UNIVERZITET U NIŠU

ELEKTRONSKI FAKULTET

**Hibridni metod steganografije na bazi LSB i phase coding metoda**

Seminarski rad

Studijski program: Računarstvo i informatika

|  |  |
| --- | --- |
| Student: | Profesor: |
| Marko Stanković, 1705 | Dr Bratislav Predić |

Modul: Softversko inženjerstvo

Niš, februar 2024. godina

**SADRŽAJ**

[**1. UVOD** 3](#_Toc157625437)

[**2. STEGANOGRAFIJA SLIKA** 4](#_Toc157625438)

[2.1 Tehnike steganografije slika 4](#_Toc157625439)

[**3. HIBRIDNE TEHNIKE STEGANOGRAFIJE** 6](#_Toc157625440)

[3.1 Pregled dostupnih hibridnih rešenja 6](#_Toc157625441)

[3.2 Razmatrano rešenje 7](#_Toc157625442)

[**4. UMETANJE BITOVA NAJMANJE TEŽINE – LSB** 9](#_Toc157625443)

[4.1 LSB tehnika u različitim formatima rasterskih slika 10](#_Toc157625444)

[**5. PHASE CODING TEHNIKA** 14](#_Toc157625445)

[5.1 Audio steganografija 14](#_Toc157625446)

[5.2 Način funkcionisanja phase coding tehnike 15](#_Toc157625447)

[**6. PRAKTIČNO REŠENJE** 18](#_Toc157625448)

[**7. ZAKLJUČAK** 23](#_Toc157625449)

# **1. UVOD**

Jedno od najvećih dostignuća ljudske civilizacije bilo je uspostavljanje tajne komunikacije. Često su se tokom velikih takmičenja, bitaka, pa čak i celih ratova, ishodi odlučivali zahvaljujući prikrivenom prenosu poruka i informacija. Kada je na kocki toliko toga, kao što je cela ratna situacija, nije iznenađujuće da se veliki trud ulaže u razvoj tajne komunikacije, ali i u njeno otkrivanje. Često se dešava da strana koja prva razotkrije algoritam tajne komunikacije protivnika odnosi pobedu.

Danas, dve naučne discipline se koriste za sakrivanje komunikacije, kriptografija i steganografija. Ove discipline su jako slične po svojoj svrsi, ali se razlikuju po principima i prirodi. Steganografija podrazumeva skrivanje tajne poruke unutar pokrivajućeg medija, personifikujući ideju pokrivenog pisanja. Cilj steganografije je da unese sumnju i spreči otkrivanje poverljivih informacija. Steganografija, iako manje popularna od kriptografije, obično očuva strukturu podataka. Sa druge strane, kriptografija, ili tajno pisanje, funkcioniše drugačije. Umesto da pošalje poruku direktno primaocu, pošiljalac transformiše informacije ili običan tekst u šifrovan tekst koristeći određeni algoritam za šifrovanje, zatim šalje primaocu, a primalac dešifruje šifrovani tekst u običan tekst kako bi pročitao originalne informacije [1]. Uopšteno govoreći, steganografija se fokusira na skrivanje tajnih poruka unutar nosača na neprimetan i nenametljiv način. Gotovo svaki digitalni format fajla može poslužiti kao nosač, ali najpogodniji su oni koji imaju visok stepen redundantnosti. Postoje različite metode i algoritmi za skrivanje podataka u različitim vrstama digitalnih formata fajlova. U zavisnosti od tipa medija u kojima se poruka sakriva razlikujemo sledeće tipove steganografije:

1. ***Tekstualna steganografija*** – tajna poruka se skriva unutar teksta. Ovo se može postići različitim sredstvima, poput korišćenja prvog slova svake rečenice, unošenja značajnih grešaka ili kodiranja informacija putem interpunkcije.

2. ***Steganografija slike*** – uključuje kodiranje tajnih informacija unutar digitalne slike. Ova tehnika se oslanja na nemogućnost ljudskog oka u detektovanju malih promena u boji ili šumu unutar slike. Na primer, jedna slika može biti sakrivena unutar druge korišćenjem najmanje značajnih bitova svakog piksela za predstavljanje skrivene slike.

3. ***Video steganografija*** – koristi sličan koncept, omogućavajući kodiranje celih video-zapisa. Pošto se digitalni video-zapisi predstavljaju kao niz uzastopnih slika, svaki frejm videa može kodirati zasebnu sliku, stvarajući koherentan skriveni video pred očima.

4. ***Audio steganografija*** – audio fajlovi služe kao nosači za skrivene informacije. Tehnike variraju od jednostavnog „backmasking“-a, gde se poruke reprodukuju unazad, do složenijih metoda koje uključuju najmanje značajne bitove svakog bajta u audio fajlu, slično kao u steganografiji slike.

5. ***Mrežna steganografija*** – lukavo skriva informacije unutar saobraćaja na mreži. Ovo uključuje skrivanje podataka unutar TCP/IP zaglavlja ili payload-a mrežnih paketa. Pošiljalac čak može preneti informacije na osnovu vremenskih razmaka između slanja različitih paketa.

Svaka vrsta steganografije pruža jedinstveni pristup tajnom komuniciranju, koristeći karakteristike različitih vrsta podataka kako bi bezbedno skrila i prenela informacije [2]. U ovom radu ćemo se zadržati na steganografiji slika i razmotriti primenu hibridnih metoda stegonagrafije kroz primenu LSB tehnike, odnosno tehnike zamene bita najmanje težine u kombinaciji sa „phase coding” metodom, koja je nešto popularnija u audio steganografiji.

# **2. STEGANOGRAFIJA SLIKA**

U savremenom svetu, digitalne slike su prisutne na gotovo svakoj internet stranici zbog jednostavnosti distribucije. Zbog toga su fajlovi slika postali najčešće korišćeni nosači u steganografskim aplikacijama, iako se njihova upotreba razlikuje u skladu sa različitim formatima. Ljudski vizualni sistem pokazuje određene slabosti, specifično nisku osetljivost prema promenama u nasumičnim obrascima i sjaju. Ove karakteristike čine ljudsko oko nesposobnim da primeti suptilne promene u boji ili uzorcima, što omogućava da se tekstualni ili grafički fajlovi neprimetno ubace u sliku koja je nosač informacije.

Na primer, kada se tekst kodira i skladišti unutar slike, rezultira se stvaranjem druge slike, poznate kao „stego slika“. Ova slika se fizički i vizuelno razlikuje od originalne slike. Kada dolazi do komunikacije između dve strane, prisluškivač vidi samo sliku koja se prenosi, ali nije svestan da se zapravo odvija skrivena komunikacija putem te slike.

Važno je napomenuti da je slika zapravo kolekcija pojedinačnih tačaka, nazvanih pikseli, koji čine različite intenzitete svetlosti u različitim delovima slike. Pikseli su predstavljeni horizontalno, red po red, a različite šeme boja koriste različit broj bitova za svaki piksel, poznatih kao dubina bita. Na primer, najmanja dubina bita u trenutnim šemama boja iznosi 8, što znači da se koristi 8 bitova za predstavljanje boje svakog piksela (odgovarajući 2^8 = 256 boja). U crno-belim i sivim slikama koristi se 8 bitova za svaki piksel i mogu prikazati 256 različitih nijansi sive. S druge strane, digitalne slike u boji koriste 24 bita za svaki piksel i koriste RGB model boja, poznat i kao prava boja [3].

## 2.1 Tehnike steganografije slika

U oblasti steganografije slika, različite metodologije su osmišljene za skrivanje informacija unutar slika, svaka svrstana u određene kategorije. Ove kategorije obuhvataju kompleksnosti prostorne manipulacije, širenje spektra, statističke promene, transformacione procese, tehnike distorzije i strategije maskiranja/filtriranja [4].

* ***Metodi prostornog domena***: Jedan značajan pravac podrazumeva direktnu manipulaciju vrednostima piksela u pokrivačkoj slici kako bi se diskretno ugradili tajni podaci. Ova prostorna manipulacija podrazumeva modifikaciju određenih vrednosti piksela tokom procesa skrivanja podataka. Razvijeno je više metoda prostornog domena, kao što su metoda umetanja najmanje značajnog bita (LSB), steganografija zasnovana na boji, metode zasnovane na mapiranju, tehnika diferenciranja vrednosti piksela, ugradnja podataka u regione ivica, metoda slučajnog umetanja vrednosti piksela (RPE) i steganografija putem metode kolaža.
* ***Tehnika širenja spektra***: Tehnika širenja spektra predstavlja osnovu za steganografiju širenjem spektra. U ovom pristupu, tajni podaci predviđeni za umetanje distribuiraju se širom celokupnog frekvencijskog opsega. Održavanje niskog odnosa signala prema šumu u svakom frekvencijskom opsegu stvara izazov u otkrivanju skrivenih podataka. Njegova robusna priroda dovela je do široke primene u vojne svrhe.
* ***Statističke tehnike***: Još jedan pravac podrazumeva promene različitih parametara pokrivačke slike kako bi se ugradili podaci. To može uključivati segmentaciju pokrivača u blokove, pri čemu se svaki bit poruke ugrađuje unutar tih blokova.
* ***Tehnika transformacionog domena***: Poznate kao tehnike transformacionog domena, ove tehnike podrazumevaju umetanje tajnih podataka unutar frekvencijskog ili transformacionog domena pokrivačke slike. Ove metode, iako kompleksnije, omogućavaju sofisticirano skrivanje podataka. Korišćene transformacije i algoritmi uključuju Integer Wavelet Transform, Curve Wavelet Transform, Discrete Fourier Transformation (DFT), Discrete Cosine Transformation (DCT), Discrete Wavelet Transformation (DWT) i tehnike bez gubitaka ili reverzibilne metode.
* ***Tehnike distorzije***: Tehnike distorzije podrazumevaju umetanje tajnih podataka putem distorzije signala. Kodirajući uređaj vrši modifikacije na pokrivačkoj slici, dok dekoder procenjuje razlike između originalne i distorzirane pokrivačke slike kako bi povratio tajnu sliku i identifikovao modifikacije koje su primenjene tokom kodiranja.
* ***Maskiranje i filtriranje***: Unutar domena tehnika maskiranja i filtriranja, tajni podaci se skrivaju modifikacijom sjaja određenih oblasti unutar originalnih podataka ili slike. Umetanje poruke odvija se unutar značajnih bitova slike, iako je ova metoda podložnija gubicima u slikama, za razliku od robusnije metode umetanja najmanje značajnog bita (LSB).

Ova široka klasifikacija omogućava raznovrsne pristupe steganografiji slika, pružajući mogućnosti prilagođavanja metoda u zavisnosti od specifičnih zahteva i karakteristika medijskog nosača informacije. Kroz ovaj rad ćemo pažljivo istražiti primenu hibridnih tehnika u kontekstu slika, pri čemu ćemo se posebno posvetiti dvema specifičnim tehnikama: LSB (Najmanje Značajni Bit) i „phase coding“. LSB predstavlja pristup u slikovnom domenu i obuhvata celu porodicu različitih algoritama koji su trenutno najrasprostranjeniji u steganografiji slika. S druge strane, „phase coding“ pripada frekvencijskom domenskom pristupu i češće se koristi u audio steganografiji. Ipak, istražićemo kako je moguće primeniti ovu tehniku u sferi slika, kao i ograničenja koja je čine manje pogodnom za širu komercijalnu primenu.

# **3. HIBRIDNE TEHNIKE STEGANOGRAFIJE**

Ideja hibridnih steganografskih tehnika proizlazi iz nastojanja da se postigne optimalno rešenje putem kombinacije dveju ili više različitih tehnika ili algoritama. Ova strategija često podrazumeva kombinaciju dva algoritma koji se međusobno dopunjuju, ističući svoje prednosti i umanjujući njihove nedostatke. No, važno je napomenuti da je ostvarivanje ovakvih hibridnih rešenja izazovno, zahtevajući pažljiv odabir tehnika, duboko istraživanje i temeljno praktično testiranje kako bi se stekla realna slika o upotrebi predloženog rešenja.

U kontekstu steganografije slika, primena hibridnih tehnika pruža mogućnost uparivanja tehnika iz istih ili različitih domena u zavisnosti od specifičnih zahteva situacije ili vrste medijskog nosača u kojem skrivamo informacije. Na primer, kombinisanje slikovnog domena, poput LSB (Najmanje Značajnog Bita), sa frekvencijskim domenom, kao što je „phase coding“, omogućava nam da iskoristimo prednosti obe oblasti, postižući optimalnu ravnotežu između kapaciteta skrivanja informacija i otpornosti na detekciju.

Unapređenje hibridnih steganografskih tehnika zahteva ne samo teorijsko poznavanje različitih algoritama, već i pažljivu analizu njihovog ponašanja u praksi. Takođe neophodno je odrediti udeo iskorišćenih kombinovanih tehnika u finalnom rešenju. Ovaj pristup omogućava stvaranje robustnih sistema za skrivanje informacija, prilagođenih konkretnim zahtevima i uslovima primene. Važnost ove oblasti naglašava se potrebom za stalnim istraživanjem i inovacijama kako bi održala korak s evolucijom tehnologije i izazovima u oblasti steganografije.

## 3.1 Pregled dostupnih hibridnih rešenja

Osnovni cilj pregleda dostupnih hibridnih rešenja jeste prepoznavanje postojećih tehnika, analiza njihovih prednosti i nedostataka, s namerom pronalaženja efikasnog pristupa za zaštitu privatnih ili osetljivih podataka. Kroz protekle decenije, predstavljeno je mnogo tehnika skrivanja podataka baziranih na steganografiji. Postoji obilje strategija za prikrivanje podataka zasnovanih na steganografiji, koristeći algoritme fokusirane na najmanje značajne bitove (LSB), omogućavajući tako prikrivanje tajnih poruka unutar prikrivajućeg medija, kao što su slike.

Chakrabarti i Samanta [5] razvili su tehniku skrivanja na dva nivoa za slike u sivim tonovima koja obezbeđuje jaču sigurnost.

Nilizadeh i Nilchi [6] kombinuju dve različite metode steganografije, matricu obrasca (MP) i najmanji značajni bit (LSB), za RGB slike. Rezultati simulacije i evaluacije pokazuju da ova metoda imaju veći kapacitet od metoda LSB i MP, za više od 1.265 testova i 4.77 puta. Rezultati takođe ukazuju da finalna „Stego-slika“ ima visok kvalitet PSNR[[1]](#footnote-1).

Amsden i Chan [7] poboljšavaju testove kapaciteta implementiranjem različitih algoritama steganografije, povećavajući količinu podataka koje pokušavaju sakriti, pre nego što kompresija slika na Fejsbuku izazove gubitak integriteta podataka.

R. Rejani i sar. [8] opisuju steganografiju zasnovanu na obrascima piksela na slikama, gde se poruka skriva unutar slike korišćenjem postojećih RGB vrednosti kad god je to moguće na nivou piksela ili uz minimalne promene. Ključ se takođe koristi za dešifrovanje poruke smeštene na nivou piksela. Radi dodatne zaštite, kako skrivena poruka, tako i ključna datoteka su u šifrovanom formatu koji može imati iste ili različite ključeve za dešifrovanje.

Kumar i sar. [9] osmislili su Hash-LSB algoritam u kombinaciji sa RSA kako bi poboljšali sigurnost podataka i procesa skrivanja podataka. Ova metoda koristi heš funkciju za generisanje obrasca radi skrivanja bitova informacije unutar Najmanje Značajnog Bita (LSB) RGB vrednosti piksela u prikrivajućoj slici. Osim toga, osigurava da je poruka enkriptovana pre nego što se sakrije, sprečavajući neovlašćeni pristup u slučaju da je poruka otkrivena od strane nekog drugog osim predviđenog primaoca. Ova enkripcija obezbeđuje da poruka ostane bezbedna u svom šifrovanom obliku.

Champakamala B.S. i sar. [10] primetili su da je ugradnja tajnih informacija unutar slika zahtevna zbog intenzivnih računskih operacija. Stoga, projektovanje u hardveru ubrzava proces steganografije.

Masud i sar. [11] unapredili su LSB tehnike za RGB slike kako bi poboljšali sigurnost skrivenih informacija.

Babya i sar. [12] predložili su tehniku obezbeđivanja podataka koristeći Diskretnu Talasnu Transformaciju (DWT). Ova metoda uključuje razdvajanje prikrivajuće slike na R, G i B ravni, ugrađivanje tajnih slika u ove ravni i izvođenje N-nivoa dekompozicije. Neke frekvencijske komponente se kombinuju, a tajne slike se izvlače iz stego slike. DWT se preferira zbog svoje sposobnosti povećanja opterećenja steganografskog procesa putem kompresije podataka, uz minimalne vidljive promene na originalnoj slici.

Reddy i Kumar [13] su predstavili novi pristup koji kombinuje steganografiju (metodu Najmanjeg Značajnog Bita) i kriptografiju (AES) kako bi uspostavili siguran način prenosa podataka putem nesigurnih ili javnih mreža. Ugrađene informacije, u obliku šifrovanog teksta, prolaze kroz proces ugradnje u „LL sub-band wavelet decomposed image“ koristeći metodu Najmanjeg Značajnog Bita. Zatim se primenjuje inverzna talasna transformacija, a rezultirajuća slika se šalje primaocu. Na kraju, na strani primaoca, slika se transformiše pomoću talasne transformacije, a šifrovan tekst se izvlači korišćenjem LSB metode.

Patel i Ragha [14] enkriptuju podatke pre nego što ih ugrade u nosački fajl. Vrše diskretnu talasnu transformaciju na prikrivajućoj slici, zatim vrše fuziju. Nakon toga, izvodi se inverzna talasna transformacija kako bi se dobila stego-slika. Poređenje sa originalnom prikrivajućom slikom daje povoljne rezultate, ukazujući na gotovo identične slike.

## 3.2 Razmatrano rešenje

U okviru ovog istraživačkog rada, detaljno ćemo razmatrati rešenje koje integriše dve steganografske tehnike kako bismo produbili razumevanje rezultata svake pojedinačno, istražujući pritom koji odabrani domen pokazuje veću efikasnost u obradi slika. Ova inovativna strategija zahteva dublju analizu kombinacije tehnike umetanja bitova najmanje težine – LSB, zajedno sa „phase-coding“ tehnikom iz frekventnog domena.

LSB tehnika, kao deo obimnije porodice različitih tehnika, stekla je popularnost zbog svoje sposobnosti da menja bitove najmanje težine u skrivajućoj slici, prilagođavajući ih bitovima informacije koja se krije. Njena opsežna primena u komercijalnim rešenjima svedoči o visokom nivou uspešnosti u steganografiji, pružajući pouzdanu platformu za bezbedno skrivanje podataka.

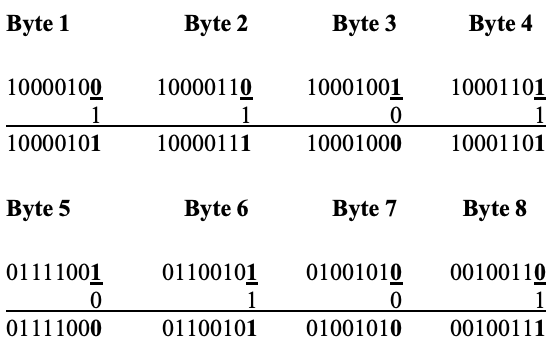
Sa druge strane, „phase-coding“ tehnika često se primenjuje u oblasti audio steganografije, imajući u vidu da audio signali već postoje u frekventnom domenu, što ih čini prikladnim za obradu faza. Ipak, primenom određene transformacije, slika se može prevesti iz prostornog u frekventni domen, omogućavajući time efikasnu upotrebu „phase-coding“ tehnike u kontekstu steganografije slika.

Analizom ove kombinacije tehnika, istražićemo dublje kako bismo razumeli ograničenja i prednosti svakog odabranih domena, pružajući sveobuhvatan uvid u kompleksnost i efikasnost ovog hibridnog pristupa. Kroz sistematsko ispitivanje, očekujemo da dobijemo jasniju sliku o optimalnim uslovima primene ovakvog pristupa u cilju bezbednog i efikasnog skrivanja informacija u slikama.

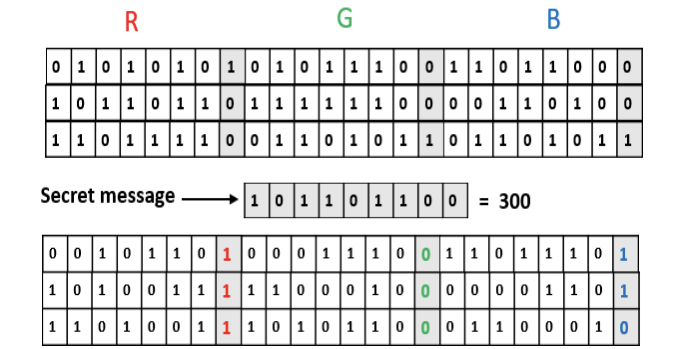
# **4. UMETANJE BITOVA NAJMANJE TEŽINE – LSB**

U sivim tonovima slika, svaki piksel je predstavljen sa 8 bitova, a poslednji bit, poznat kao Najmanje Značajan Bit (LSB – Least Significant Bit), utiče na vrednost piksela samo za „1“. Korišćenjem ove karakteristike, podaci mogu biti neprimetno skriveni unutar slike. Alternativno, razmatranje poslednja dva bita kao LSB bitova, koji utiču na vrednost piksela za „3“, omogućava skladištenje dodatnih podataka.

LSB steganografija uključuje zamenu najmanje značajnog bita slike podacima. Budući da je ova metoda osetljiva na steganoanalizu, jedna mera zaštite predstavlja šifrovanje sirovih podataka pre nego što se oni integrišu u sliku. Iako šifrovanje može povećati vremensku složenost, istovremeno pruža veći nivo sigurnosti. Ovaj jednostavan pristup podrazumeva zamenu najmanje značajnih bitova nekih ili svih bajtova unutar slike bitovima tajne poruke. Na primer, ukoliko je potrebno 8 bajtova podataka kako bi se sakrila brojka „213“ u ASCII kodu (11010101), koristi se LSB metoda, kako je prikazano na slici 1 [15].

*Slika 1. Sakrivanje brojke 213 sa LSB tehnikom*

Svaki RGB piksel u slici (24 bita) omogućava skladištenje 3 bita unutar svakog piksela, modifikujući jedan bit za svaku RGB komponentu predstavljenu bajtom. Slika veličine 800 × 600 piksela može da primi 180.000 bajtova ili 1.440.000 bitova ugrađenih tajnih poruka. LSB nosačke slike koristi se kao informacija za ugrađivanje, kako je ilustrovano na slici 2. Ovaj metod obezbeđuje efikasno ugrađivanje tajne poruke uz minimalne promene u polovini bitova slike, koristeći nesposobnost ljudskog oka da primeti nijanse boja i male varijacije u intenzitetu koje proizlaze iz promena u LSB. [16]



*Slika 2. Skrivanje tajne poruke u RGB slici*

Ukoliko metoda koristi samo najmanje značajan bit (samo jedan bit u svakom pikselu). Veličina podataka (tajne poruke) koju možemo ugraditi u sliku izračunava se na sledeći način:

S = M \* N - X

Gde je S veličina tajne poruke, M je broj redova na slici, dok je N broj kolona na slici. X predstavlja veličinu zaglavlja koje se šalje zajedno sa tajnom porukom. Ovo u praksi može biti algoritam koji se koristio za kodiranje originalne poruke ili ključ za dekodiranje.

LSB metoda ugrađivanja postavlja osnovu za mnoge tehnike skrivanja poruka unutar multimedijalnih nosača podataka. Njena svestranost seže do različitih područja podataka, uključujući skrivanje poruka u vrednostima boja RGB podataka ili u koeficijentima frekvencije JPEG slike. Metoda LSB ugrađivanja takođe se može primeniti na različite formate i vrste podataka, čineći je ključnom tehnikom steganografije u savremenoj upotrebi.

## 4.1 LSB tehnika u različitim formatima rasterskih slika

1. ***BMP format***

Iako BMP slike pružaju dobar kontejner za podatke zbog njihove ogromne veličine i fleksibilnosti u prikazu boja, njihova primena u steganografiji sa tehnikom bita najmanje težine (LSB) predstavlja jedinstvene izazove. U poređenju s drugim formatima slika, bitmape pokazuju veću osetljivost na modifikacije bita najmanje težine, što potencijalno dovodi do kompromitovanja nevidljivosti skrivene poruke. Ova povećana osetljivost proizlazi iz inherentne strukture BMP formata, gde se vrednost svakog piksela predstavlja pojedinačnim bajtovima, što čini suptilne promene lakše uočljivim.

Uprkos ovoj inherentnoj ranjivosti, BMP-ovi i dalje imaju potencijal kao nosači steganografskih informacija, posebno kada se prioritet daje kapacitetu podataka u odnosu na apsolutno prikrivanje. Njihova sposobnost da prime velike informacije unutar RGB kanala svakog piksela omogućava efikasno ugrađivanje tajne poruke. Međutim, izbor dubine ugrađivanja, tj. broj modifikovanih najmanje značajnih bitova po pikselu, zahteva pažljivo razmatranje. Povećanje dubine ugrađivanja povećava kapacitet podataka, ali istovremeno povećava rizik od vizuelnih artefakata i statističkih anomalija, što potencijalno otkriva prisustvo skrivene poruke.

Za scenarije koji zahtevaju visok kapacitet podataka, može biti potrebna dubina ugrađivanja veća od jednog bita po pikselu. Međutim, takvi pristupi često dolaze uz troškove kvaliteta slike. Modifikacija više najmanje značajnih bitova unutar svakog kanala boje može dovesti do primetnih promena teksture i nijansi boja, umanjujući vizuelnu celovitost slike. Ovaj kompromis između kapaciteta podataka i kvaliteta slike postaje posebno izražen u bitmapama sa ograničenim paletama, gde promene na nekoliko piksela mogu značajno uticati na ukupan vizuelni prikaz.

Stoga, uspešna steganografija najmanje značajnog bita u BMP-ovima zahteva delikatan balans između ovih suprotstavljenih faktora. Konkretna primena, željeni nivo tajnosti i same karakteristike slike sve utiču na optimalnu dubinu ugrađivanja. Balansiranje ovih razmatranja omogućava efikasno korišćenje BMP-ova u steganografiji, iskorišćavajući njihov kapacitet podataka dok se minimizira rizik od otkrivanja putem vizuelne ili statističke analize. [17]

1. ***PNG format***

Korišćenje PNG formata za LSB steganografiju ističe se kao visoko preporučljiva opcija. LSB, koji funkcioniše unutar prostornog domena, stavlja poseban naglasak na minimalnu prisutnost buke ili grešaka. U tom kontekstu, PNG se izdvaja kao optimalan format zbog korišćenja kompresije bez gubitaka. Ova ključna karakteristika osigurava besprekorno čuvanje zamena koje se vrše tokom celokupnog procesa LSB steganografije. PNG ne samo da pruža značajan kapacitet za skladištenje, već takođe isporučuje visokokvalitetne slike nakon steganografije, efikasno prikrivajući promene i čineći ih neprimetnim prilikom nonšalantnog vizuelnog pregleda.

LSB metoda omogućava diskretno skladištenje tajnih poruka, bilo unutar bitova najmanje težine pojedinačnih RGB vrednosti piksela boje ili u odgovarajućim bitovima kombinovane RGB vrednosti boje. PNG-ova efikasnost u prikrivanju više poruka čini primenu LSB u PNG posebno povoljnom za scenarije gde je naglasak na obimu širenja informacija umesto na detaljima.

Ipak, važno je postići delikatan balans, jer povećanje broja promenjenih bitova povećava verovatnoću detekcije od strane ljudskog oka. LSB steganografska tehnika korišćena sa PNG formatom, u suštini, posvećena je širenju poruka bez uvođenja bilo kakvih oblika vizuelnih artifakata.

Zaključujemo da, dobar odnos između PNG formata i LSB steganografije pruža snažan i efikasan mehanizam za prikrivanje informacija, balansirajući nijanse operacija u prostornom domenu, kompresije bez gubitaka i nijansiranu manipulaciju vrednosti piksela. Ova kombinacija ne samo da obezbeđuje visok nivo sigurnosti, već održava i vizuelnu celovitost slike, čineći je svestranim izborom za slučajeve gde su i prikrivanje informacija i kvalitet slike od suštinskog značaja. [18]

1. ***GIF format***

Iako GIF slike nude kompaktni format za čuvanje grafike, njihova dubina od 8 bitova ograničava sposobnost za skrivanje informacija u poređenju sa BMP ili PNG formatom. Iako sva tri formata mogu efikasno koristiti LSB tehniku za ugrađivanje podataka, struktura GIF-a bazirana na indeksiranoj paleti boja uvodi jedinstvene izazove u steganografskim primenama.

Zbog svoje indeksirane prirode, GIF slike čuvaju informacije o boji unutar palete. Svaki piksel je predstavljen jednim bajtom, koji predstavlja indeks za određenu boju unutar palete. Da bi se poboljšala efikasnost, boje se obično raspoređuju od najčešće korišćenih do najređe korišćenih. Međutim, ovaj sistem baziran na paleti zahteva pažljivo razmatranje kada se GIF slike koriste kao nosioci za skrivene podatke.

Promena LSB-a piksela unutar GIF slike može nenamerno da promeni indeks palete boja, što potencijalno vodi do vidljivih promena boje. Stepen promene zavisi od sličnosti susednih ulaza u paleti – značajne razlike rezultuju u uočljivim promenama, dok slični ulazi minimalizuju vizuelne razlike. Opšte govoreći, otkrivanje čak i suptilnih promena slike u GIF-ovima čini LSB tehnike manje sigurnim u poređenju sa drugim formatima slika. Da bi se ublažili ovi nedostaci, preporučuju se sledeće strategije:

* Izolovati paletu kada uzastopne boje imaju minimalne razlike
* Uvesti nove boje slične postojećim u paleti boja
* Koristiti 8-bitne crno-bele GIF slike, koje sadrže 256 nijansi sive, da bi se sprečile postepene promene boje

Adresiranjem ovih problema sa paletom, steganografske aplikacije mogu efikasnije koristiti GIF slike uz održavanje većeg stepena skrivanja. [16]

|  |  |  |
| --- | --- | --- |
| FORMAT | PREDNOSTI | MANE |
| BMP | * ***Kapacitet podataka:*** BMP format pruža veliki kapacitet podataka zbog svoje ogromne veličine i RGB kanala za svaki piksel, što omogućava efikasno ugrađivanje tajnih poruka. * ***Fleksibilnost u prikazu boja***: Mogućnost prikaza širokog spektra boja pomaže u očuvanju vizuelne celovitosti slike. | * ***Osetljivost na modifikacije bita najmanje težine:*** Struktura BMP formata čini ga osetljivim na promene, što može dovesti do kompromitovanja nevidljivosti skrivene poruke. * ***Rizik od vizuelnih artefakata:*** Povećanje dubine ugrađivanja povećava rizik od vizuelnih artefakata i statističkih anomalija, što može otkriti prisustvo skrivene poruke. |
| PNG | * ***Kompresija bez gubitaka:*** PNG koristi kompresiju bez gubitaka, čuvajući tako zamene vršene tokom LSB steganografije. * ***Visok kvalitet slike:*** Visokokvalitetne slike nakon steganografije efikasno prikrivaju promene, čineći ih neprimetnim vizuelnim pregledom. | * Osetljivost na vizuelnu detekciju: Povećanje broja promenjenih bitova povećava verovatnoću detekcije od strane ljudskog oka. |
| GIF | * ***Kompaktnost formata:*** GIF format pruža kompaktnost, iako sa ograničenom dubinom od 8 bitova. * ***Indeksirana paleta boja:*** Raspoređivanje boja od najčešće korišćenih do najređe korišćenih doprinosi efikasnosti. | * ***Ograničen kapacitet podataka:*** Dubina od 8 bitova ograničava kapacitet podataka u poređenju sa drugim formatima. * ***Vizuelna osetljivost:*** Promene LSB-a mogu uticati na indeks palete boja, vidljivo menjajući boje slike. * ***Osetljivost na vizuelno otkrivanje:*** Čak i suptilne promene mogu biti otkrivene, čineći GIF manje sigurnim u upotrebi LSB tehnika. |

*Tabela 1. Pregled prednosti i mana primene LSB tehnike nad svakim od formata rasterskih slika*

# **5. PHASE CODING TEHNIKA**

Phase coding tehnika je steganografski metod u frekventnom, odnosno transformacionom domenu. Ove tehnike podrazumevaju umetanje tajnih podataka unutar frekvencijskog ili transformacionog domena prenosne slike. Metode u frekventnom domenu, iako složenije, omogućavaju sofisticirano skrivanje podataka. Glavni problem ovog domena je što se sama slika nalazi u prostornom domenu, pa je prvi korak njeno prevođenje u frekventni domen, što se postiže Furijeovom transformacijom. Ova transformacija razlaže sliku u njene frekventne komponente. Nakon toga, metod se svodi na primenu sličnu kao kod audio steganografije, jer se sada i transformisana slika i audio signal nalaze u frekventnom domenu. Poslednji korak je, naravno, primena inverzne Furijeove transformacije. Sada kada razumemo način primene phase coding metode na slici u kojoj krijemo informacije, potrebno je dublje razumeti njeno funkcionisanje. Analiziraćemo primenu ove tehnike u audio steganografiji, a kasnije ćemo kroz praktični deo rada videti njenu upotrebu i na samoj slici. Važno je naglasiti da prilikom primene izolovane phase coding tehnike na slici očekujemo izazove vezane za opažljivost, otpornost i mogućnost detekcije. Ljudski vizualni sistem može biti osetljiv na promene u informacijama faze, što može rezultirati vidljivim artefaktima. Dodatno, metoda možda neće biti toliko otporna na različite operacije obrade slika ili napade. Važno je pažljivo razmotriti ograničenja i potencijalne nedostatke ove metode u poređenju sa već ustanovljenim tehnikama u ovoj oblasti.

## 5.1 Audio steganografija

Audio steganografija podrazumeva neprimetno sakrivanje informacija unutar audio datoteka i predstavlja moćan način tajne komunikacije i prenosa podataka. Ova tehnika koristi ograničenja ljudskog sluha i načina percepcije zvuka, eksploatišući bitna maskirajuća svojstva glasnih zvukova nad tišim. U poređenju sa slikovnim i video formatima, audio steganografija nudi izrazite prednosti. Primetno je da audio datoteke poseduju znatno veći kapacitet za ugrađivanje podataka u poređenju sa formatima slika, dok video formati, uprkos svojoj veličini, često se suočavaju sa praktičnim ograničenjima i nedostaju im robusni steganografski algoritmi.

Windows Audio-Visual (WAV) format služi kao popularna platforma za audio steganografiju zbog svoje fleksibilnosti i dobro definisane strukture. U okviru WAV datoteke, dve primarne oblasti olakšavaju prikrivanje podataka: okruženje za skladištenje i digitalno predstavljanje samog audio signala. Istraživači su razvili raznovrsni niz tehnika za efikasno ugrađivanje tajnih poruka u digitalni signal zvuka. Najzastupljenije metode za skrivanje podataka u WAV datotekama su:

* ***Kodiranje najmanje značajnog bita (LSB):*** Ovaj pristup ugrađuje informacije u najmanje značajne bitove audio signala, u suštini šapućući tajnu poruku u pozadinskoj buci.
* ***Phase coding:*** Neprekidnim manipulisanjem fazom određenih audio komponenti, informacije se mogu kodirati, slično kao da se kodirana poruka postavlja u suptilne vibracije zvučnih talasa.
* ***Spread spectrum***: Ova tehnika distribuira skrivene podatke kroz širok spektar frekvencija.
* ***Echo Data Hiding***: Tajne poruke mogu se ugraditi u prirodne odjeke prisutne u audio signalu, slično kao da se ostavljaju kodirani šapati u oslabljenim odjecima pećine.

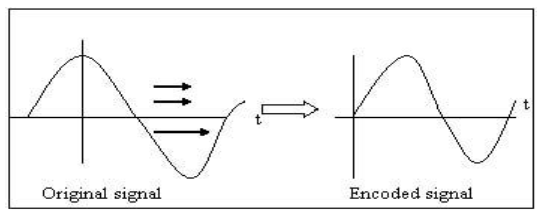
Prednosti velikog kapaciteta podataka i raznovrsnih tehnika ugrađivanja čine audio steganografiju uzbudljivom i dinamičnom oblasti istraživanja. Ovo polje nastavlja da se razvija, pomerajući granice prikrivanja informacija i transformišući samu suštinu zvuka, temelj komunikacije, u tihog saučesnika u razmeni tajnih poruka. [19]

## 5.2 Način funkcionisanja phase coding tehnike

***Phase coding***, ili ***fazno kodiranje,*** predstavlja inovativnu tehniku za skrivanje informacija unutar audio signala, nadograđujući se na slabosti metoda koje se oslanjaju na unošenje buke. Umesto otvorenog ubacivanja šuma ili mešanja u tehničke bitove, ova metoda koristi suptilne promene faza u okviru faznog spektra digitalnog signala kako bi se poruka u njega neprimetno ugnezdila. To rezultuje nečujnim izmenama u pogledu odnosa signala i buke, što ljudsko uho ne može da registruje.

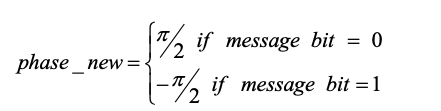
Ključna prednost faznog kodiranja leži u njegovoj sposobnosti da poruku integriše u audio signal bez narušavanja zvučnog kvaliteta. Ovo se postiže tako što se inicijalna faza prvog segmenta audio zapisa zamenjuje referentnom fazom koja predstavlja podatke koje želimo da sakrijemo. Da bi se sačuvala koherentnost signala, faze narednih segmenata se prilagođavaju tako da se održi relativna fazna veza između njih.

Ovaj pristup predstavlja odstupanje od konvencionalnih metoda jer se fokusira na manipulaciju faznih informacija umesto otvorenog ubacivanja buke. Na taj način maksimalno iskorišćava karakteristike ljudske percepcije zvuka i buke, čineći izmene u faznom spektru praktično neprimetnim za slušaoca.

*Slika 3. Izgled signala sa enkodiranom informacijom korišćenjem phase coding tehnike*

Da bismo enkodirali poruku korišćenjem tehnike kodiranja faza potrebno je da ispratimo sledeće korake [20]:

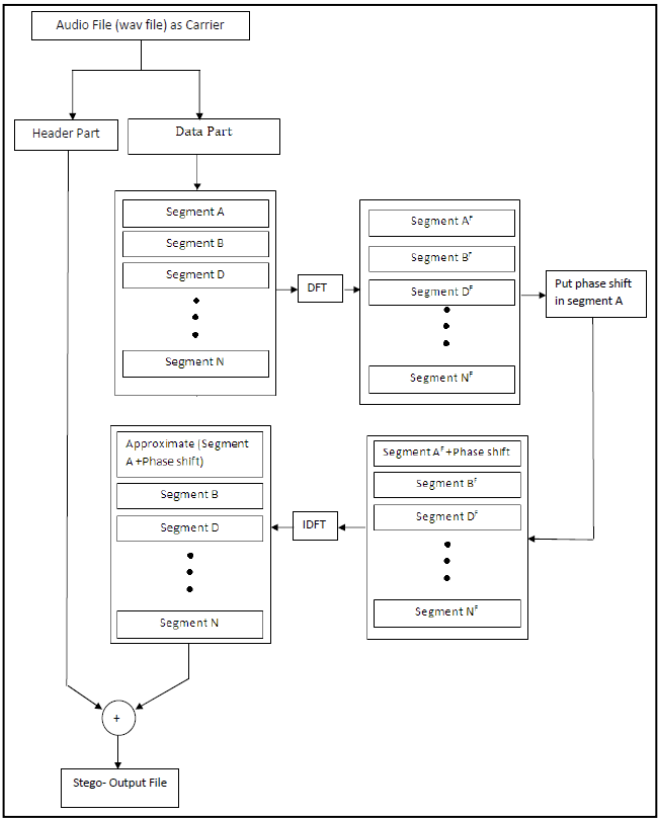
1. Podelimo originalni audio signal na manje segmente koji su iste veličine kao i poruka koju treba sakriti u signalu
2. Primenimo diskretnu Furijeovu transformaciju (DFT) nad svakim segmentom kako bismo dobili matricu faza i magnituda Furijeove transformacije
3. Izračunamo razlike faza između susednih segmenata
4. Ugradimo tajnu poruku u prvi segment audio signala prateći formulu datu na slici 4



*Slika 4. Formula za umetanje tajne poruke u fazu signala*

1. Izračunamo novu matricu faza korišćenjem nove faze prvog segmenta i originalne razlike faza
2. Koristeći novu matricu faza i originalnu matricu magnituda, zvučni signal se rekonstruiše primenom inverzne Diskretne Furijeove transformacije, a zatim se, finalno, segmenti zvuka ponovo spajaju

Da bi primalac mogao otkriti skrivenu poruku unutar audio datoteke, potrebno je da ima informaciju o trajanju datoteke. Korišćenjem diskretne Furijeove transformacije (DFT), primalac može pristupiti fazama i izvući skrivene informacije. Jedno ograničenje povezano sa procesom kodiranja jeste smanjena stopa prenosa podataka. Ovo ograničenje proizlazi iz činjenice da se tajna poruka kodira isključivo unutar početnog segmenta signala. Iako proširenje dužine signala može potencijalno rešiti ovaj problem, istovremeno uvodi primetniju promenu u odnosima između frekvencija svake komponente faze unutar signala. Ova povećana uočljivost ugrožava skrivanje kodiranja. Stoga se ova tehnika primenjuje samo u scenarijima gde proces kodiranja generiše ograničenu količinu podataka, kao što je ugradnja vodenih žigova ili drugih informacija malog kapaciteta [21].



*Slika 5. Flow dijagram procesa enkodiranja poruke u audio signal phase coding tehnikom*

# **6. PRAKTIČNO REŠENJE**

Ideja praktične implementacije podrazumeva implementaciju jednostavnog oblika hibridne tehnike steganografije slike u programskom jeziku Python. Hibridna tehnika kombinovaće dve osnovne metode – umetanje bita najmanje težine (LSB) i fazno kodiranje (phase coding). U prethodnim poglavljima smo istražili prednosti i mane ovih metoda. Sada ćemo kroz praktičan primer analizirati slike u kojima je poruka sakrivena pojedinačno primenjujući svaku od ovih tehnika, kao i njihovu kombinaciju.

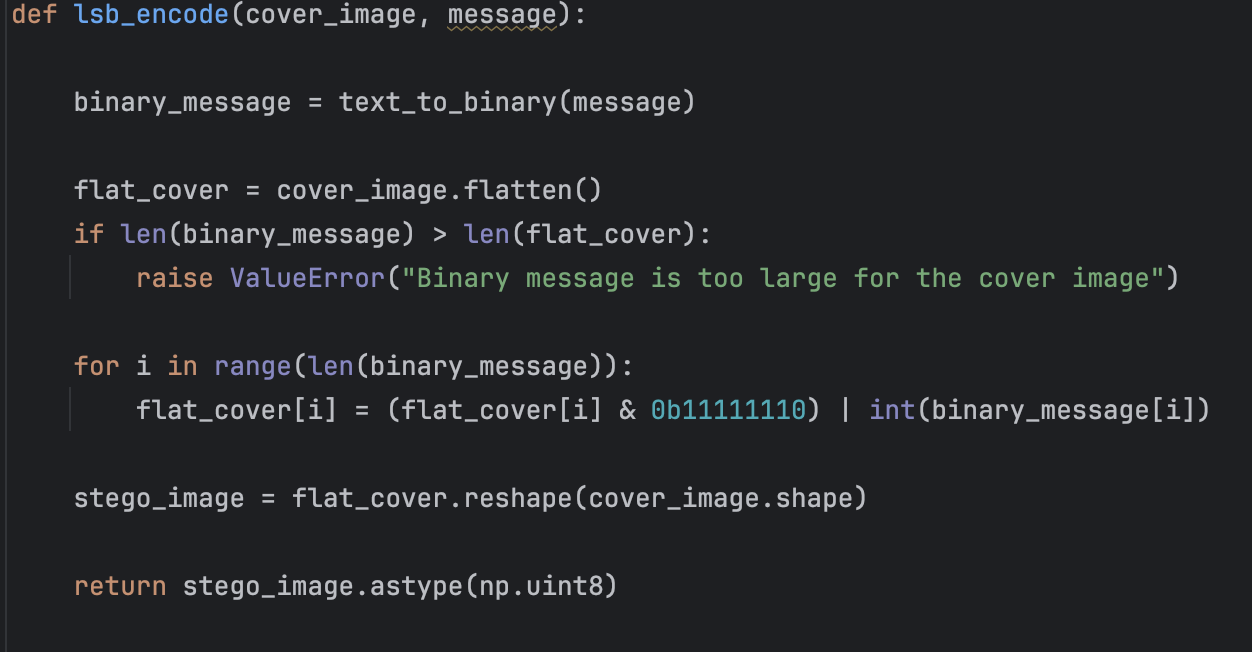
U procesu implementacije, fokusiraćemo se na jasnu demonstraciju koraka koje svaka od tehnika podrazumeva. Prvo, koristićemo LSB za skrivanje poruke u prostornom domenu slike. Zatim ćemo primeniti fazno kodiranje kako bismo sakrili informacije u transformacionom domenu. Nakon toga, hibridna tehnika će biti primenjena, objedinjujući ove dve metode. Praktičan primer omogućiće nam da proučimo kako se ove tehnike ponašaju individualno i u kombinaciji.

Cilj praktičnog rešenja nije samo eksperimentisanje s tehnikama steganografije, već i analiza rezultirajućih slika. Pitanja koja postavljamo obuhvataju potencijalno narušavanje poruke, prisustvo vizuelnih artefakata i uticaj na ukupni kvalitet slike. Ova analiza ima za cilj pružanje dubljeg uvida u funkcionalnost svake tehnike i njihovu praktičnu primenu u kontekstu zaštite podataka i očuvanja vizuelnog integriteta slika. Kroz ovo istraživanje, stremimo ka boljem razumevanju kako se ove metode ponašaju u različitim scenarijima i njihovoj efikasnosti u praktičnim aplikacijama steganografije slika.

Naše rešenje počinje sa LSB metodom koju smo spominjali više puta tokom ovog rada. Dakle, ideja je da bitove najmanje težine zamenimo sa bitovima podatka koji želimo da sakrijemo. Mi ćemo u ovom rešenju pokušati da sakrijemo tekstualnu poruku. Pre svega, potrebne su nam pomoćne funkcije sa kojima ćemo prevesti zadatu tekstualnu poruku u binarni niz. Ove funkcije prikazane su na slici 6.

*Slika 6. Pomoćne funkcije za transformaciju stringa u binarni niz i obrnuto*

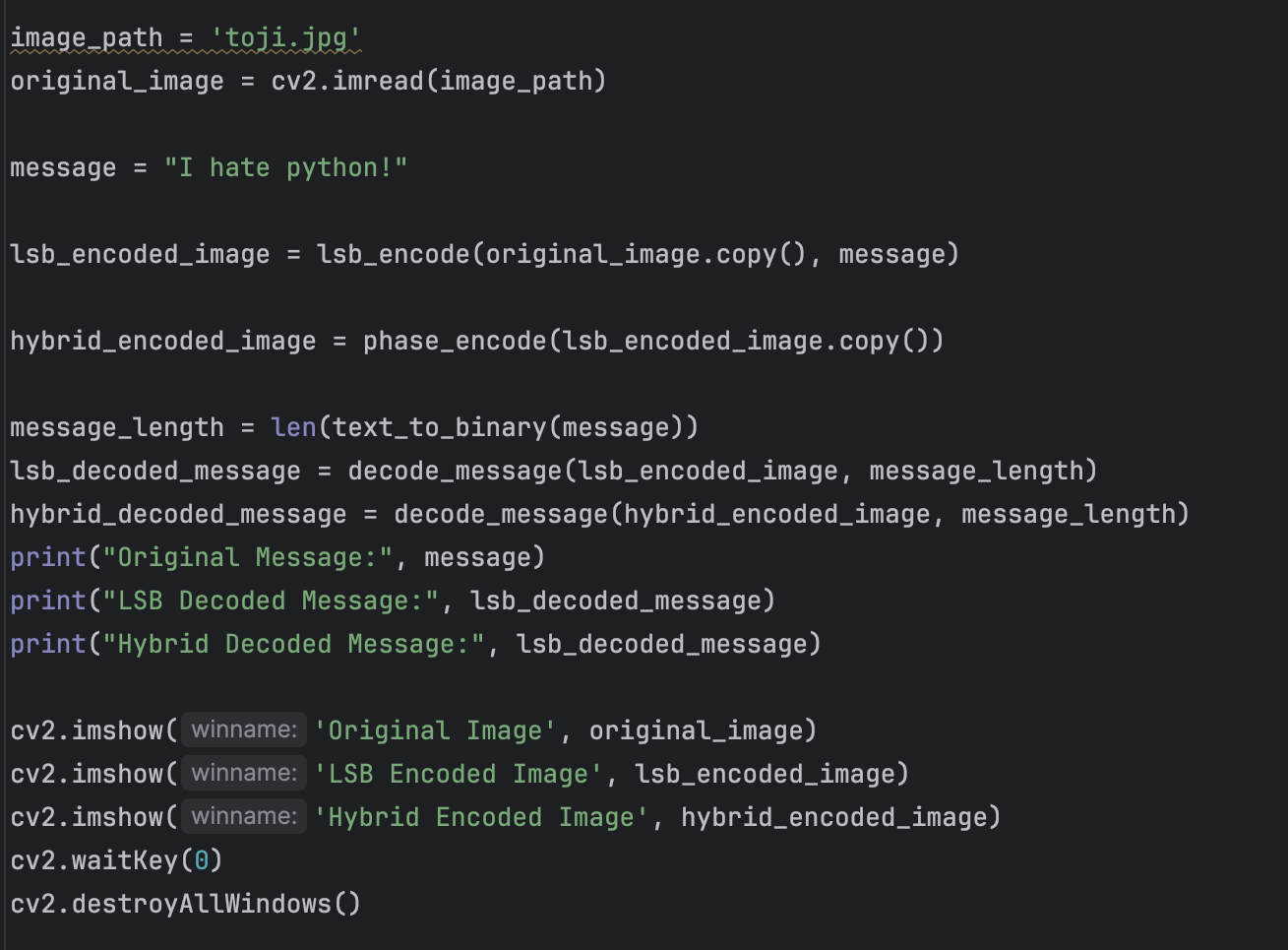
Sada kada imamo osiguran način da tekstualnu poruku predstavimo nizom bitova, moguće je i da sakrijemo ove bitove u okviru naše slike korišćenjem LSB metoda. Za ovu svrhu kreiraćemo funkciju ***lsb\_encode.*** Ova funkcija će primati dva parametra, cover\_image, odnosno sliku koja će biti nosilac naše poruke, kao i message parametar, što zapravo predstavlja sam podatak, odnosno tekstualnu poruku koju treba sakriti. Funkcija će nam vratiti sliku u kojoj je zapravo enkodirana naša poruka. Implementacija funkcije data je na slici 7.

*Slika 7. Funkcija koja implementira LSB metod steganografije*

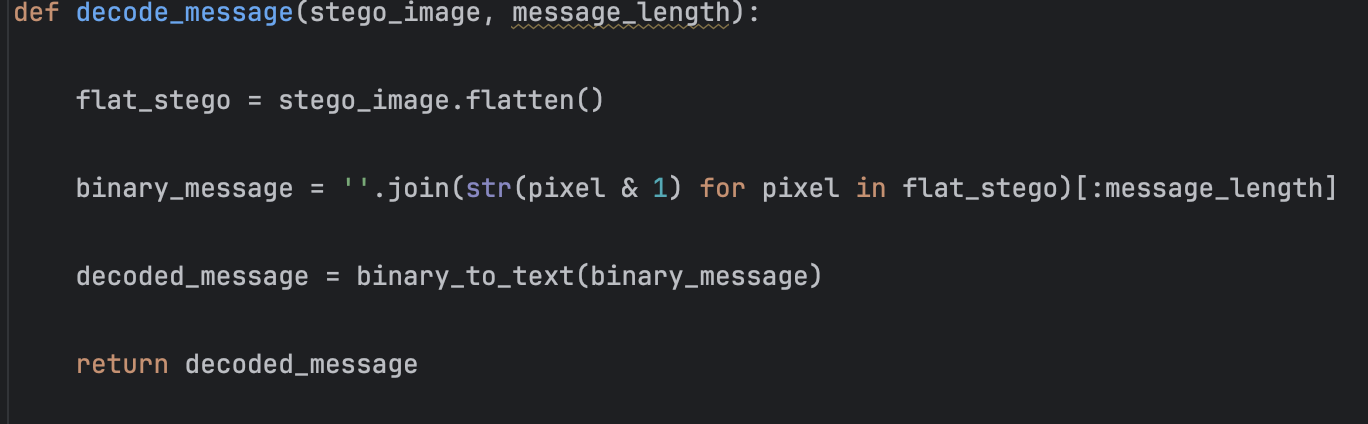
Funkcija se odvija kroz nekoliko koraka. Najpre se tekstulana poruka prevodi u niz bitova korišćenjem gore napomenutih pomoćnih funkcija. Nakon toga se koristi *flatten* funkcija kako bi se prosleđena slika transformisala u jednodimenzionalni niz bitova. Potom, sledi provera dužine prosleđene poruke. Naime, ako je dužina poruke veća od izravnatog niz bitova naše slike onda nije moguće izvršiti sakrvianje poruke u ovoj konkretnoj slici zbog premale količine dostupnih bitova. Nakon toga se kroz for petlju vrši umetanje bita najmanje težine u svakom pojedinačnom bajtu podatka. Na kraju, potrebno je još samo povratiti naš jednodimenzionalni niz u dimenzionalnost originalne slike i normalizovati vrednosti. Nakon enkodiranja slike rezultat je sledeći.

*Slika 8. Poređenje originalne slike i LSB enkodirane slike*

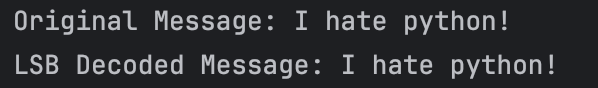
Dakle, možemo opaziti da ne dolazi do opadanja u kvalitetu originalne slike. Takođe nema primetnih vizuelnih artefakata. Iskorišćena je jpg slika sa puno detalja da bi se izrazila osobina LSB tehnike o kojoj smo govorili – iako očekujemo gore rezultate od slika visokog kvaliteta, to ipak nije slučaj zbog prirode ljudskog oka i načina registrovanja slike. Na slici 9 dat je deo koda koji smo iskoristili za pozive odgovarajućih funkcija za enkodiranje, kao i za prikaz slika. Za prikaz slika koristimo openCV biblioteku.

*Slika 9. Prikaz poziva funkcija za enkodiranje slika, prikaz istih i proveru poruka*

Sledeći važan korak je provera validnosti sakrivene poruke. Za ovu svrhu treba obezbediti funkciju za dekodiranje skrivene poruke, kako bismo mogli da je poredimo sa originalnom porukom. Ova funkcija će imati dva ulazna parametra, stego\_image, odnosno sliku u kojoj je sakrivena poruka, kao i parametar message\_length, što je zapravo očekivana dužina enkodirane poruke. Prosto ćemo proći kroz svaki piksel slike i pokupiti bit najmanje težine dok ne popunimo našu poruku unapred zadate dužine. Funkcija za dekodiranje poruke data je na slici 10.

*Slika 10. Funkcija za dekodiranje skrivene poruke iz slike*

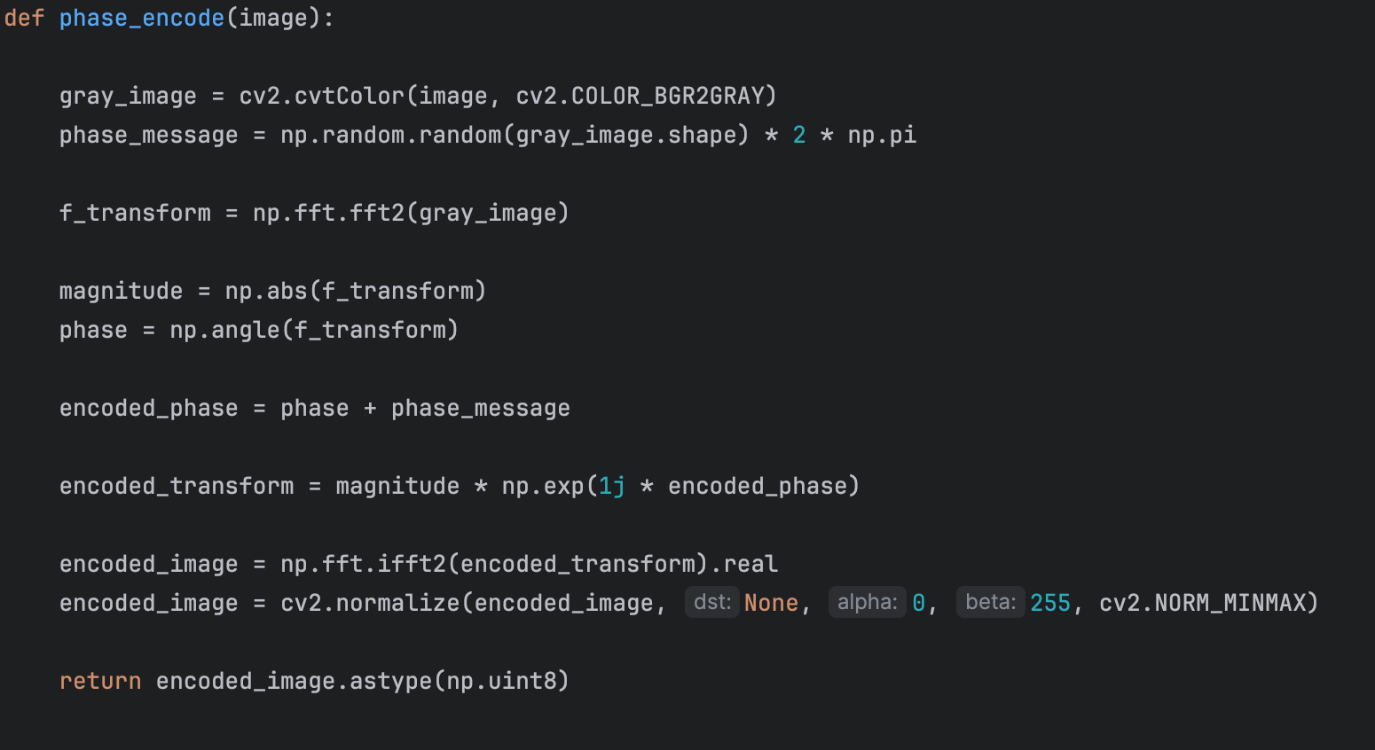
Vidimo da za našu poruku „I hate python!”, koju želimo dobro da sakrijemo, pri pozivu funkcije za dekodiranje dobijamo identičnu poruku na izlazu. Odnosno, naša poruka je uspešno sakrivena u okviru slike. Izlaz iz programa možemo videti na slici 11.



*Slika 11. Poređenje originalne poruke i LSB enkodirane poruke*

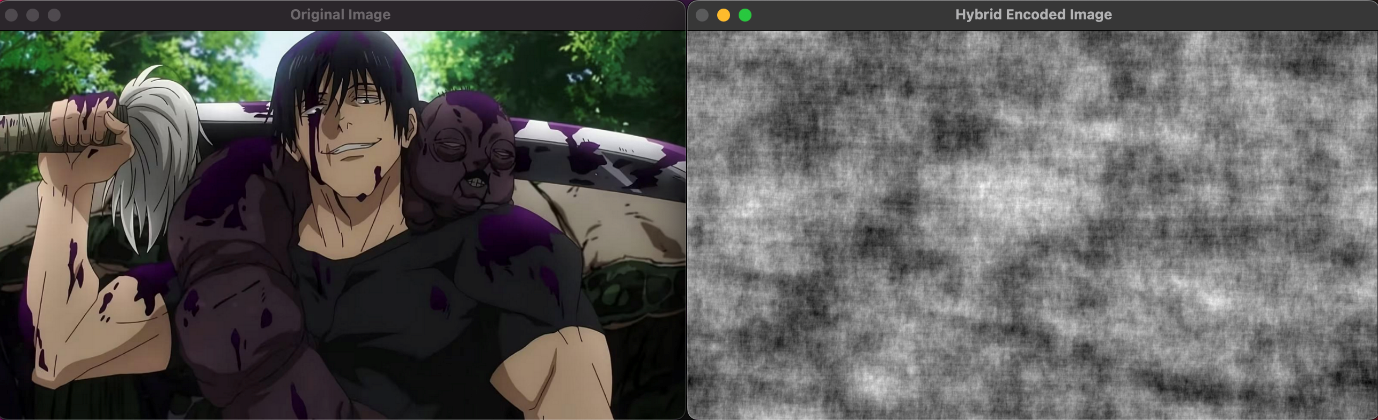
Zaključak je da korišćenjem jednostavne LSB metode je moguće uspešno sakriti poruku. Važno je napomenuti da su zadovoljeni osnovni koncepti steganografije, odnosno sakriveni podatak se ne vidi u nosiocu podatka i nema tragova sakrivanja, odnosno slika koja prenosi podatak nema vizuelnih promena.

Naš sledeći zadatak je da vidimo da li uvođenje dodatnog steganografskog koraka u vidu phase coding tehnike poboljšava dobijeni rezultat. Željeni rezultat je da imamo još jedan korak sigurnosti, koji bi otežao dekodiranje, ali da ispoštujemo koncepte steganografije, odnosno da ovaj dodatni korak ne uvede pogoršanje u kvalitetu slike ili eventualne vizuelne artefakte. Za ovu svrhu treba implementirati funkciju koja će vršiti fazno kodiranje slike. Implementacija ove funkcije data je na slici 12.

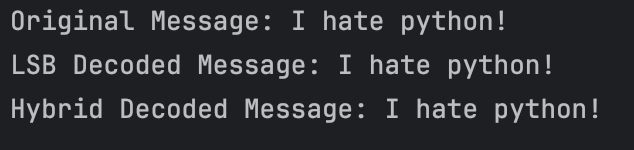
*Slika 12. Funkcija koja implementira phase coding steganografski metod*

Vidimo da ova funkcija ima samo jedan ulazni parametar, sliku čiju ćemo fazu modifikovati. Pre svega potrebno je prevesti sliku u sivi format kako bi bilo moguće dobijanje njenog frekventnog domena. Zatim je potrebno generisati fazu poruke koju želimo sakriti. Kako je poruka već sakrivena LSB metodom možemo generisati nasumičnu fazu koja će predstavljati dodatni korak enkripcije. Glavni korak je primena Furijeove transformacije kako bismo preveli našu sliku iz prostornog domena u frekventni, odnosno transformacioni domen. Nakon toga računamo magnitudu i fazu naše slike. Na izračunatu fazu dodajemo fazu naše poruke i na osnovu magnitude dobijamo enkodirani signal. Konačno, primenom izverzne Furijeove transformacije vraćamo naš signal u prostorni domen slike. Potrebno je još samo izvršiti normalizaciju i naša slika je spremna.

Međutim, u prethodnom delu rada smo napomenuli da promena faze slike nije preporučeni pristup. Razlog za ovo se krije u prirodi ljudskog oka, naime ono je osetljivo na vizuelne promene faze. Dok naš sluh teško razlikuje promene faze u audio signalima, što je i glavno mesto primene phase coding tehnike, isto se ne može reći i za fazne promene u okviru jedne slike. Nažalost, ova očekivana mana phase coding tehnike jasno dolazi do izražaja kada poredimo dobijeni rezultat sa originalnom slikom.

*Slika 13. Poređenje originalne slike i hibridno enkodirane slike*

Lako je uočiti da je slika dobijena našim predloženim hibridnim metodom enkodiranja potpuno neprepoznatljiva u poređenju sa originalnom slikom. Promena slike u crno-beli format bi bila prihvatljiva promena, jer bismo možda mogli da ograničimo primenu metoda na isključivo crno bele slike, ali vidimo da je osim toga došlo i do kompletnog narušavanja integriteta slike. Kada pročitamo našu enkodiranu poruku, vidimo da je ona zadržala svoj originalni oblik.



*Slika 14. Poređenje originalne poruke, LSB enkodirane poruke i poruke enkodirane hibridnim metodom*

Ipak, iako je poruka efektivno sakrivena narušili smo osnovni princip steganografije, a to je da medij u kome sakrivamo naše podatke mora da ostane nepromenjen, odnosno ne smemo imati tragove sakrivanja podatka. Uzimajući ovo u obzir, lako zaključujemo da naše rešenje nije dalo očekivane rezultate i ne može se primeniti u komercijalne svrhe jer prestaje da bude steganografski metod i prelazi u domen kriptografije.

# **7. ZAKLJUČAK**

Prolaskom kroz LSB metod steganografije videli smo da on predstavlja ustanovljeni standard u modernoj steganografiji slika. Njegova lakoća primene ukombinovana sa efektivnošću sakrivanja podataka ostaje neprikosnoveno rešenje. Videli smo da je LSB metod moguće primeniti na bilo kom formatu slika i da je uvek moguće dobiti zadovoljavajuće rešenje.

Upravo ove osobine metode umetanja bita najmanje težine su i bila inspiracija za kreiranje našeg hibridnog rešenja. Ideja je bila da pomešamo standard steganografije sa „wild-card” opcijom koja jeste phase coding metoda. Phase coding je svoje mesto pronašao u audio steganografiji. Razlog za ovo je nemogućnost ljudskog uha da registruje promene u fazi audio signala. Uočili smo, ipak, da primenom Furijeove transformacije možemo prevesti željenu sliku, koja je naš nosilac podatka, u frekventni domen. Kada se slika nađe u ovom domenu moguća je primena phase coding tehnike, odnosno moguće je kodiranje faze naše slike. Iako ovo nije preporučeni metod, jer je ljudsko oko osetljivo na promene u fazi video materijala, hteli smo da vidimo da li uparivanje ove naizgled nestabilne tehnike u domenu slika, sa ustanovljenim rešenjem koje jeste LSB tehnika, može da proizvede potencijalno bolje rezultate.

Nažalost, mane phase coding tehnike su predstavljale preveliki teret, što smo pokazali kroz naše praktično rešenje. Promena faze slike proizvela je preveliki broj vizuelnih artefakata koji su učinili našu sliku neprepoznatljivom. Iako je originalna poruka ostala nepromenjena, odnosno uspešno sakrivena, tragovi samog sakrivanja su bili više nego primetni. Ovim smo pali osnovni test steganografije, a to je da tragovi sakrivanja ne smeju da postoje, tj. treće lice nikako ne sme da primeti da je došlo do prikrivanja podataka. Naše rešenje potencijalno može da nađe primenu u kriptografiji, što je i cešća primena hibridnih steganografskih rešenja. Retko možemo da nađemo dve steganografkse motode koje daju bolje rezultate od samo jednog metoda, pa mnogo češće vidimo da se uparuju kriptografske tehnike, kojima se poruka prvo enkodira, a onda se ovako enkodirana poruka sakrije primenom neke od steganografskih metoda. Svakako, ako se zadržimo na domenu steganografije, naše rešenje nikako neće moći da pronađe mesto na prostoru komercijalne primene, što smo pokazali ovim radom i opovrgnuli našu početnu hipotezu o kombinovanju LSB i phase coding tehnika.

**LITERATURA**

|  |  |
| --- | --- |
| [1] | „Difference between Steganography and Cryptography,“ Geeks for Geeks, 27 Mart 2023. [Na mreži]. Available: https://www.geeksforgeeks.org/difference-between-steganography-and-cryptography/. [Poslednji pristup Januar 2024]. |
| [2] | D. Tidmarsh, „A Guide to Steganography: Meaning, Types, Tools, & Techniques,“ EC Council: Cybersecurity Exchange, 12 April 2023. [Na mreži]. Available: https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/what-is-steganography-guide-meaning-types-tools/. [Poslednji pristup Januar 2024]. |
| [3] | E. Ali, Sohrawordi i P. Uddin, „A Robust and Secured Image Steganography using LSB and Random Bit Substitution,“ *American Journal of Engineering Research (AJER),* t. 8, br. 2, pp. 39-44, Februar 2019. |
| [4] | A. Divya i S. Thenmozhi, „Steganography: Various Techniques In Spatial and Transform Domain,“ *International Journal of Advanced Scientific Research and Management,* t. 1, br. 3, pp. 81-29, Mart 2016. |
| [5] | S. Chakrabarti i D. Samanta, „A novel approach to Digital Image Steganography of key-based encrypted text,“ u *2015 International Conference on Electrical, Electronics, Signals, Communication and Optimization (EESCO)*, 2015. |
| [6] | A. Nilizadeh i A. R. Naghsh-Nilchi, „A novel steganography method based on matrix pattern and LSB algorithms in RGB images,“ u *2016 1st Conference on Swarm Intelligence and Evolutionary Computation (CSIEC)*, 2016. |
| [7] | N. D. Amsden i L. Chen, „Analysis of Facebook steganographic capabilities,“ u *IEEE International conference on computing, Networking and Communications*, 2015. |
| [8] | R. Rejani, D. Murugan i V. Krishnan, „Pixel pattern based steganography on images,“ *Ictact Journal On Image And Video Processing,* t. 5, br. 3, 2015. |
| [9] | A. Kumar i R. Sharma, „A Secure Image Steganography Based on RSA Algorithm and Hash LSB Technique,“ *International Journal of Advanced Research in Computer Science and Software Engineering,* t. 3, br. 7, 2013. |
| [10] | .. Champakamala, K. Padmini i .. K. Radhika, „Least Significant Bit algorithm for image steganography,“ *International Journal of Advanced Computer Technology (IJACT).* |
| [11] | M. Karim, S. Rahman i I. Hossain, „A New Approach for LSB Based Image Steganography using Secret Key,“ u *International Conference on Computer and Information Technology (ICCIT)*, 2011. |
| [12] | D. Babya, J. Thomasa, G. Augustinea, E. Georgea i N. Michaela , „A Novel DWT based Image Securing Method using Steganography,“ u *International Conference on Information and Communication Technologies (ICICT 2014)*, 2014. |
| [13] | I. Reddy i A. Kumar, „Secured Data Transmission Using Wavelet Based Steganography and Cryptography by Using AES Algorithm,“ u *International Conference on Computational Modeling and Security (CMS 2016), Elsevier Publication*, 2016. |
| [14] | K. Patel i L. Ragha, „Binary Image Steganography in wavelet domain,“ u *IEEE International conference on industrial instrumentation and control (ICIC)*, 2015. |
| [15] | W. I. A. Al-Mazaydeh, „Image Steganography using LSB and LSB+Huffman Code,“ *International Journal of Computer Applications,* t. 99, br. 5, pp. 17-22, Avgust 2014. |
| [16] | M. M. Hashim, M. S. M. Rahim, F. A. Johi, M. S. Taha i H. S. Hamad, „Performance evaluation measurement of image steganography techniques with analysis of LSB based on variation image formats,“ *International Journal of Engineering & Technology,* t. 7, br. 4, pp. 3506-3514, 2018. |
| [17] | E. E. A. b. Elgabar, „Comparison of LSB Steganography in BMP and JPEG Images,“ *International Journal of Soft Computing and Engineering (IJSCE),* t. 3, br. 5, pp. 91-95, 2013. |
| [18] | B. Sinha, „Comparison of PNG & JPEG Format for LSB Steganography,“ *International Journal of Science and Research (IJSR),* t. 4, br. 4, pp. 198-201, 2013. |
| [19] | M. S. Yadnya, B. Kanata i M. K. Anwar, „Using Phase Coding Method for Audio Steganography with the Stream Cipher Encrypt Technique,“ u *First Mandalika International Multi-Conference on Science and Engineering 2022, MIMSE 2022 (Informatics and Computer Science)*, 2022. |
| [20] | M. S. Atoum, G. Sulong, A. Zeki i S. Ibrahimn, „Exploring the Challenges of MP3 Audio Steganography,“ u *2013 International Conference on Advanced Computer Science Applications and Technologies (ACSAT)*, 2013. |
| [21] | S. Kumar, B. Barnali i G. Banik, „LSB Modification and Phase Encoding Technique of Audio Steganography Revisited,“ *International Journal of Advanced Research in Computer and Communication Engineering,* t. 1, br. 4, 2012. |

1. Peak Signal-to-Noise Ratio – odnos između maksimalne vrednosti signala u šuma [↑](#footnote-ref-1)