(stego_arr, 0, 255).astype(np.uint8)
   stego_img = Image.fromarray(stego_arr)
   stego_img.save(stego_image_path)
   ```

   Rezultat je stego slika, vizuelno slična originalnoj.

6. **Ekstrakcija tajnih podataka**: Da bi se izdvojili tajni podaci, postupa se obrnuto:

   - Učita se stego slika i konvertuje u grayscale.
   - Primeni se DWT, dobije se LH (ili drugi podopseg) koji sadrži skrivene bitove.
   - Iz koeficijenata se pročita odgovarajući broj bitova.
   - Za tekstualnu poruku, ako znamo dužinu poruke, znamo i koliko bitova čitati (broj_karaktera * 8).
   - Za tajnu sliku, prvo se pročita širina i visina (16 + 16 = 32 bita), a zatim se izvuče onoliko bitova koliko je potrebno za sve piksele (w*h*8 bita).
   - Pošto se bitovi izdvoje, pretvaraju se nazad u znakove ili piksele. Za piksele, `bits_to_image` funkcija sklapa sliku iz dobijenih bitova.

Tačnosti i potencijalni problemi

Kao što je spomenuto, DWT koristi realne brojeve. Za ugrađivanje bitova u koeficijente ponekad se koriste `round()` ili `rint()` kako bi se obezbedilo da koeficijenti budu približno celobrojni i da možemo jednostavno manipulisati LSB-om. Ovo može dovesti do blagih odstupanja pri rekonstrukciji, ali u većini slučajeva su ta odstupanja minimalna i ne utiču drastično na vidljivost ili čitljivost tajnih podataka.

Takođe, kapacitet za umetanje zavisi od veličine slike-nosioca i veličine odabranog podopsega. Ako je tajna poruka ili slika prevelika, možda neće stati u raspoložive koeficijente. Kod sadrži proveru i izbacuje grešku ako nema dovoljno kapaciteta.

Za još bolji kvalitet i manje šuma, mogu se uvesti dodatne tehnike:

- Skaliranje koeficijenata pre umetanja.
- Korišćenje višestrukih podopsega za raspodelu podataka.
- Primena integer wavelet transformacije (lifting šema) kako bi se izbegli problemi sa zaokruživanjem realnih brojeva.

Primeri korišćenja

Skrivanje teksta:

- Pretpostavimo da imamo cover sliku "lenna.png" i tajnu poruku "Hello, this is a secret!".
- Pozovemo:

```
embed_message_in_image("lenna.png", "Hello, this is a secret!", "stego_text.png")
```

- Dobićemo "stego_text.png" koja sadrži tajnu poruku.
- Za izdvajanje:

```
extracted_msg=extract_message_from_image("stego_text.png", len("Hello, this is a secret!"))
```

- `extracted_msg` će sadržati originalni tekst.

Skrivanje slike:

- Imamo cover sliku npr. "lenna.png" (512x512), i tajnu sliku npr. "delfin64.png" (64x64).
- Pozovemo:

```
embed_image_in_image("lenna.png", "delfin64.png", "stego_image.png")
```

- Dobijamo "stego_image.png" sa skrivenom slikom.
- Ekstrakcija:

```
extracted_img = extract_image_from_image("stego_image.png")
extracted_img.save("extracted_secret.png")
```

- Rezultat je "extracted_secret.png" koja reprodukuje originalnu tajnu sliku.

Prikazani pristup iskorišćava DWT da bi se tajni podaci skrili u manje primetnim komponentama slike. Korišćenjem biblioteka `pywt`, `Pillow` i `numpy` implementacija je pojednostavljena:

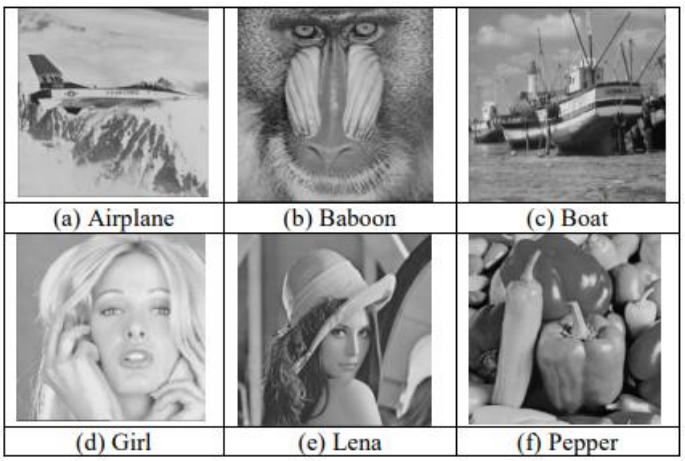
- `pywt` za direktnu i inverznu talasnu transformaciju.
- `Pillow` za rad sa slikama i njihovu konverziju između različitih formata i modova.
- `numpy` za efikasno rukovanje podacima i manipulaciju pikselima i koeficijentima.

Ova metodologija prikazuje osnovni koncept, ali se lako može proširiti i poboljšati. Može se uvesti kriptografija za dodatnu sigurnost, naprednije tehnike umetanja (višeslojni DWT, različiti talasi, robustni embedding šematski pristupi), ili upotreba integer DWT za stabilnije rezultate. Ipak, i u ovom obliku metodologija dovoljno jasno ilustruje korake, korišćenje biblioteka i način na koji se steganografija može implementirati u transformacionoj domeni.

5. Eksperimentalni podaci i analiza performansi DWT steganografije

Eksperimentalni Podaci

Eksperimenti su sprovedeni na šest standardnih test slika: „Airplane“, „Baboon“, „Boat“, „Girl“, „Lena“ i „Pepper“. Sve slike su dimenzija 512×512 piksela i predstavljaju sive slike sa 8-bitnom dubinom. Rezultati su analizirani za dva režima rada: **promenljivi režim** i **fiksni režim**, sa fokusom na kapacitet umetanja podataka i očuvanje kvaliteta slike, izraženog kroz PSNR.



Kapacitet i PSNR u promenljivom režimu

Algoritam je prilagođen tako da omogućava umetanje podataka u različitim kapacitetima, pri čemu je analiziran uticaj umetanja na kvalitet slike. Tri scenarija umetanja podataka analizirana su u promenljivom režimu:

- **Nizak kapacitet (Slučaj 1)**: Mali broj bitova se umeće po pikselu, što omogućava maksimalno očuvanje vizuelnog kvaliteta slike sa PSNR vrednostima iznad 50 dB.
- **Srednji kapacitet (Slučaj 2)**: Umeće se veći broj bitova u skladu sa kompromisom između steganografskih zahteva i vizuelnog kvaliteta slike. PSNR vrednosti u ovom režimu su između 46 i 48 dB.
- **Visok kapacitet (Slučaj 3)**: Najveći broj bitova se umeće, što omogućava veći kapacitet umetanja, ali može rezultirati smanjenjem PSNR vrednosti do oko 44 dB. Ovaj režim je koristan u situacijama gde je skrivanje podataka prioritet.

Promenljivi režim pruža fleksibilnost korisnicima koji mogu da odaberu odgovarajući nivo umetanja podataka prema svojim potrebama, u zavisnosti od zahteva kvaliteta slike i količine podataka za skrivanje.

Slika	Slučaj 1 (Nizak kapacitet)	Slučaj 2 (Srednji kapacitet)	Slučaj 3 (Visok kapacitet)
Airplane	376,710	507,856	573,206
Baboon	376,835	507,670	573,392
Boat	376,598	507,867	573,318
Girl	377,038	507,940	573,422
Lena	376,942	507,856	573,550
Pepper	377,125	507,946	573,184

Tabela 1: Kapacitet umetanja podataka (u bitovima)[12]

PSNR (Peak Signal-to-Noise Ratio) je merna jedinica koja se koristi za procenu kvaliteta slike nakon obrade. Što je PSNR vrednost viša, to znači da su promene na slici minimalne i da su umetanje podataka i kvalitet slike gotovo neprimetni. PSNR vrednosti iznad 50 dB ukazuju na vrlo visok kvalitet slike, dok vrednosti oko 40–45 dB ukazuju na umeren kvalitet.

Slika	Slučaj 1 (Nizak kapacitet)	Slučaj 2 (Srednji kapacitet)	Slučaj 3 (Visok kapacitet)
Airplane	50.86	46.00	44.77
Baboon	50.76	46.19	44.97
Boat	50.75	46.14	44.93
Girl	50.77	46.08	44.88
Lena	50.80	46.09	44.90
Pepper	50.80	46.08	44.90

Tabela 2: PSNR vrednosti (u dB)[13]

[12] https://gigvvy.com/journals/ijase/articles/ijase-200612-4-3-275.pdf

PSNR u Fiksnom Režimu

Ovaj pristup je koristan kada je potrebno održati doslednost u umetanju podataka, bez obzira na specifične karakteristike pojedinačnih slika. U fiksnom režimu, umetanje podataka ima unapred definisanu količinu (u ovom slučaju **524,288 bita**) po svakoj slici (256×256 piksela ×4 bita po pikselu ×2 sub-opsega).

- 256×256: Predstavlja dimenziju slike u pikselima, tj. 256×256256 \times 256256×256.
- 444: Broj bitova po pikselu koji se umeću.
- 222: Broj pod-opsega (sub-opsega) u okviru diskretne talasne transformacije (DWT).

Slika	Slučaj 1 PSNR (u dB)	Slučaj 2 PSNR (u dB)
Airplane	43.22	46.75
Baboon	39.00	46.54
Boat	42.38	46.72
Girl	42.78	46.81
Lena	43.27	46.84
Pepper	43.45	46.78

Tabela 3: PSNR vrednosti u fiksno[14]m režimu

Analiza Performansi

Eksperimentalni rezultati ukazuju na nekoliko ključnih karakteristika predložene metode.

1. **Kapacitet umetanja podataka**

Promenljivi režim pruža fleksibilnost u pogledu umetanja podataka:

- **Nizak kapacitet (Slučaj 1):** Metoda omogućava umetanje približno 376,000 bita, uz minimalan uticaj na kvalitet slike (PSNR > 50 dB).
- **Srednji kapacitet (Slučaj 2):** Kapacitet raste na preko 507,000 bita, uz očuvanje visokog kvaliteta slike (PSNR ~46 dB).
- **Visok kapacitet (Slučaj 3):** Maksimalan kapacitet umetanja doseže do 573,000 bita, pri čemu PSNR ostaje iznad 44 dB, što je još uvek prihvatljivo za većinu vizuelnih aplikacija.

U fiksnom režimu, kapacitet je ograničen, ali se postiže viši PSNR zbog strožih kriterijuma umetanja.

[14] https://gigvvy.com/journals/ijase/articles/ijase-200612-4-3-275.pdf

2. Kvalitet slike

PSNR vrednosti potvrđuju da predložena metoda očuva vizuelni kvalitet slike čak i pri visokom kapacitetu umetanja. Uslov očuvanja niskofrekventnog podopsega (LL) netaknutim doprinosi očuvanju kvaliteta, jer LL sadrži najveći deo informacija o slici koje su važne za ljudsku percepciju.Na primer:

- Za sliku „Airplane“, PSNR u slučaju visokog kapaciteta je 44.77 dB, dok je za nizak kapacitet impresivnih 50.86 dB.
- Slični rezultati primećeni su za sve ostale test slike, sa malim varijacijama u zavisnosti od teksture slike (slika „Baboon“ ima niži PSNR zbog složenosti teksture).

3. Bezbednost

Predloženi algoritam koristi ključnu matricu za očuvanje sigurnosti i tačno izdvajanje podataka, dok umetanje u visokofrekventne podopsege smanjuje uticaj na vizuelni kvalitet slike.

4. Efikasnost u visokofrekventnim opsezima

Predložena metoda umetanja u visokofrekventne opsege (HL, LH, HH) efikasno koristi karakteristike talasne transformacije. Ovo smanjuje uticaj na vizuelni kvalitet slike, jer ljudska percepcija nije toliko osetljiva na promene u ovim opsezima.

5. Poređenje sa drugim metodama

Kada se uporedi sa metodama poput „Side Match“ steganografije, predložena metoda postiže bolje PSNR vrednosti pri istom kapacitetu umetanja, kako je prikazano u Tabeli 4.Side Match je jedna od popularnih tehnika steganografije koja se koristi za umetanje podataka u digitalne slike na način koji minimizuje uticaj na vizuelni kvalitet slike. Ova tehnika se zasniva na analizama susednih piksela u slici i njihovoj vrednosti kako bi se umetnuli podaci na način koji smanjuje mogućnost otkrivanja skrivenih informacija.

Slika	Metoda	PSNR (dB)	Kapacitet (bitovi)
Lena	Side Match	45.03	267,242
Lena	Predložena	52.78	267,242
Baboon	Side Match	34.93	483,758
Baboon	Predložena	46.74	483,758

Tabela 4: Poređenje sa metodom „Side M[15]atch“

Predložena metoda nadmašuje „Side Match“ metod u pogledu očuvanja kvaliteta slike, posebno za složene teksture poput slike „Baboon“.

[15] https://gigvvy.com/journals/ijase/articles/ijase-200612-4-3-275.pdf

6. Zaključak

Diskretna talasna transformacija (DWT) predstavlja veoma moćan alat u oblasti steganografije zasnovane na slikama zbog svoje sposobnosti skrivanja podataka u frekvencijskim opsezima uz minimalan uticaj na vizuelni kvalitet. Ipak, primena DWT u steganografiji suočava se sa različitim tehničkim i bezbednosnim izazovima. Tehnički izazovi uključuju visoku računarsku složenost kod obrade slika visoke rezolucije ili primene složenih dekompozicija, kao i ograničenja u kapacitetu skrivenih podataka usled veličine slike i odabranih frekvencijskih komponenti. Takođe, manipulacije slikama kao što su komprimovanje ili promene osvetljenja mogu oštetiti umetnute informacije, smanjujući efikasnost ekstrakcije.

Pored tehničkih izazova, postoje i značajni bezbednosni rizici koji mogu ugroziti integritet i sigurnost podataka. Otkrivanje skrivenih informacija ostaje potencijalna pretnja, s obzirom na to da napadači mogu koristiti analize statistike ili frekvencijskih obrazaca za detekciju umetnutih podataka. Dodatni rizici uključuju pokušaje manipulacije skrivenih podataka, ugrožavanje enkripcijskih ključeva, kao i sofisticirane napade koji ciljaju steganografske tehnike. Zbog toga su potrebni stalni napori za unapređenje metoda enkripcije, autentifikacije i zaštite integriteta informacija.

Rešenja za prevazilaženje ovih izazova uključuju optimizaciju algoritama DWT za smanjenje računarskih zahteva, primenu paralelnog računanja ili specijalizovanih hardverskih rešenja. Takođe, kombinacija DWT sa metodama za otklanjanje osetljivosti na manipulacije slikama, kao što su redundante reprezentacije, može poboljšati otpornost sistema. Osim toga, upotreba jakih kriptografskih protokola za zaštitu enkripcijskih ključeva i kontinuirano unapređenje tehnika steganografije ključni su koraci u odgovoru na napredne napade. Ovi pristupi naglašavaju potrebu za sveobuhvatnim i integrisanim pristupom u rešavanju izazova DWT steganografije kako bi se obezbedila sigurnost, integritet i neprimetnost skrivenih informacija u digitalnim slikama.

7. Reference

Literatura i izvori

1. E. Ghasemi, J. Shanbehzadeh, N. Fassihi, “High Capacity Image Steganography using Wavelet Transform and Genetic Algorithm”, Proc. IMECS, 2011.
2. A. Ibaida, I. Khalil, “Wavelet Based ECG Steganography for Protecting Patient Confidential Information in Point-of-Care Systems”, IEEE Trans. Of Biomed. Eng., vol. 60, pp. 3322-3330, Dec. 2013.
3. Parul, Manju, Harish Rohil, “Optimised Image Steganography using Discrete Wavelet Transform”, Int. Journal of Recent Development in Eng and Tech., vol. 2, pp. 75–81, Feb. 2014.
4. Hamad A. A, Ali A, Majid A. A, Waleed A, “High Capacity Image Steganography Based on Haar DWT for Hiding Miscellaneous Data”, IEEE Jordan Conf. on Applied Electrical Eng. and Comp. Tech., March 2015
5. S.Ahani, S. Ghaemmaghami, “Colour Image Steganography Method Based on Sparse Representation”, IET Image Process, vol. 9, pp. 496-505, 2015.
6. A. Westfeld, "F5—a steganographic algorithm," Proceedings of the 4th International Workshop on Information Hiding, Springer-Verlag, 2001.
7. R. Chandramouli, N. Memon, "Analysis of LSB based image steganography techniques," Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing, 2001.
8. M. K. Khan, H. Shah, "A survey on DWT based digital image watermarking techniques," Journal of Digital Imaging, vol. 26, no. 3, pp. 378-390, 2013.
9. N. Provos, P. Honeyman, "Hide and seek: An introduction to steganography," IEEE Security & Privacy, vol. 1, no. 3, pp. 32-44, 2003.
10. J. Fridrich, M. Goljan, R. Du, "Reliable detection of LSB steganography in grayscale and color images," IEEE Transactions on Image Processing, vol. 15, no. 10, pp. 2859-2871, 2006.