UNIVERZITET SINGIDUNUM
BEOGRAD
DEPARTMAN ZA POSLEDIPLOMSKE STUDIJE

DOKTORSKA DISERTACIJA

Jedna nova klasa hibridnih steganografskih metoda u prostornom domenu

MENTOR:

Prof. dr Milan Milosavljević

STUDENT: Predrag Milosav

BROJ INDEKSA: 2018/460024

Beograd, 2023.god.

Mentor:

Prof. dr Milan Milosavljević, mentor, redovni profesor

Univerziteta Singidunum

Članovi komisije:

1. Prof. dr Milan Milosavljević, mentor, redovni profesor

Univerziteta Singidunum

2. Prof. dr Mladen Veinović, redovni profesor

Univerziteta Singidunum

3. Dr Zoran Banjac, viši naučni saradnik

Institut Vlatacom

Datum odbrane disertacije:

_____

Zahvalnica

Zahvaljujem se mentoru prof. dr Milanu Milosavljeviću kao i komentoru, dr Zoranu Banjcu, na kontinuiranoj podršci, dragocenim savetima i učestvovanju tokom izrade ove doktorske disertacije. Zahvaljujem Institutu Vlatacom, koji mi je pružio priliku i omogućio vreme i resurse za vršenje istraživanja, kao i veliku podršku tokom izrade disertacije. Takođe, zahvaljujem se i članovima tima sektora za kriptografiju, čiji sam bio deo, u realizaciji projekta razvoja uređaja za šifrovanje i bezbednu razmenu fajlova: master informatičaru Dejanu Tomiću i dipl. inž. elektrotehnike i računarstva Tijani Aleksić.

Posvećeno mojim roditeljima

Rezime

Osnovni cilj ovog istraživanja je predlog steganografskog sistema baziranog na ključu (*key-based*) u kojem je poboljšan odnos kapaciteta i metrika kvaliteta slike koji predstavlja stego-objekat uz smanjenje detektabilnosti skrivenog sadržaja. Glavni doprinos predloženog steganografskog sistema je novi algoritam za odabir stego oblasti. Algoritam za odabir oblasti stego-nosioca baziran je na grupisanju piksela objekata prikrivanja u unapred određen broj klastera. Cilj ovakvog odabira stego-oblasti (klastera) je grupisanje što je više moguće homogenih delova slike kako bi se ta područja popunila sa što manje pravougaonih oblika. Budući da podaci o definisanim pravougaonicima predstavljaju ključ sistema, kapacitet dodatnog tajnog kanala se na ovaj način minimizira. Na dobijenim stego-nosiocima vrši se ugradnja testnog slučajnog sadržaja kako bi se procenila njegova detektabilnost. Kombinacijom predložene metode odabira područja sa steganografskom metodom minimalne decimalne razlike (*MDD*), kreiran je sistem sa optimalnim odnosom između detektabilnosti tajnog sadržaja, kvaliteta i kapaciteta nosioca kao i dužine stego-ključa. Konačno, analizom dobijenih rezultata date su smernice o načinu upotrebe predloženog sistema kao i važni zaključci vezani za način odabira steganografskih nosilaca. Predloženi koncept dobija svoju verifikaciju u jednom praktičnom sistemu za siguran prenos datoteka kontrolisane kriptografske snage.

Ključne reči: steganografija, kriptografija, adaptivna steganografija, *K-means*, bit najmanje težine, minimalna decimalna razlika, histogram, RMSE, PSNR, SSIM, stego-analiza

Naučna oblast: Računarstvo i informatika

Sadržaj:

Spisak tabela

Spisak slika

Lista skraćenica i stranih izraza

AES (eng. *Advanced Encryption Standard*)……	*Napredni enkripcioni standard*
Alice&Bob……	*Žargonski naziv za stranu A i stranu B komunikacije*
Availability……	*Dostupnost*
Blind……	*Slep, slepa metoda procene derivata koja ne zahteva originalni objekat*
Bpp (Bits per Pixel)……	*Način izražavanja kapaciteta stego-objekta u zavisnosti od broja izmenjenih bita po pikselu nosioca*
C++……	*Programski jezik za razvoj softvera*
Confidentiality……	*Poverljivost*
Cropping……	*Obrezivanje, izrezivanje*
DSSIM (*Structural Dissimilarity)*……	*Strukturalna različitost*
Eavesdropper……	*Prisluškivač, onaj koji neovlašćeno prisluškuje komunikaciju*
Fingerprint……	*Otisak prsta, lični pečat*
Fragile……	*Krhko, lomljivo*
FSIM (Features Similarity Index Matrix)……	*Karakteristika matrice indeksa sličnosti*
GMSD (Gradient Magnitude Similarity Deviation)……	*Intenzitet devijacije sličnosti gradijenta*
Greyscale……	*Slika sivih nijansi*
Full HD (Full High Definition)……	*Standard rezolucije slike i digitalnog emitovanja slike - 1080p*
HVS (Human Visual System)……	*Ljudski (humani) sistem vizualizacije*
Inital bias……	*Početna pristrasnost, inicijalno ponašanje*
Integrity……	*Integritet*
Intruder……	*Provalnik, onaj koji neovlašćeno ulazi u kanal komunikacije*
IQA (Image Quality Assessment)……	*Procena kvaliteta slike*
JPG, JPEG (Joint Photographic Experts Group)……	*Vrsta formata digitalne slike kompresovane sa gubicima*
K-means……	*Metoda grupisanja vektorskom kvantizacijom*
Key-based……	*Bazirano na ključu, metoda bazirana na ključu*
LS (Least Significant)……	*Najmanjeg značaja*

LSB (Least Significant Bits)……	*Bit najniže težinske vrednosti / biti najnižih težinskoh vrednosti*
Man-in-the-middle……	*Tip napada gde se napadač nalazi u sredini komunikacionog kanala*
MDD (Minimal Decimal Difference)……	*Metoda minimalne decimalne razlike*
MSB (Most Significan Bits)……..	*Biti najviših težinskih vrednosti*
MSE (*Mean Square Error)……*	*Srednja kvadratna greška*
MS-SSIM (Multi Scale Structural Similarity)……	*Višestruka strukturalna sličnost*
Nonblind……..	*Suprotno od slep, metoda procene derivata koja zahteva originalni objekat*
Obfuscation……..	*Zamagljivanje, prikrivanje zamagljivanjem*
OpenCV……	*Softverska biblioteka za obradu slika javno dostupnog koda*
PDH (Pixel Difference Histogram)	*Histogram razlike vrednosti piksela*
Pixels-To-Impact……	*Broj piksela slike na koji se utiče, apsolutna ili relativna vrednost*
Png (Portable Network Graphics)……..	*Vrsta formata digitalne slike koja dozvoljava različite nivoe kompresije*
PSNR (*Peak Signal to Noise Ratio)……..*	*Vršni odnos signal/šum*
PVD (Pixel Value Differencing)……	*Metoda razlike vrednosti piksela*
Q Index (Quality Indeks)……	*Indeks kvaliteta*
QT……	*Razvojni softverski alat*
RGB (*red-green-blue*)……..	*Označavanje kanala u slikama u boji crvena-zelena-plava*
RMSE (*Root Mean Square Error)……*	*Koren srednje kvadratne greške*
RNG (Random Number Generator)……	*Generator slučajnih brojeva*
Robust……	*Robustan, robusno*
Rx ……	*Prijemna strana komunikacije*
Salt&pepper……	*Tip šuma u slici koji ima efekat pojave sitnih belih i crnih tačaka*
Semifragile……	*Delimično lomljivo*
SIFT (Scale-Invariant Transformation)……	*Transformacija invarijantnog (nepromenljivog) opsega*
SNR (Signal to Noise Ratio)……	*Odnos signal/šum*
SSIM (Structural Similarity Index)……	*Indeks strukturalne sličnosti*
Stego-attack……	*Stego-napad, napad na steganografski sadržaj*
SURF (Speeded-up Robust Features)……	*Ubrzana tehnika robusnih karakteristika*
Tx……	*Predajna strana komunikacije*
Watermarking……	*Vodeni žig, tehinika obeležavanja vodenim žigom*

1. Uvod

Sigurnost informacija počiva na tri osnovna stuba: poverljivost, integritet i dostupnost komunikacionog kanala - Confidentiality, Integrity, Availability. Poverljivost znači prikrivanje osetljivih informacija, softvera ili protokola od treće strane koja nema ovlašćeni pristup istim. Integritet znači pouzdanost podataka i može se obezbediti samo ako su podaci dobijeni iz pouzdanih izvora i ako se blagovremeno a dovoljno često ažuriraju. Dostupnost znači mogućnost korišćenja informacija ili resursa na način i u vreme kada želi konkretan korisnik. Ako izuzmemo državne službe i organizacije (vojska, policija, bezbednosna služba) koje na odgovarajućoj teritoriji imaju svoje, fizički izolovane, komunikacione mreže, dolazimo do jednostavnog zaključka da je svaki pojedinac (ili organizacija) koji koristi globalnu komunikacionu mrežu izložen različitim sajber pretnjama i opasnostima. Bivstvovanje u sajber svetu nosi sa sobom mnoge rizike i izazove. Da bi kretanje, u tom virtualnom prostoru, bilo bezbednije potrebna su izvesna znanja o mogućim pretnjama kao i poštovanje skupa pravila koje jednim imenom nazivamo – bezbednosna kultura. Za pojedinca (ili organizaciju), u cilju unapređenja sigurnosti svojih informacija (uzimajući u obzir tri pomenuta postulata) potrebna je, pre svega, odgovarajuća edukacija koja dalje implicira upotrebu razvijenih alata i tehnologija. Sajber bezbednost je oblast koja je u fokusu poslednjih godina i koja raste i razvija se u različitim pravcima enormnom brzinom. Centralna tačka sajber bezbednosti, a samim tim i pomenute bezbednosne kulture, je kriptografija i njoj srodne naučne discipline. Stoga je razvoj pomenutih alata i tehnologija kao i implementacija novih, efikasnijih i bezbednijih rešenja, u oblasti kriptografije, danas nasušna potreba civilizacije.

1.1. Identifikacija problema i predlog rešenja

U skladu sa napretkom kompjuterskih i komunikacionih tehnologija, obrade signala i mašinskog učenja, evidentan je kontinuirani napredak sistema za analizu saobraćaja. Ovakvi sistemi, instalirani na velikim telekomunikacionim čvorištima, svakodnevno obrađuju ogromnu količinu saobraćaja, stvarajući mogućnost nezakonitog narušavanja privatnosti komunikacija [1]. Povećanjem snage ovakvih sistema, postoji potreba za razvojem novih steganografskih tehnika, poboljšavajući njihovu robusnost i otpornost na stego-analizu i stego-napade. Razvoj novih tehnika, koje dovode do poboljšanja navedenih karakteristika stego-objekata, podrazumeva korišćenje složenijih algoritama, a veća procesorska snaga potrebna za ovu vrstu obrade je cena koju treba platiti. Poboljšanje kvaliteta (izraženog kroz numeričke parametre za procenu kvaliteta) stego-objekata kombinacijom različitih metoda i tehnika, kvantifikovanih kroz različite parametre stego-nosioca, jedan je od glavnih ciljeva u ovom kontekstu. Osim toga, jedan od ciljeva razvoja novih metoda i tehnika je smanjenje preciznosti prepoznavanja postojanja tajnog sadržaja u stego-objektu.

1.2. Doprinos disertacije

Osnovni doprinos istraživanja jeste razvoj modernog, konkurentnog i kvalitetnog sistema adaptivne steganografije koji, svojim osobinama, zadovoljava aktuelne standardne bezbedne komunikacije. Ideja za pokretanje razvoja i implementacije efikasnog sistema sigurne razmene podataka je potreba da se dokaže izvodljivost i potvrdi upotrebna vrednost jednog ovakvog sistema. Razvoj algoritma adaptivne steganografije koji, sa jedne strane nije previše procesorski zahtevan, dok sa druge strane po kvalitativnim i bezbednosnim kriterijumima može da parira znatno složenijim sistemima, implicira budući širok spektar primene ovakvog

sistema. Podizanjem svesti o bezbednosti komunikacija, od nivoa prosečnog konzumenta internet servisa pa do velikih organizacija kojima je neophodno da štite svoju komunikaciju, otvaraju se višestruke mogućnosti upotrebe ovakvog sistema bezbedne razmene podataka. Mogućnosti buduće implementacije ovakvih sistema su ogromne sa višestrukim ciljevima, od čuvanja privatnih podataka, bezbedne razmene poverljivih podataka, sigurne komunikacije iz nebezbednih okruženja, sprečavanja curenja poverljivih poslovnih ili državnih informacija…

U poglavljima koja slede biće prikazana motivacija za ovakvo istraživanje, polazna teoretska osnova, implementacija ideje, dizajn obavljenih eksperimenata kao i analiza dobijenih rezultata. Konačno, biće apostrofirane konkretne prednosti primene ove metodologije za dizajn budućih korisničkih aplikacija za bezbednu razmenu podataka.

1.3. Kriptografija

Reč kriptografija (ili kriptologija) potiče od starogrčkih reči „*kryptos*“ što znači – „tajno“ i „*graphien*“ što znači – „pisanje“, ili „*logia*“ – što znači „nauka/proučavanje“. Kriptografija je drevna tehnika sigurne komunikacije koja odgovarajućim metodama modifikuje čitljive poruke tako da one na svom komunikacionom putu budu nerazumljive malicioznoj, potencijalnoj trećoj strani kojoj poruke nisu inicijalno namenjene. Kriptografija je tokom svoje istorije više imala formu umetnosti, vešte i visprene igre nadmudrivanja strane koja komunicira i strane koja želi da otkrije tu komunikaciju. Period do početka 20. veka ili do Drugog svetskog rata, tehnološki posmatrano, smatra se erom klasične kriptografije. Prva polovina 20. veka, dva svetska rata i ubrzani razvoj tehnike i tehnologije, pre svega u vojne svrhe, učinio je i to da kriptografija postane naučna disciplina. Početak digitalne ere, u periodu nakon završetka Drugog svetskog rata, smatra se početkom ere moderne kriptografije. Da bi jedan kriptografski sistem bio potpun potrebno je da postoji nekoliko elemenata:

- Strane koje žele bezbedno da komuniciraju, prijemna i predajna, u literaturi često obeleženi kao *Tx* i *Rx*, odnosno *Alice* i *Bob*.
- Komunikacioni kanal.
- Treća strana koja neovlašćeno želi da presretne (otkrije, ošteti, promeni ili uništi) poverljivu komunikaciju Alise i Boba, u literaturi često označena kao *Eve* (od engleskog *eavesdropper*) ili *Trudy* (od engleskog *intruder*).
- Primenjeni kriptografski algoritam koji Alisa i Bob koriste za svoju bezbednu komunikaciju.
- Primenjeni kriptografski ključ, koji se u sistemu smatra tajnim.
- Otvoreni tekst (*plain text*) je poruka koja je u svojoj otvorenoj formi jedan od ulaza u kripto-algoritam na predajnoj strani i koji je (očekivani) izlazni objekat algoritma na prijemnoj strani.
- Šifrat (*cypher text*) – izlazni (nečitljivi) objekat kripto-algoritma na predajnoj strani koji putuje komunikacionim kanalom i predstavlja jednu od ulaznih veličina algoritma na prijemnoj strani.

U ovakvoj podeli kriptografski algoritam i ključ zajedno čine kriptografski protokol koji u opštem slučaju predstavlja skup pravila koji razumeju i poštuju strane u komunikaciji a u cilju obezbeđivanja njene tajnosti i privatnosti.

Kriptografija, još od svoje drevne forme pa sve do modernih kriptografskih sistema, ima svoja dva osnovna cilja: prvi cilj je obezbeđivanje privatnosti komunikacije, dok je drugi cilj obezbeđivanje autentičnosti i integriteta poruke.

Kako je već navedeno kriptografija se, po svom istorijskom razvoju, može podeliti na klasičnu i modernu. Klasična kriptografija se prema tipovima šifara deli na [2]:

- Šifre transpozicije (transpozicija kolona, dvostruka transpozicija kolona)
- Šifre supstitucije (monoalfabetske, poligramske, polialfabetske)
- One-time-pad
- Kodne knjige
- Moderna kriptografija se deli na:
- Simetrična kriptografija (sekvencijalne šifre, blokovske šifre)
- Asimetrična kriptografija (kriptografija javnim ključem, digitalni potpis)

Zbog prirode ovog rada poseban akcenat treba staviti na simetrične kriptografske sisteme a u okviru njih na blokovske šifre. Razlog za to je što bi se implementacija sistema steganografije, predložena u ovom radu, mogla na odgovarajući način kombinovati sa kriptografskim sistemom pomenute klase. Blokovski šifarski sistemi podelom otvorenog teksta na delove iste, fiksne, definisane dužine odgovarajućim algoritmom generišu blokove šifrata, ponavljajući isti postupak dovoljan broj puta. Šifrat jednog bloka dobija se nad jednim blokom otvorenog teksta ponavljanjem funkcije F određeni broj rundi. Funkcija F ima osobinu da zavisi od izlaza prethodne runde i upotrebljenog ključa K. Blokovske šifre su koncipirane tako da kombinuju svojstva difuzije, konfuzije i kompletnosti. Tipični predstavnici ovakvih šifarskih sistema su: DES, 3DES i AES.

AES (Advanced Encryption System) je algoritam komplikovane matematičke strukture sa svojstvima takvim da je otporan na poznate napade, na modernim računarima može se izvršiti veoma brzo uz mogućnost paralelizacije procesa, sa mogućnošću implementacije na različitim procesorskim arhitekturama i smart karticama. Neke od karakteristika AES su sledeće:

- Dužina bloka otvorenog teksta može biti 128,192 i 256 bita

- Dužina ključa (nezavisno od dužine bloka otvorenog teksta) može biti 128, 192 ili 256 bita
- U zavisnosti od dužine ključa, proces nad jednim blokom otvorenog teksta se obavlja od 10 do 16 rundi
- Svaka runda podrazumeva 4 različite funkcije (nelinearni sloj – zamena bajtova, sloj linearnog mešanja- pomeranje redova, nelinearni sloj – mešanje kolona, dodatni sloj ključa). U engleskoj literaturi ove 4 funkcije se označavaju kao: SBox, ShiftRow, MixColumns, AddRoundKey.

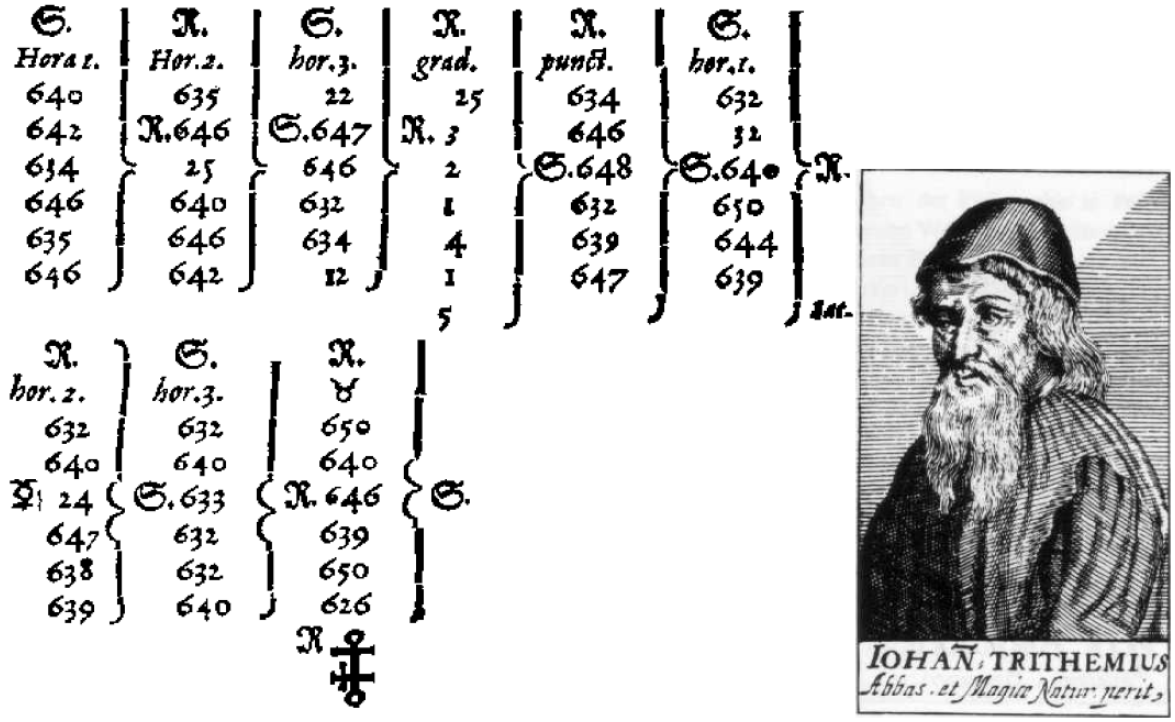
AES algoritam ima svojstvo da se sve operacije obavljaju nad dvodimenzionalnim nizovima bita, odnosno nad matricama stanja odgovarajuće veličine. Proces šifrovanja i proces dešifrovanja obalja se tako što se ulazni blok podataka kopira u odgovarajuću matricu nad kojom se dalje sprovode pomenute funkcije manipulacije bitima. Pošto je proces (enkripcije ili dekripcije) nad jednim blokom završen, podaci se kopiraju u izlazni blok dostupan za dalju upotrebu. Ulazni podaci AES algoritma se tretiraju kao blokovi podataka upakovani u matrice dimenzije 4x4.

AES256 je predstavnik originalne ideje opisanog algoritma sa osobinom da koristi ključ dužine 256 bita (16 bajtova). Snaga AES256 ogleda se u tome da je modernim računarima potrebno 2,29*1032 godina za razbijanje ovog algoritma brutalnom silom. Takođe je potrebno akcentovati da šifrat dobijen ovakvim algoritmom ima sve osobine slučajnog binarnog niza što je važan podatak za koncipiranje eksperimenata kojim se ovaj rad bavi u narednim poglavljima.

1.4. Tehnike ugrađivanja sadržaja

Steganografija je izvedena od grčke reči "*stego*" što znači - "prikriven" i "*graphia*" što znači - "pisanje". Steganografija je drevna tehnika tajne komunikacije a saznanja o najranijim oblicima njene upotrebe potiču još iz stare Kine. Tajna poruka je bila ispisana vrlo finom svilom ili papirom, a zatim je smotana u kuglu i zalivena vosak, da bi je glasnik nakon toga progutao ili vešto sakrio. Na drugoj strani planete, Herodot je spomenuo u jednom od svojih fundamentalnih istorijskih dela, u periodu oko 400. godine pre nove ere, o tradiciji i veštini tajnog pisanja. On u svojim spisima spominje sukobe između Grčke i Persije, gde kralj po imenu *Histiaeus* ohrabruje *Aristagoru* iz Mileta na ustanak protiv persijskog kralja. Brijao bi glave svojih najpouzdanijih slugu i tetovirao skalpove tajnom porukom a potom čekao da kosa izraste. Nakon toga, sluga bi putovao između granica ne noseći sa sobom ništa sporno. Na mestu prijema tajne poruke bi mu glava bila ponovo obrijana a poruka bi bila pročitana i prenesena. Još jedna drevna tehnika bazirana je na ispisivanju tajnih poruka citrusnom tečnosti (npr. limunovim sokom), gde bi kao takva bila neprimetna i nevidljiva potencijalnom napadaču dok se na mestu prijema mogla pročitati koristeći plamen, uz čiju pomoć napisana poruka postaje vidljiva i čitljiva [3]. Sa napretkom nauke, a pre početka ere digitalnih komunikacija, razvijen je jedan poseban pravac u hemiji koji se upravo bavi načinima i tehnikama tajnog pisanja a potom i mehanizmima ekstrakcije tajne poruke.

Johannes Trithemius (1462-1516) bio je nemački kaluđer. Njegovo delo: „Steganografija: umetnost kroz koju je pisanje skriveno a koja za otkrivanje napisanog zahteva upotrebu ljudskog uma.", objavljena kao trilogija na latinskom. Prva dva dela njegovih spisa su neke od prvih knjiga o kriptologiji u kojima se opisuju metode sakrivanja poruke u pisanoj formi. Treći deo trilogije je nezavisna knjiga o okultnoj astrologiji i sadrži niz tabela brojeva [4].



Slika 1. Johannes Trithemius

U novije vreme, tokom Drugog svetskog rata, Nemci su izmislili upotrebu mikrotačaka. Slika koja sadrži veoma važne detalje smanjena je na veličinu mikrotačaka. Takav način prenosa tajne poruke smatra se nedavnom evolucijom steganografije. Još jedan primer steganografije je tokom vijetnamskog rata kada su zarobljene američke oružane snage pokretima ruku, tokom fotografskih sesija, slali odgovarajuće znake kako bi preneli neke vojne tajne .

Tokom istorije i drevnih tehnika tajnog pisanja uglavnom se nije mogla napraviti jasna granica između kriptografije i steganografije. U eri digitalnih komunikacija, tehnike kriptografije i steganografije su međusobno divergirale i nastavile svoj razvoj u nezavisnim pravcima. Ova činjenica ne znači da se, pomenute tehnike, međusobno ne kombinuju ali je danas potpuno razgraničen koncept gde se kriptografija koristi da sakrije sadržaj poruke dok se steganografija koristi da sakrije postojanje tajne poruke. Kombinovanje ovih tehnika u modernim sistemima podrazumeva da se prvo obavi proces šifrovanja a potom proces sakrivanja tajnog sadržaja u

odgovarajući nosilac. Tehnika ugrađivanja tajnog sadržaja, u digitalnoj eri, našla je svoju primenu ne samo u cilju prenosa poruke. Slične tehnike ugradnje tajnog sadržaja u odabrani nosilac generalno se može koristiti za autentifikaciju i zaštitu autorskih prava. Ovakva tehnika naziva se tehnikom Vodenog Žiga (*Watermarking*). Vodeni žig se može koristiti za kreiranje svojevrsnog digitalnog potpisa, kako bi on bio prepoznatljiv. Takvom tehnikom obeležavanja se može koristiti za označavanje digitalne datoteke tako da žig bude vidljiv (vidljivi vodeni žig) ili vidljiv samo njenom kreatoru (nevidljiva oznaka). Glavna svrha vodenog žiga je sprečavanje ilegalnog kopiranja ili polaganje prava na vlasništvo nad digitalnim medijima. Iako su, u tehničkom smislu, principi utiskivanja poruke slični, steganografija ima za cilj prenos tajne poruke, dok tehnika vodenog žiga ima za cilj zaštitu i potvrdu autentičnosti digitalne datoteke nad kojom je primenjena.

1.4.1. Steganografija

Steganografija je naučna disciplina koja se, u svojoj najgrubljoj podeli, deli na tehničku steganografiju i lingvističku steganografiju [5]. Predmet ovog rada i istraživanja je fokusiran na tehničku steganografiju. Sa početkom razvoja moderne kriptografije, nakon Drugog svetskog rata, i početkom upotrebe računara i računarskih algoritama u toj oblasti javila se potreba i za adekvatnim steganografskim procesima u digitalnom domenu. Šifrat koji je, sa početkom moderne kriptografije i sa početkom računarske ere, prešao u digitalnu formu bilo je potrebno utisnuti u adekvatan steganografski nosilac. Da bi se tehnika smatrala steganografskom potrebna su četiri elementa [6]:

- Objekat prikrivanja (nosilac): izvorni objekat koji se koristi kao nosilac za skrivanje informacija.
- Poruka: tajne informacije koje želimo sakriti.

- Stego-objekat: rezultat utiskivanja poruke ili tajne informacije u početni objekat prikrivanja (nosilac).
- Stego-metoda: algoritam koji se koristi za ugrađivanje i izdvajanje poruka u i iz stego-objekta.

Kako bi skup pojmova bio kompletan potrebno je definisati još dva pojma:

- stego-oblast je deo (područje) objekta prikrivanja (nosioca) u kojem se izvodi steganografski proces.
- Stego-ključ, metode bazirane na ključu (*key-based*), gde je ključ informacija o načinu izvedbe steganografske metode na predajnoj strani (*Tx*) koju je potrebno poslati na prijemnu stranu (*Rx*) kako bi tajna informacija bila pravilno ekstrahovana.

Kapacitet nosioca označava količinu skrivenih informacija koju stego-objekt može preneti. Izražava se u apsolutnim iznosima u bajtovima ili relativno u procentima u odnosu na veličinu samog stego-objekta. Skup numeričkih vrednosti kojim se procenjuje kvalitet stego-objekta naziva se parametrom za procenu kvaliteta. U slučaju različitih tipova steganografskih procesa, koji kao stego-objekte generišu različite tipove fajlova, koriste se i različiti parametri za procenu kvaliteta. Pored navedenog, još jedna važna karakteristika steganografskog algoritma je svojstvo neprimetnosti (detektabilnosti) promene statističkih karakteristika nosioca, što pokazuje koliko je teško utvrditi postojanje skrivenog sadržaja. Konačno, stalni problemi vezani za steganografske tehnike su kompromis između kapaciteta stego-nosioca, kvaliteta i robusnosti stego-objekta, kao i procesorske snage potrebne za izvršavanje specifičnog algoritma. Danas se kao steganografski nosilac može koristiti digitalna datoteka u bilo kom formatu. Najčešće korišćeni tipovi digitalnih datoteka koji se danas koriste kao stego-

nosioci su slike, audio i video fajlovi kao i fajlovi u pdf formatu. Zbog same razlike u prirodi navedenih tipova datoteka, došlo je i do izvesne divergencije steganografskih tehnika za različite tipove nosioca. Poseban vid steganografije, koji se sve više aktuelizuje u poslednjih nekoliko godina, je steganografija mreže ili mrežnog protokola. Cilj ovog tipa steganografije je prikrivanje podataka korišćenjem mrežnih protokola kao što su TCP, UDP, ICMP, IP i drugih, kao objekte prikrivanja. Steganografija u mreži ili mrežnom protokolu može biti bazirana i implementirana na nivou skrivenih kanala koji se javljaju u mrežnom sloju OSI modela [7]. U modernoj računarskoj literaturi često se pominje izraz „obfuskacija“ (engl. - *obfuscation*) što bi u prevodu sa engleskog jezika značilo „zamagljivanje“. Potrebno je napraviti jasnu distinkciju između kriptografije, obfuskacije i steganografije. Već je pomenuto da kriptografija služi kako bi sakrili sadržaj poruke dok steganografija ima funkciju skrivanja postojanja same poruke. Obfuskacija, kao metoda, ima ulogu zamagljivanja u cilju težeg tumačenja eksponiranog objekta. Za objekat nad kojim je primenjena metoda obfuskacije možemo reći da posmatrač ima svest da on postoji ali ne razume jasno njegov sadržaj, iako nad njim nije primenjena metoda kriptografije koja bi zahtevala definisani kriptografski algoritam i odgovarajući kriptografski ključ. Proces „zamagljivanja“, odnosno obfuskacije, često se koristi nad kompajliranim kodom, kako bi potencijalnom napadaču, koji je svestan njegovog postojanja, otežao pristup i uvid u isti.

U poslednjih nekoliko godina steganografija nalazi sve veću primenu, ne samo u prenosu tajnih poruka, već i u zaštiti podataka o ličnosti, privatnih i medicinskih podataka. Pregršt radova, različitih autora, objavljenih u prethodnih petnaest godina bavi se upotrebom steganografije u cilju zaštite medicinskih podataka pacijenata [8]. Radiologija, kao posebna grana medicine, svojim tehnikama nastoji da vizualizuje ljudsko telo i njegove delove u cilju otkrivanja patoloških promena kako bi se one pravovremeno lečile. Pomenuta radiološka

vizuelizacija, sa jedne strane, i potreba za zaštitom privatnih i medicinskih podataka pacijenta, sa druge strane, otvorila je vrata za bližu međusobnu saradnju steganografije i radiologije kao, prethodno ne tako bliskih, naučnih disciplina. Ovakva, novonastala, simbioza naučnih disciplina dovela je do značajne aktuelizacije upotrebe steganografskih metoda u nosiocima koji sada imaju formu i osobine radioloških slika. Efekat ovakve simbioze učinio je da jedan poseban pravac razvoja steganografije modifikuje postojeće i razvija nove metode upravo za specifične (radiološke) tipove nosilaca [9].

1.4.2. Tehnika vodenog žiga - Watermarking

Digitalni vodeni žig je tehnika zaštite koja se koristi u oblasti sigurnosti informacija, zaštite autorskih prava, autentifikacije podataka i kontrole emitovanja. Vodeni žig je ugrađen u štićeni nosilac, koji može biti audio, video ili drugi tip digitalne datoteke, na način takav da je izobličenje uzrokovano ugradnjom dovoljno malo da bi moglo biti primećeno. U isto vreme, ugrađeni vodeni žig mora biti dovoljno pouzdan i robustan da izdrži konvencionalnu degradaciju, izmene ili namerne napade. Osim toga, za prihvatljive nivoe izobličenja i robusnosti, potrebno je da se što više podataka ugradi u određeni nosilac i tako poveća njegov kapacitet. Podilchuk i Delp predstavili su opšti okvir za ugrađivanje i detekciju/dekodiranje vodenih žigova [10], uzimajući u obzir njihove razlike u implementaciji i različitim algoritmima i primenama vodenih žigova u kontekstu autorskih prava. Tehnologija digitalnog vodenog žiga razvijena je kao pogodan alat za identifikaciju izvora, kreatora, vlasnika, distributera ili ovlašćenog korisnika dokumenta ili digitalnog sadržaja. Takođe se može koristiti za identifikaciju i praćenje podataka koji se ilegalno distribuiraju. Postoje dva glavna koraka u procesu obeležavanja digitalnim vodenim žigom: 1) ugrađivanje vodenog žiga u kojem je on umetnut u sadržaj nosioca i 2) izdvajanje vodenog žiga, u kojem se on izdvaja iz nosioca. Danas postoji niz algoritama za utiskivanje vodenih žigova.

Važno je definisati kriterijume za njihov opis i klasifikaciju kako bi se razumeo način njihove primene. Pa tako postoje slepi (*blind*) i ne slepi (*nonblind*) vodeni žigovi u zavisnosti da li je originalni nosilac potreban za njihovu ekstrakciju ili nije potreban. Dalje, primetni vodeni žigovi naspram neprimetnih u zavisnosti da li autor nosioca, koji se štiti, želi da žig bude uočljiv ili neuočljiv kako bi se kasnije dokazala zloupotreba. Takođe jedna od podela može biti na privatne i javne vodene žigove u zavisnosti od ciljne grupe koja ima mogućnost da ih prepozna i ekstrahuje. Po analogiji na podelu kriptografskih algoritama, tehnike vodenih žigova mogu se takođe podeliti na simetrične i asimetrične. Jedna od važnih podela vodenih žigova je i na krhke (*fragile*) i robusne (*robust*). Ideja je da su krhki vodeni žigovi dizajnirani tako da budu oštećeni ili uništeni čak i pri najmanjoj promeni njihovog nosioca dok robusni vodeni žigovi imaju osobinu da zadrže svoju formu i u slučajevima veoma invanzivnih napada na njihove nosioce. Polu-krhki (*semifragile*) su razvijeni kako bi detektovali svaki pokušaj napada ili neovlašćene modifikacije nosioca dok, sa druge strane, dozvoljavaju pojedine vrste modifikacija ili obrade svojih nosilaca. Takođe, po analogiji na osnovnu podelu steganografskih metoda, podela tehnika vodenog žiga može biti i na one koji se implementiraju u prostornom domenu u odnosu na one koje se implementiraju u frekvencijskom domenu nosioca.

Ako govorimo o podeli prema tipovima aplikacija za koje se koriste vodeni žigovi postoje:

- Tipovi vodenih žigova za zaštitu autorskih prava
- Vodeni žigovi za potvrdu i verifikaciju autentičnosti njihovih nosilaca i autora
- *Fingerprint* vodeni žigovi koji služe da nedvosmisleno dokažu autentičnost i jedinstvenost digitalnih dokumenata

- Vodeni žigovi koji imaju namenu za kontrolu, proveru i utvrđivanje kopiranja i umnožavanja digitalnog sadržaja
- Vodeni žigovi koji služe za kontrolu, nadzor i upravljanje uređajima i sistemima

Detaljan pregledni rad sa prikazom različitih tehnika vodenog žiga i mogućnosti njihovih aplikacija prikazan je u [11] i [12].

1.5. Metode za procenu kvaliteta slike

Cilj svakog steganografskog algoritma je postizanje najučinkovitijeg finalnog proizvoda sistema, odnosno stego-objekta: minimizacija vizuelnih izobličenja i veći kapacitet stego-objekta, veća otpornost na stego-analitičke alate i napade, veća robusnost stego-objekta, bolje performanse izražene u numeričkim vrednostima za procenu kvaliteta nosioca, manje vremena obrade potrebno za utiskivanje i ekstrakciju tajnog sadržaja. Da bi se precizno okarakterisala efikasnost algoritama, bilo je potrebno definisati različite metode evaluacije i metrike koje jasno kvantifikuju kvalitet dobijenih stego-objekata kao izlaznih veličina sistema [13]. U literaturi postoje dve vrste metrike kvaliteta vizualne slike:

1. Ne-slepe (*nonblind*) metode su zasnovane na matematičkom proračunu razlike između ulazne slike (slike nosioca – objekta prikrivanja) i izlazne slike nakon utisnutog sadržaja (stego-objekta). Jasno je da takvi matematički alati zahtevaju dve slike kao ulazne argumente — osnovnu i steganografski modifikovanu.

2. Slepe (*blind*) metode ne zahtevaju originalnu sliku kao referencu za matematičke proračune, već se njihova procena zasniva na statistici prepoznavanja oblika, gde je primenjeni algoritam zasnovan na neuralnim mrežama i mašinskom učenju. Ovakve procene

kvaliteta slike se baziraju na unapred obučenim (istreniranim) sistemima pa samim tim dobijeni rezultati mogu varirati od načina, intenziteta i kvaliteta obuke neuralne mreže pomoću koje je vršeno merenje.

Predmet ovog rada je analiza generisanih stego-objekata i određivanje njihovog kvaliteta isključivo pomoću metrika koja pokazuju izobličenja u odnosu na originalne objekte prikrivanja. Stoga, u daljoj analizi, fokus će biti isključivo na *nonblind* metrikama.

Na osnovu [14] i [15] odabrane metode za procenu kvaliteta slike (*Image Quality Assessment*) i izračunavanje pojedinačnih (*nonblind*) metričkih podataka primenjene u ovom radu su sledeće:

MSE – *Mean Square Error* (srednja kvadratna greška):

$$MSE = \frac{1}{H \times W} \sum_{i=1}^{H \times W} (C_i - S_i)^2 \qquad (1)$$

MSE je najčešći i bazični procenitelj merenja kvaliteta slike. To je potpuna referentna metrika i vrednosti bliže nuli su bolje. Varijansa estimirajućeg objekta u odnosu na inicijalno ponašanje originalne slike je obuhvaćena računom srednje kvadratne greške. MSE može biti varijansa estimirajućeg objekta u slučaju procene bez inicijalnog poznavanja procenitelja. Na osnovu MSE dalje je moguće izračunati koren srednje kvadratne greške (RMSE) i koren srednje kvadratne devijacije (RMSD) koji tada imaju osobine standardne devijacije, odnosno apsolutne mere disperzije. MSE se takođe može predstaviti kao srednja kvadratna devijacija (MSD) objekta procenjivanja. MSE ili MSD predstavlja prosek kvadrata grešake. Greška je razlika između procenitelja i procenjenog ishoda. To je funkcija rizika, s obzirom na očekivanu vrednost kvadrata greške ili kvadrata gubitaka.

RMSE – *Root Mean Square Error* (koren srednje kvadratne greške):

$$RMSE = \sqrt{MSE} \qquad (2)$$

RMSE je još jedna vrsta tehnike merenja greške koja se koristi obično za merenje razlika između vrednosti načinjenih distorzija slike i originalne vrednosti. RMSE procenjuje veličinu greške i to je savršena mera tačnosti koja se koristi za percipiranje razlike nastalih promena tokom procesa obrade slike.

SNR – *Signal to Noise Ratio* (odnos signal/šum)

$$SNR = 10\,log_{10}\left(\frac{\sum_{i=1}^{H\times W} C_i^2}{\sum_{i=1}^{H\times W}(C_i - S_i)^2}\right) \qquad (3)$$

Odnos signal/šum (*SNR*) se koristi kod fotografije i video produkcije za karakterizaciju kvaliteta slike. Osetljivost (digitalnog ili analognog) filmskog sistema za snimanje obično se opisuje u terminima nivoa signala koji daje granični nivo *SNR*. Industrijski standardi definišu osetljivost u smislu ekvivalenta *ISO* parametra za osetljivost senzora, koristeći *SNR* pragove (pri prosečnoj osvetljenosti scene) od 40:1 za "odličan" kvalitet slike i 10:1 za "prihvatljiv" kvalitet slike. *SNR* se obično kvantifikuje u decibelima (dB) snage signala u odnosu na snagu šuma, iako se u polju slike koncept "snage" ponekad uzima kao veličina naponskog signala. Tako da SNR od 20 dB najčešće znači odnos 100:1 optičke snage.

PSNR – Peak Signal to Noise Ratio (vršni odnos signal/šum)

PSNR se koristi za izračunavanje odnosa između maksimalno moguće snage signala i snage distorzionog šuma koja utiče na kvalitet njegove reprezentacije. Ovaj odnos dve slike se izračunava i izražava u decibelima. *PSNR* se obično računa pomoću logaritamske skale zbog širokog dinamičkog opsega signala. Odnos vršnog signala i šuma je najčešće korišćena mera procene kvaliteta kompresije slike sa gubicima usled primenjenih kodeka. Signal se smatra

originalnim podacima, a šum je greška nastala kompresijom ili izobličenjem. *PSNR* se smatra približnom procenom ljudske percepcije kvaliteta slike nastalom promenama, kompresijom i izobličenjima. Kod degradacije, usled kompresije, kvaliteta slike i videa, vrednost *PSNR* varira od 30 do 50 dB za 8-bitni prikaz podataka i od 60 do 80 dB za 16-bitno predstavljene podatke. *PSNR* se numerički izračunava pomoću sledećeg izraza:

$$PSNR = 10\,log_{10}\left(\frac{Max^2}{MSE}\right) \qquad (4)$$

gde je *Max* najveća vrednost intenziteta piksela po kanalu, npr. 255

SSIM – Structural Similarity Index **(indeks strukturalne sličnosti)**

Metoda indeksa strukturalne sličnosti je model zasnovan na percepciji. U ovoj metodi, degradacija slike se smatra promenom percepcije u strukturnim informacijama. *SSIM* takođe korespondira sa nekim drugim važnim činjenicama zasnovanim na percepciji, kao što su maskiranje osvetljenosti, kontrastno maskiranje, itd. Termin strukturne informacije naglašava jako međuzavisne piksele ili prostorno bliske piksele. Ove međusobne zavisnosti piksela upućuju na neke važnije informacije o vizuelnim karakteristikama slike. Maskiranje svetla je pojam gde je zona izobličenja slike manje vidljiva na rubovima oblasti. Sa druge strane maskiranje kontrasta je pojam koji opisuje izobličenja koja su manje vidljiva u teksturama slike.

$$SSIM(x,y) = \frac{(2\mu_x\mu_y+C_1)(2\sigma_{xy}+C_2)}{(\mu_x^2+\mu_y^2+C_1)(\sigma_x^2+\sigma_y^2+C_2)}\sigma_y \qquad (5)$$

gde su $\mu_x, \mu_y, \sigma_x, \sigma_y$ i σ_{xy} srednje vrednosti, standardne devijacije i kros-varijanse za slike x i y.

Q index (indeks kvaliteta)

Više različitih autora bavilo se definisanjem što je moguće boljeg i sveobuhvatnijeg parametra za procenu kvaliteta slike. Ideja je razvoj parametra koji će upotrebom matematičkih formula što je moguće bliže dati rezultat koji korespondira sa vizuelnom impresijom posmatrača slike. U anglosaksonskoj literaturi ovaj vizuelni doživljaj slike od strane posmatrača često se skraćeno obeležava *HVS – Human Visual System*. Autori radova [16] i [17] razvili su parametar pod imenom *Q Index,* gde su matematičkim izrazima i kvantifikacijom kvaliteta slike pomoću istih pokušali da uspostave korespodenciju sa ljudskim subjektivnim doživljajem. Q indeks može uzimati vrednosti od 0 do 1 gde se boljim kvalitetom smatraju vrednosti bliže 1, koje ukazuju na manju vizuelnu degradaciju generisane slike.

GMSD – *Gradient Magnitude Similarity Deviation*

Još jedan od parametara za procenu slike opisan je u [18]. Ova metoda koristi gradijent magnitude piksela izraženih kroz parametar osvetljenja i nijanse po RGB kanalima. Odgovarajućim filtriranjem slike dobijaju se težinski koeficijenti promene gradijenta koje je moguće uporediti sa koeficijentima dobijenim na isti način za izmenjenu sliku. Primenom matematičkih formula nad dve matrice generisanih težinskih koeficijenata dobija se jedinstvena vrednost *GMSD* parametra koji kvantifikuje nastalu distorziju u izmenjenoj slici. *GMSD* može uzimati vrednosti od 0 do 1 a boljim kvalitetom se smatraju vrednosti bliže nuli, koje ukazuju da su nastale razlike u intenzitetu gradijenata generisane slike manje. Parametar je korišćen u ovom radu za fino određivanje kvaliteta generisanih stego-objekata.

Na osnovu [19], [20] i [21] usvojena je metodologija kojom se inicijalna procena kvaliteta stego-objekata vrši bazičnim metrikama – *MSE* i *RMSE*. Nakon grube procene kvaliteta, sledeća (finija) faza procene vrši se pomoću parametara vezanih za odnos signala i šuma *SNR*

i *PSNR*. Konačna procena uključuje i parametre koji procenjuju narušenu strukturu slike uzimajući u obzir vrednosti susednih piksela, distorzije piksela u različitim pravcima i izobličenja usled maskiranja osvetljenja, što kroz numeričke vrednosti pokazuju parametri *SSIM*, *GMSD* i *Q indeks*.

Pored navedenih tehnika i metrika korišćenih za procenu kvaliteta slike u ovom radu postoji još nekoliko različitih parametara koji ovom prilikom nisu uzeti u obzir. Ovi parametri mogu biti kandidati za dodatnu procenu kvaliteta u daljem radu i istraživanju a nastavku navodimo neke od njih.

Napredna verzija *SSIM*-a pod naziva se ***Multi Scale Structural Similarity - MS-SSIM***. Ova metoda procenjuje strukturne sličnosti na različitim slikama u različitim domenima. Kao i *SSIM*, promena osvetljenja, kontrasta i strukture se smatraju važnim za izračunavanje strukturne sličnosti na više nivoa poređenja između dve slike. Ova izvedena metoda procene kvaliteta neretko daje bolje i preciznije rezultate od bazične metode na osnovu koje je nastala.

Druga verzija *SSIM*-a, nazvana trokomponentni ***SSIM* (*3-SSIM*)** koja odgovara činjenici: ljudski vizuelni sistem bolje opaža razlike u tekstuiranim nego u glatkim regionima. Ovaj trokomponentni *SSIM* model predložen je u [22] gde je slika dekomponirana na tri važna svojstva kao što su ivica, tekstura i glatka regija. Rezultirajuća metrika se izračunava kao ponderisani prosek strukturne sličnosti za tri pomenute kategorije. Predložene procene težinskih koeficijenta su 0,5 za ivice, 0,25 za teksturu i 0,25 za glatke regije.

DSSIM - *Structural Dissimilarity* (strukturalna različitost)

Ova metoda procene se bazira na izvornoj *SSIM* metodi i izračunava se kao:

$$DSSIM(x,y) = \frac{1-SSIM(x,y)}{2} \qquad (6)$$

Na osnovu izraza vidi se da je parametar direktno i isključivo vezan za *SSIM* što bi značilo da dominantna uloga u njegovoj vrednosti zavisi od osvetljenja, kontrasta i strukture, odnosno korelacije bliskih piksela.

FSIM – *Features Similarity Index Matrix* (karakteristika matrice indeksa sličnosti)

Karakteristika indeksa sličnosti kombinuje dve metode: Faznu kongruenciju slike i intenzitet gradijenta o kom je već bilo reči. Ovakva simbioza metoda je usvojena jer fazna kongruencija ističe karakteristike slike u frekvencijskom domenu i invarijantna je u odnosu na kontrast dok je intenzitet gradijenta upravo osetljiv na promenu kontrasta. Matematički izraz za izračunavanje FSIM upravo i predstavlja proizvod stepena vrednosti dobijenih za parametar fazne kongruencije i parametar intenziteta gradijenta i detaljno je objašnjen u [23].

$$S_L(x) = [S_{PC}(x)]^{\alpha} * [S_G(x)]^{\beta} \qquad (7)$$

Gde je S_L ukupni indeks sličnosti, dok su S_{PC} i S_G indeksi fazne kongruencije i magnitude gradijenta. Parametri α i β su relativni i služe za ponderisanje važnosti svakog od parametara.

1.6. Histogrami

Histogram slike je grafički prikaz broja piksela na slici u funkciji njihovog intenziteta. Histogrami se sastoje od skupa diskretnih vrednosti, pri čemu svaka diskretna vrednost predstavlja odgovarajući intenzitet. Diskretne vrednosti često nazivamo usvojenim izrazom iz anglosaksonske literature – *binovi*. Histogram se izračunava statističkom obradom svih piksela na slici i dodeljivanjem vrednosti svakom binu, u zavisnosti od intenziteta pojavljivanja piksela određene decimalne vrednosti. Konačna vrednost bina predstavlja broj piksela koji su joj dodeljeni. Broj binova u kojima je podeljen ceo raspon intenziteta obično je reda kvadratnog korena ukupnog broja piksela. Histogrami slike su važan alat za analizu slika. Omogućavaju da

jednim pogledom uočite osvetljenje slike kao i raspon vrednosti sive boje (za *grayscale* slike). Takođe se može odmah uočiti šum i distorzija usled kvantizacije u vrednostima histograma slike. Fotografi često koriste histogram kao pomoć da pokažu distribuciju snimljenih tonova i provere da li su detalji slike izgubljeni zbog preeksponiranih (preosvetljenih) ili previše zatamnjenih oblasti.

Ukoliko je reč o 8-bitnim (*grayscale*) slikama vrednosti po apscisi (tonske varijacije) su ograničene od 0 do 255 dok vrednosti po ordinati zavise od veličine slike, odnosno od ukupnog broja piksela koje slika sadrži. Leva strana horizontalne ose predstavlja tamna područja, sredina predstavlja vrednosti srednjih tonova, a desna strana predstavlja svetla područja. Histogram za vrlo tamnu sliku imaće većinu svojih binova na levoj strani i u sredini grafikona.

Slika 2. Objašnjenje histograma sive (grayscale) slike

Suprotno tome, histogram za vrlo svetlu sliku s nekoliko tamnih područja i/ili oblasti imaće većinu svojih binova na desnoj strani i u sredini grafikona.

Ukoliko histogram posmatramo kao matematičku funkciju, ovakvo preslikavanje nije bijekcija. U opštem slučaju, ovakva funkcija jeste surjektivna ali ne zadovoljava uslov injektivnosti. Činjenica da ovakvo preslikavanje nije bijektivno implicira da ne postoji inverzna funkcija, kojom bi na osnovu histograma mogli da rekonstruišemo originalnu sliku. Za teoretske

potrebe, ukoliko bi veštački generisali sliku (bez obzira na veličinu i dimenzije) koja predstavlja gradijent od crne boje (#00) do bele boje (#FF) dobili bi potpuno ravan histogram.

1.6.1. Kolor histogrami

Kolor histogram slike predstavlja distribuciju kompozicije različitih boja na slici. Prikazuje raspodelu različitih vrsta boja i broj piksela za svaku od boja koje se pojavljuju na slici. Odnos između kolor histograma i histograma osvetljenja je da se kolor histogram može opisati i kao više histograma osvetljenja, od kojih svaki prikazuje distribuciju osvetljenja za svaki od pojedinačnih kanala boje (RGB – crveni, zeleni plavi). Kao i za histogram sive (*grayscale*) slike, kolor histogram takođe predstavlja statističku raspodelu boja bez obzira na poziciju piksela u prostornom domenu.

Za razliku od histograma sive (*grayscale*) slike, gde je jednostavno uočiti količinu piksela odgovarajuće nijanse, kod kolor histograma to nije moguće. Na osnovu preklapanje tri sloja (za RGB kanale) na istom grafikonu nije moguće zaključiti tačnu nijansu konkretnog piksela. Da bi ovaj problem bio rešen razvijeni su različiti tipovi višedimenzionalnih histograma. Različite analize slike i različite potrebe opredeljuju koji će tip višedimenzionalnog histograma biti upotrebljen. Jedan od načina da se predstave konkretne nijanse piksela moguć je pomoću specifičnog tipa histograma, koji za osnovu ima 3D matricu, oblika kocke, opsega po svakoj osi od 0 do 255, gde svaka osa predstavlja jedan od 3 RGB kanala. Veličina sfere, pozicionirane u konkretnom čvoru 3D matrice, predstavlja skaliranu, proporcionalnu količinu piksela konkretne nijanse. Zbog potreba algoritma predloženog u ovom radu, upravo ovakav tip 3D histograma je korišćen u daljem opisu i analizi.

1.6.2. Histogrami razlike piksela (*PDH*)

Histogrami razlike piksela predstavljaju posebnu klasu histograma. *PDH* analiza se izvodi izračunavanjem vrednosti razlike između svakog para piksela. Par se sastoji od dva uzastopna piksela, u definisanom pravcu i smeru. Vrednosti ove razlike će biti od -255 do +255 uključujući 0, za svaki od 3 kanala (RGB). Učestalost svake od ovih vrednosti razlike se računa i predstavlja na grafikonu. Grafikon je iscrtan, sa vrednostima razlike u pikselima na X-osi i frekvencijom pojavljivanja na Y-osi. Dobijena kriva naziva se *PDH*. Ovakva kriva se može iscrtavati za svaki od kanala a jedan od pristupa je i izračunavanje srednje vrednosti za sva tri kanala, za odgovarajuće pozicije po apscisi za svaki od kanala. Da bi ovakva analiza bila sprovedena potrebno je na istom grafiku iscrtati familiju krivih (dve ili više), prvo za originalnu sliku a potom i za njene derivate dobijene nakon primene odgovarajućih izmena, bilo u prostornom ili frekvencijskom domenu. Odstupanja krive, iscrtane na osnovu slike derivata, u odnosu na krivu iscrtanu na osnovu originalne slike nedvosmisleno ukazuju na učinjene promene. Takođe, obično se očekuje da *PDH* originalne slike bude glatka kriva dok pojedine metode manipulacije pikselima izazivaju pojavu neravnina (*ripple*) u *PDH* karakteristici. Pojava (značajnijih) neravnina *PDH* krive nedvosmisleno ukazuje na izvesne promene nastale manipulacijom bita originalne slike. Zbog ovakvog efekta *PDH* je u poslednje vreme često korišćena metoda stego-analize i obično se kombinuje sa drugim stego-analitičkim alatima. Kako je ova metoda postala veoma relevantna u poslednje vreme, jedna grupa autora fokusirala se na istraživanja naprednijih metoda stego-analize upotrebom bazične *PDH* metode [24], dok se druga grupa autora fokusirala na istraživanje novih steganografskih metoda otpornih na *PDH* analizu [25], [26]. U okviru analize dobijenih rezultata u ovom radu, u poglavlju 5.2 su, uz komentare, predstavljeni neki od generisanih *PDH* dijagrama.

1.7. Struktura disertacije

U prvom, uvodnom, delu opisana je potreba za razvojem novih i efikasnijih metoda za bezbednu razmenu i čuvanje podataka. Dat je uvodni opis tehnika kriptografije i steganografije kao i opis alata koji su korišćeni tokom obrade i analize dobijenih podataka. Pored identifikacije problema, naznačeni su mogući pravci rešavanja i naznačen je doprinos ove disertacije kao i struktura ostalih poglavlja u disertaciji.

U drugom poglavlju detaljno su opisane upotrebljene steganografske metode. Opisane bazične metode su neophodna osnova za razvoj složenijih procesa adaptivne i hibridne steganografije. Da bi tema steganografije bila zaokružena, na kraju drugog poglavlja predstavljene su metode stego-analize, opisani algoritmi kojima su analizirani generisani stego-nosioci i dat je komentar vezan za potencijalne stego-napade.

U trećem poglavlju detaljno je opisan predlog sistema hibridne steganografije sa akcentom na algoritam za apriori obradu steganografskih nosilaca.

Četvrto poglavlje predstavlja dizajn obavljenih eksperimenata.

Peto poglavlje daje detaljnu analizu dobijenih rezultata u smislu kvaliteta stego-objekata, njihovih kapaciteta kao i otpornosti na stego-analizu.

Na osnovu obavljenih eksperimenata i analiziranih rezultata u šestom poglavlju predstavljeni su zaključci vezani za izbor kvalitetnog stego-nosioca kao i optimalnog načina obrade.

Zaključak i pravci daljeg istraživanja dati su u sedmom poglavlju.

2. Steganografske metode u slici

Kako je već navedeno u poglavlju 1.4, steganografske metode moguće je izvršiti u različitim tipovima nosilaca. Jedan od najčešće korišćenih tipova nosilaca je slika u nekom od svojih digitalnih formata. Kako je slika sastavljena od piksela a pikseli predstavljeni, na odgovarajući način (jednim od definisanih standarda), binarnim sadržajem jasna je implikacija da steganografija u slici podrazumeva manipulaciju bitima, sastavnim delovima piksela. Da bi se u takvom sistema manipulisalo pikselima razvijene su različite metode i različiti pristupi problemu. Ono što je zajedničko kod svih steganografskih metoda za ovakav tip objekta prikrivanja je optimizacija karakteristika kako samog procesa tako i finalnog produkta. To znači da je cilj svakog steganografskog algoritma postizanje što boljih performansi: manje uočljivosti tajnog sadržaja, veći kapacitet, veća otpornost na stego-analitičke alate i napade, veća robusnost stego-objekta, bolje performanse izražene u numeričkim vrednostima za procenu kvaliteta stego-objekta, manje vreme obrade potrebno za ugrađivanje i izdvajanje tajnog sadržaja, bolja efikasnost algoritma. Načelno gledano, steganografske metode u slici se dele na metode u prostornom domenu i metode u frekvencijskom domenu [27].

2.1. Pregled steganografskih metoda

Steganografija u prostornom domenu uključuje manipulaciju bitima u digitalnom zapisu objekta prikrivanja. U slučaju steganografije slike, manipulacija bitovima uključuje promenu pojedinačnih vrednosti piksela, bilo da se radi o crno-beloj (*grayscale*) slici ili slici u boji. Studija u [28] daje izvrstan teorijski pregled različitih tehnika u prostornom domenu, osobenosti svake od njih, kao i uporedne karakteristike, prednosti i nedostatke. Tehnike steganografije u prostornom domenu možemo podeliti u nekoliko osnovnih kategorija:

1. *LSB* (*less significant bit*) steganografija

2. Steganografija zasnovana na *RGB* (*red-green-blue*) kanalima
3. Steganografija zasnovana na razlici vrednosti piksela *(Pixel Value Differencing - PVD*)
4. Steganografija zasnovana na mapiranju
5. Steganografija zasnovana na paleti boja
6. Kolažna steganografija
7. Steganografija proširenog spektra
8. Steganografija zasnovana na kodovima

Svaka od ovih kategorija sadrži nekoliko specifičnih algoritama objašnjenih i detaljno opisanih u [28]. Važan rad, sa detaljno opisanim, uporednim karakteristikama stego-metoda (dobrobiti, izazovi, kapacitet, vizuelne performanse.) [29] je odlična polazna tačka za izbor tehnika koje je moguće koristiti za istraživanja i testiranja. Ova studija daje precizno klasifikovani, tabelarni prikaz karakteristika svake od steganografskih metoda različitih tipova koji mogu dati smernice o načinu kombinovanja metoda kako bi postigli bolje performanse po više različitih kriterijuma: složenosti implementacije, potrebna procesorska snaga, složenost utiskivanja tajnog sadržaja, složenost ekstrakcije, kapacitet nosioca, robusnost stego-objekta, otpornost stego-objekta na stego-analizu i stego-napade.

2.2. *LSB* steganografska metoda

Jedna od osnovnih i najjednostavnijih steganografskih metoda u slici, u prostornom domenu je *LSB* metoda. Naziv je dobila od engleske skraćenice *Least Significant Bits* – biti najmanje težinske vrednosti, što intuitivno ukazuje na način kako je metoda koncipirana. Neki od prvih radova objavljenih na temu *LSB* steganografije u slici sada su stari više od dvadeset godina [30]. Standardna *LSB* metoda steganografije u prostornom domenu slike uključuje promenu

K bita manje težinske vrednosti pojedinačnog piksela slike p_i. Pretpostavimo da imamo tajnu poruku *M* sastavljenu od *n* bita koju želimo poslati u steganografskom nosiocu modifikujući *K* bita svakog piksela (slika sivih nijansi - *greyscale*). *LSB* metoda zahteva sekvencijalnu ekstrakciju *k* bitova iz M koji će biti ugrađeni u odgovarajući piksel nosioca p_i. Označimo ovu kombinaciju bitova sa m_k. Ugrađivanjem m_k (*K* bita) u svaki piksel, 8-k *MSB* bita svakog piksela će zadržati svoju originalnu vrednost. Takva operacija zahteva

$$i_{max} = \begin{cases} n \div k, n \bmod k = 0 \\ n \div k + 1, n \bmod k > 0 \end{cases} \quad (8)$$

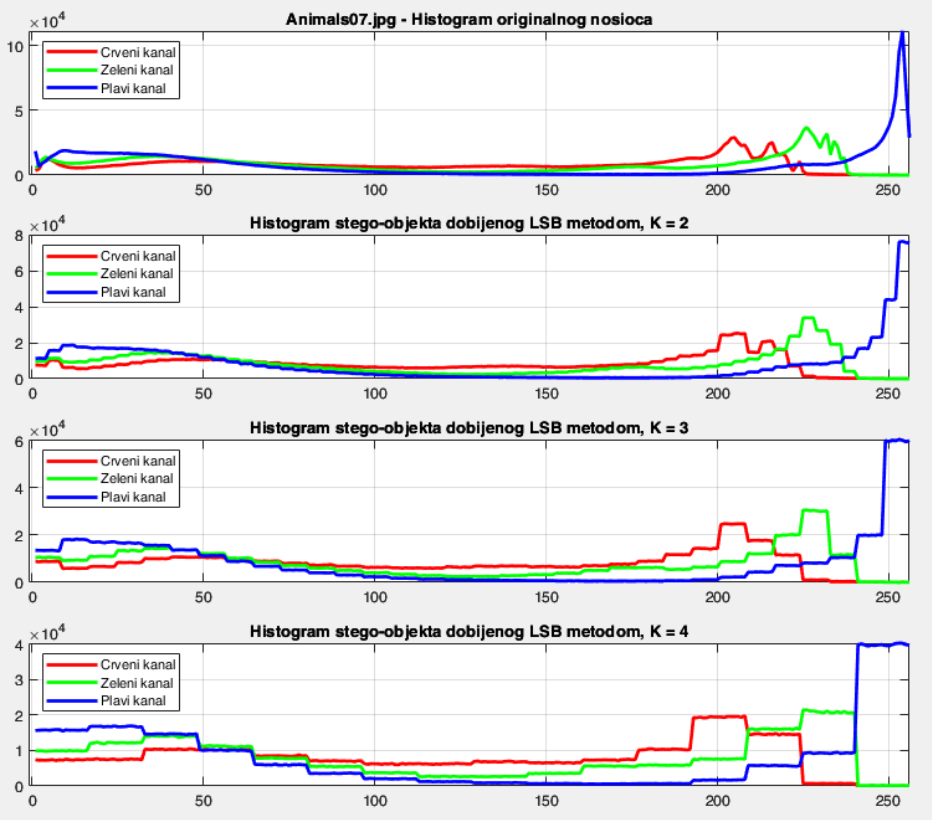
piksela, gde ÷ predstavlja operaciju celobrojnog deljenja, a *mod* predstavlja ostatak operacije celobrojnog deljenja. Možemo izvesti sličan proces koristeći sliku u boji (*RGB*) i u tom slučaju bismo promenili *K* bita u svakom od 3 kanala. Tada je

$$i_{max} = \begin{cases} n \div (k * 3), n \bmod k = 0 \\ n \div (k * 3) + 1, n \bmod k > 0 \end{cases} \quad (9)$$

piksela potrebno za prenos željene informacije, dužine *n* bita. Za takav algoritam, *K* bita najmanje težinske vrednosti za svaki modifikovani piksel (ili kanal) p_i' na prijemnoj strani treba biti pročitano u nizu, prema obrascu piksela koji se koristi na strani slanja (R_x). Ova steganografska metoda smatra se osnovnom metodom u prostornom domenu iz razloga svoje jednostavnosti a i u istorijskom smislu. Metoda, zahvaljujući svojoj jednostavnosti, ne zahteva nikakav dodatni proces obrade pa samim tim ni dodatnu procesorsku snagu. Proces utiskivanja i ekstrakcije je simetričan na predajnoj i prijemnoj strani.

Kapacitet stego-objekata generisanih ovom metodom se može veoma jednostavno i intuitivno izračunati kao *K*/8. Pa tako, na primer, ako vršimo izmenu 3 bita najmanje težinske vrednosti kapacitet nosioca je 3/8*100%, odnosno 37,5%. Pored dobrih svojstava, ova metoda ima nekoliko nedostataka, a jedan od njih je značajno povećanje izobličenja sa

povećanjem *K* vrednosti. Testiranja su pokazala da minimalnim porastom vrednosti *K* dolazi do značajnih degradacija parametara za ocenu kvaliteta (*PSNR, SSIM*…). Još jedna loša osobina je kvantizacija histograma originalnog stego-nosioca. Naime, izmenom *K* bita najmanje težinske vrednosti dolazi do kvantizacije stego-objekta u 2^{8-k} zona. Slika 3 pokazuje efekat kvantizacije histograma sa promenom parametra *K*.



Slika 3. Efekat kvantizacije histograma stego-objekata upotrebom LSB steganografske metode za različite vrednosti parametra K

Ovakav efekat distorzije histograma može biti veoma poguban ukoliko bi stego-objekat bio podvrgnut stego-analizi. Kada je reč o stego-analizi, ova metoda je veoma neotporna na neke od metoda analize, posebno na RS. Analiza rezultata u narednim poglavljima će pokazati veoma loše performanse stego-objekata generisanih ovom metodom u kontekstu RS stego-analize, odnosno visoke vrednosti estimiranih izmena nastalih u procesu steganografije.

Iako je *LSB* metoda davno patentirana, omasovljenjem upotrebe računara, velika grupa autora se i danas bavi istraživanjem u toj oblasti, uglavnom kombinujući je sa drugim metodama ili uzimajući nju kao referencu za poređenje sa rezultatima dobijenim kao proizvod svojih, predloženih naprednijih metoda. Radovi [31], [32] kao i [33] predstavljaju istraživanja novijeg datuma na temu *LSB* steganografije u prostornom domenu slike.

2.3. *MDD* steganografska metoda

Govoreći o *LSB* metodi steganografije u poglavlju 2.2 pokazano je da je najveća decimalna razlika u vrednostima piksela pre i nakon promene *K* bita najmanje težine je $d_{max} = 2^k - 1$. Metoda minimalne decimalne razlike (*MDD – Minimal Decimal Difference*) razvijena je sa idejom da se d_{max} koeficijent smanji što je više moguće. Za razliku od klasične *LSB* metode, koja nije uzela u obzir decimalnu vrednost originalnog piksela, *MDD* metoda uzima u obzir ove vrednost i menja originalnu vrednost piksela dodavanjem odgovarajućeg koeficijenta d_i (pozitivnog ili negativnog) s ciljem da binarna reprezentacija nove dobijene decimalne vrednosti za poslednjih *K* bita najmanje težinske vrednosti ima vrednost m_k koju želimo preneti na prijemnu stranu. Ovim pristupom možemo izračunati minimalne i maksimalne vrednosti koeficijenata u zavisnosti od broja *K*:

$$-2^{K-1} + 1 \leq d_i \leq 2^{K-1} \qquad (10)$$

Na primer: ako je vrednost *K* = 3, za klasičnu *LSB* metodu, decimalna razlika originalnog i modifikovanog piksela može biti u rasponu: 0≤ d_i ≤7, dok je: -3 ≤ d_i ≤ 4 za *MDD*. Stoga je očekivano unapređenje kod *MDD* metode manja distorzija stego-objekta koja će se odraziti na numeričke vrednosti za ocenu kvaliteta slike (*RMSE, PSNR, SSIM*…), kao i na vizuelni doživljaj slike. Takva ideja može imati mnogo različitih softverskih implementacija, a jedna od njih je uvođenje dodatne funkcije koja će izračunati koeficijente d_i za odgovarajuće

kombinacije, u zavisnosti od *K*, koje želimo preneti, m_k, i originalne decimalne vrednosti piksela. Vrednost piksela za slanje rezultat je zbira originalne decimalne vrednosti piksela i izračunatog koeficijenta: $p_i' = p_i + d_i$. U slučaju prenosa *K* = 2 bita u svakom pikselu p_i , funkcija transformacije prikazana je u tabeli 1, gde su po kolonama kombinacije 2 bita tajne poruke m_k, a po vrstama kombinacije poslednja 2 bita binarne reprezentacije originalnih vrednosti piksela p_i. Za razliku od *LSB* metode gde se na predajnoj strani radi jednostavan proces supstitucije bita, kod *MDD* metode se *K* bita najmanje težine piksela na koji utičemo dobija superponiranjem koeficijenata iz ovakvih tabela sa postojećim vrednostima (p_i), a u zavisnosti od poruke koju želimo da prenesemo (m_k).

Tabela 1. Vrednost koeficijenata d_i za K=2 bita koje želimo da izmenimo, gde je po kolonama poruka koja se prenosi - mk, a po vrstama vrednosti originalnih piksela nosioca - pi

	00	**01**	**10**	**11**
00	0	+1	+2	-1
01	-1	0	+1	+2
10	+2	-1	0	+1
11	+1	+2	-1	0

Slične tabele kao što je tabela 1, (veličine $2^k \times 2^k$), mogu se kreirati za druge vrednosti *K* bita koje želimo da prenesemo.

Imajući u vidu da vrednost svakog piksela p_i može biti u rasponu od 0-255, a vrednost koeficijenata d_i može biti i pozitivna i negativna, potrebno je rešiti problem graničnih zona - margina. Rešenje ovog problema je skaliranje svih vrednosti p_i od ruba intervala do prve, najbliže, prihvatljive vrednosti p_{im} u zavisnosti od mogućih vrednosti d_i, koja zavisi od broja *K*:

$$p_{im} = \begin{cases} 2^{k-1} - 1, & p_i < 2^{k-1} - 1 \\ p_i, & 2^{k-1} - 1 \le p_i \le 255 - 2^{k-1} \\ 255 - 2^{k-1}, & p_i > 255 - 2^{k-1} \end{cases} \qquad (11)$$

Jednačina 11 jasno pokazuje da će se granične zone povećavati sa povećanjem koeficijenta *K* i performanse *MDD* algoritma će, u najgorem slučaju, biti jednake performansama klasične *LSB* metode.

Ekstrakcija bitova na prijemnoj strani se vrši na isti način kao u osnovnoj metodi - sekvencijalnim čitanjem *K LSB* bitova iz i_{max} modifikovanih piksela Stego-objekta.

Slika 4 prikazuje blok dijagram predloženog algoritma.

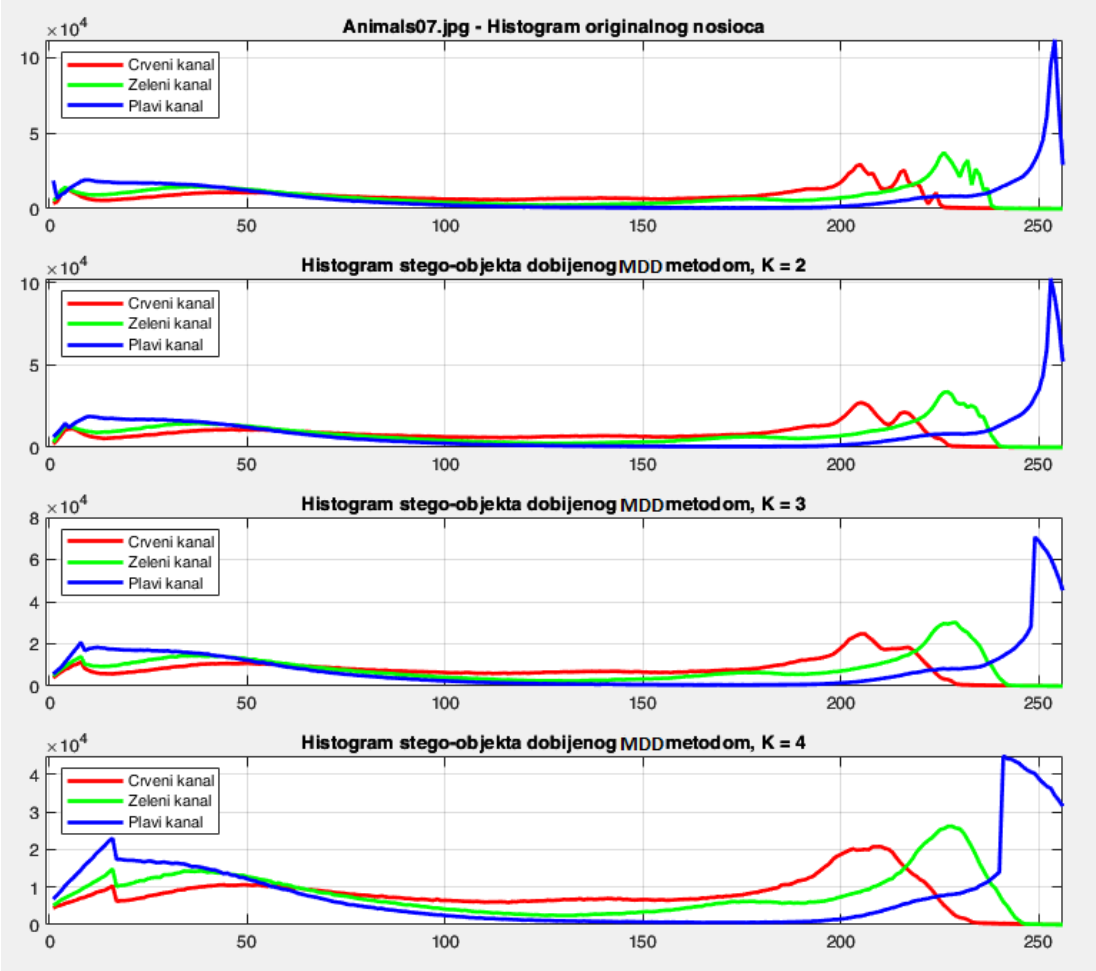
Slika 4. Blok dijagram jednog od načina realizacije MDD metode

Treba napomenuti da su neki autori takođe svoje ideje bazirali na dodavanju pozitivnih i negativnih vrednosti postojećoj decimalnoj vrednosti piksela, dok se neki autori, kao Van Dijk - Willems [34], bave predkodiranjem tajnih bita imali slične ideje o tome kako modifikovati *K* najmanje težinske vrednosti, koji za neke kodove mogu imati sličan efekat kao i *MDD* metoda.

U radovima [35] i [36] dat je detaljan opis predložene metode gde su pokazane prednosti u odnosu na originalnu *LSB* metodu, na osnovu koje je *MDD* metoda razvijena. Jasno je da će kapaciteti stego-nosilaca za obe metode biti identični dok je pokazana dominantnost *MDD*

metode u kontekstu kvaliteta stego-objekata izraženih pomoću parametara za procenu kvaliteta.

Slika 5 pokazuje izobličenja histograma stego-objekata generisanih *MDD* metodom u odnosu na histogram originalnog nosioca. Poređenjem histograma sa slike 5 sa histogramima na slici 3 jasno se vidi manji stepen distorzije stego-objekata generisanih *MDD* metodom u odnosu na nosioce generisane *LSB* metodom. Takođe, uočljivo je da kod histograma stego-objekata dobijenih *MDD* metodom ne postoji efekat kvantizacije kao i u slučaju *LSB* metode. Rezultati dobijeni eksperimentima prikazanim u narednim poglavljima i njihova analiza pokazaće dominantnost *MDD* metode i u kontekstu otpornosti na proces stego-analize.



Slika 5. Histogram stego-objekata upotrebom MDD steganografske metode za različite vrednosti parametra K

2.4. *PVD* steganografska metoda

Metoda razlike vrednosti piksela (*PVD – Pixel Value Differencing*) objavljena je od strane autora Da-Chun Wu i Wen-Hsiang Tsai 2003. godine. Razvijeni algoritam uzima vrednosti dva susedna piksela i na način opisan u [37], menja njihove vrednosti u skladu sa tajnim podacima koje treba preneti. Stego-objekat sa novodobijenim vrednostima piksela se na prijemnoj strani obrađuje algoritmom asimetričnim u odnosu na algoritam obrade na predajnoj strani. Ukoliko se *PVD* algoritam implementira na slikama u boji, uzimaju se vrednosti odgovarajućih kanala susednih piksela. Za razliku od *LSB* metode steganografije, gde se svaki piksel (ili svaki kanal piksela) posmatra nezavisno, kod *PVD* steganografije otvara se mogućnost različitog kombinovanja susednih piksela. Pa tako se susednim pikselima mogu smatrati oni koji se nalaze u istoj vrsti stego-nosioca (slike) sa leva na desno, oni koji se nalaze jedan iznad drugog ili dva piksela koja se nalaze na dijagonali minijaturnog bloka sačinjenog od 4 piksela kvadratnog oblika. Jedan od ustaljenih načina pristupa odabira susednih piksela, koji se može smatrati univerzalnim ukoliko nije poznato da li je broj piksela po horizontalnoj dimenziji paran ili neparan, je taj da se susedni pikseli uzimaju sa leva na desno u jednoj vrsti, da bi se u sledećoj vrsti algoritam odabira kretao sa desna na levo. Na taj način bi, u slučaju neparnog broja piksela po horizontalnoj dimenziji, poslednji piksel u prvoj vrsti za svog parnjaka imao piksel ispod sebe, u drugoj vrsti. Radovi [38] i [39] bave se posebnim (hibridnim) načinima izbora piksela i utiskivanja tajnog sadržaja, bazirani na *PVD* metodi.

Za razliku od *LSB* metode, gde je kapacitet stego-nosioca jednoznačno određen, brojem bita koji će biti primenjen u svakom pikselu K (ili $3*K$ – za slike u boji), kod *PVD* metode kapacitet nije moguće apriori odrediti ili izračunati. Tačan podatak o kapacitetu stego-objekta moguće je izračunati tek nakon obavljenog procesa steganografije na osnovu broja utisnutih tajnih

bita i podatka o veličini stego-nosioca. Empirjiski je utvrđeno da je taj procenat oko 18,75% (3/16, 3 bita tajnog sadržaja na dva susedna piksela) za većinu realnih slika, odnosno stego - nosilaca. Za potrebe eksperimenta kreirana je slika generisana od slučajnih vrednosti (u opsegu 0-255) za svaki piksel, za svaki kanal. Kapacitet stego-objekta dobijenog *PVD* metodom za ovakav, eksperimentalni nosilac, iznosio je 34.1%. Imajući u vidu kako *PVD* algoritam funkcioniše i za koje vrednosti susednih piksela postoji najveći mogući kapacitet ugradnje, kreirana je slika gde svaki neparni piksel u jednoj vrsti ima vrednosti koja se nalazi na ¼ intervala 0-255, odnosno 64, dok svaki parni piksel u vrsti ima vrednost koja se nalazi na ¾ intervala 0-255, odnosno 192. Kada je *PVD* metoda steganografije sprovedena nad ovakvim, eksperimentalnim, stego-nosiocem, dobijen je teoretski maksimalan kapacitet od 43,75% (7/16, 7 bita tajnog sadržaja na dva susedna piksela). Takođe je važno napomenuti da vizualna distorzija stego-objekta dobijenog *PVD* metodom (ukoliko uzimamo susedne piksele jedne vrste, sa lava na desno, redom) ima karakteristike takve da postanu uočljive vertikalne pruge. Kompletna prethodna analiza kapaciteta stego-objekata dobijenih *PVD* metodom kao i efekat pojavljivanja vertikalnih pruga, kao vizuelne distorzije, implicira pogodnost upotrebe *PVD* metode na horizontalnim i vertikalnim ivicama objekata i figura elemenata nosioca. Nekoliko autora se u svojim radovima upravo vezuje za ovu karakteristiku *PVD* metode steganografije. Primer je rad [40] .

2.5. Metode adaptivne steganografije

Pod pojmom adaptivna steganografija podrazumeva se kombinovanje šireg skupa različitih tehnika kao što su obrada slike, upotreba različitih kodova, statistička analiza, međusobna kombinacija različitih steganografskih metoda itd. Do sada su se u razvoj metoda adaptivne steganografije bavili različiti autori. Pregledni radovi [41] i [42] pružaju odličnu klasifikaciju

različitih tipova steganografije i mogućnost kombinovanja različitih metoda, dok lista referenci u citiranim radovima predstavlja ozbiljnu osnovu za rad i dalja naučna istraživanja. Dok su neki autori radili na kombinovanju različitih tipova steganografskih metoda kako bi poboljšali performanse stego-objekata ([43] , [44]), drugi su se bavili apriornom obradom objekata prikrivanja pre nego što su zapravo utiskivali tajni sadržaj. Primer adaptivne steganografije nastale kao rezultat kombinovanja nekoliko različitih metoda opisan je u radu [45], kao i poboljšana verzija predstavljena u [46]. U radu [47] Gandharba Swain predlaže svoju metodu i pokazuje određenu prednost u kvalitetu stego objekata u odnosu na autore [45]. Dodatno, kao predstavnika ove vrste adaptivne steganografije, važno je spomenuti rad autora [48]. Da bi se prikrila tajna poruka, moguće je koristiti ceo stego-nosilac ili samo neke njegove zone koje se nazivaju stego-oblastima, odabrane na osnovu definisanih kriterijuma. Neki autori koriste različite metode za odabir delova objekta prikrivanja. Tako su, na primer, autori rada [49] koristili detekciju rubova na objektu prikrivanja, dok je Abid Yahya u [50] dao komparativne karakteristike adaptivnih steganografskih metoda (u određenim oblastima nosioca) koristeći *Scale-Invariant Feature Transform* (SIFT) i algoritmi ubrzanih robusnih karakteristika (SURF) za odabir specifičnih područja nosioca. U [51] je predloženo grupisanje, ali unutar prethodno definisanih kontura, koncipirajući ovu metodu baziranu na ključu.

Na principu stego-ključa (*key-based*) mogu biti bazirane i adaptivne steganografske metode a i one koje, načelno, ne smatramo adaptivnim. Metoda bazirana na ključu zahteva dodatne informacije na prijemnoj strani (Rx) kako bi tajni sadržaj mogao pravilno biti ekstrahovan. Stego-ključ za različite stego-metode može imate različite forme. Tako na primer, za *PVD* metodu, izloženu u poglavlju 2.4, stego-ključ može biti način izbora susednih bita ukoliko se susedni biti drugačije biraju za svaku sesiju. Ukoliko metoda adaptivne steganografije podrazumeva upotrebu različitih kodova, stego-ključ može biti informacija o upotrebljenom

načinu kodovanja. Kada se radi o adaptivnoj steganografiji gde se apriori vrši obrada nosioca, stego-ključ može predstavljati informaciju o odabranim stego-oblastima, gde će se obavljati proces steganografije. Postojanje stego-ključa povećava složenost sistema ali ujedno implicira povećanje sigurnosti, zbog nedostupnosti ovih informacija napadaču. Povećanje sigurnosti se ogleda u činjenici da će algoritam za obradu nosioca izabrati različitu kombinaciju stego-oblasti za različite nosioce. Stoga stego-napadač (Eva) ima dodatni problem u analizi različitih nosilaca, uz očekivanje da će obavljena stego analiza primljenih stego-objekata pokazati nizak nivo mogućnosti otkrivanja postojanja tajnog sadržaja. Povećanje složenosti sistema u odnosu na klasični proces steganografije ogleda se u:

- Obrada/priprema stego-nosioca radi određivanja stego-oblasti koje će se koristiti;
- Steganografski proces u definisanim oblastima na Tx strani;
- Obezbeđivanje načina za prenos informacija o stego-oblastima na prijemnu stranu (nezavisni kanal) kako bi se primljeni stego-objekt kasnije obradio na odgovarajući način;
- Proces izdvajanja tajnog sadržaja iz odabranih područja na prijemnoj strani.

2.6. Metode stego-analize

Stego-analiza je postupak koja za cilj ima otkrivanje primenjenih postupaka steganografije u digitalnom sadržaju za koji postoji indicija da predstavlja stego-objekat. Spoznaja činjenice da je neki digitalni sadržaj stego-objekat, prepoznavanje skrivenih podataka i njihovo eventualno izdvajanje je krajnji cilj stego-analize. Stego-analiza uključuje nekoliko zadataka koji se odnose na skrivene podatke u digitalnom mediju kao što je predviđanje korisnog opterećenja koje se koristi za ugradnju podataka, predviđanje steganografskih tehnika koje se koriste i proces

klasifikacije da li datoteke sadrže skrivene podatke ili ne. Kolokvijalno se može reći da postoji potpuna analogija u odnosu steganografije prema stego-analiza kao u odnosu kriptografije prema kripto-analizi. Rad [52] daje osnovne postulate tehnika stego-analize dok rad novijeg datuma [53] daje pregled različitih, modernih, pristupa ove discipline. Na osnovu podele predstavljene u pomenutom radu stego-analiza se generalno može podeliti u 3 podgrupe:

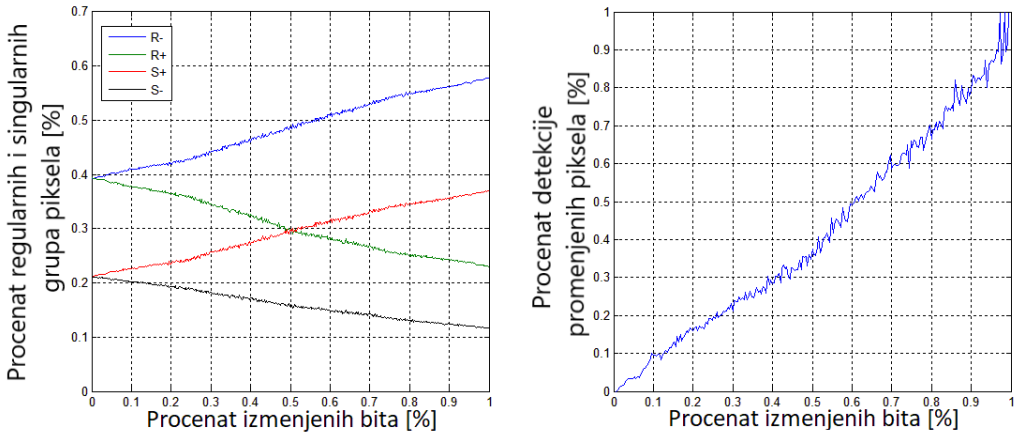
- ***Signature Steganalysis* –** Podrazumeva postupke otkrivanja upotrebe konkretne (očekivane) steganografske metode strane od interesa (*modus operandi*).
- **Statističa Stego-analiza** - Podrazumeva generisanje i analizu statističkih karakteristika i svojstava digitalnog sadržaja sa koji postoji sumnja da su stego-objekti. Ovakve metode analize često kao rezultat imaju numerički podatak koji označava procenu (verovatnoću) izmenjenog digitalnog sadržaja. Naprednije statističke analize, pored osnovnog podatka procene, mogu pružiti i dodatne informacije o količini izmenjenih podataka, zonama gde je došlo do stego-izmena, ukazati na primenjenu stego-metodu…
- ***Deep Steganalysis* –** Duboka stego-analiza podrazumeva konceptualno razrađene ili potpuno razvijene metode, novijeg datuma, bazirane na neuralnim mrežama i dubokom učenju.

Treba napomenuti da stego-analiza može biti obavljena u slučaju da je poznat originalni objekat prikrivanja ili da on nije poznat. U slučaju unapred poznatog objekta prikrivanja neki od navedenih zadataka stego-analize postaju trivijalni. U idealnom, teorijskom, slučaju rezultat stego-analize podrazumevao bi kompletnu ekstrakciju tajnog sadržaja, rekonstrukciju originalnog objekta prikrivanja i potpunu spoznaju primenjene stego-metode (način

utiskivanja i ekstrakcije tajnog sadržaja kao i stego-ključ). Ovakav slučaj je u realnim okolnostima praktično nemoguć i zato je značajan samo u teorijskom domenu.

2.6.1. RS stego-analiza

Početkom ozbiljnijeg i intenzivnijeg razvoja stego-metoda javila se potreba i za razvojem boljih i moćnijih stego-analitičkih alata. Krajem 20. i početkom 21. veka, kao direktan odgovor na *LSB* metodu steganografije razvijena je RS metoda stego-analize [54], [55]. Metoda se bazira na proceni količine regularnih i singularnih grupa piksela za različite vrednosti procenata izmenjenih piksela. Na osnovu ovih procena izračunava se konačni procenat izmenjenih piksela. Rezultat analize predstavljen je na slici 6 a pored toga izračunava se i numerička vrednost P_{rs}, izražena u opsegu od 0 do 1, koja predstavlja konačnu estimaciju izmenjenih piksela za sliku. U slučaju slike u boji analiza se vrši za svaki od tri kanala da bi se konačan rezultat uzeo po jednom od dva kriterijuma: ili kao srednja vrednost dobijenih rezultata ili kao najgori slučaj od tri moguća.



Slika 6. RS dijagram stego-analize i dijagram estimacije izmenjenih bita

Razvojem novijih stego-metoda kao i upotrebom tehnika adaptivne steganografije dovedena je u pitanje efikasnost ovog algoritma, razvijenog za detekciju *LSB* steganografije.

Radovi [56] i [57] daju analize efikasnosti RS algoritma u slučaju upotrebe modernijih stego-metoda.

Jedna od karakteristika RS metode stego-analize je postojanje takozvane inicijalne procene izmenjenog sadržaja - P_{ib} (*inital bias*). Ovaj parametar predstavlja kvantifikovanu procenu o (nepostojećim) podacima ugrađenim u sliku nosioca koja, zapravo, nije prethodno steganografski tretirana. Reklo bi se da parametar P_{ib} kvantifikuje *falš-pozitivne* vrednosti procene. Analiza rezultata koja će biti predstavljena u ovom radu uzima prosečnu vrednost parametra P_{ib} za referentnu, kada je u pitanju granica prihvatljivosti za parametar P_{rs} . U cilju objedinjavanja parametara P_{rs} i P_{ib} u jedinstveni matematički izraz, uzimajući u obzir i realni procenat piksela nosioca koji menjano, definisana je formula:

$$p_d = \frac{|p_{ib} - p_{rs}|}{cp} \qquad (12)$$

gde parametar *cp* predstavlja procenat piksela na koje je vršen uticaj, izražen u opsegu od 0 do 1. Ovakva matematička relacija implicira različite vrednosti za parametre P_{rs} i P_d , za isti stego-objekat, gde parametar P_d može uzimati vrednosti i veće od 1. Kao što je srednja vrednost parametra P_{ib} (za 100 nosilaca) uzeta kao referentna za vrednosti P_{rs} za pojedinačni stego-objekat, isti kriterijum je upotrebljen i kada je u pitanju parametar P_d .

2.7. Metode stego-napada

Stego-napadom (*stego-attack*) naziva se metoda (mera) koja za cilj ima oštećenje ili potpuno uništenje steganografskog sadržaja u stego-objektu. Ovakvu meru je moguće sprovesti ciljano, ukoliko je unapred poznato da je konkretni digitalni sadržaj stego-objekat, ili preventivno ukoliko apriori ne postoje indicije da je u pitanju stego-objekat. Načelno se

metode ciljanog i preventivnog stego-napada razlikuju iako se obavljaju nad istim ulaznim objektima i imaju isti cilj. Postupci uništavanja ili oštećenja izdvojenog, prepoznatog ili pretpostavljenog sadržaja se smatraju invanzivnijom merom koja ide u paraleli ili nakon stego-analize. Stego-napad se obavlja nad stego-objektom na liniji komunikacije od pošiljaoca (Tx/Alice) prema primaocu (Rx/Bob), po scenariju poznatom kao *man-in-the-middle,* a sa ciljem opstrukcije tajne komunikacije. Prema stepenu invanzivnosti stego-napadi se mogu podeliti u tri kategorije:

- **Sirovi stego-napadi –** Ova vrsta napada podrazumeva direktnu, sirovu i uočljivu promenu stego-objekta, dajući jasnog doznanja da je izvršena promena izvršena. Ako je u stego-objekat u formi slike, ovakva vrsta napada može podrazumevati kropovanje (*cropping*), sečenje ili vidljivu promenu u pikselima.

- **Diskretni stego-napadi –** Ova vrsta napada podrazumeva upotrebu sofisticiranijih metoda promene stego-objekta kako prijemnoj strani (Rx/Bob) ne bi direktno bilo dato do znanja da je stego-napad izvršen. Ovakva vrsta napada može da podrazumeva kompresiju slike, promenu veličine, izvesno filtriranje ili dodavanje šuma.

- **Sofisticirani stego-napadi** – Napadi koji se obavljaju preventivno bilo da postoji ili da ne postoji indicija o postojanju steganografskog sadržaja. Za ovu potrebu razvijeni su posebni algoritmi koji se nazivaju metodama sterilizacije slike. Sterilizacija, u kontekstu steganografije, predstavlja metodu podvrgavanja digitalnog sadržaja odgovarajućim algoritmima koji za cilj imaju minimalnu ali dovoljnu izmenu, na bitskom nivou. Pomenuta izmena ni na koji način ne bi trebalo da bude primećena na prijemnoj strani komunikacije dok, sa druge strane, svaki potencijalno prisutan steganografski sadržaj bi trebalo biti dovoljno oštećen da bi se smatrao

neupotrebljivim. U poslednjih par godina tema sterilizacije je došla u fokus istraživanja mnogih autora a neki od referentnih radova su [58], [59], [60] i [61].

Stego-napadi se po svojoj metodologiji mogu podeliti na sledeće:

- **Napad odabranom porukom** – Vrsta napada gde se poznatom tajnom porukom generiše fiktivni stego-objekat koji će se u daljoj analizi, nad realnim stego-objektima, koristiti kao referentni.
- **Napad odabranom metodom** – Vrsta napada gde se poznatom stego-metodom generiše fiktivni stego-objekat koji će se u daljoj analizi, nad realnim stego-objektima, koristiti kao referentni.
- **Napad poznatim nosiocem** – Vrsta napada u kojoj su dostupni i originalni, nepromenjeni nosilac i stego-objekat.
- **Napad poznatim stego-sadržajem** – Tip napada za koji napadač zna da skrivena poruka postoji, a stego-objekat se analizira za obrasce koji bi mogli biti korisni u budućim napadima.
- **Napad poznatom stego-metodom** - Napad u kojem je alat (algoritam) poznat pa su tako dostupni i originalni objekat prikrivanja i stego-objekat.

3. Opis sistema hibridne steganografske metode u prostornom domenu

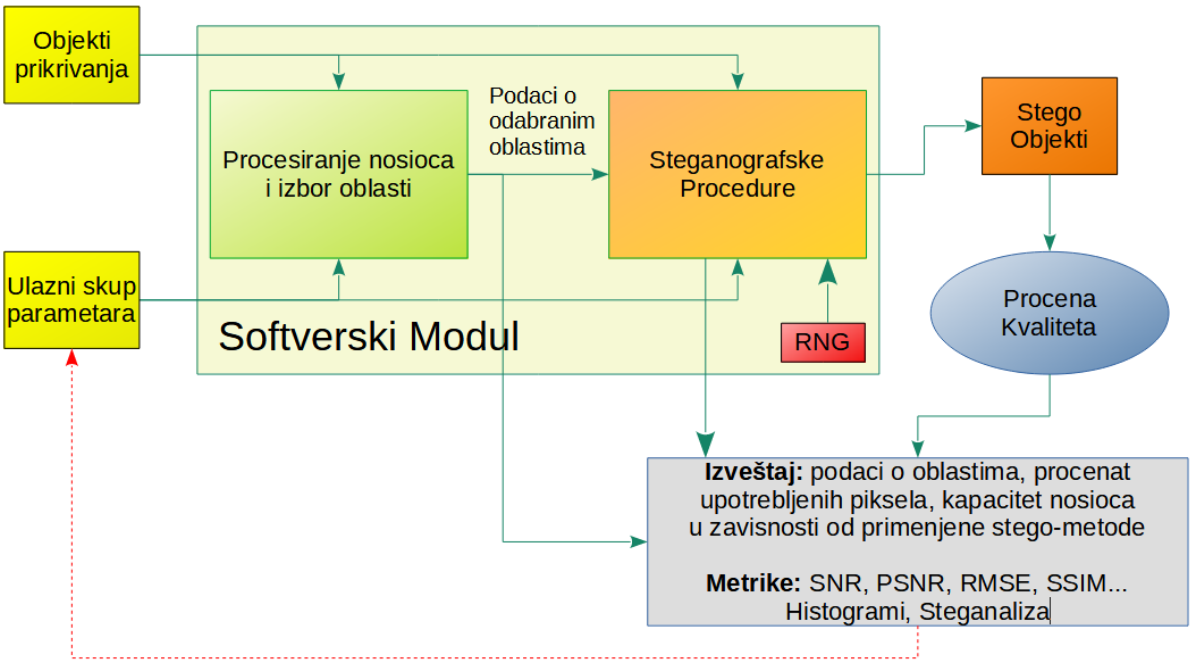
Ideja se zasniva na razvoju algoritma koji, kao ulaznu veličinu, koristi nekompresovane slike u *png* formatu (stego-nosači, objekti prikrivanja), kao i skup parametara koji se koriste za podešavanje algoritma za izračunavanje stego-oblasti kao i odgovarajućih steganografskih procedura.

Algoritam, na najvišem nivou, dizajniran je tako da sadrži dva modula koji su sekvencijalno povezani: ulazni modul obavlja obradu slike i prosleđuje informacije o stego-oblastima drugom modulu koji obavlja proces steganografije na stego nosiocu, u stego-oblastima. Pošto se steganografija može smatrati procedurom koja se primenjuje nakon procedure šifrovanja tajne poruke, sadržaj koji je utisnut u nosiocu ima svojstva (pseudo) slučajnog binarnog sadržaja (slika 7, *RNG* blok). Izlaz algoritma su stego-objekti i izveštaji o stego-oblastima, procenat piksela na koje će se vršiti uticaj i kapacitet nosioca u zavisnosti od primenjenih stego-metoda.

Razlog za odabir *png* ulaznog formata je mogućnost korišćenja datoteka stego-nosioca i stego-objekta u sirovom formatu, bez dodatne kompresije. Ukoliko se kao ulaz postavi kompresovana slika u *jpg* formatu, ona će prethodno biti dekompresovana, konvertovana u *png* format a potom dalje procesuirana. U tom smislu, procenti promenjenih piksela mogu se direktno prikazati a njihova veličina se može izraziti u bajtovima kao i sva statistika koja će u nastavku biti izračunata i diskutovana. Blok dijagram sistema je prikazan na slici 7.

Izračunavanje metrika za ocenu kvaliteta nad generisanim stego-objektima, analiza dobijenih rezultata u kombinaciji sa izveštajem kreiranim tokom obrade nosioca u predloženom

algoritmu, ima za cilj uspostavljanje korelacije između karakteristika objekta prikrivanja, ulaznog skupa parametara i željenih performansi izlaznog stego-objekta.

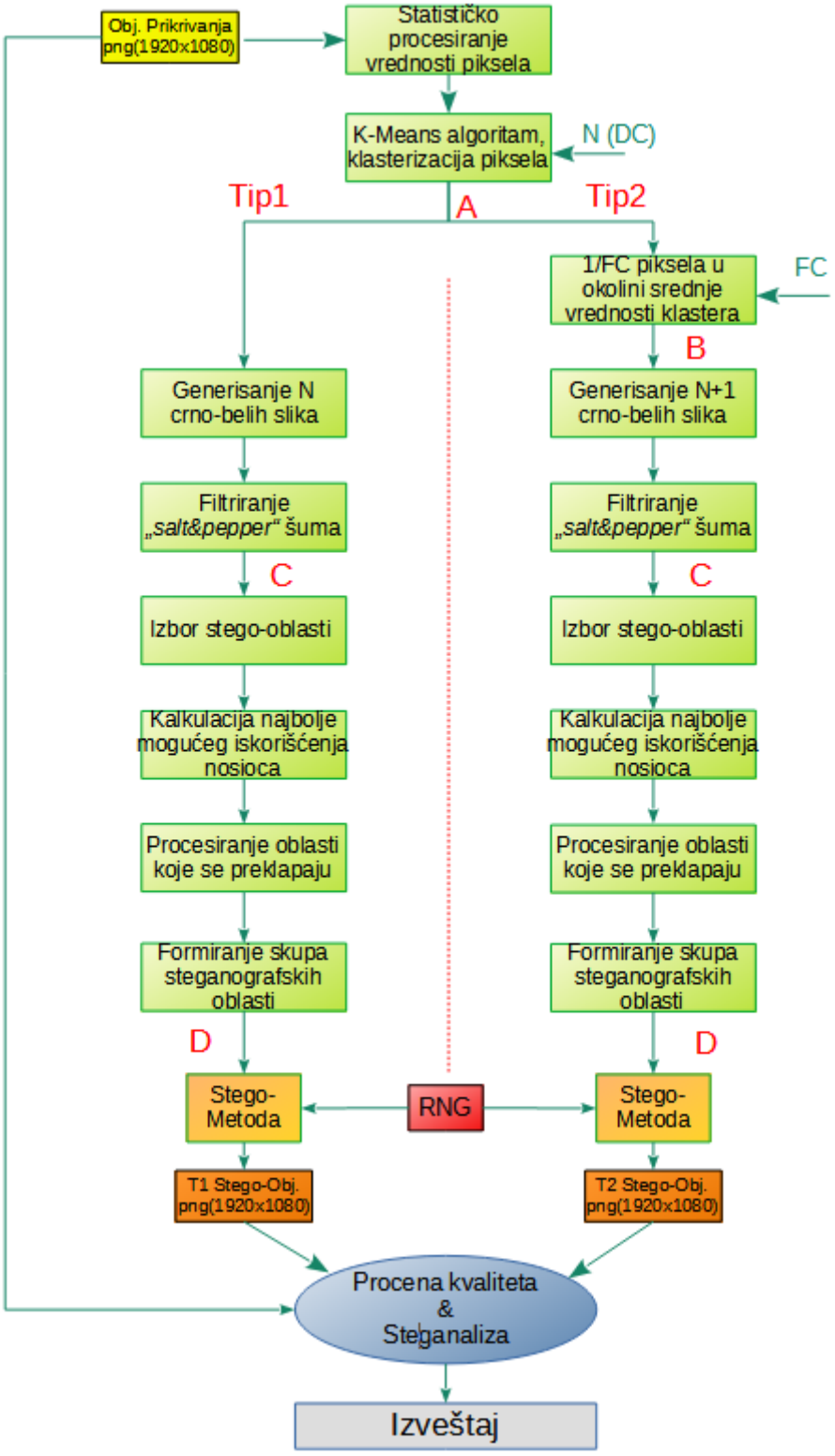


Slika 7. Blok dijagram hibridne steganografske metode u prostornom domenu

3.1. Algoritam za izračunavanje steganografskih oblasti

Slika 8 prikazuje detaljan blok dijagram sistema. Boje pojedinih delova algoritma odgovaraju bojama prikazanim na slici 1. U ovom poglavlju fokus je na podsistemu koji se bavi proračunom stego-oblasti i ti delovi tog podsistema su prikazani zelenom bojom na blok dijagramu.

Iterativni *K-means* algoritam se izvodi nad decimalnim vrednostima piksela ulaznog fajla u png formatu, na sva tri kanala (RGB), što rezultira grupisanjem svih piksela u *N* klastera, gde je *N* ulazni parametar algoritma (broj dominantnih boja).



Slika 8. Detaljan blok dijagram algoritma za izračunavanje steganografskih oblasti, za tip1 i tip2 vrstu obrade

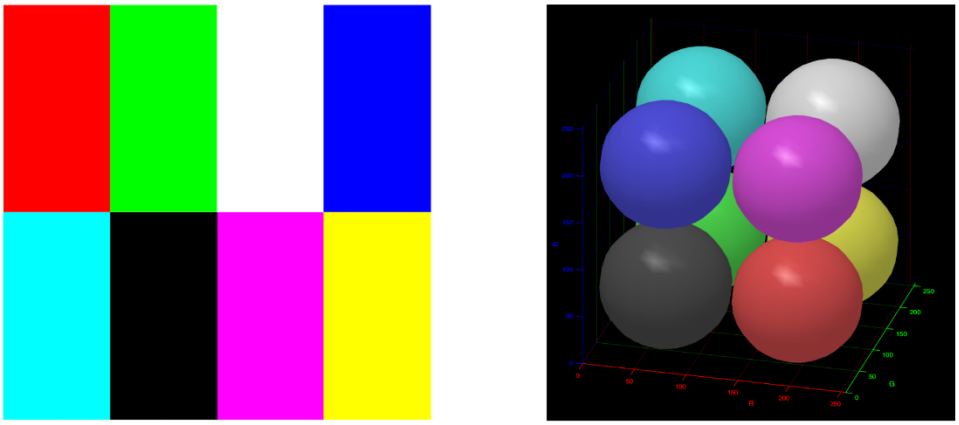
Iterativni algoritam *K-means* izvodi se na sledeći način:

- Korak 1: Određivanje srednje vrednosti svih piksela (A0);
- Korak 2: Podela svih piksela u dva nova klastera (C1 i C2) po *K-means* algoritmu i izračunavanje novih srednjih vrednosti (A1 i A2), koje smatramo dominantnim bojama, za novoformirane klastere;
- Korak 3: Ako je ulazna vrednost $N > 2$, vrši se analiza svakog od klastera C1 i C2, pa se potom procenjuje u kojem klasteru postoje veća odstupanja od srednjih vrednosti A1 i A2. Pretpostavimo da je odabran klaster C2 koji ima veća odstupanja piksela od srednje vrednost A2. *K-means* algoritam se ponovo izvodi na odabranom klasteru C2, pa se zatim kreiraju dva nova klastera koji nasleđuju klaster C2. Nazvaćemo nove klastere C21 i C22 i izračunate su nove srednje vrednosti A21 i A22. Sada imamo ukupno tri klastera C1, C21 i C22 kao i njihove tri srednje vrednosti A1, A21 i A22, koje smatramo dominantnim bojama;
- Korak 4: Ako je $N > 3$, posmatramo tri postojeća klastera C1, C21 i C22 i na isti način kao u koraku 3, biramo koji će od postojećih klastera biti podeljen na dva nova, a potom se izračunavaju i nove srednje vrednosti. Kao rezultat, dobijamo četiri klastera sa četiri srednje vrednosti.

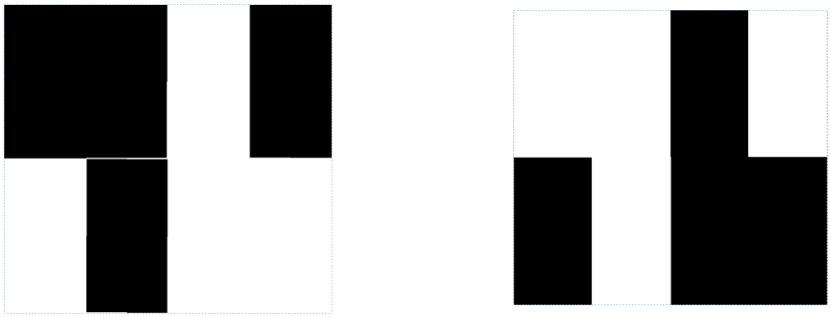
Za veće vrednosti ulaznog parametra N algoritam se izvodi iterativno kao što je objašnjeno u koracima 3 i 4.

Predloženi algoritam obrade tipa 1 kreira N crno-belih slika gde su pikseli klastera $c = i$ prikazani belom bojom, dok su pikseli koji pripadaju klasterima $c \neq i$ prikazani crnom bojom, gde i uzima vrednosti od 1 do N, gde je N broj potrebnih klastera. Za potrebe boljeg

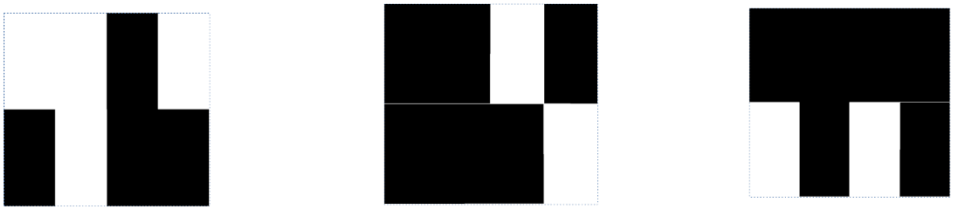
razumevanja rada algoritma kreirana je slika sa 8 različitih boja tako da se svaka boja nalazi u temenu kocke ograničenog (RGB) prostora, prikazano na slici 9a.



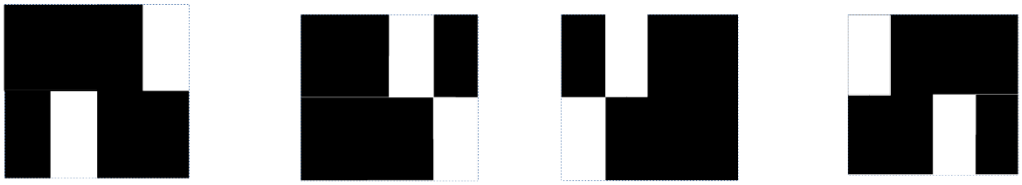
a) Originalna test slika i njena raspodela piksela u 3D RGB domenu



b) Klasterizacija piksela u 2 oblasti i prikaz raspodele u prostornom domenu



c) Klasterizacija piksela u 3 oblasti i prikaz raspodele u prostornom domenu



d) Klasterizacija piksela u 4 oblasti i prikaz raspodele u prostornom domenu

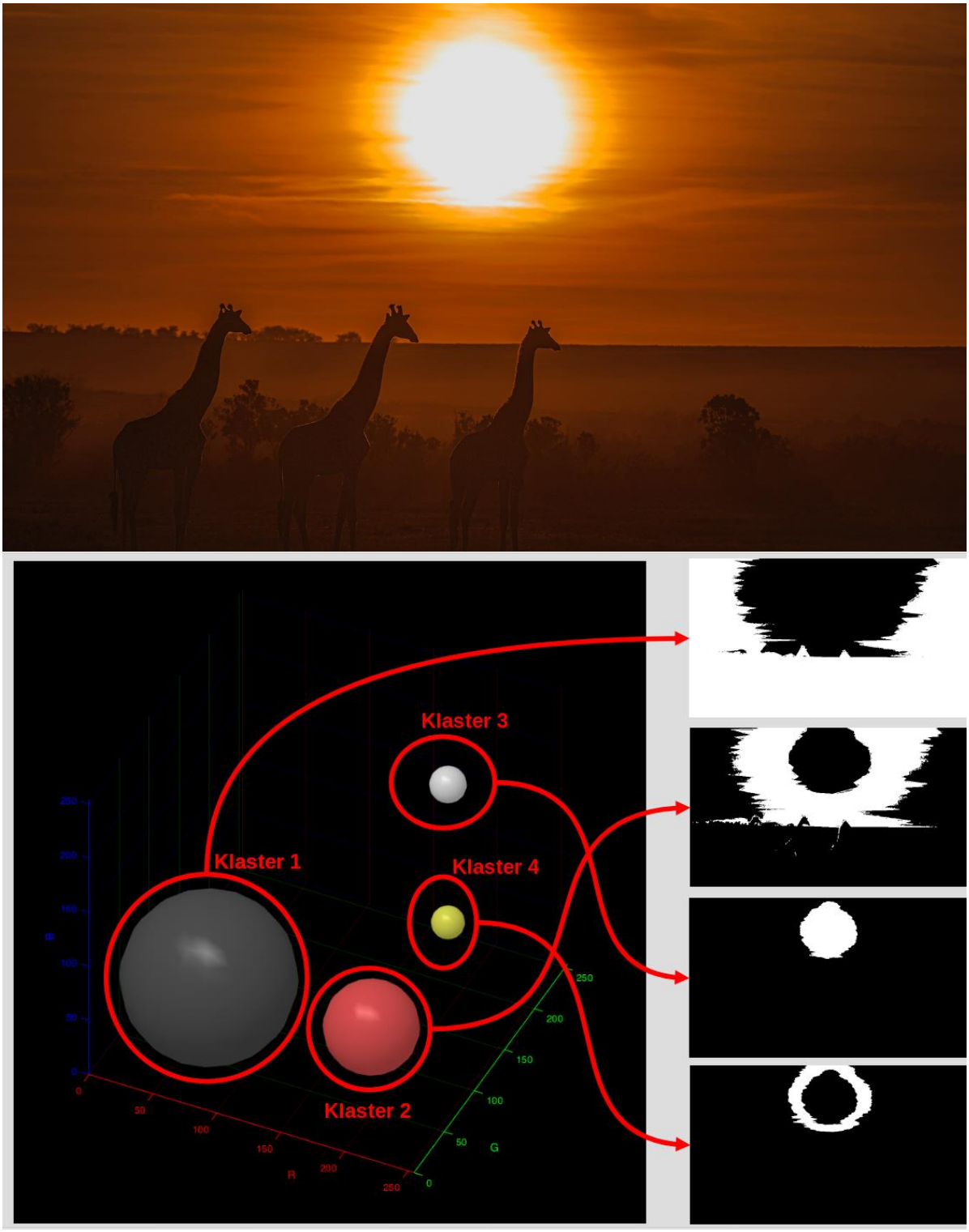
e) Klasterizacija piksela u 8 oblasti i prikaz raspodele u prostornom domenu

Slika 9. Test primer rada predloženog algoritma; a)Test slika i njen 3D histogram; b,c,d,e) Kreirane crno-bele slike za klasterizaciju u 2,3,4 i 8 oblasti respektivno

Produkt algoritma u tački A na slici 8 su crno-bele slike, pa su tako na slici 9b-e predstavljene crno-bele slike za vrednosti ulaznog parametra *N*=2,3,4,8 respektivno. Uočavamo korelaciju originalne slike (slika 9a) i crno belih slika za *N*=2 (slika 9b), gde je algoritam podelio sve piksele u dva klastera: Klaster 1 – bela, roze, žuta i crvena boja; Klaster 2 – svetlo plava, tamno plava, zelena i crna boja. Na slici 9c , za *N*=3, vidimo efekat deljenja Klastera 1 iz prethodnog slučaja na dva nova klastera, dok Klaster 2 iz prethodnog slučaja zadržava svoju formu. Na slici 9d, za *N*=4, vidimo efekat klasterizacije u 4 različita klastera, gde svaki od njih sadrži po dve bliske boje iz 3D raspodele (boje iz susednih temena ograničenog prostora oblika kocke). Konačno slika 9e, za *N*=8, pokazuje klasterizaciju u 8 različitih klastera gde svaki od njih sadrži piksele iste boje koji se nalaze u jednom od temena 3D raspodele. Takav efekat ogleda se u kreiranju 8 crno-belih slika gde je na svakoj od njih belom bojom prikazano ono što se nalazi u jednom od 8 temena raspodele u 3D prostoru.

Sada, umesto slike generisane za teoretske potrebe, posmatrajmo realnu sliku. Slika 10 prikazuje originalnu sliku i način distribucije piksela originalne slike u 3D (RGB) prostoru, gde je veličina svake sfere direktno proporcionalna broju piksela određene nijanse i načina u kojoj su pikseli podeljeni u četiri klastera.

Pošto smo u tački A algoritma sa slike 8 generisali odgovarajući broj crno-belih slika, dalja obrada se nastavlja na njima. U levoj grani algoritma na slici 8 (tip obrade 1) vrši filtriranje *salt&pepper* (uklanjanje pojedinačnih piksela kako bi se maksimizirale pojedinačne bele zone). U tački "C", sledeća dva algoritamska bloka ("Izbor stego oblasti" i "Kalkulacija najbolje mogućeg iskorišćenja nosioca") prihvataju *N* crno-belih slika, procenjuju veličinu belih područja i pokušavaju da izračunaju pravougaonike za svaku crno-belu sliku kako bi identifikovali najbolji mogući način da se popuni dato belo područje.

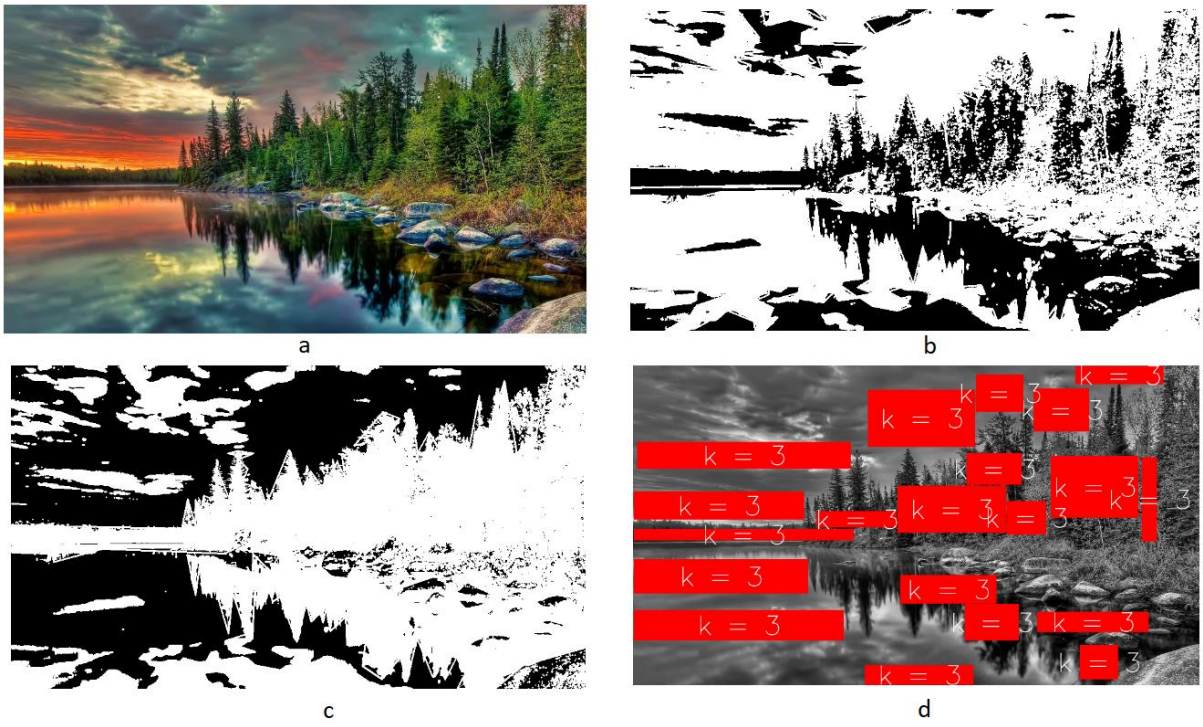


Slika 10. Primer rada predloženog algoritma na realnoj slici za tip1 obradu - Originalna slika, klasterizacija piksela prikazana u 3D RGB prostoru za N=4, kao i odgovarajući crno-beli produkti

Važno je da broj izračunatih pravougaonika ne prelazi definisanu granicu (ulazna veličina), a takođe je potrebno odbaciti pravougaonike čija je veličina manja od definisane minimalne vrednosti. Izlazne informacije iz gore-navedenog algoritamskog bloka predstavljaju skup

pravougaonika definisanih za svaku crno-belu sliku, konkretno pozicije piksela gornjeg levog i donjeg desnog vrha pravougaonika. Sledeći blok algoritama (“Procesiranje oblasti koje se preklapaju”) prihvata informacije o izračunatim pravougaonicima i proverava da li postoji moguće preklapanje pojedinačnih pravougaonika kreiranih na različitim crno-belim slikama. Ako postoji preklapanje, algoritam vrši odgovarajuću reviziju veličina pravougaonika tako da, s jedne strane, nema preklapanja između njih, a s druge strane, njihova veličina ostane što veća moguća. Pojava slučajeva gde dolazi do preklapanja pravougaonika generisanih na različitim crno-belim slikama je upravo posledica *salt&pepper* filtriranja. Konačno, formira se skup svih pravougaonika, selektovanih na *N* crno-belih slika uz eventualnu reviziju, a algoritamski blok neposredno ispred tačke „D“ („Formiranje skupa steganografskih oblasti“) izračunava procenat stego-oblasti u određenom nosiocu, odnosno količinu poverljivih informacija koju nosilac može preneti. Za potrebe vizualnog izveštaja, odabrani pravougaonici su nacrtani u različitim bojama na verziji originalne slike predstavljenoj u nijansama sive, tako da gledalac može lakše videti njihov položaj i veličinu, slika 11. U predloženom algoritmu mogu se koristiti različiti geometrijski oblici. Razlog odabira pravougaonika, kao geometrijske figure koju će algoritam koristiti za formiranje stego-oblasti, je taj što više pravougaonika može lako ispuniti nepravilnu površinu slike, s jedne strane, dok sa druge strane informacije o poziciji i veličini određenog pravougaonika mogu se preneti minimalnom količinom podataka (položaj gornjeg levog piksela temena i položaj donjeg desnog piksela temena). Povećanjem vrednosti ulaznog parametra *N* dobija se više crno-belih slika, od kojih će svaka imati manji postotak bele površine, što podrazumeva generisanje manjih pravougaonika, a samim tim i smanjenje kapaciteta nosioca. Kako informacije o generisanim pravougaonicima (stego-oblastima) prenosimo posebnim komunikacionim kanalom na prijemnu stranu, imalo bi smisla definisati maksimalan broj mogućih stego-oblasti na jednom nosiocu kako

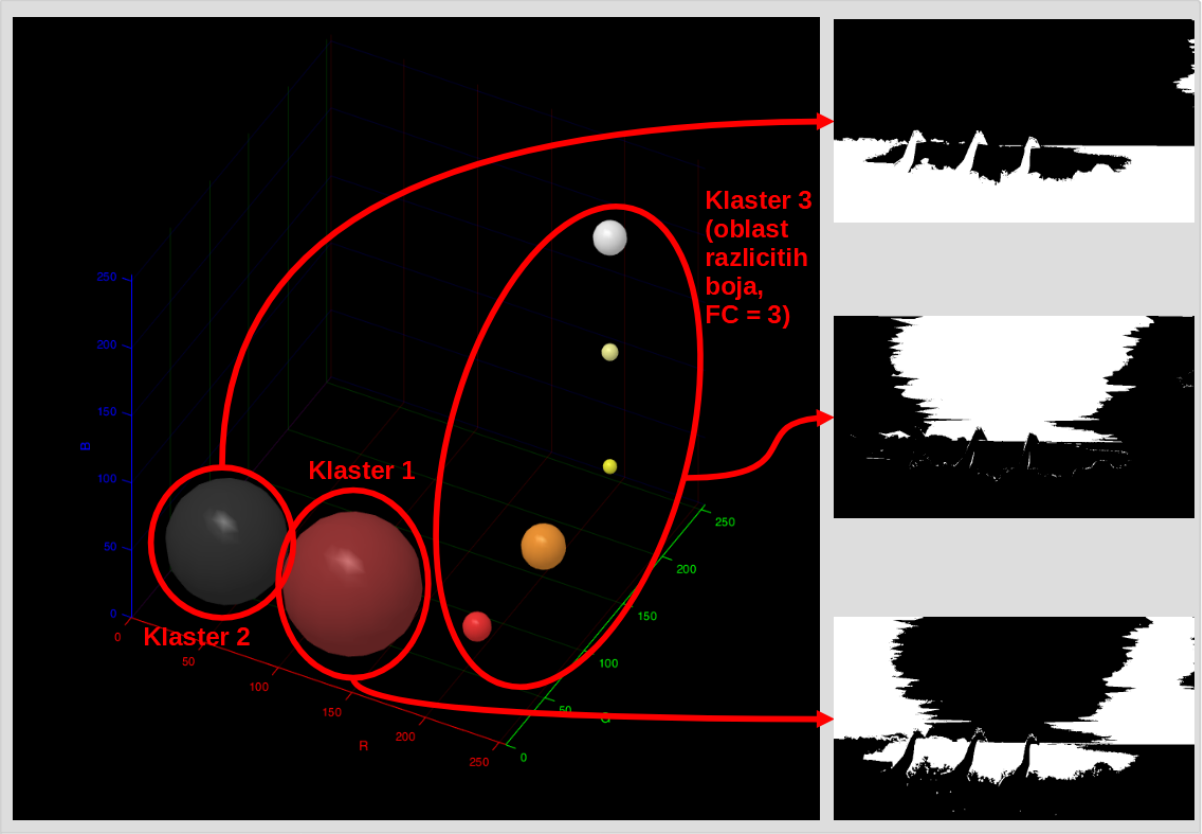
informacija o njima ne bi bila previše velika. U ovom slučaju, broj maksimalnih pravougaonika je ograničen na manje ili jednako 20. Na osnovu predstavljene ideje, očekuje se da će se kapaciteti nosioca razlikovati u zavisnosti od vrste objekta prikrivanja, tako da slike sa velikim površinama u sličnoj ili istoj boji/nijansi će imati veći kapacitet, dok će slike bez velikih zona u sličnim nijansama imati manji kapacitet.



Slika 11. a) Originalni objekat prikrivanja; b,c) crno-beli derivati obrade predloženim algoritmom, d) raspored odabranih pravounika prikazan na sivoj (grayscale) varijanti originalnog nosioca

Sada pogledajmo desnu granu algoritma na slici 8 (tip 2 obrade), primećuje se algoritamski blok iza tačke "A" - *1/FC* piksela u okolini srednje vrednosti klastera. Ideja se razlikuje od prethodne ideje opisane za levu granu algoritma. Zapravo, cilj je odabrati *1/FC* piksela oko srednjih vrednosti boja za pojedinačnih *N* klastera (Z_i, $i = 1, 2, \ldots, N$) i kreirati *N* podskupova piksela sastavljenih od njih. Ove podskupove deklarišemo kao nove klastere, dok svi ostali pikseli koji dovoljno odstupaju od srednjih vrednosti, za svaku zonu Z_i, kreiraju jedinstvenu, novu zonu *Z"* - Klaster 3 (slika 12). Kao što je prikazano na desnoj grani algoritma na slici 8,

dalji tok obrade i proračuna površine je identičan levoj grani algoritma, samo što sada umesto *N* crno-belih slika algoritam traži stego - oblasti na *N + 1* crno-belih slika. Ovim pristupom ćemo steganografski proces izvoditi posebno u zonama dominantnih boja, a posebno u zoni koja ne pripada nijednoj od *N* dominantnih, takozvanih „šarenih zona“. Govoreći o *LSB* steganografiji, pretpostavka je da u šarenim zonama postoji mogućnost izmene više bitova manje težine i istovremeno smanjenje vizualne degradacije kvaliteta stego-objekta, uz postizanje većeg kapaciteta stego-nosioca.



Slika 12. Primer rada predloženog algoritma na realnoj slici za tip2 obradu - Klasterizacija piksela prikazana u 3D RGB prostoru za DC=2, FC=3, kao i odgovarajući crno-beli produkti (za nosilac sa slike 10)

Crno bele slike na slici 12 su pandan crno-belim produktima na slici 10 za desnu granu algoritma (slika 8), odnosno tip obrade 2. U ovom slučaju, broj dominantnih boja je *DC* = 2, a koeficijent filtriranja je *FC* = 3. Algoritam, nakon procesa klasterizacije, dodeli piksele

pripadajućim klasterima a potom vrši filtriranje i sve piksele koji ne pripadaju *1/FC* okolini dominantnih boja proglašava pripadajućem novom klasteru 3 – tzv. oblast različitih boja. Za razliku od tipa obrade 1 sada umesto *N* crno-belih slika kao derivat obrade imamo *N+1* crno-belu sliku, na kojima se nastavlja dalja obrada, kako je to prethodno objašnjeno

3.2. Sistem adaptivne steganografije upotrebom Algoritma za Selekciju Steganografskih Oblasti i *MDD* steganografske metode

Na osnovu objašnjenja kompletnog algoritma, treba napomenuti da je složenost reda $O(n^3)$, gde je *n* broj piksela nosioca po jednoj dimenziji. Procesna snaga i dodatno vreme potrebno za izvršenje algoritma ovog nivoa složenosti je cena koju treba platiti za povećanje sigurnosti sistema. Treba napomenuti da povećanje rezolucije objekata prikrivanja može značajno povećati potrebnu procesorsku snagu i/ili vreme obrade. Kako se, u opštem slučaju, u ovakvom sistemu mogu upotrebiti različiti stagnografski algoritmi, kako u prostornom tako i u frekvencijskom domenu, (slika 7 – blok: Stegnografske procedure), nivo složenosti celokupnog sistema može biti i veći od $O(n^3)$.

3.2.1. Procedura ugradnje/utiskivanja tajnog sadržaja

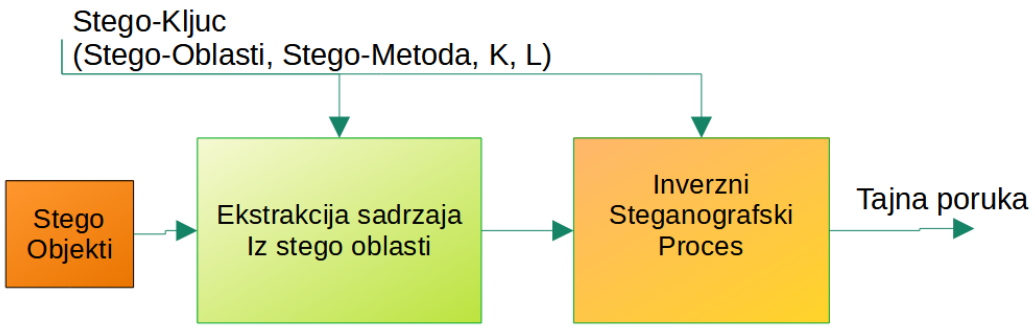
Budući da su oblasti nosioca u koje će se utisnuti tajni sadržaj definisani opisanim algoritmom, navedenim pravougaonicima se dodeljuju serijski brojevi (indeksi). Ukoliko kao steganografsku metodu koristimo neku iz familije *LSB* metoda, proces ugrađivanja tajnih informacija se obavlja u pikselima, po vrstama, s leva na desno, u indeksiranim pravougaonim oblastima, respektivno. Kako *MDD* metoda pripada pomenutoj familiji, postoje uslovi da i ona bude implementirana na prethodno objašnjen način. Kada se radi o *PVD* metodi, njena karakteristika je da koristi decimalne vrednosti dva susedna piksela, kao što je objašnjeno u

poglavlju 2.4. Ukoliko usvojimo princip da pomenuta dva piksela koja se koriste za parcijalnu primenu *PVD* metode budu dva uzastopna piksela u istoj vrsti tada je moguće implementirati identičan scenario, upotrebom pravougaonih stego oblasti, gde bi bilo poželjno da širine pomenutih pravougaonika sadrže paran broj piksela.

3.2.2. Procedura ekstrakcije tajnog sadržaja

Pošto informacije o pozicijama pravougaonika i njihovim serijskim brojevima (indeksima) stižu na prijemnu stranu preko posebnog (nezavisnog) kanala, algoritam koristi ove informacije (*Stego-Key*), pristupa određenim oblastima stego-objekta prema indeksu i vrši ekstrakciju sadržaja. Kao što je prikazano na slici 13, nakon izdvajanja sadržaja iz definisanih područja, izvodi se inverzni proces steganografije, bez obzira da li se ekstrakcija vrši iz pojedinačnog piksela, što je svejstveno za *LSB* familiju metoda ili iz para susednih piksela, što je svojstveno *PVD* metodi.

Kada je u pitanju *MDD* metoda, na osnovu pomenutih uputstava, jasno je da se kompletan sistem ugrađivanja i ekstrakcije tajnog sadržaja obavlja na uobičajen način sa jedinom razlikom što sada proces obavljamo u oblastima nosioca umesto preko njegove cele površine.



Slika 13. Blok dijagram ekstrakcije steganografskog sadržaja iz stego-objekta kreiranog predloženim algoritmom

4. Dizajn eksperimenta

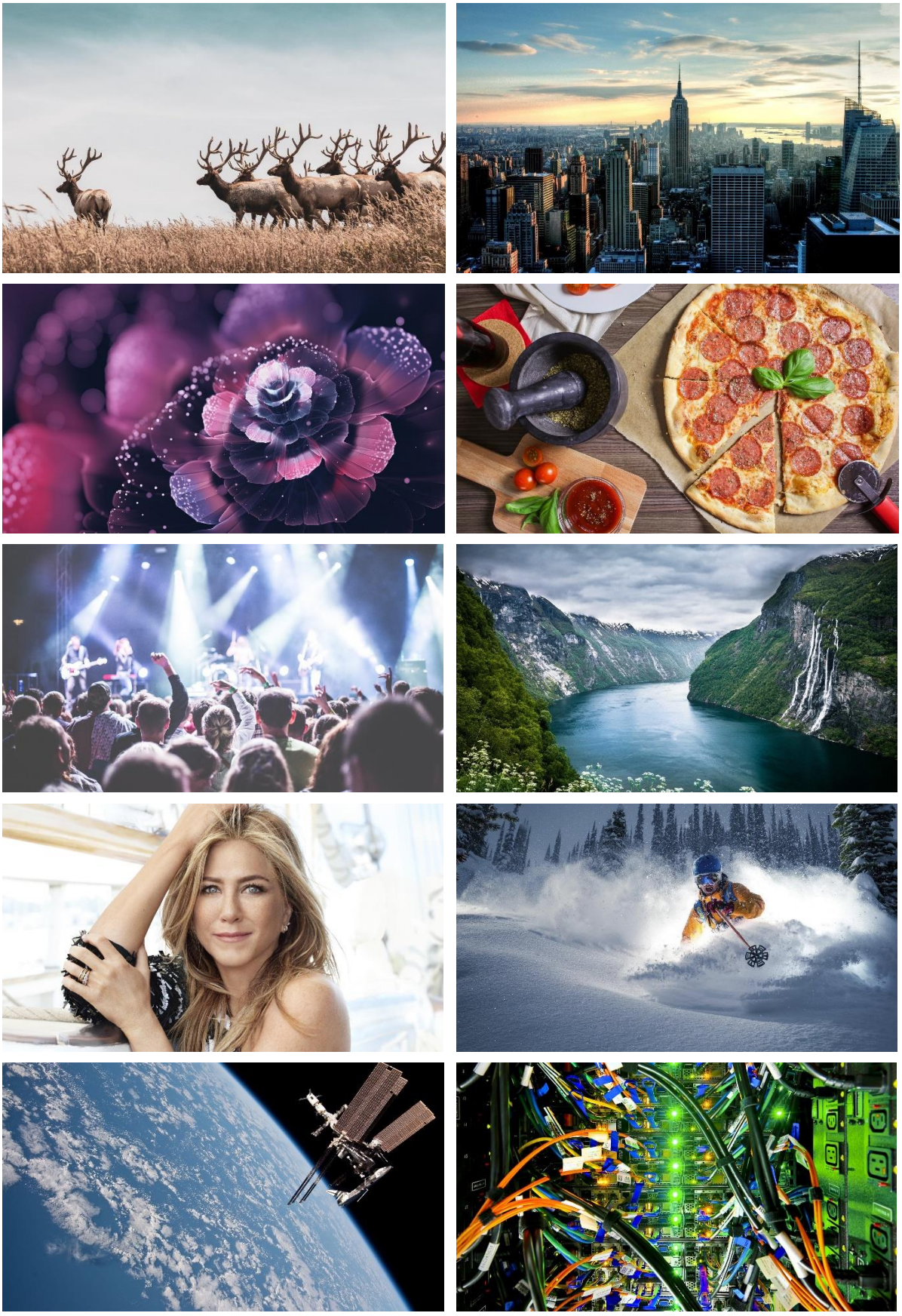
Kada je u pitanju steganografija u prostornom domenu, metode *LSB* i *PVD* su među najčešće korišćenim tehnikama, pa mnogi autori često upoređuju njihove karakteristike i međusobno ih kombinuju. Za osnovnu steganografsku metodu u ovom radu korišćena je *MDD* metoda opisana u [35], [36] , kao i u poglavlju 2.4. *MDD* metoda je derivat osnovne *LSB* metode i u odnosu na nju ima značajne prednosti u kvalitetima stego-objekata, koji su prikazani u [35], [36]. Za potrebe eksperimenta izvršeno je međusobno poređenje stego-objekata dobijenih navedenim metodama (*MDD/LSB, PVD*), uz očekivanje da će *MDD* metoda biti dominantna i na taj način opravdati zašto je korišćena u ovom radu. U delu koji se bavi analizom rezultata urađeno je poređenje kvaliteta stego-objekata dobijenih metodom adaptivne steganografije, u kontekstu kapaciteta, kvaliteta stego-objekata i otpornosti na stego-analizu.

Kao što je opisano u poglavlju 3, algoritam za izračunavanje stego-oblasti prosleđuje informacije o veličinama i pozicijama pravougaonika modulu koji izvodi proces steganografije. Zbir broja piksela svih pravougaonika predstavlja ukupan broj piksela koji će biti izmenjeni tokom procesa steganografije, ova vrednost se u literaturi često naziva - *PixelsToImpact*. Ova veličina može se predstaviti kao apsolutna vrednost, a može i kao procenat ukupnog broja piksela objekta prikrivanja. Kapacitet nosioca (*Cap*) za *MDD* metodu izračunava se kao:

$$Cap = PixelsToImpact[\%] \times K/8 \qquad (13)$$

gde *K* predstavlja broj bitova najmanje težine koje menjamo u svakom kanalu (*RGB*) odgovarajućeg piksela.

Eksperiment se izvodi u dve faze, kao što je prikazano levom i desnom granom algoritma na slici 8, na skupu podataka posebno dizajniranom za ovu svrhu. Kreiran je skup podataka koji



Slika 14. Primeri slika iz skupa nad kojim je vršena obrada za različite tematske kategorije

se sastoji od 100 slika za svaku od 10 odabranih tema (priroda, ljudi, fantazija, hrana, svemir, životinje, sport, gradovi, tehnologija, muzika), slika 14 – set slika. Analiza se vrši na celom skupu dobijenih podataka (poglavlje 9. – Apendix) dok će neki reprezentativni rezultati biti prikazani u daljem tekstu. Kako bi dobijeni rezultati bolje prikazali ponašanje različitih tipova nosilaca, ulazni skup slika je odabran tako da sadrži slike čije vizuelne performanse imaju dijametralne karakteristike. Pa tako, neke od odabranih slika imaju velike oblasti sličnih boja i nijansi dok druge slike iz skupa imaju male oblasti sličnih nijansi i izražene šarene oblasti. Neke od odabranih slika imaju izoštrene detalje na njima dok one druge imaju zamućene detalje. Na nekim slikama dominiraju pravilni oblici dok na onim drugim dominiraju nepravilni oblici. Ovakvim izborom ulaznih nosilaca očekuje se da će numeričke vrednosti, dobijene eksperimentom, pokazati smernice u cilju boljeg i pravilnijeg izbora nosilaca u zavisnosti od efekata koje želimo da postignemo. Dobijeni rezultati i njihova analiza treba da pokažu navedene razlike u vizuelnom doživljaju predloženih slika. Važno je napomenuti da su svi korišćeni png nosioci slike punog (full) *HD* formata, dimenzija 1920 × 1080 piksela, u boji, tri kanala. Veličina svakog od korišćenih medija je: 1B × 3Ch(rgb) × 1920 × 1080 = 6075 KB. Pre opisivanja eksperimenata i testova, treba napomenuti da je kompletna implementacija algoritma razvijena u programskom jeziku C++, u razvojnom okruženju *QT* i da je *OpenCV* biblioteka korišćena kao alat za obradu slika.

Softver je dizajniran tako da je moguće sačuvati navedene crno-bele derivate obrade u okviru detaljnog izveštaja. Nakon što izračuna stego-oblast nosioca i označi ih na slici u sivoj verziji originala (slika 7), softver kreira i tekstualni izveštaj koji sadrži podatke o pravougaonicima (koordinate gornjeg levog i donjeg desnog piksela), ukupno broj piksela uključenih u pravougaonike, kao i procenat navedenih piksela u odnosu na ukupan broj piksela. Kako se stego-metode kategorije *LSB* mogu izvoditi sa različitim brojem *K* bita koje menjamo, ovaj

parametar je u testu uzeo vrednosti *K* = 2, 3 i 4. U radu [62] prikazani su rezultati sličnog eksperimenta gde je *K*=5 bita i ni u jednom slučaju ovi rezultati nisu bili prihvatljivi, s toga u ovom radu vrednost od *K*=5 bita na koje vršimo uticaj nije korišćen niti uzet kao relevantan. Kao što je ranije objašnjeno, zbog karakteristika *PVD* metode, nije moguće odabrati broj bita koji će se modifikovati u procesu steganografije, za svaki kanal ili za svaki piksel, pa će se ova metoda izvoditi na uobičajen način , preko celog objekta prikrivanja ili preko stego-oblasti.

Ideja metode obrade tipa 2 bazirana je na desnoj grani algoritma opisanog u poglavlju 3. U ovom eksperimentu, broj dominantnih boja (*DC*) je fiksiran na *N* = 2, dok se koeficijent filtriranja menja kao *FC* = 1 , 2, 3, 4. Razlog zašto je parametar *N* fiksiran na broj 2 je taj što su u tom slučaju svi pikseli podeljeni u samo dve velike zone i stoga efekti kasnijeg filtriranja oko srednje vrednosti nijanse za odgovarajući klaster prema *FC* koeficijentu su bolji i jasniji. Slučaju gde je *FC* = 1 je trivijalan jer tada filtriranje ne postoji i tada bi se tip 2 obrade sveo na tip 1 vrstu obrade. Modul za izvođenje stego-metode, za *MDD*, implementiran je sa mogućnošću uticaja na *K* bitova i u oblastima koje pripadaju zonama Z_i' kao uticaj na *L* bitova u zonama Z" (tzv. "šarene" oblasti). U ovom slučaju, kapacitet nosioca se izračunava na sedeći način:

$$Cap = PixelsToImpact[\%](Z') \times \frac{K}{8} + PixelsToImpact[\%](Z'') \times \frac{L}{8} \qquad (14)$$

gde je $Z' = \sum_{i=0}^{N} Z_i'$ a vrednost *N* predstavlja broj klastera.

Da bi se kvalitetno predstavilo ponašanje stego-objekata za tip 2 obrade uzimane su sledeće vrednosti za parametre *K* i *L* respektivno: (2,3), (2,4), (3,3), (3,2),(3,4), (4,2), (4,3)

5. Analiza dobijenih rezultata

U Sekciji 4 je opisano kako se izvodi eksperiment. Način kako je tip 1 obrade sproveden nad 100 odabranih nosilaca implicira da je kao rezultat dobijeno 1200 stego-objekata nad kojima

su vršene procene kvaliteta kao i stego-analiza. Tip 2 obrade nad 100 objekata prikrivanja obavljen je na ukupno 21 način (7 načina odabira parova za vrednosti *K* i *L*; upotreba 3 različita koeficijenta filtriranja) što, u ovom slučaju, implicira da je kao rezultat dobijeno 2100 stego-objekata nad kojima su takođe vršene procene kvaliteta i stego-analiza. Ukupna količina dobijenih podataka, za svaki od tipova obrade (tip 1 i tip 2) je uvezena u softverski alat *MS Excel* kako bi se podacima lakše manipulisalo. Odgovarajućim filtracijama podataka i računanjem srednjih vrednosti za različite slučajeve od osnovnog skupa izlaznih podataka dobijeni su derivati koji podrazumevaju statistiku po pojedinačnim nosiocima, statistiku po načinima primenjene obrade i konačno procenu generisanih rezultata pomoću alata opisanih u poglavlju 1.5. Odabrani deo podataka biće prikazan u ovoj sekciji i komentarisan dok će svi dobijeni podaci biti predstavljeni u prilogu ovom radu (poglavlje 9 - Apendix).

Tabela 2. Rezultati obrade stego-objekata generisanih pomoću nosioca Music08.jpg za tip1 vrstu obrade, ¼ skupa dobijenih rezultata

Redni broj	Broj dominantnih boja	Broj piksela na koje vrsimo uticaj	K	Veličina poruke LSB MDD	Veličina poruke PVD	Procenat iskorišćenja LSB MDD	bpp LSB MDD	Procenat iskorišćenja PVD	bpp PVD
1	1	2063532	2	1547649	1191433	25,0	6	19,15200	4,59660
2	1	2063532	3	2321473	1191433	37,50	9	19,15200	4,59660
3	1	2063532	4	3095298	1191433	50,00	12	19,15200	4,59660
4	2	1043480	2	782610	595069	12,58100	3,01930	9,56580	2,29580
5	2	1043480	3	1173915	595069	18,87100	4,52900	9,56580	2,29580
6	2	1043480	4	1565220	595069	25,16100	6,03870	9,56580	2,29580
7	4	635202	2	476401	359628	7,65820	1,83800	5,78110	1,38750
8	4	635202	3	714602	359628	11,48700	2,75700	5,78110	1,38750
9	4	635202	4	952803	359628	15,31600	3,67590	5,78110	1,38750
10	8	456912	2	342684	257202	5,50870	1,32210	4,13450	0,99229
11	8	456912	3	514026	257202	8,26300	1,98310	4,13450	0,99229
12	8	456912	4	685368	257202	11,01700	2,64420	4,13450	0,99229
Srednja vrednost za obavljeni stego-proces preko celog nosioca						37,50000	9,00000	19,51681	4,68405
Srednja vrednost za obavljeni stego-proces u stego-oblastima						14,27573	3,42618	7,46319	1,79116
Ukupna srednja vrednost						18,98474	4,55638	9,65835	2,31805

Tabela 3. Rezultati obrade stego-objekata generisanih pomoću nosioca Music08.jpg za tip1 vrstu obrade, 2/4 skupa dobijenih rezultata

Redni broj	LSB MSE	LSB RMSE	LSB SNR	LSB PSNR	LSB SSIM	LSB GMSD	LSB Q	LSB Prs	LSB Pd
1	2,48050	1,57490	39,89900	44,18500	0,97619	0,00335	0,99965	0,91485	0,91403
2	10,51200	3,24230	33,62700	37,91400	0,91437	0,01728	0,99853	0,95394	0,95331
3	44,16200	6,64550	27,39400	31,68000	0,75660	0,06153	0,99386	0,78741	0,78596
4	1,25030	1,11810	42,87400	47,16100	0,98627	0,00291	0,99982	0,52768	1,03820
5	5,31490	2,30540	36,58900	40,87600	0,95147	0,01469	0,99926	0,42672	0,83753
6	22,83800	4,77890	30,25800	34,54400	0,86278	0,05084	0,99682	0,31457	0,61466
7	0,75844	0,87088	45,04500	49,33200	0,99048	0,00256	0,99989	0,37276	1,19970
8	3,25150	1,80320	38,72300	43,01000	0,96693	0,01275	0,99954	0,27542	0,88192
9	14,60400	3,82150	32,19900	36,48600	0,90765	0,04499	0,99797	0,17836	0,56508
10	0,54392	0,73751	46,48900	50,77500	0,99275	0,00245	0,99992	0,29862	1,33140
11	2,35490	1,53460	40,12400	44,41100	0,97532	0,01211	0,99967	0,21237	0,93994
12	10,91800	3,30420	33,46300	37,74900	0,93118	0,04108	0,99848	0,12511	0,54390
Srednja vrednost za obavljeni stego-proces preko celog nosioca				37,90453	0,87453	0,02592	0,99326	1,03208	0,95271
Srednja vrednost za obavljeni stego-proces u stego-oblastima				42,82517	0,93898	0,01922	0,99732	0,41240	1,23604
Ukupna srednja vrednost				41,51025	0,93433	0,02221	0,99862	0,44898	0,88380

Tabela 4. Rezultati obrade stego-objekata generisanih pomoću nosioca Music08.jpg za tip1 vrstu obrade, 3/4 skupa dobijenih rezultata

Redni broj	MDD MSE	MDD RMSE	MDD SNR	MDD PSNR	MDD SSIM	MDD GMSD	MDD Q	MDD Prs	MDD Pd
1	1,49490	1,22270	42,09800	46,38500	0,98732	0,00133	0,99982	0,00839	0,00315
2	5,48740	2,34250	36,45100	40,73700	0,94947	0,00558	0,99926	0,00905	0,00381
3	21,57900	4,64530	30,50400	34,79100	0,82920	0,02172	0,99699	0,03119	0,02606
4	0,75505	0,86894	45,06400	49,35100	0,99253	0,00114	0,99990	0,00353	0,00344
5	2,76720	1,66350	39,42400	43,71000	0,97038	0,00479	0,99962	0,00121	0,00805
6	10,87800	3,29820	33,47900	37,76500	0,90045	0,01901	0,99848	0,00760	0,00466
7	0,45940	0,67779	47,22200	51,50900	0,99469	0,00101	0,99994	0,00455	0,00230
8	1,68750	1,29900	41,57200	45,85800	0,97898	0,00428	0,99977	0,00141	0,01257
9	6,59080	2,56730	35,65500	39,94100	0,93038	0,01724	0,99908	0,00126	0,01306
10	0,33015	0,57459	48,65700	52,94400	0,99585	0,00091	0,99995	0,00383	0,00650
11	1,21230	1,10100	43,00800	47,29500	0,98362	0,00397	0,99983	0,00672	0,00661
12	4,73800	2,17670	37,08800	41,37500	0,94617	0,01615	0,99933	0,00372	0,00698
Srednja vrednost za obavljeni stego-proces preko celog nosioca				40,17423	0,90621	0,01019	0,99487	0,14516	0,11268
Srednja vrednost za obavljeni stego-proces u stego-oblastima				44,90783	0,95188	0,00817	0,99794	0,14029	0,34132
Ukupna srednja vrednost				44,30508	0,95492	0,00809	0,99933	0,00687	0,00810

Tabela 5. Rezultati obrade stego-objekata generisanih pomoću nosioca Music08.jpg za tip1 vrstu obrade, 4/4 skupa dobijenih rezultata

Redni broj	PVD MSE	PVD RMSE	PVD SNR	PVD PSNR	PVD SSIM	PVD GMSD	PVD Q	PVD Prs	PVD Pd
1	4,14140	2,03500	37,67300	41,95900	0,96821	0,00027	0,99942	0,01339	0,00817
2	4,14080	2,03490	37,67300	41,96000	0,96825	0,00033	0,99942	0,00607	0,00081
3	4,14280	2,03540	37,67100	41,95800	0,96823	0,00027	0,99942	0,02462	0,01946
4	1,78860	1,33740	41,31900	45,60600	0,98109	0,00017	0,99975	0,00005	0,01036
5	1,78730	1,33690	41,32200	45,60900	0,98106	0,00017	0,99975	0,00535	0,00019
6	1,78650	1,33660	41,32400	45,61100	0,98106	0,00017	0,99975	0,00132	0,01306
7	1,05140	1,02540	43,62700	47,91300	0,98646	0,00014	0,99985	0,00152	0,01220
8	1,04870	1,02410	43,63800	47,92400	0,98647	0,00014	0,99985	0,00119	0,01329
9	1,05000	1,02470	43,63200	47,91900	0,98647	0,00014	0,99985	0,00151	0,02210
10	0,74875	0,86530	45,10100	49,38700	0,98905	0,00013	0,99989	0,00086	0,02776
11	0,74943	0,86570	45,09700	49,38300	0,98904	0,00013	0,99989	0,00113	0,01874
12	0,74947	0,86572	45,09700	49,38300	0,98904	0,00012	0,99989	0,00370	0,00707
Srednja vrednost za obavljeni stego-proces preko celog nosioca				40,01188	0,95773	0,00203	0,99713	0,43848	0,34704
Srednja vrednost za obavljeni stego-proces u stego-oblastima				46,21982	0,97718	0,00111	0,99910	0,25052	0,81230
Ukupna srednja vrednost				46,21767	0,98120	0,00018	0,99973	0,00506	0,01277

Tabela 2 – tabela 5 predstavljaju puni dataset za obrađeni nosilac „Music08.jpg“ tipom 1 načina obrade. Veza između navedenih tabela je njihova prva kolona „Redni broj“. Tabela 1 prikazuje način obrade nosilaca, broj dominantnih boja koji biramo za svaki od testova kao i broj *K* bita koje menjamo u svakom testu. Takođe, tabela 1 prikazuje opšte informacije o broju piksela na koji vršimo uticaj kao i kapacitetu nosioca za odgovarajuću primenjenu steganografsku metodu. Tabela 2 predstavlja rezultate procene kvaliteta i stego-analize stego-objekata za primenjenu *LSB* metodu. Tabela 3 predstavlja rezultate procene kvaliteta procene kvaliteta i stego-analize stego-objekata za primenjenu *MDD* metodu. Tabela 4 predstavlja rezultate procene kvaliteta procene kvaliteta i stego-analize stego-objekata za primenjenu *PVD* metodu.

Tabela 6. Rezultati obrade stego-objekata generisanih pomoću nosioca Music08.jpg za tip2 vrstu obrade, ¼ skupa dobijenih rezultata

R. Br.	Koef. Filt.	Broj piksela u klasterima	Broj piksela u šarenim oblastima	K	L	Veličina poruke LSB MDD	Veličina poruke PVD	Procenat iskorišćenja LSB/MDD	bpp LSB MDD	Procenat iskorišćenja PVD	bpp PVD
1	2	463646	239746	2	3	617448	396507	9,92550	2,3821	6,37390	1,5297
2	2	463646	239746	2	4	707353	396507	11,37100	2,7290	6,37390	1,5297
3	2	463646	239746	3	2	701411	396507	11,27500	2,7061	6,37390	1,5297
4	2	463646	239746	3	3	791316	396507	12,72000	3,0529	6,37390	1,5297
5	2	463646	239746	3	4	881220	396507	14,16600	3,3998	6,37390	1,5297
6	2	463646	239746	4	2	875278	396507	14,07000	3,3768	6,37390	1,5297
7	2	463646	239746	4	3	965183	396507	15,51500	3,7237	6,37390	1,5297
8	3	456884	241492	2	3	614341	395031	9,87560	2,3701	6,35020	1,5240
9	3	456884	241492	2	4	704901	395031	11,33100	2,7195	6,35020	1,5240
10	3	456884	241492	3	2	695113	395031	11,17400	2,6818	6,35020	1,5240
11	3	456884	241492	3	3	785673	395031	12,63000	3,0311	6,35020	1,5240
12	3	456884	241492	3	4	876232	395031	14,08600	3,3805	6,35020	1,5240
13	3	456884	241492	4	2	866445	395031	13,92800	3,3428	6,35020	1,5240
14	3	456884	241492	4	3	957004	395031	15,38400	3,6921	6,35020	1,5240
15	4	384668	259760	2	3	580731	363081	9,33530	2,2405	5,83660	1,4008
16	4	384668	259760	2	4	678141	363081	10,90100	2,6163	5,83660	1,4008
17	4	384668	259760	3	2	627571	363081	10,08800	2,4212	5,83660	1,4008
18	4	384668	259760	3	3	724981	363081	11,65400	2,7970	5,83660	1,4008
19	4	384668	259760	3	4	822391	363081	13,22000	3,1728	5,83660	1,4008
20	4	384668	259760	4	2	771822	363081	12,40700	2,9777	5,83660	1,4008
21	4	384668	259760	4	3	869232	363081	13,97300	3,3535	5,83660	1,4008
Sr. Vrednosti		435066	246999					12,33473	2,9603	6,18690	1,4848

Tabela 7. Rezultati obrade stego-objekata generisanih pomoću nosioca Music08.jpg za tip2 vrstu obrade, 2/4 skupa dobijenih rezultata

Redni broj	LSB MSE	LSB RMSE	LSB SNR	LSB PSNR	LSB SSIM	LSB GMSD	LSB Q	LSB Prs	LSB Pd
1	1,76680	1,32920	41,37200	45,65900	0,97901	0,00723	0,99975	0,39021	1,13480
2	5,45300	2,33520	36,47800	40,76400	0,95615	0,02803	0,99923	0,36404	1,05770
3	2,67500	1,63550	39,57100	43,85800	0,97259	0,01157	0,99963	0,34480	1,00100
4	3,60070	1,89750	38,28000	42,56700	0,96239	0,01322	0,99950	0,31928	0,92573
5	7,29400	2,70070	35,21500	39,50100	0,93946	0,02979	0,99898	0,28018	0,81046
6	11,34800	3,36870	33,29500	37,58100	0,92893	0,03963	0,99842	0,28337	0,81987
7	12,28700	3,50540	32,95000	37,23600	0,91865	0,03995	0,99829	0,24764	0,71454
8	1,76140	1,32720	41,38600	45,67200	0,98240	0,00710	0,99975	0,38468	1,12660
9	5,37380	2,31810	36,54100	40,82800	0,96301	0,02273	0,99925	0,36895	1,07990
10	2,64390	1,62600	39,62200	43,90800	0,97204	0,01196	0,99963	0,32523	0,95004
11	3,56950	1,88930	38,31800	42,60500	0,96458	0,01349	0,99950	0,30414	0,88744
12	7,19830	2,68300	35,27200	39,55900	0,94511	0,02518	0,99899	0,28290	0,82435
13	11,20000	3,34670	33,35200	37,63800	0,92772	0,04134	0,99844	0,25178	0,73197
14	12,14200	3,48450	33,00100	37,28800	0,92025	0,04159	0,99831	0,22503	0,65255
15	1,77300	1,33150	41,35700	45,64400	0,97895	0,00734	0,99975	0,37854	1,20110
16	5,77700	2,40350	36,22700	40,51400	0,95462	0,02885	0,99919	0,35406	1,12240
17	2,29760	1,51580	40,23100	44,51800	0,97531	0,01161	0,99968	0,33339	1,05580
18	3,30570	1,81820	38,65200	42,93800	0,96446	0,01337	0,99954	0,30092	0,95137
19	7,30280	2,70240	35,20900	39,49600	0,94013	0,03057	0,99898	0,26874	0,84780
20	9,78760	3,12850	33,93700	38,22400	0,93792	0,03903	0,99864	0,27371	0,86379
21	10,78200	3,28350	33,51700	37,80400	0,92714	0,03935	0,99850	0,23413	0,73643
Srednja vrednost				41,13343	0,95290	0,02395	0,99914	0,31027	0,92836

Tabela 8. Rezultati obrade stego-objekata generisanih pomoću nosioca Music08.jpg za tip2 vrstu obrade, 3/4 skupa dobijenih rezultata

Redni broj	MDD MSE	MDD RMSE	MDD SNR	MDD PSNR	MDD SSIM	MDD GMSD	MDD Q	MDD Prs	MDD Pd
1	0,97174	0,98577	43,96900	48,25500	0,98815	0,00250	0,99987	0,01025	0,01472
2	2,82150	1,67970	39,33900	43,62600	0,96966	0,00902	0,99961	0,00734	0,00615
3	1,40380	1,18480	42,37100	46,65800	0,98241	0,00390	0,99981	0,00054	0,01391
4	1,86750	1,36660	41,13100	45,41800	0,97650	0,00441	0,99974	0,00055	0,01388
5	3,71970	1,92860	38,13900	42,42600	0,95797	0,00951	0,99948	0,00619	0,00276
6	4,99080	2,23400	36,86200	41,14900	0,94644	0,01574	0,99930	0,00047	0,01690
7	5,45230	2,33500	36,47800	40,76500	0,94055	0,01593	0,99924	0,00470	0,02936
8	0,97269	0,98625	43,96400	48,25100	0,99003	0,00217	0,99987	0,00663	0,00406
9	2,88630	1,69890	39,24100	43,52700	0,97595	0,00760	0,99960	0,00920	0,01170
10	1,38700	1,17770	42,42300	46,71000	0,98196	0,00398	0,99981	0,00467	0,00175
11	1,85370	1,36150	41,16400	45,45100	0,97765	0,00436	0,99974	0,00142	0,01141
12	3,76410	1,94010	38,08800	42,37400	0,96358	0,00826	0,99947	0,00110	0,01234
13	4,91950	2,21800	36,92500	41,21200	0,94398	0,01612	0,99931	0,00271	0,00758
14	5,38310	2,32020	36,53400	40,82000	0,93969	0,01624	0,99925	0,00132	0,01168
15	0,96740	0,98357	43,98800	48,27500	0,98808	0,00253	0,99987	0,01262	0,02367
16	2,96890	1,72310	39,11800	43,40500	0,96857	0,00903	0,99958	0,01045	0,01671
17	1,20800	1,09910	43,02300	47,31000	0,98378	0,00378	0,99983	0,01084	0,01795
18	1,71080	1,30800	41,51200	45,79900	0,97755	0,00435	0,99976	0,00454	0,00233
19	3,71380	1,92710	38,14600	42,43300	0,95802	0,00974	0,99948	0,00358	0,00540
20	4,17390	2,04300	37,63900	41,92500	0,95168	0,01536	0,99942	0,00031	0,01593
21	4,67320	2,16180	37,14800	41,43500	0,94548	0,01557	0,99935	0,00444	0,00264
Srednja vrednost				44,15352	0,96703	0,00858	0,99959	0,00495	0,01156

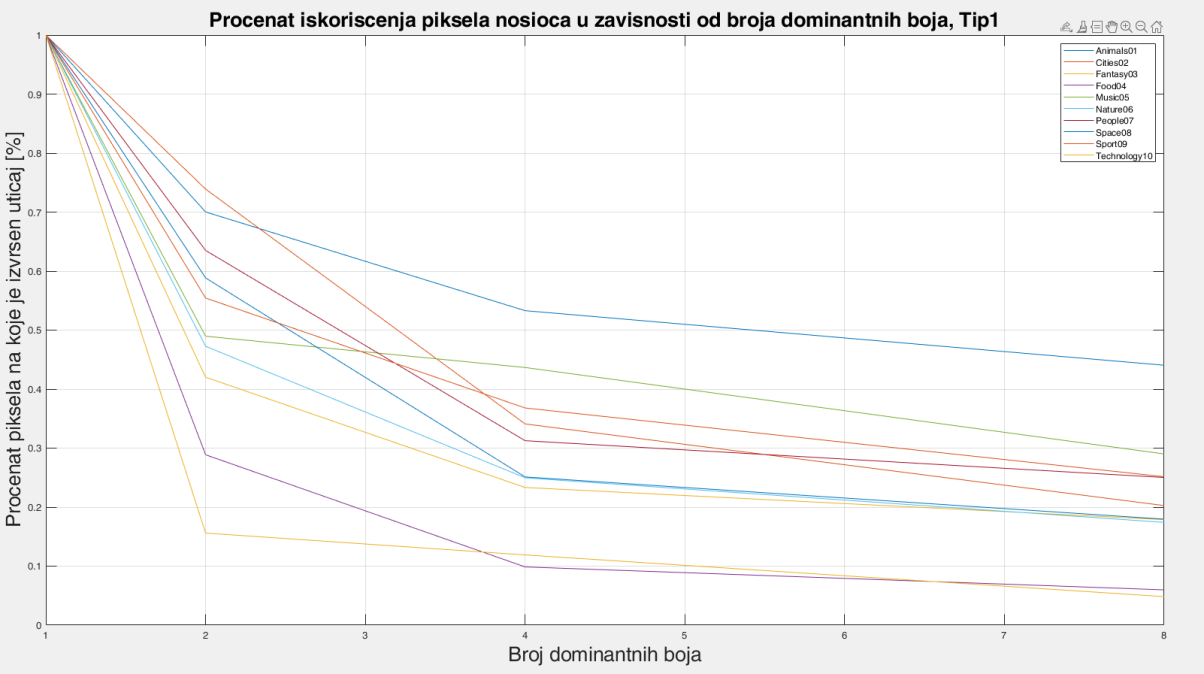
Tabela 9. Rezultati obrade stego-objekata generisanih pomoću nosioca Music08.jpg za tip2 vrstu obrade, 4/4 skupa dobijenih rezultata

Redni broj	PVD MSE	PVD RMSE	PVD SNR	PVD PSNR	PVD SSIM	PVD GMSD	PVD Q	PVD Prs	PVD Pd
1	1,08710	1,04270	43,48100	47,76800	0,98522	0,00015	0,99985	0,00172	0,01042
2	1,08770	1,04290	43,47900	47,76600	0,98521	0,00015	0,99985	0,00258	0,00791
3	1,08620	1,04220	43,48500	47,77200	0,98525	0,00015	0,99985	0,00472	0,00160
4	1,08840	1,04320	43,47600	47,76300	0,98522	0,00015	0,99985	0,00073	0,01334
5	1,08760	1,04290	43,47900	47,76600	0,98521	0,00015	0,99985	0,00203	0,00953
6	1,08890	1,04350	43,47400	47,76100	0,98521	0,00015	0,99985	0,00145	0,01124
7	1,09040	1,04420	43,46800	47,75500	0,98518	0,00015	0,99985	0,00249	0,02283
8	1,13840	1,06700	43,28100	47,56800	0,98552	0,00015	0,99984	0,00206	0,00949
9	1,13850	1,06700	43,28100	47,56800	0,98552	0,00015	0,99984	0,00191	0,00995
10	1,13480	1,06530	43,29500	47,58200	0,98554	0,00016	0,99984	0,00097	0,01850
11	1,13910	1,06730	43,27800	47,56500	0,98551	0,00015	0,99984	0,00304	0,00658
12	1,13510	1,06540	43,29400	47,58000	0,98553	0,00015	0,99984	0,00634	0,00321
13	1,13580	1,06570	43,29100	47,57800	0,98552	0,00015	0,99984	0,00261	0,00787
14	1,13780	1,06670	43,28300	47,57000	0,98550	0,00015	0,99984	0,00211	0,00934
15	1,00750	1,00370	43,81200	48,09800	0,98574	0,00014	0,99986	0,00168	0,02232
16	1,00600	1,00300	43,81800	48,10500	0,98576	0,00014	0,99986	0,00043	0,01555
17	1,00710	1,00360	43,81300	48,10000	0,98575	0,00014	0,99986	0,00431	0,00306
18	1,00530	1,00260	43,82100	48,10800	0,98577	0,00014	0,99986	0,00195	0,02319
19	1,00730	1,00360	43,81300	48,09900	0,98573	0,00014	0,99986	0,00155	0,01195
20	1,00630	1,00320	43,81700	48,10300	0,98576	0,00014	0,99986	0,00156	0,01192
21	1,00460	1,00230	43,82400	48,11100	0,98578	0,00014	0,99986	0,00068	0,01473
Srednja vrednost				47,81362	0,98550	0,00015	0,99985	0,00223	0,01164

Tabela 6 – tabela 9 predstavljaju puni dataset za obrađeni nosilac „Music08.jpg“ načinom obrade tipa 2. Veza između navedenih tabela je njihova prva kolona „Redni broj“. Tabela 5 prikazuje način obrade nosilaca, koeficijent filtriranja koji biramo za svaki od testova kao i brojeve *K* i *L* bita koje menjamo u svakom testu. Takođe, tabela 5 prikazuje opšte informacije o broju piksela na koji vršimo uticaj kao i kapacitetu nosioca za odgovarajuću primenjenu steganografsku metodu. Tabela 6 predstavlja rezultate procene kvaliteta i stego-analize stego-objekata za primenjenu *LSB* metodu. Tabela 7 predstavlja rezultate procene kvaliteta procene kvaliteta i stego-analize stego-objekata za primenjenu *MDD* metodu. Tabela 8 predstavlja rezultate procene kvaliteta procene kvaliteta i stego-analize stego-objekata za primenjenu *PVD* metodu.

5.1. Analiza kapaciteta i kvaliteta nosilaca i generisanih stego-objekata

Za tabele koje se odnose na tip obrade 1, konkretno - tabela 2, jasno se uočava da procenat piksela na koje vršimo uticaj opada sa povećanjem broja dominantnih boja. Takav efekat prikazan je na slici 15 gde je prikazan grafikon zavisnosti procenta piksela na koje vršimo uticaj u odnosu na broj odabrani dominantnih boja, kao ulazni parametar predloženog algoritma. Takođe, na slici 15 vidimo da je dinamika opadanja procenta pogođenih piksela različita za različite nosioce. Razlog za to je upravo posledica vizuelnih efekata nosilaca u kontekstu količine različitih boja, veličina oblasti u istim ili sličnim nijansama, oblika i detalja koji se pojavljuju na svakom od nosilaca. Za nosioce sa izraženim detaljima, sitnim oblastima različitih boja ovaj procenat će brže opadati sa porastom broja dominantnih boja, dok kod nosilaca sa velikim oblastima u istim ili sličnim nijansama, procenat piksela na koje je izvršen uticaj će sporije opadati sa porastom broja dominantnih boja.



Slika 15. Procenat piksela nosioca u stego-oblastima u zavisnosti od načina klasterizacije za tip 1 vrstu obrade

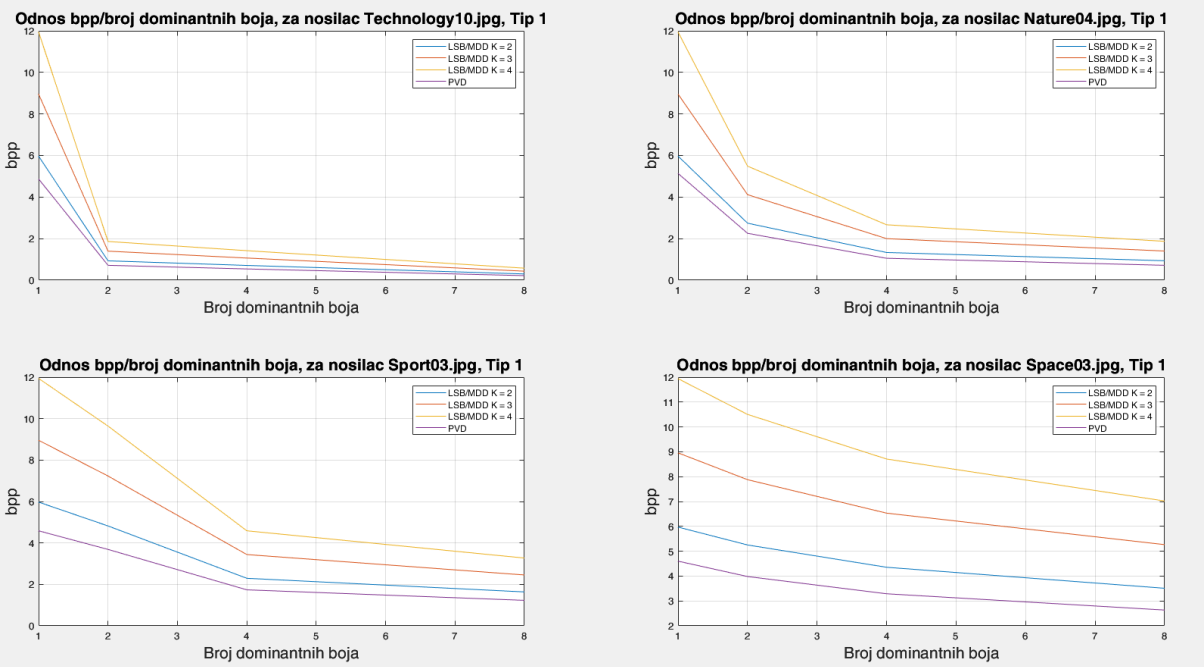
Tabela 10. Srednja vrednost procenta piksela na koje utičemo u zavisnosti od ulaznih parametara algoritma na uzorku od 100 nosilaca

Tip Obrade	**Tip 1, DC=2**	**Tip 1, DC=4**	**Tip 1, DC=8**	**Tip 2, FC=2**	**Tip 2, FC=3**	**Tip 2, FC=4**
[%]	53,16	35,06	24,59	36,0	34,65	34,37

Tabela 10 daje prikaz srednjih vrednosti procenata piksela na koje vršimo uticaj primenom predloženog algoritma uz prikazani način promene parametara, bez obzira na kasnije primenjenu steganografsku metodu.

Da bi imali kompletan uvid u ponašanje kapaciteta steganografskih nosilaca potrebno je analizu procenta piksela na koje vršimo uticaj kombinovati i sa podacima o primenjenoj steganografskoj metodi. Slika 16 daje prikaz ponašanja kapaciteta nosilaca (izraženih pomoću uobičajene vrednosti *bpp – Bits Per Pixel*) u zavisnosti broja odabranih dominantnih boja i primenjenog steganografskog algoritma. Zajedničko za sva četiri predložena nosioca je taj da kapaciteti generalno opadaju sa padom broja *K* za primenjenu *LSB*/*MDD* metodu, dok je

ubedljivo najmanji kapacitet za *PVD* metodu steganografije. Ova pojava je već diskutovana u opisima pojedinačnih steganografskih metoda tako da je u ovoj analizi fokus na diskusiji različite brzine opadanja parametra *bpp* kao i različitih oblika familija karakteristika na svakom od četiri grafika sa slike 16. Malo međusobno rastojanje familije grafika za nosilac Technology01.jpg, nagli pad vrednosti *bpp* od vrednosti *DC*=1 do vrednosti *DC*=2 ukazuje da se radi o nosiocu sa velikim brojem boja i sitnih detalja tako da već za *DC*=2 algoritam određuje vrlo mali broj piksela na koje će se dalje vršiti uticaj. Kapacitet (*bpp*) i za veće vrednosti *DC* nastavlja da opada ali znatno sporije. Za razliku od nosioca Technology01.jpg posmatrajmo grafikon za suprotan slučaj a dobar predstavnik je nosilac „Space03.jpg“. Na grafiku promene kapaciteta sa „Space03.jpg“ uočavamo mnogo veću razliku među karakteristikama iste familije što ukazuje da je u pitanju nosilac gde će algoritam predložen u ovom radu već za *DC*=2 odabrati oblasti u kojima se procentualno nalazi veliki broj piksela.



Slika 16. Vrednosti bpp u zavisnosti od broja dominantnih boja, za 4 različita nosioca, za tip 1 vrstu obrade

Kada u velikim oblastima obavljamo stego metode sa različitim vrednostima dolazi do udaljavanja karakteristika iste familije, što nije bio slučaj kod nosioca Technology01.jpg, naprotiv.

Do sada je pokazano kako parametar *DC* algoritma za odabir oblasti kao i primenjena steganografska metoda (uzimajući u obzir parametar *K*) utiču na kapacitet nosioca. Pokazano je da kapacitet, generalno, opada sa povećanjem parametra *DC* kao i sa smanjenjem koeficijenta *K*, za *LSB/MDD* metodu. Slika 17 predstavlja dva 3D diskretna grafika. Prvi grafikon na slici 16 predstavlja zavisnost parametra *bpp* od nezavisno promenljivih parametara *DC* i *K* (*DC* = 1 – zelena boja; *DC* = 2 – žuta boja; *DC* = 4 – plava boja; *DC* = 8 – crvena boja) za *MDD* metodu. Vrednosti za *bpp* se nalaze na presečnim tačkama za pomenute vrednosti *DC* kao i parametra K, po drugoj dimenziji, koji uzima vrednosti *K* = 2,3,4. Kompletan grafikon sačinjen je od ukupno 1200 tačaka (100 nosilaca, obrađenih na 12 različitih načina). Kada je u pitanju steganografski proces preko cele površine nosioca (*DC* = 1, zelena boja) imamo nagomilavanje u samo 3 tačke (*bpp*= 6, za *K* = 2; *bpp* = 9, za *K* = 3; *bpp* = 12, za *K* = 4), što je bilo potpuno očekivano, a što pokazuju i početne vrednosti grafika na slici 16 (za *DC* = 1). Kada se radi o elementima grafika žute, plave i crvene boje, uočava se da visine "stubova" rastu od zadnjeg-levog ka prednjem-desnom delu grafika. Ukoliko bi postavili zamišljenu horizontalnu ravan na odgovarajućoj visini (vrednosti *bpp*) u prikazanom opsegu, presek zamišljene ravni i odgovarajućih „stubića" grafika, dao bi nam smernice koje nosioce bi mogli da upotrebimo i sa kojim tipom obrade ukoliko bi želeli da dobijemo odgovarajući kapacitet stego-objekta.

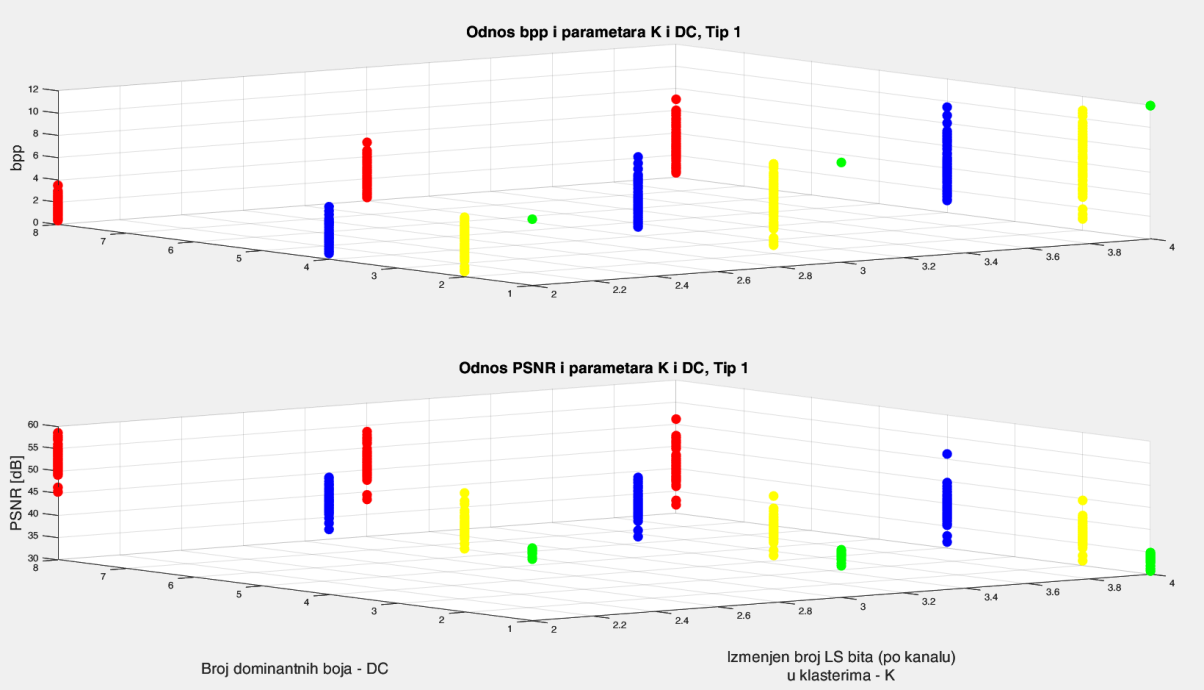
Tabela 11. Srednje vrednosti bpp za LSB/MDD metodu, za tip 1 vrstu obrade, u zavisnosti od ulaznih parametara algoritma, DC i K

	DC=2,K=2	**DC=2,K=3**	**DC=2,K=4**	**DC=4,K=2**	**DC=4,K=3**	**DC=4,K=4**	**DC=8,K=2**	**DC=8,K=3**	**DC=8,K=4**
bpp	3,19	4,78	6,38	2,13	3,18	4,24	1,64	2,27	3,01

Tabela 12. Srednje vrednosti bpp za PVD metodu za tip 1 vrstu obrade u zavisnosti od ulaznog parametra DC

	DC = 2	**DC = 4**	**DC = 8**
bpp	2,45	1,64	1,21

Tabela 11 i tabela 12 predstavljaju prikaz srednjih vrednosti parametra bpp za *LSB*/*MDD* i *PVD* metode respektivno, za različite vrednosti ulaznih parametara algoritma obrade *DC* i, kada je u pitanju *LSB*/*MDD* metoda, parametra *K*. Rezultati su dobijeni obradom pomenutog ulaznog skupa od 100 različitih nosilaca. Važno je uočiti način promene parametra *bpp*, kao i njegove apsolutne vrednosti za različite metode, za različitu kombinaciju ulaznih parametara. Efekat opadanja srednje vrednosti parametra *bpp* sa porastom vrednosti parametra *DC*, kao i odnos apsolutnih vrednosti parametra za različite steganografske metode mogao se naslutiti i na osnovu ponašanja karakteristika prikazanih na slici 16, za predstavljene konkretne nosioce, u tom slučaju.



Slika 17. Vrednosti bpp i PSNR u zavisnosti od parametara algoritma K i broja dominantnih boja, za tip 1 vrstu obrade

Ukoliko bi u analizu uključili i jednu od tipičnih metrika za procene kvaliteta slike (opisane u poglavlju 1.5) *PSNR* (izraženom u dB), dobijamo donji grafikon slike 17 za tip 1 vrstu obrade, *MDD* metodu. Kako su parametri *bpp* i *PSNR* očekivano u opoziciji, na ovom grafiku vidimo da vrednosti *PSNR* opadaju gledano iz zadnjeg-levog ugla (*DC* = 8, *K* = 2) ka prednjem-desnom uglu grafika (*DC* = 1, *K* = 4). Ovim smo, takođe, pokazali da je moguće postaviti horizontalnu ravan za željenu *PSNR* vrednost a da će preseci segmenta grafika za zamišljenom ravni dati odgovor koje nosioce koristi i za odgovarajući tip obrade. Potrebno je naglasiti da su grafici spojeni u sliku 17 u cilju prikazivanja efekta obrnute proporcionalnosti parametara *PSNR* i *bpp*.

Ukoliko bi na identičan način kreirali grafike za *LSB* metodu, prvi grafikon sa slike 17 bi bio potpuno identičan dok bi drugi grafikon sa slike 17 bio identičnog oblika, spušten za apsolutni nivo od 3-5dB. Sa druge strane, ovakav 3D grafikon ne bi imalo smisla kreirati za *PVD* metodu jer u tom slučaju ne postoji parametar *K* tako da bi se broj zavisno promenljivih sveo na jednu što bi rezultovalo 2D grafiku. Na takvom 2D grafiku (gde bi *DC* bila nezavisno promenljiva) imali bi znatno niže vrednosti za *bpp* (tabela 2) i za prosečno 2dB više vrednosti za *PSNR* (tabela 4 i tabela 5).

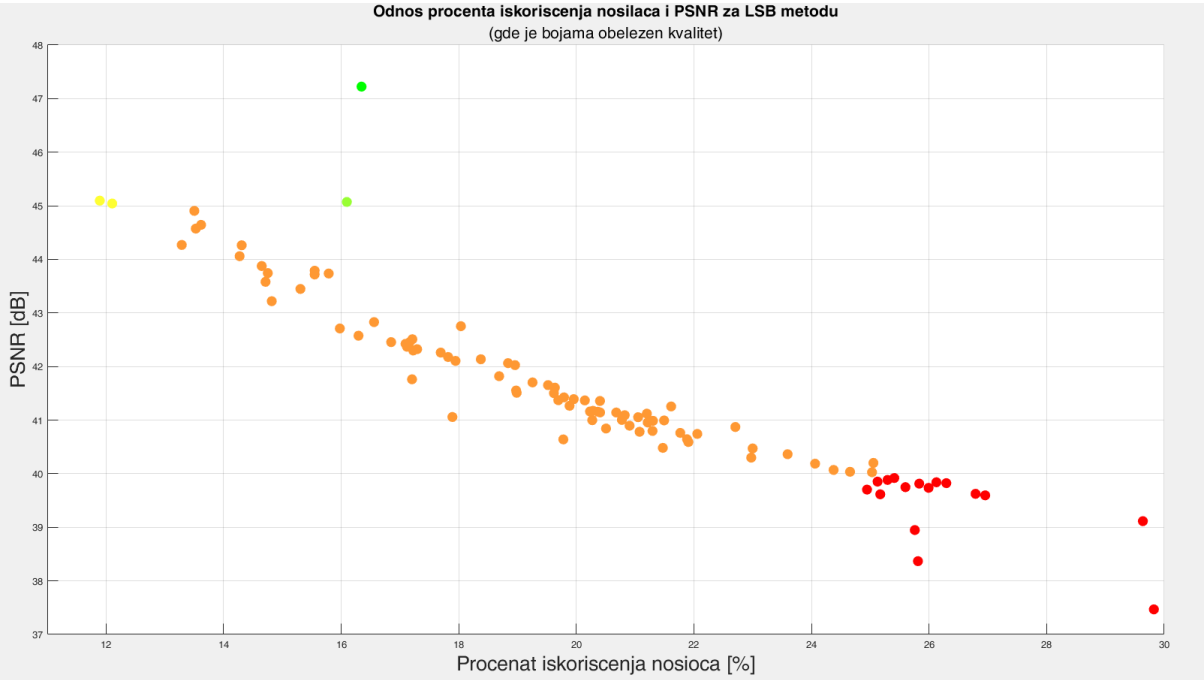
Radovi [63] i [23] bave se procenom kvaliteta slike u zavisnosti od vrednosti njihovih metrika. Na osnovu zaključaka i smernica izloženim u navedenim radovima, a u skladu sa metrikama opisanim u poglavlju 1.5, definisane su odgovarajuće zone kvaliteta predstavljene u tabeli 13. Poslednje dve kolone tabele se odnose na veličinu parametara stego-analize P_{rs} i P_d opisanim u poglavlju 2.6.1. Odabrane granične vrednosti za P_{rs} i P_d su 0,15 i to je posledica izračunate srednje vrednosti parametra P_{ib} (na radnom uzorku od 100 slučajno odabranih nosilaca) koja upravo toliko iznosi. U daljoj analizi svi stego-objekti kojima su vrednosti P_{rs} i P_d ispod granice

0,15 smatraće se takvim da stego-analiza nije otkrila izmene i postojanje tajnog sadržaja u njima.

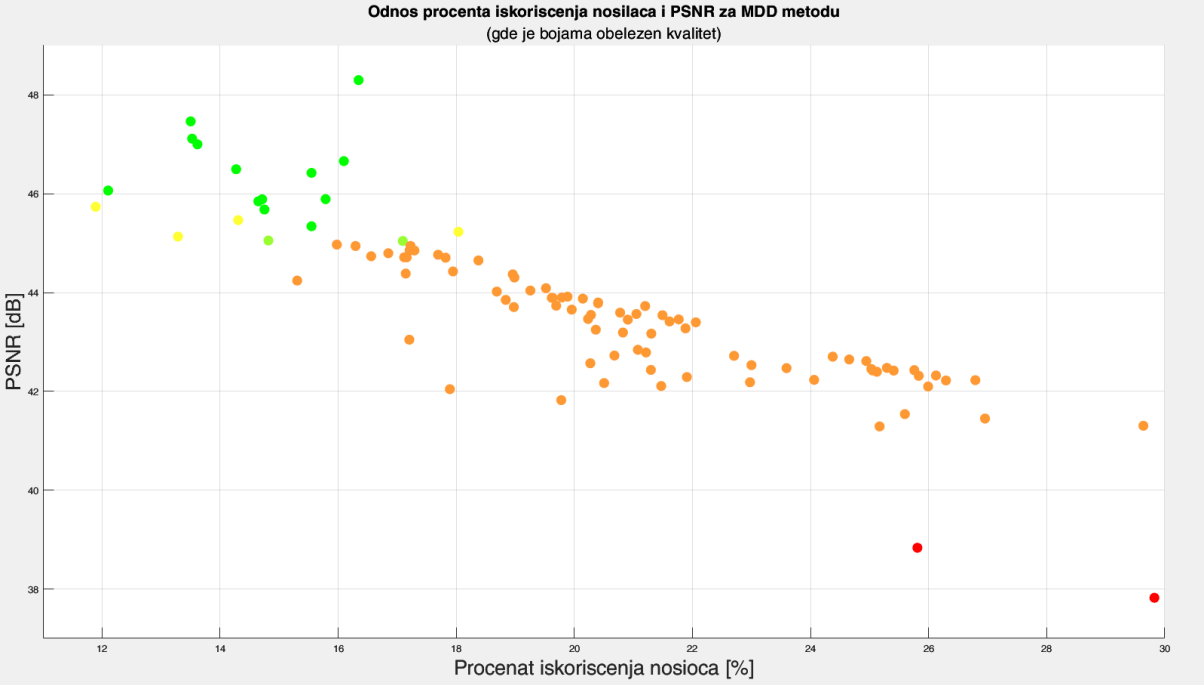
Tabela 13. Zone kvaliteta stego-objekata u zavisnosti od vrednosti metrika kvaliteta

Metrika	PSNR[dB]	SSIM	GMSD	Q	P_{rs}	P_d	Boja na grafiku
Odličan	> 45	> 0,95	< 0,008	> 0,999	< 0,15	< 0,15	●
Vrlo dobar	> 45	> 0,95	>= 0,008	<= 0,999	< 0,15	< 0,15	●
Dobar	> 45	< 0,95	>= 0,008	<= 0,999	< 0,15	< 0,15	●
Zadovoljava	> 40	< 0,95	>= 0,008	<= 0,999	< 0,15	< 0,15	●
Ne zadovoljava	< 40	< 0,95	>= 0,008	<= 0,999	< 0,15	< 0,15	●
Ne prolazi stego-analizu	/	/	/	/	> 0,15	> 0,15	●

Da bi se bolje razumelo ponašanje i performanse svakog od odabranih 100 nosilaca i njihovih derivata u formi stego-objekata, na osnovu ukupnog skupa dobijenih podataka za tip 1 vrstu obrade, izračunate u srednje vrednosti parametara za svaki od njih. Na taj način smo filtriranjem i usrednjavanjem skupa podataka za svaki od 1200 stego-objekata sveli na skup srednjih vrednosti za svaki od 100 nosilaca. Skup srednjih vrednosti parametara za svaki od nosilaca predstavljen je posebnom tabelom prikazanom u Apendix I i Apendix II. Slika 18 prikazuje ponašanje usrednjenih *PSNR* vrednosti za svaki od nosilaca u zavisnosti od srednje vrednosti procenta iskorišćenja, za *LSB* metodu (za različite ulazne vrednosti algoritma *DC* i *K*). Dobijene vrednosti prikazane na grafiku su dodatno obojene odgovarajućim bojama iz tabele 13 kako bi se u potpunosti stekao utisak o kvalitetima dobijenih stego objekata. Uočavamo da srednja vrednost *PSNR* vrednost skoro linearno opada sa porastom srednje vrednosti iskorišćenja nosioca, gde većina nosilaca je obojena narandžastom bojom i nalazi se u zoni kvaliteta - Zadovoljava.



Slika 18. Odnos srednjih vrednosti procenta iskorišćenja i srednjih vrednosti PSNR na uzorku od 100 nosilaca, za LSB metodu, za tip 1 vrstu obrade

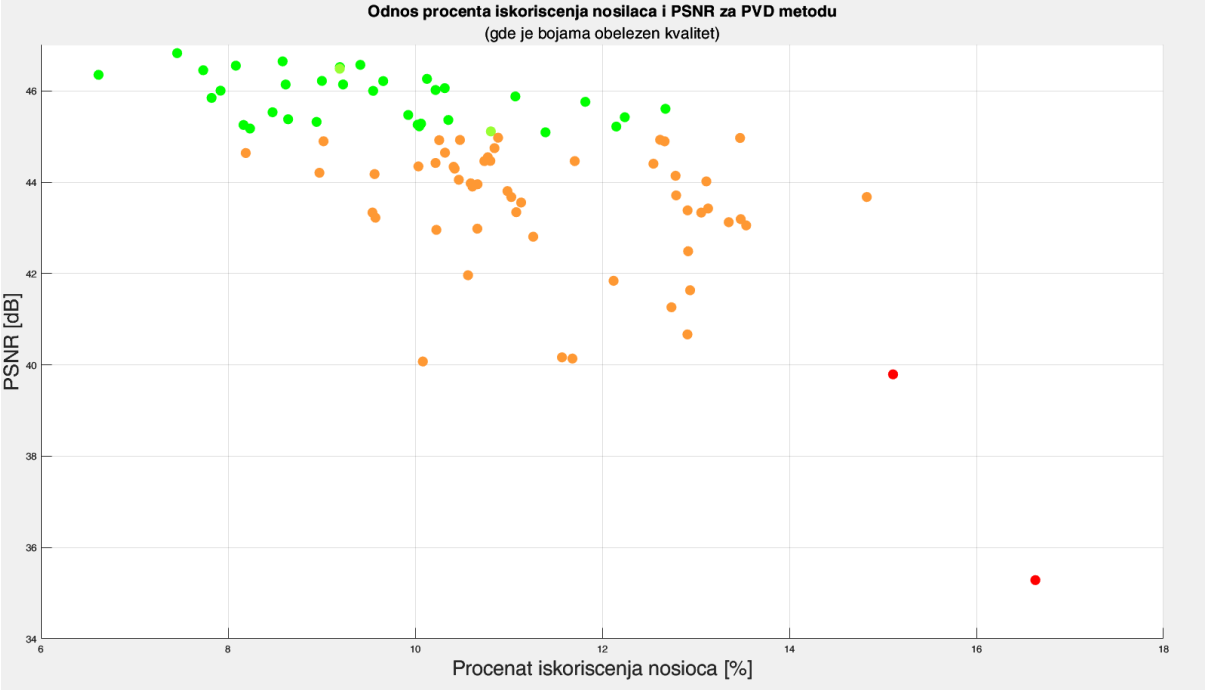


Slika 19. Odnos srednjih vrednosti procenta iskorišćenja i srednjih vrednosti PSNR na uzorku od 100 nosilaca, za MDD metodu, za tip 1 vrstu obrade

Slika 19 predstavlja pandan slici 18 za *MDD* metodu. Ono što je uočljivo je da su vrednosti po ordinati pomerene za nekoliko decibela na više kao i da je veće odstupanje od linearnosti u

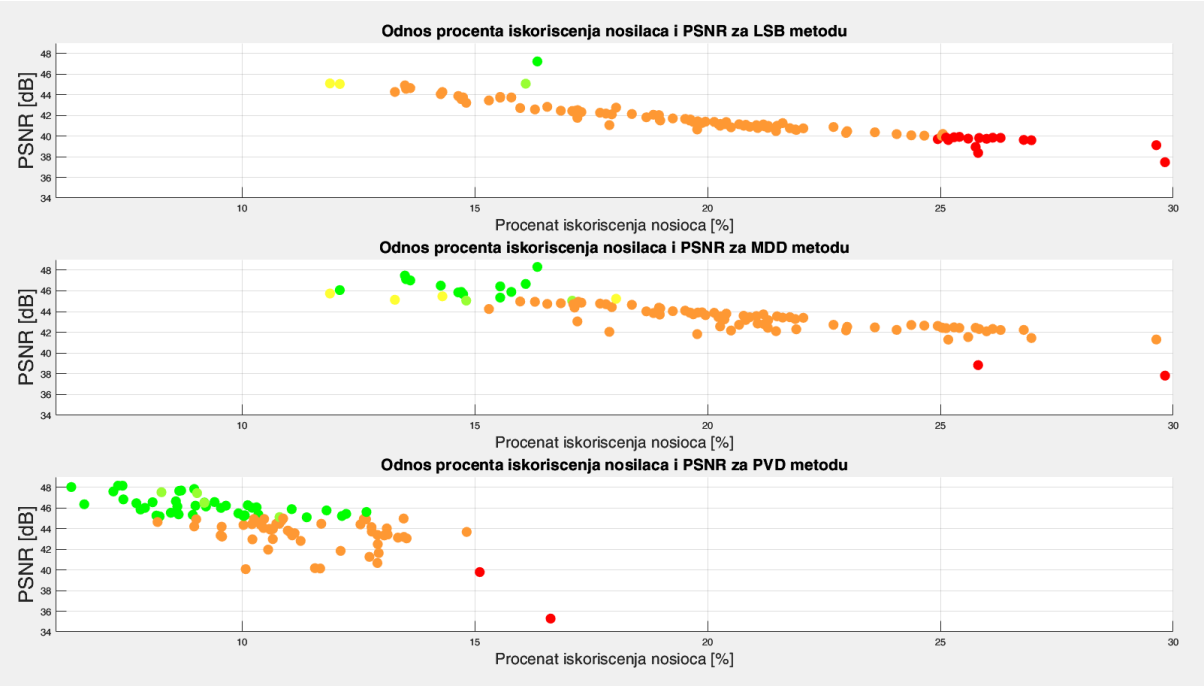
prikazanoj karakteristici. Takođe, posmatranjem boja pojedinih tačaka uočavamo veći broj nosilaca koji imaju ocene odličan i vrlo dobar u skladu sa zonama definisanim tabelom 13. Pomenuto veće odstupanje u linearnosti ukazuje mogućnost bolje manipulacije izmenama *LS* bita u jednoobraznim i šarenim oblastima što će posebno biti analizirano za tip 2 način obrade. Ovde takođe treba obratiti pažnju da je odlične i vrlo dobre ocene moguće dobiti za maksimalni kapacitet od 16-17% a svi kapaciteti veći od toga povlače sa sobom i značajniju degradaciju kvaliteta stego objekta.

Slika 20 je pandan slici 18 i slici 19 za *PVD* metodu. Uočljivo je nekoliko razlika u odnosu na grafike za *LSB* i *MDD* metodu. Još uočljivije odstupanje od linearnosti karakteristike je posledica same prirode *PVD* metode i načina na koji je ona koncipirana, gde kapaciteti nosilaca zavise od prirode njihovih piksela. Pored toga uočljivo je da su *PSNR* vrednosti pomerene za 1-2dB naviše a cena koja je za to plaćena su smanjeni kapaciteti nosilaca.



Slika 20. Odnos srednjih vrednosti procenta iskorišćenja i srednjih vrednosti PSNR na uzorku od 100 nosilaca, za PVD metodu, za tip 1 vrstu obrade

Takođe, uočljiv je i veći broj stego-objekata koji imaju odličnu ili vrlo dobru ocenu po zonama kvaliteta definisanim u tabeli 13, što je takođe posledica smanjenog kapaciteta. Da bi napravili bolje vizuelno poređenje kreirana je slika 21 gde su sva tri prethodna grafika poređani jedan ispod drugog u istim opsezima vrednosti za apscisu i ordinatu.

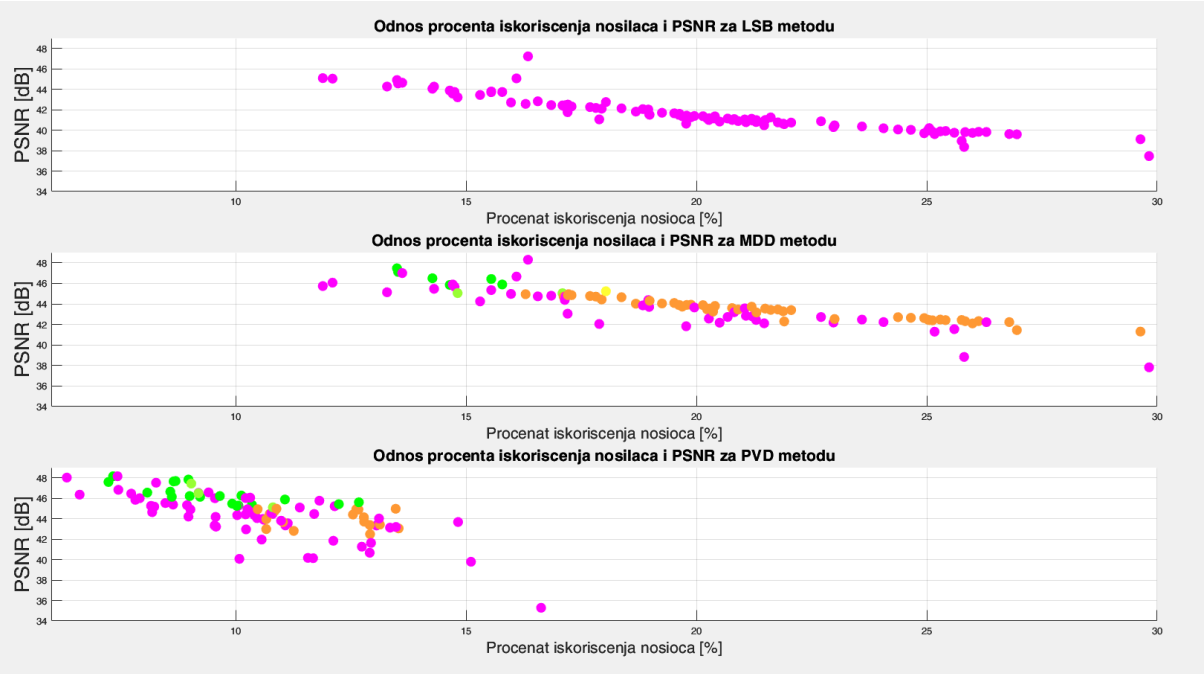


Slika 21. Komparativni odnos srednjih vrednosti procenta iskorišćenja i srednjih vrednosti PSNR na uzorku od 100 nosilaca, za LSB, MDD i PVD metodu, za tip 1 vrstu obrade

Ovakav prikaz jasno pokazuje prethodno diskutovana ponašanja stego-objekata, gde se uočava kretanje srednjih vrednosti *PSNR* u zavisnosti od srednjih vrednosti kapaciteta. Takođe, ovakav prikaz daje izvesne upute o načinu izbora nosioca, stego metode koje ćemo primeniti i željenih performansi stego-objekta.

Ukoliko sada u analizu, pored metrika za procenu kvaliteta stego-objekata, uključimo i rezultate stego-analize po kriterijumima predstavljenim u tabeli 13 dobija se slika 21. Ovi grafikoni su vrlo slični grafikonima sa slike 21 uz dodatak da su roze bojom obeleženi svi

nosioci koji ne zadovoljavaju definisani kriterijum stego-analize, bez obzira na njihovu ocenu dobijenu na osnovu metrika.

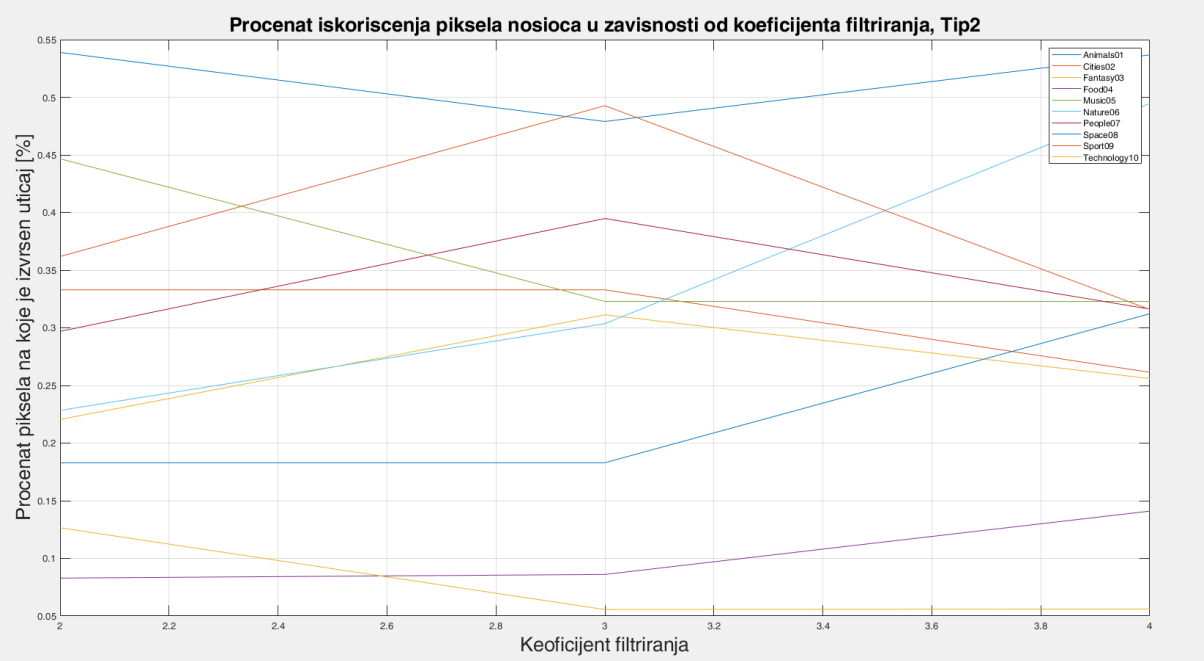


Slika 22. Komparativni odnos srednjih vrednosti procenta iskorišćenja i srednjih vrednosti PSNR, za LSB, MDD i PVD metodu, za tip 1 vrstu obrade, uz akcenat na stego-objekte koji ne zadovoljavaju uslov stego-analize

Ovde se jasno uočava koji broj kandidata "prolazi" stego-analizu, koji su kvaliteti pomenutih kandidata i koliki su srednji kapaciteti tih stego-objekata. Interesantno je da za *LSB* metodu nijedan od stego-objekata ne zadovoljava uslove stego-analize. Kod *MDD* i *PVD* metode sličan broj stego-objekata "prolazi" stego-analizu gde su pri tome kod *MDD* metode stego-objekti sa većim kapacitetima i lošijim ocenama kvaliteta u odnosu na stego-objekte dobijene *PVD* metodom. Kako se u poslednjoj analizi radi isključivo sa srednjim vrednostima procenta iskorišćenja i srednjim vrednostima metrika za procenu kvaliteta stego-objekta jasno je da je cilj procena i odabir optimalnog tipa nosioca. Slika 22 pokazuje da kandidate za takav odabir treba tražiti na grafikonu za *MDD* metodu među stego-objektima koji imaju odlične ili vrlo dobre ocene kvaliteta, sa jedne strane, a viši kapacitet od stego-objekata dobijenih *PVD*

metodom, sa druge strane. U daljoj analizi biće diskutovana pomenuta problematika i date smernice za odabir odgovarajućeg tipa nosioca u cilju dobijanja optimalnih performansi stego-objekta. Tabela sa kompletnim rezultatima na osnovu kojih su dobijeni grafikoni slika 19 – slika 22, data je u Apendix I.

Ako se sada za tip 2 obrade uradi analiza procenta piksela na koje vršimo uticaj u zavisnosti od koeficijenta filtriranja, kao što je to prethodno urađeno za tip 1 obrade dobija se grafikon prikazan na slici 23.

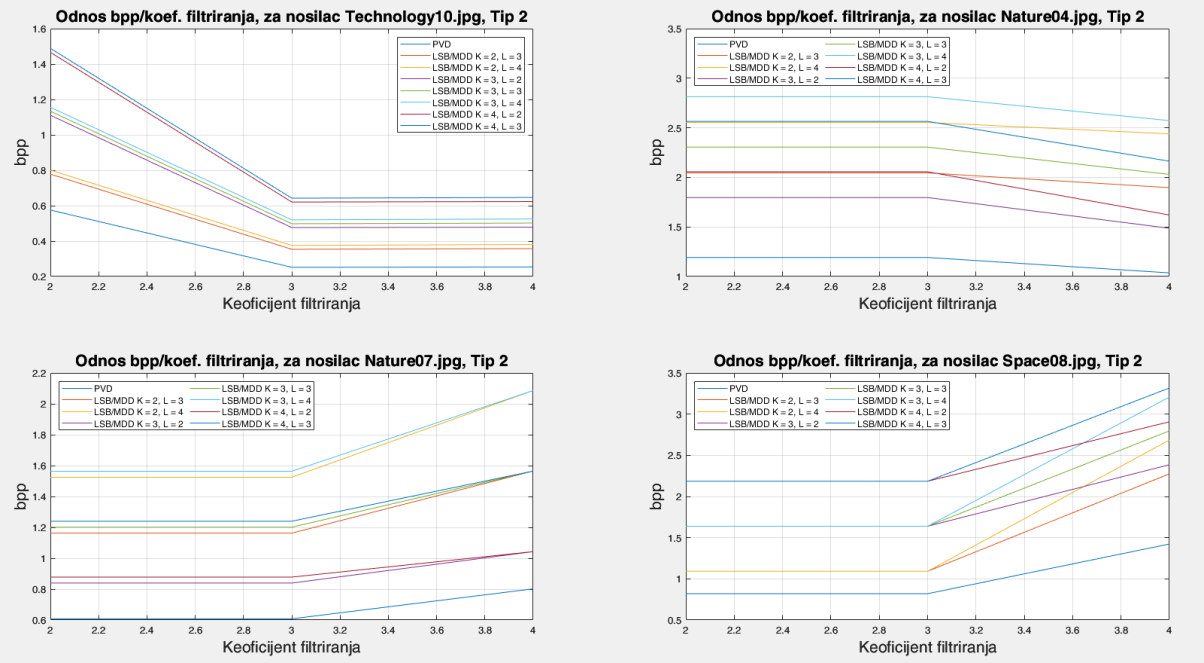


Slika 23. Procenat piksela nosioca u stego-oblastima u zavisnosti od koeficijenta filtriranja za tip 2 vrstu obrade

Slika 23 je svojevrsni pandan slici 15 (za tip 1 način obrade). Za razliku od grafikona na slici 15 gde vrednosti procenta piksela na koje vršimo uticaj uvek opadaju sa porastom vrednosti *DC*, za tip 2 način obrade to nije slučaj. Prikazano je ponašanje promene procenta piksela za 10 slučajno odabranih nosilaca (iz skupa od ukupno 100), obrađenih *MDD* i *PVD* metodama, i jasno se vidi da je moguće da karakteristika konstantno opada, konstantno raste, raste pa opada, opada pa raste ili zadržava istu vrednost u nekom segmentu grafikona. Razlog za takvo

ponašanje je upravo karakteristika tipa 2 načina obrade gde se formira *(N+1).* klaster baš kako je to objašnjeno u poglavlju 3. Promena veličine tog *(N+1).* klastera za različite vrednosti koeficijenta *FC* zapravo diktira kako će se ponašati karakteristika.

Ukoliko sada u analizu uključimo i tip primenjene steganografske metode kao i upotrebljene vrednosti parametara *K* i *L* (broj *LS* bita koje menjamo) kod *LSB* i *MDD* metode možemo posmatrati ponašanje parametra *bpp*, što daje kompletniju sliku. Slika 24 sačinjena je od četiri grafikona sa familijama karakteristika za četiri odabrana, karakteristična nosioca.

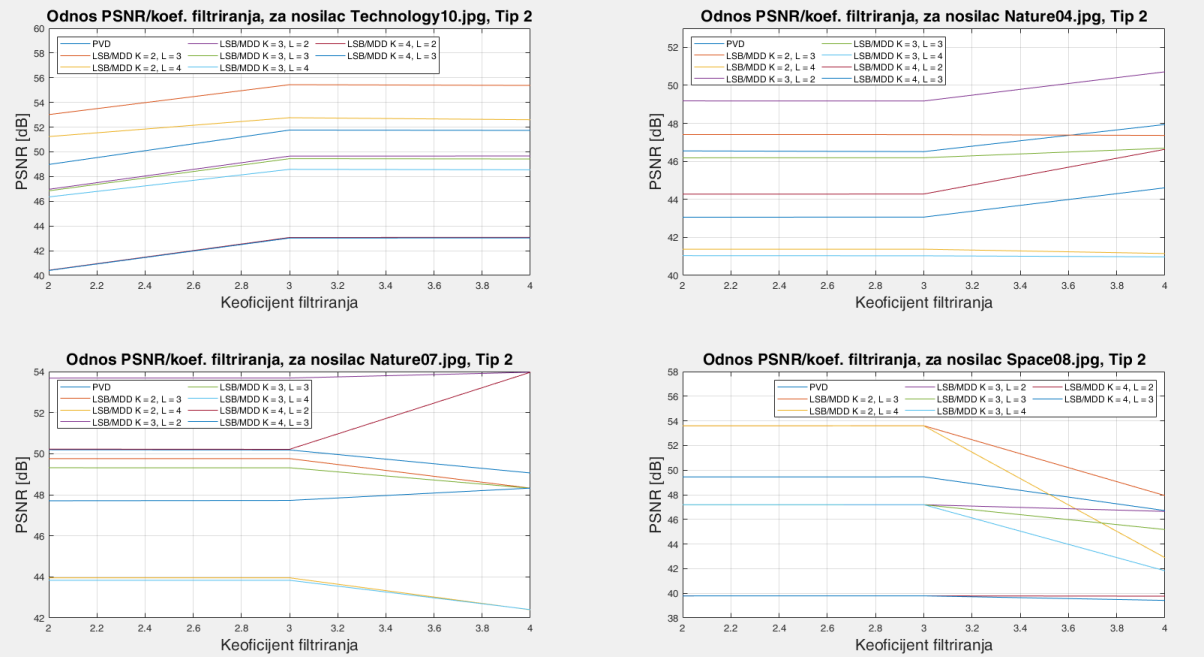


Slika 24. Vrednosti bpp u zavisnosti od koeficijenta filtriranja, za 4 različita nosioca, za tip 2 vrstu obrade

Na prvom grafikonu, za nosilac „Technology10.jpg“ uočavamo da su karakteristike ekvidistantne za različite vrednosti koeficijenta filtriranja. Takvo ponašanje implicira da je odnos piksela u dva klastera sa dominantnim bojama i u trećem klasteru („šarenih boja“) proporcionalan za različite vrednosti parametra *FC*. Tipičan primer, pogodan za diskusiju, je i četvrti grafikon sa familijom karakteristika za nosilac „Space08.jpg“. Potpuno preklapanje

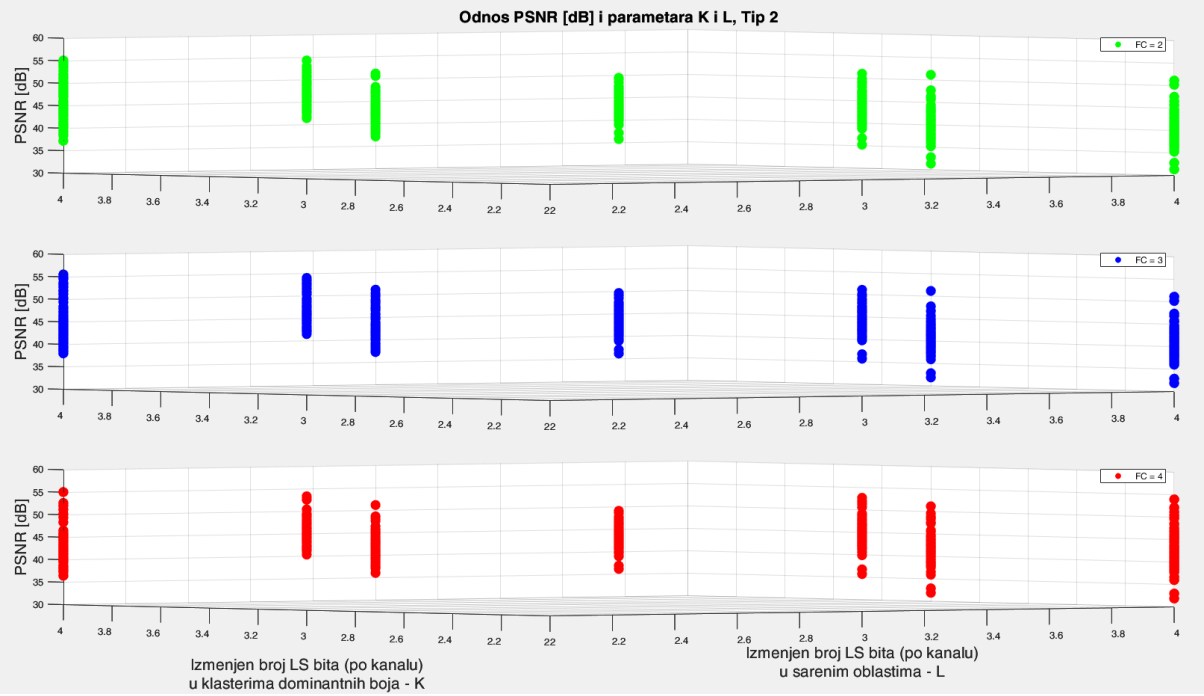
karakteristika za vrednosti *FC* od 2 do 3 govori o tome da u ovom slučaju jedan od parametara *K* ili *L* nema nikakvog uticaja na *bpp* dok onaj drugi ima potpuni uticaj (verovatniji slučaj je da parametar *L* nema uticaja). Od trenutka kada *FC* dobije vrednost 3, prethodno preklopljeni grafici se odvajaju i rastu različitim brzinama. Ovo ukazuje na povećanje ukupnog broja piksela na koje vršimo uticaj gde sada značajnu ulogu imaju i parametar *K* i parametar *L*, odnosno procenat piksela u „šarenoj“ oblasti.

Slika 25 predstavlja četiri grafikona za identične nosioce kao na slici 24 ali sada je zavisno promenljiva parametar *PSNR* (stego-objekata dobijenih *MDD* i *PVD* metodama) koji je u opoziciji sa parametrom *bpp*. Zanimljivo je uočiti da se na prvom grafiku, za nosilac „Technology10.jpg“ gubi efekat ekvidistantnosti a razlog tome je različit efekat degradacije stego-objekta u slučajevima kada se menja 2,3 ili 4 bita najmanje težine. Upravo zbog gubitka efekta ekvidistantnosti nije odgovarajuće reći da su *PSNR* i *bpp* obrnuto proporcionalni, što je kod tip 1 način obrade bilo moguće.



Slika 25. Vrednosti PSNR u zavisnosti od koeficijenta filtriranja, za 4 različita nosioca, za tip 2 vrstu obrade

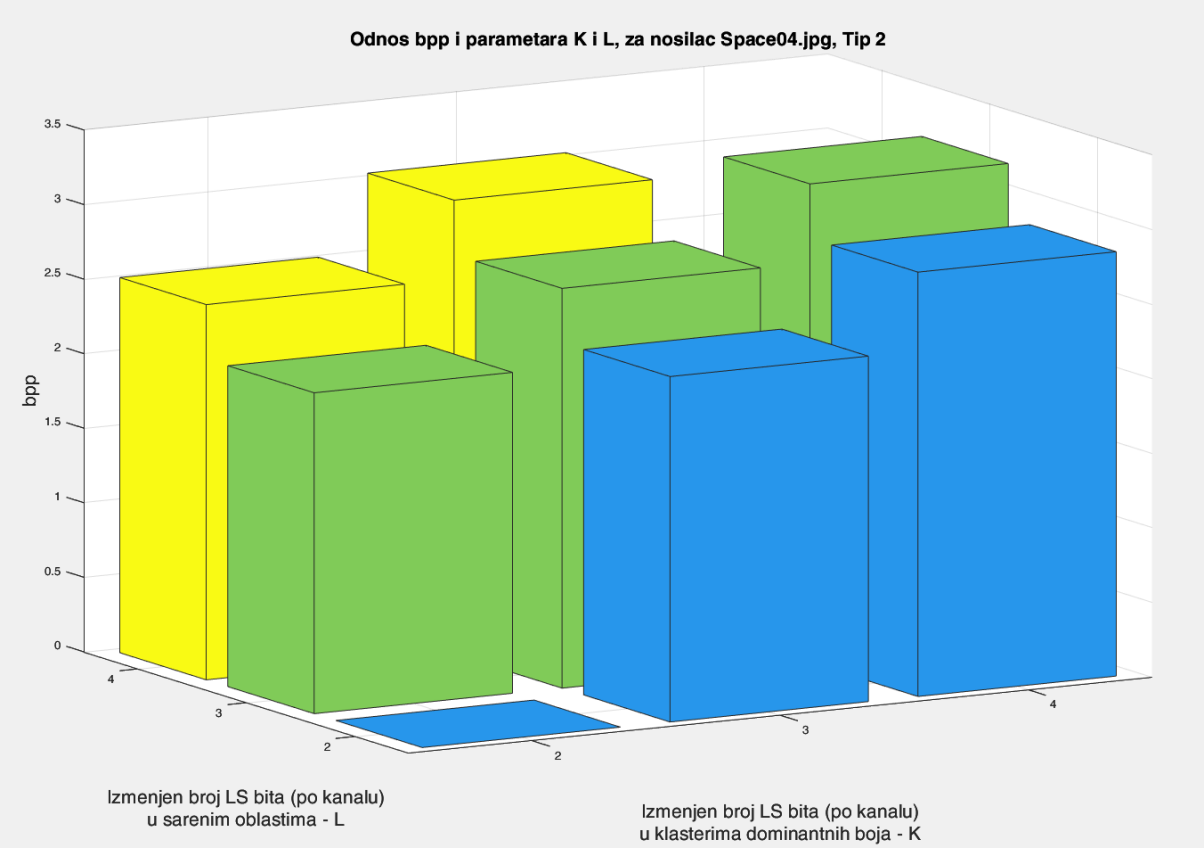
Slika 26 predstavlja tri 3D grafikona gde su na osama u horizontalnoj ravni vrednosti promenljivih *K* i *L*, odnosno broja bita najmanje težine koje menjamo u klasterima odnosno u „šarenim“ oblastima stego-nosioca. Na vertikalnoj osi, zavisno promenljiva, je jedna od metrika za ocenu kvaliteta – *PSNR*. Svaki od grafikona predstavlja vrednosti za po jedan različit koeficijent filtriranja *FC* = 2,3,4 respektivno. Kao što se može videti, svaki od grafikona sadrži tačke raspoređene u sedam vertikalnih vrednosti, za različite kombinacije *K* i *L* (2-3, 2-4, 3-2, 3-3, 3-4, 4-2, 4-3). Svaki od vertikalnih segmenata grafikona sadrži 100 vrednosti, za svaki od nosilaca, gde je ukupno generisano 2100 različitih stego-objekata. Jasno se vidi da vertikalni segmenti grafikona koji se nalaze na vrednostima gde K ili L uzimaju vrednost 4 imaju najveću visinu.



Slika 26. Srednje vrednosti PSNR u zavisnosti od koeficijenta K i L, za različite koeficijente filtriranja, za tip 2 vrstu obrade

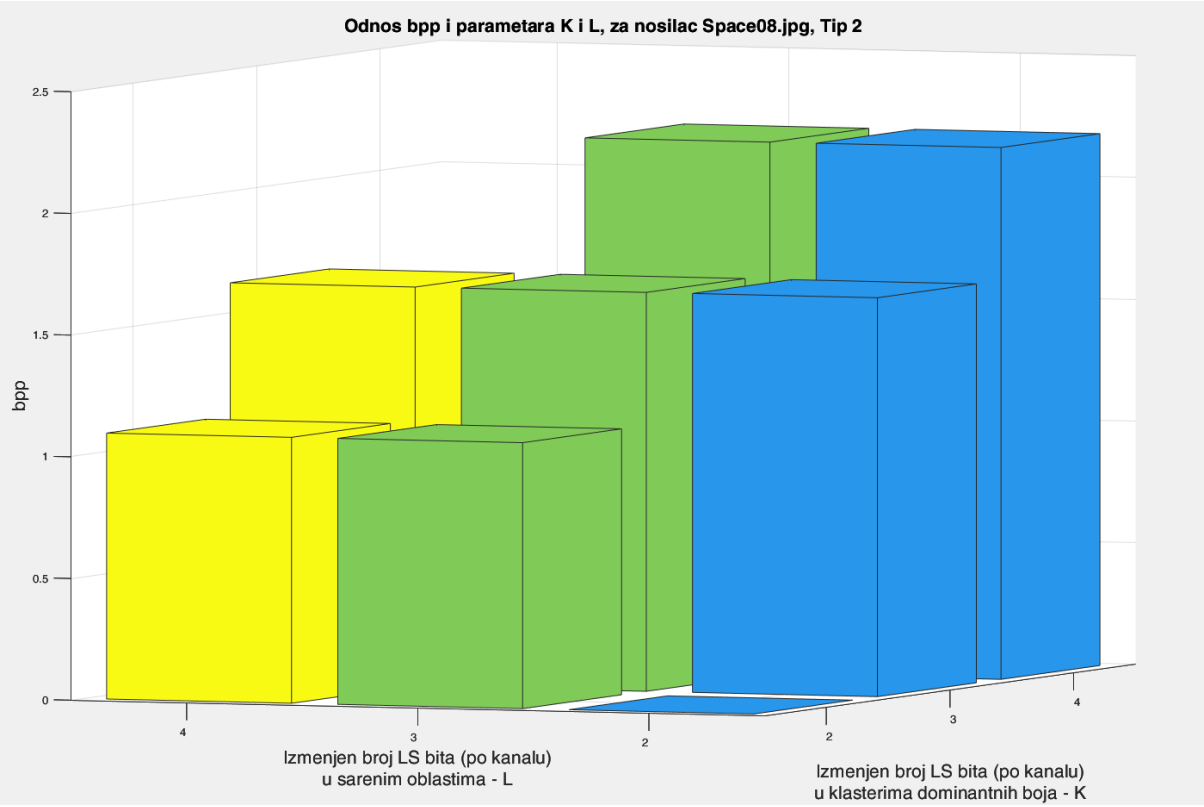
Ovo je pokazatelj da je najveća degradacija stego-objekta (najniža tačka vertikalnog segmenta grafikona) ukoliko u oblastima dominantno menjamo 4 bita najmanje težinske vrednosti ali to

ne mora biti slučaj ukoliko su nosioci takvih karakteristika da smo minimalno uticali na piksele menjajući 4 bita a dominantno uticali na piksele menjajući 2 bita (najviša tačka vertikalnog segmenta grafikona). Sa druge strane, vertikalni segmenti grafikona najmanje visine su upravo oni gde za *K* i *L* uzimamo vrednosti 2 i 3, pa tako dolazi do najmanje razlike u mogućim degradacijama stego-objekta izraženih pomoću *PSNR*. Takođe je zanimljivo uočiti da su sva tri grafikona (za tri različite vrednosti *FC*) praktično identični. Ukoliko bi testiranje bilo vršeno na većem uzorku od 100 stego-nosilaca grafici bi postali potpuno identični. To je dokaz da za dovoljno veliku populaciju uzoraka (različitih slika, različitih osobina i karakteristika) praktično nema razlike u statistici da li koristimo koeficijent filtriranja 2, 3 ili 4. Ovakav efekat je u direktnoj korelaciji sa ponašanjem grafika na slici 23.



Slika 27. Ponašanje bpp u zavisnosti od parametara K i L za nosilac Space04.jpg, za tip 2 vrstu obrade

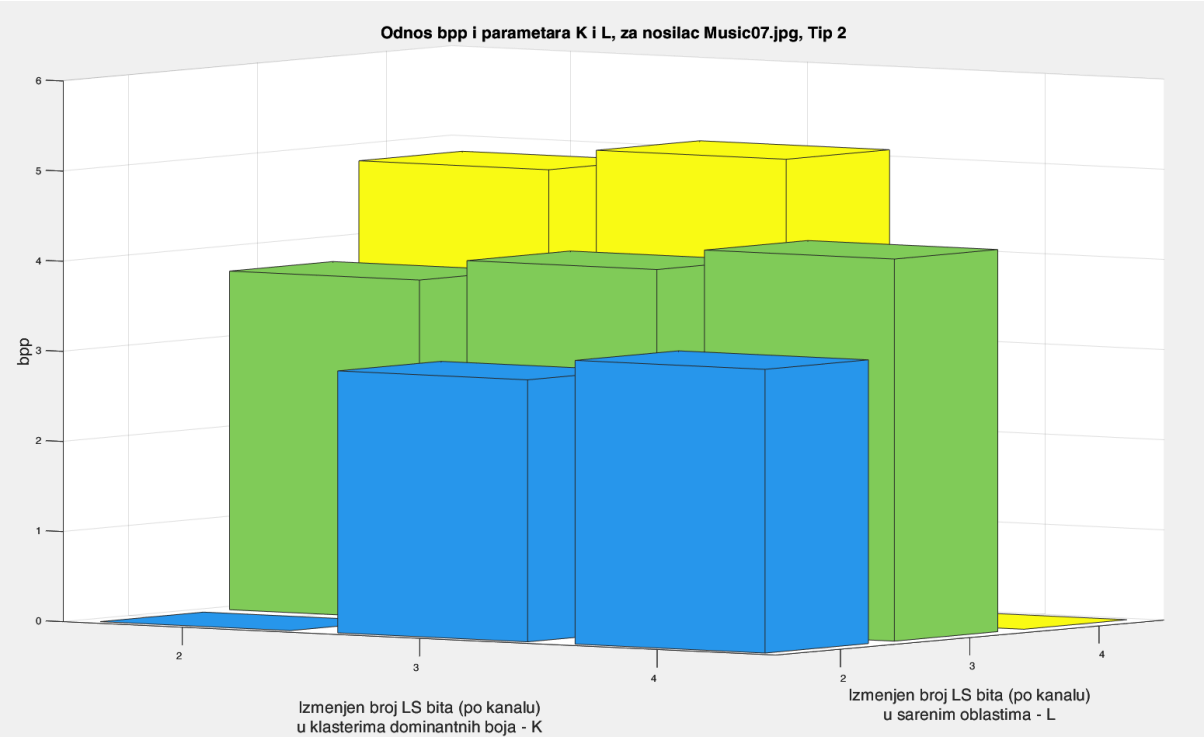
Slika 27 – slika 29 pokazuju ponašanje kapaciteta nosioca *bpp* u zavisnosti od promene parametara *K* i *L*. Na svakoj od slika prikazano je ponašanje po jednog karakterističnog stego-nosioca što će biti komentarisano u daljem tekstu.



Slika 28. Ponašanje bpp u zavisnosti od parametara K i L za nosilac Space08.jpg, za tip 2 vrstu obrade

Slika 27 pokazuje ponašanje nosioca „Space04.jpg“ za tip 2 način obrade, gde je *FC* = 2. Po vrednostima elemenata histograma vidimo da procentualno ima više piksela u klasterima jer promenom parametra *K* vršimo veći uticaj na ukupni kapacitet nosioca. Promena vrednosti parametra *L* ima uticaj ali ne toliko značajan koliko parametar *K*. Na slici 28 prikazano je ponašanje parametra *bpp* za nosilac „Space08.jpg“ i to za tip 2 obrade gde je vrednost koeficijenta filtriranja jednaka 3. Elementi histograma pokazuju da ne dolazi ni do kakve promene za promenu vrednosti parametra *L* što implicira da pri pomenutom načinu obrade ne dobijamo odabrane piksele u „šarenim“ oblastima već samo u dva klastera. Slika 29

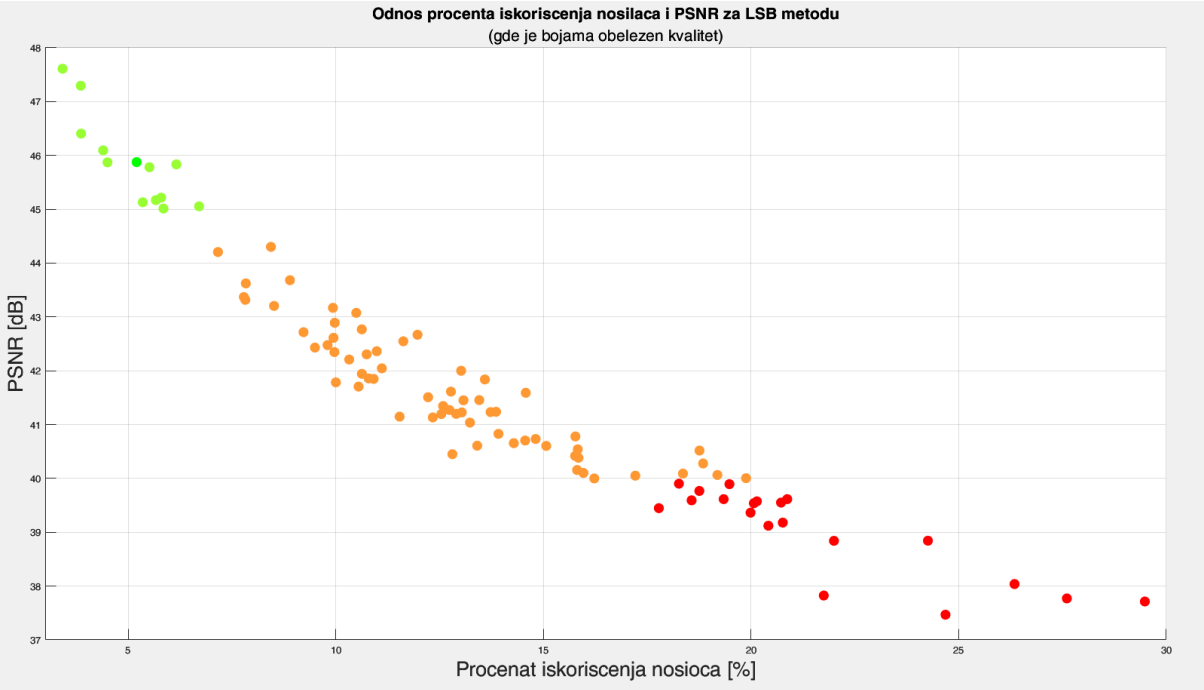
karakteristična je na svoj način i prikazuje promenu *bpp* u zavisnosti od parametara *K* i *L* za nosilac „Music07.jpg“, tip 2 način obrade, *FC* = 4. Na ovom histogramu uočava se dominantan uticaj *L* parametra što implicira da se mnogo veći procenat piksela na koje utičemo nalazi u „šarenim“ oblastima, što umanjuje uticaj vrednosti parametra *K*.



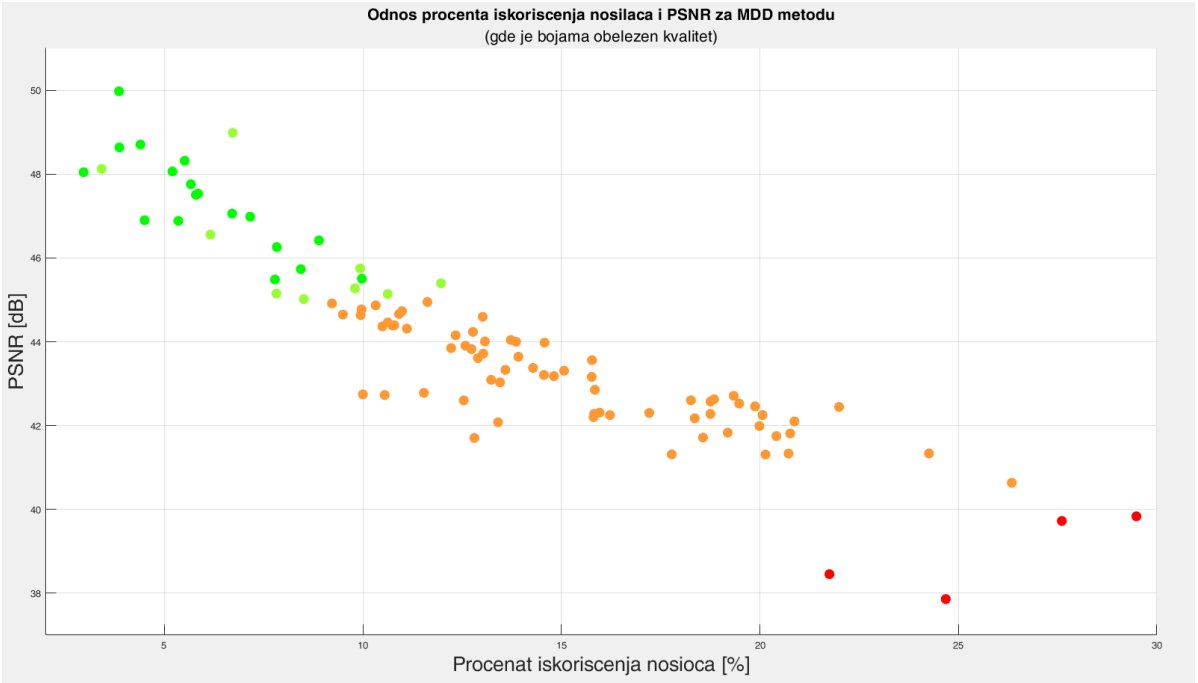
Slika 29. Ponašanje bpp u zavisnosti od parametara K i L za nosilac Music07.jpg, za tip 2 vrstu obrade

Slika 30 predstavlja pandan slici 18 za tip obrade 2 gde je prikazana zavisnost srednjih vrednosti *PSNR* za svaki od 100 nosilaca u zavisnosti od srednje vrednosti procenta iskorišćenja nosioca, za *LSB* metodu. U skladu sa zonama kvaliteta definisanim u tabeli 13, različitim bojama su obeleženi elementi grafika. Vrednost *PSNR* poprilično linearno opada sa porastom procenta iskorišćenja nosioca a „odlične“ i „vrlo dobre“ ocene uzimaju samo nosioci čija srednja vrednost iskorišćenja ne prelazi 7%. Slika 31 daje prikaz odnosa *PSNR* i procenta iskorišćenja nosioca na identičan način kao slika 30 ali za *MDD* metodu. Ono što međusobno

razlikuje grafikone sa pomenute dve slike je nešto veće odstupanje elemenata grafika od interpolirane linearne prave, za *MDD* metodu.



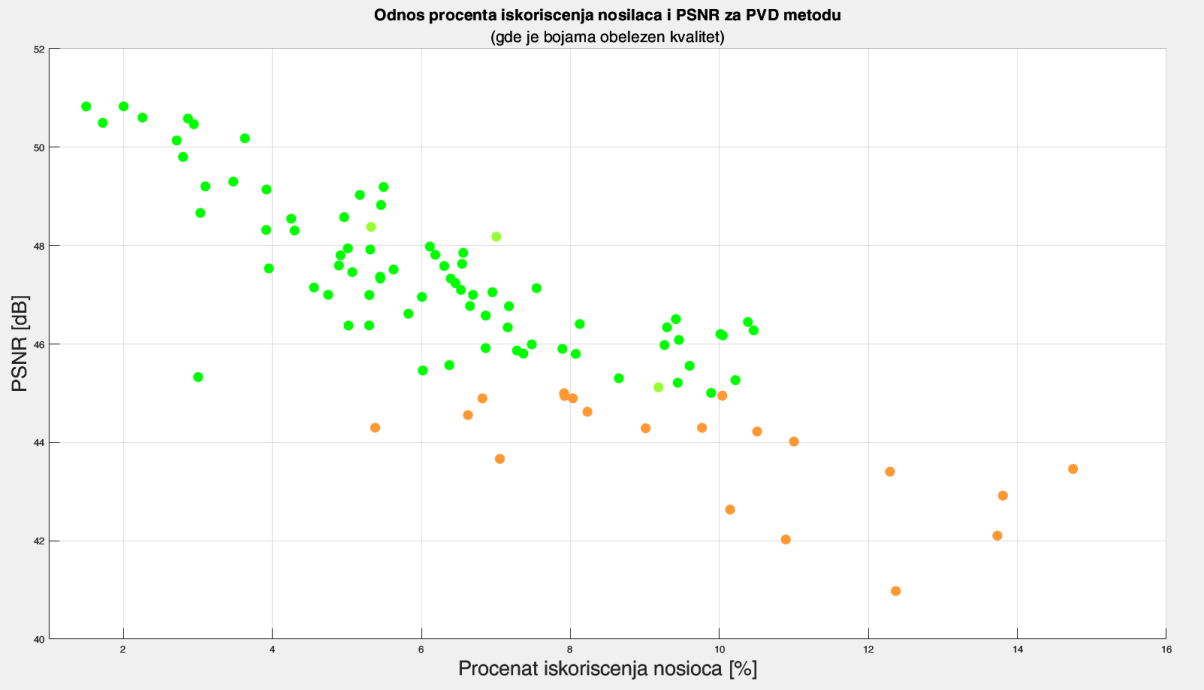
Slika 30. Odnos srednjih vrednosti procenta iskorišćenja i srednjih vrednosti PSNR na uzorku od 100 nosilaca, za LSB metodu, za tip 2 vrstu obrade



Slika 31. Odnos srednjih vrednosti procenta iskorišćenja i srednjih vrednosti PSNR na uzorku od 100 nosilaca, za MDD metodu, za tip 2 vrstu obrade

Takođe, uočava se da su ocene kvaliteta nosilaca (u skladu sa zonama kvaliteta definisanih u tabeli 13) nešto bolje u odnosu na isto poređenje za *LSB* metodu, pa u ovom slučaju nosioci sa „odličnom“ i „vrlo dobrom“ ocenom imaju srednje vrednosti kvaliteta do 10%.

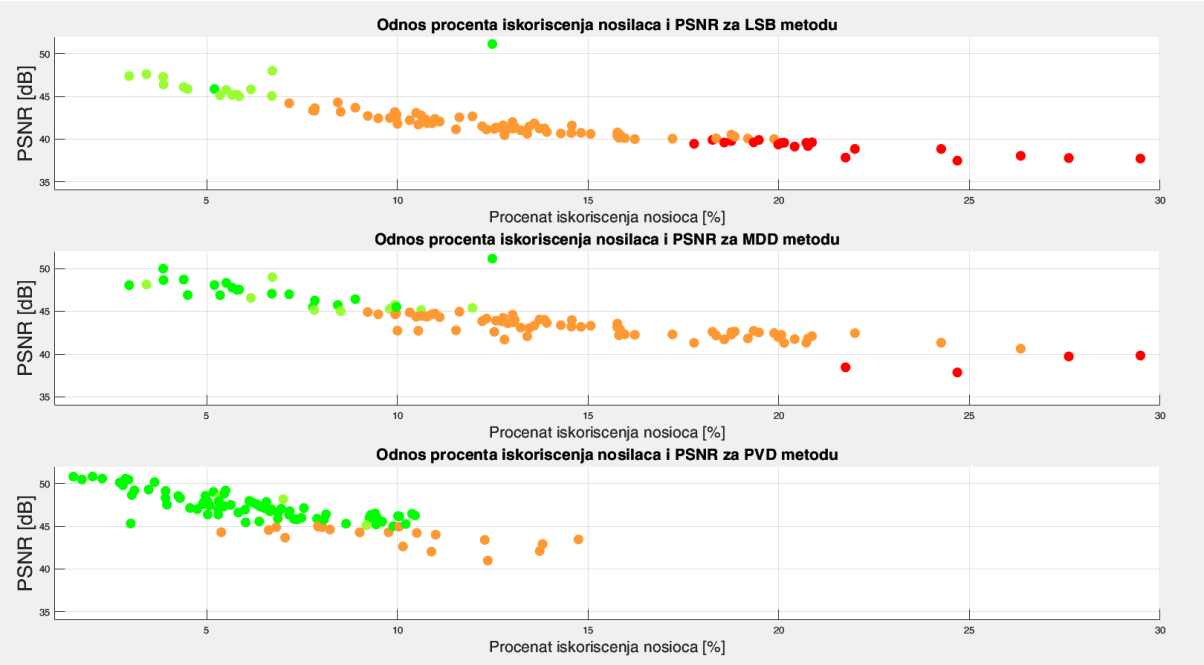
Kada je reč o *PVD* metodi i odnosu srednjih vrednosti *PSNR* i srednjih vrednosti procenta iskorišćenja nosioca, slika 32 pokazuje zavisnost. I baš kao što korespondiraju grafikoni na slika 18 - slika 20, za tip 1 načina obrade, takvo isto međusobno ponašanje postoji i za tip 2 vrstu obrade. Na slici 32 uočava se još veće rasipanje elemenata grafika od interpolirane linearne prave. Nosioci ocenjeni kao „odlični“ i „vrlo dobri“ takođe imaju srednju vrednost procenta iskorišćenja do 10% ali za razliku od *MDD* metode procenti iskorišćenja ne prelaze 15%.



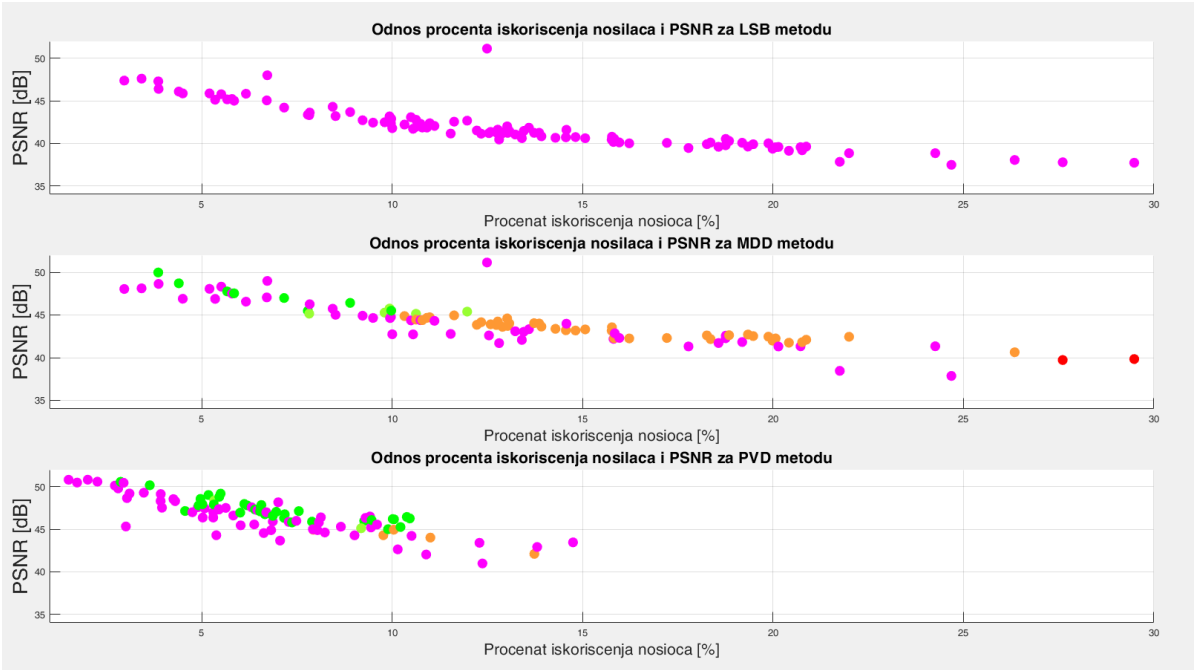
Slika 32. Odnos srednjih vrednosti procenta iskorišćenja i srednjih vrednosti PSNR na uzorku od 100 nosilaca, za PVD metodu, za tip 2 vrstu obrade

Kako bi se bolje razumeo međusobni odnos zavisnosti *PSNR* od procenta iskorišćenja nosioca za različite stego-metode, za tip 2 obrade kreirana je slika 33 koja sadrži 3 uporedna grafikona.

Baš kao što je to bio slučaj za tip 1 vrstu obrade, za prosečno bolje ocene za stego-objekte kreirane *PVD* metodom plaća se cena u smanjenom kapacitetu nosilaca.

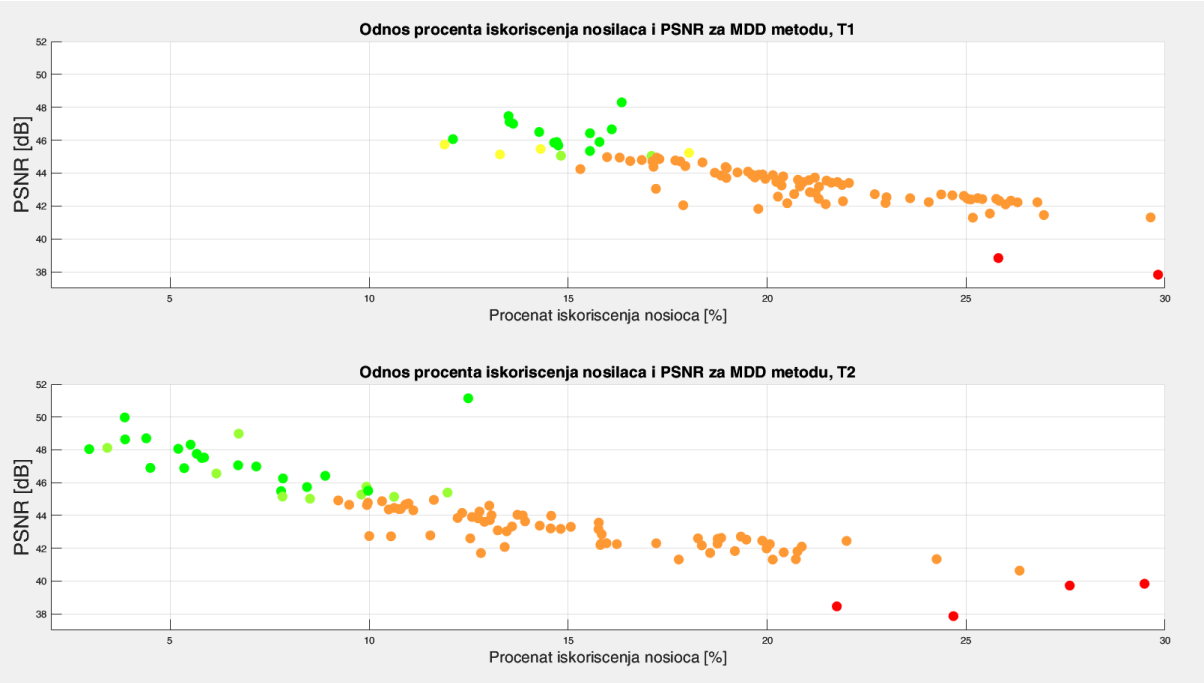


Slika 33. Komparativni odnos srednjih vrednosti procenta iskorišćenja i srednjih vrednosti PSNR na uzorku od 100 nosilaca, za LSB, MDD i PVD metodu, za tip 2 vrstu obrade



Slika 34. Komparativni odnos srednjih vrednosti procenta iskorišćenja i srednjih vrednosti PSNR, za LSB, MDD i PVD metodu, za tip 2 vrstu obrade, uz akcenat na stego-objekte koji ne zadovoljavaju uslov stego-analize

Ukoliko bi u ocenu kvaliteta uključili i kriterijum koji diktira stego-analiza (u skladu sa tabelom 13), grafikoni na slici 33 bi se transformisali u grafikone na slici 34, gde su roze bojom označeni nosioci koji ne zadovoljavaju definisani kriterijum stego-analize. Uočava se da nijedan stego-objekat generisan *LSB* metodom ne zadovoljava kriterijum stego-analize. Kod *MDD* i *PVD* metode broj nosilaca koji zadovoljavaju kriterijum stego-analize je sličan, a smanjeni kapacitet kod PVD metode je cena koja je plaćena za bolje ocene stego objekata, kako je i ranije navedeno.



Slika 35. Komparativni odnos srednjih vrednosti PSNR, za MDD metodu, za tip 1 i tip 2 vrstu obrade

Kako je tema ovog rada upotreba *MDD* stego-metode u kombinaciji sa algoritmom za odabir stego oblasti, u narednom delu ćemo se fokus biti isključivo na pomenutoj metodi i komparaciji stego-objekata dobijenih tipom 1 i tipom 2 načinom obrade. Slika 35 je derivat slike 19 i slike 31 gde su u istim opsezima koordinatnih sistema prikazani rezultati za tip 1 i tip 2 načina obrade za *MDD* metodu. Ovo poređenje daje jasne smernice da ukoliko želimo da odaberemo nosilac takav da nam je kapacitet prioritet, u odnosu na kvalitet, trebalo bi

odabrati i tip 1 obrade. Sa druge strane, ukoliko nam je prioritet kvalitet generisanih stego-objekata, veća je verovatnoća da će tip 2 obrade dati bolji rezultat po cenu sniženog kapaciteta.

Ovde posebno treba uzeti u obzir činjenicu da su na grafikonima prikazane srednje vrednosti svih stego-objekata koji su derivati pojedinačnog nosioca. To posebno ima značaja ako uzmemo u obzir da su u kompletnu statistiku ušli i stego-objekti gde se za parametar *K* i *L* uzima vrednost 4 što u izvesnoj meri povećava srednju vrednost kapaciteta ali sa druge strane drastično degradira kvalitet stego-objekata. Tabela 14 daje prikaz srednje vrednosti odnosa *PSNR* i srednje vrednosti kapaciteta za sve stego-objekte, generisane *MDD* metodom, za tip 1 i tip 2 vrstu obrade, gde u statistiku nisu ušli stego-nosioci gde parametra *K* ili *L* imaju vrednost 4.

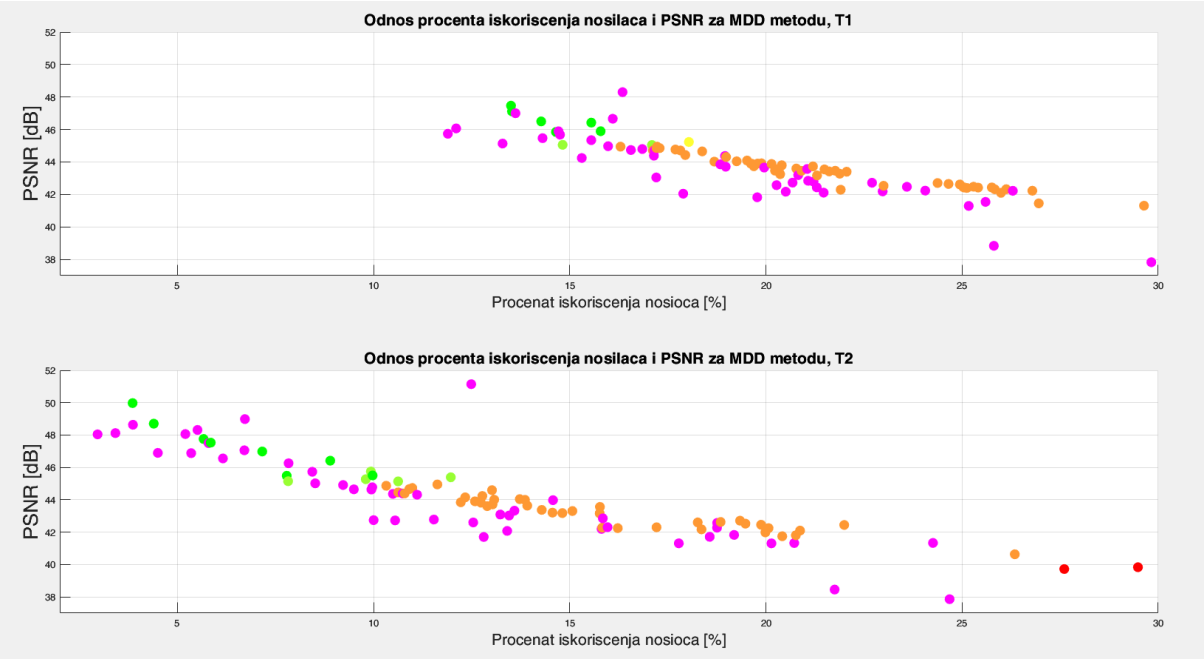
Tabela 14. Komparacija srednjih vrednosti PSNR i kapaciteta nosilaca za Tip 1 i Tip1 vrstu obrade, za MDD metodu steganografije

MDD metoda	Srednja vrednost PSNR[dB]	Srednja vrednost bpp	Srednja vrednost kapaciteta[%]
Tip 1	47,944	2,868	11,951
Tip 2	46,836	2,838	11,828

Zanimljiva je činjenica da je odnos srednjih vrednosti *PSNR* i *bpp* bolji kod Tipa 1 načina obrade.

Slika 36 predstavlja dopunu slike 35 ukoliko bi u analizu uključili i kriterijum stego-analize u skladu sa granicama definisanim tabelom 13. Iako tabela 14 ukazuje da generalno bolji odnos kvaliteta i kapaciteta imamo kod tipa 1 načina obrade, slika 36 nam ukazuje da je veća verovatnoća odabrati nosilac koji će imati „odličnu“ ili „vrlo dobru“ ocenu a da pri tome i zadovoljava uslove stego-analize. Ideja i cilj ovog poglavlja jesu putokaz ka ispravnom načinu

izbora nosioca kao i na optimalnom odabiru načina obrade, u skladu za željenim performansama. Na samom kraju ovog poglavlja, a na osnovu svih prikazanih analiza, biće elaboriran ispravan način odabira nosioca.



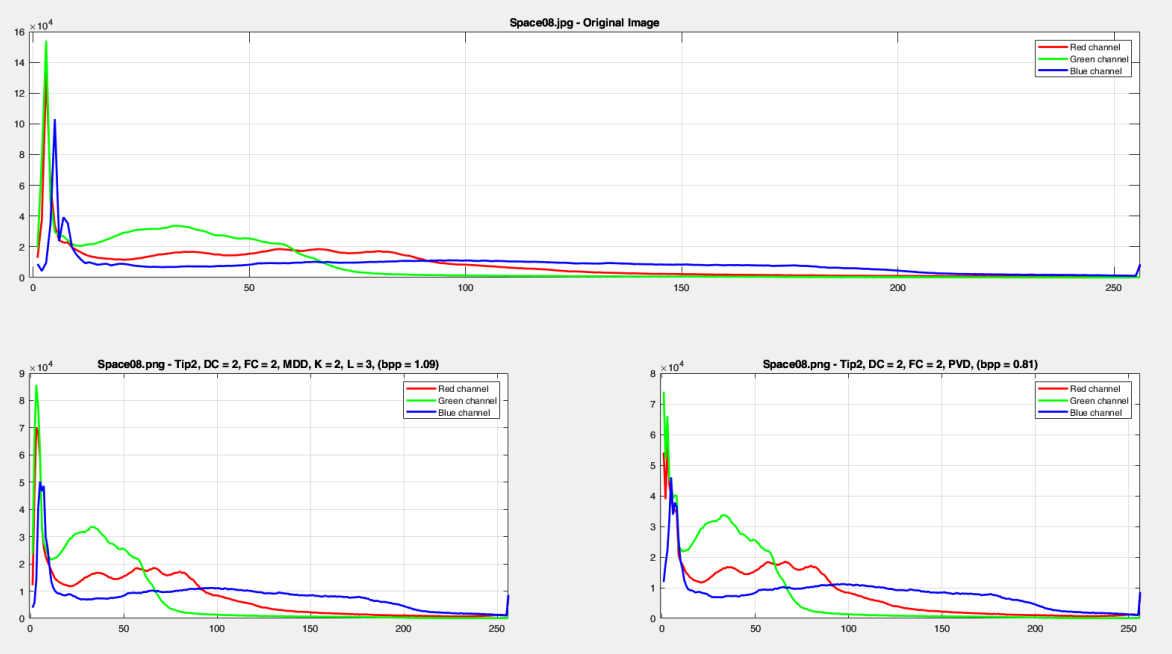
Slika 36. Komparativni odnos srednjih vrednosti PSNR, za MDD metodu, za tip 1 i tip 2 vrstu obrade, uzimajući u obzir uslove stego-analize

5.2. Analiza histograma generisanih stego-objekata

Da bi analiza generisanih stego-objekata bila kompletna potrebno je analizirati i histograme dobijenih stego-objekata, napraviti njihovo poređenje i izvesti zaključke. U sekciji 1.6 je dato objašnjenje histograma, njihovo ponašanje u različitim slučajevima i korelacija između ponašanja efekata na originalnoj slici i efekata na njenom histogramu. Na narednih nekoliko slika i grafikona biće prikazani histogrami i familije histograma generisanih stego-objekata i njihovo poređenje. U radovima [35], [36] je već bilo reči o ponašanju histograma stego-objekata generisanih pomoću *MDD* i *LSB* metode. Analizirano je ponašanje histograma u slučajevima kada se proces steganografije obavlja preko cele površine nosioca (cele slike) i kada se obavlja samo u nekim oblastima. Takođe je diskutovan efekat kvantizacije histograma

za slučaj *LSB* metode kao i povećanja distorzije nego kod primene *MDD* metode. Da bi analiza bila potpuna potrebno je u obzir uzeti i stego-objekte dobijene *PVD* metodom i diskutovati efekte na histogramima koji se javljaju.

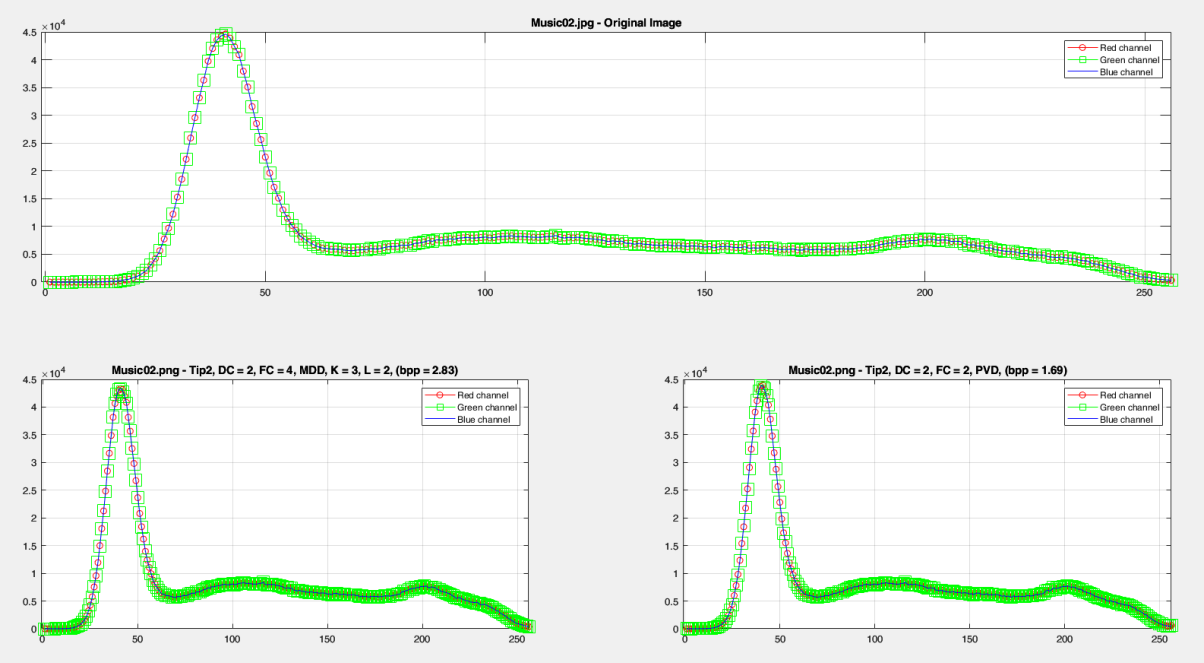
Slika 37 pokazuje histogram originalnog stego-nosioca „Space08.jpg“, histogram stego-objekta dobijenog *MDD* metodom, sa navedenim parametrima obrade, i histogram stego-objekta dobijenog *PVD* metodom. Treba obratiti pažnju na izobličenja histograma stego-objekata u odnosu na histogram originalne slike koja postoje ali koja nisu značajna. Takođe je važno uočiti veća izobličenja histograma stego-objekta dobijenog *PVD* metodom u odnosu na histogram stego-objekta dobijenog *MDD* metodom za tamnije nijanse (niske vrednosti po *RGB* kanalima) iako je količina informacija koju stego-objekat nosi (izražena pomoću bpp) manja u slučaju *PVD* metode.



Slika 37. Komparativni prikaz histograma nosioca kao i stego-objekata dobijenih MDD i PVD metodom

Slika 38 prikazuje tri grafikona: za originalni “Music02.jpg“ nosilac, za stego-objekat dobijen *MDD* metodom i stego-objekat dobijen *PVD* metodom. Potpuno preklapanje vrednosti po

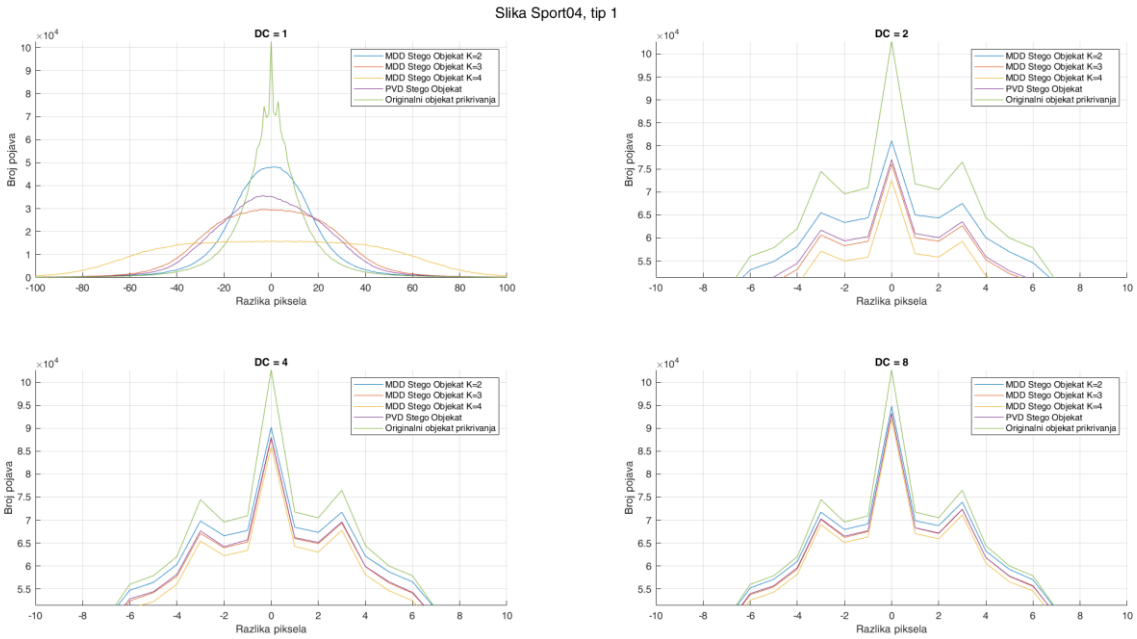
RGB kanalima je posledica toga da je metodom kolor histograma obrađena slika koja je *grayscale* (sivih nijansi). Na grafikonima uočavamo minimalna izobličenja za histograme stego-objekata u odnosu na histogram originalnog nosioca. Kao i u prethodnom slučaju, za isti stepen izobličenja stego-objekat dobijen *MDD* metodom ima značajno veći kapacitet, izražen pomoću parametra *bpp*.



Slika 38. Komparativni prikaz histograma nosioca kao i stego-objekata dobijenih MDD i PVD metodom, za grayscale sliku

Kada je u pitanju analiza histograma razlike piksela (*PDH*), slika 39 pokazuje četiri grafikona sa familijama histograma za nosilac „Sport04.jpg“ i stego-objekte dobijene različitim metodama i primenom različitih parametara obrade. Svaki od četiri grafikona predstavlja familiju histograma za različit ulazni parametar algoritma *DC*, za tip1 način obrade. Za steganografski proces preko cele površine nosioca (*DC*=1) uočavamo značajna odstupanja, uz ogromno izobličenje krivih u odnosu na oblik karakteristike za originalnu sliku. Izobličenje je najveće za stego-objekat *MDD* metode gde je parametar K=4 dok se stego-objekat dobijen *PVD* metodom po kvalitetu nalazi između objekata dobijenih *MDD* metodom za *K*=2 i *K*=3. Tabela

15 daje pregled odnosa *bpp* i *PSNR* vrednosti za stego-objekte čiji su histogrami prikazani na prvom grafikonu slike 39.



Slika 39. Komparativni prikaz familija PDH za stego-objekte dobijene obradom nosioca Sport04.jpg

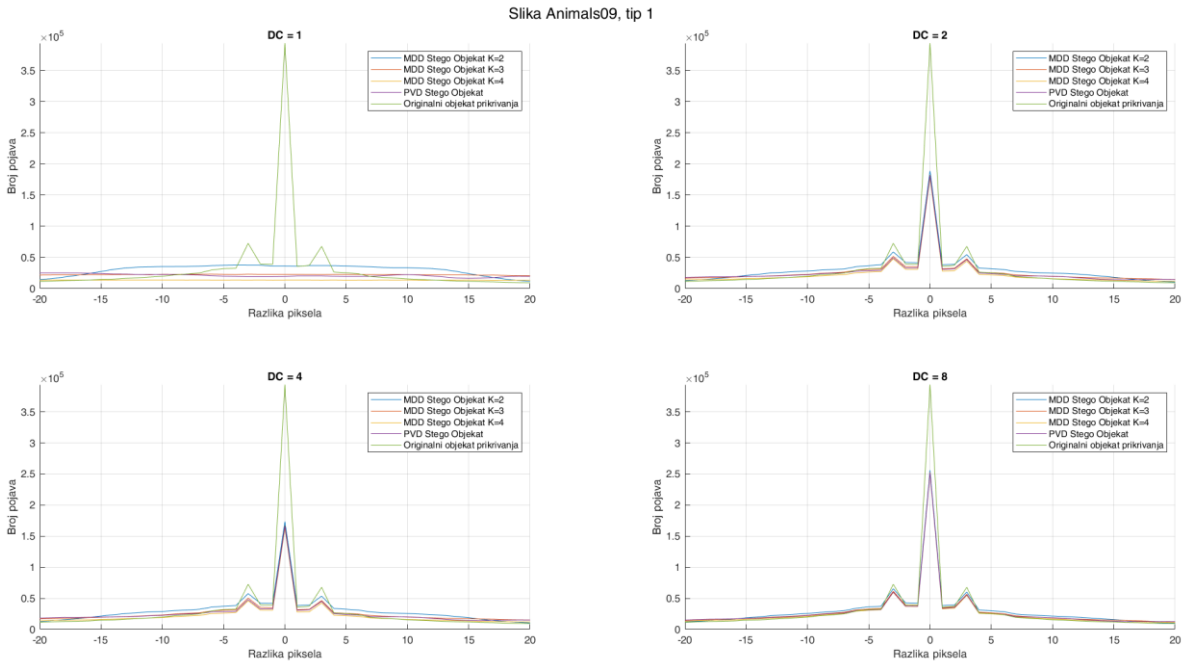
Tabela 15. Vrednosti parametara bpp i PSNR za stego-objekte dobijene tipom 1 načina obrade, preko cele površine slike (DC=1), obradom nosioca Sport04.jpg

	MDD, K=2	**MDD, K=3**	**MDD, K=4**	**PVD**
bpp	5,97	8,96	11,94	4,53
PSNR[dB]	46,37	40,7	34,72	42,42

Zanimljivo je uočiti manja izobličenja *PDH* karakteristike za stego-objekat dobijen *MDD* metodom, za *K*=2, gde su pri tome vrednosti bpp i *PSNR* veće nego za stego-objekat dobijen *PVD* metodom.

Ukoliko obradu vršimo u stego-oblastima, na grafikonima se uočava da familija histograma prati oblik originalne karakteristike, što nije bio slučaj kod obrade preko cele površine nosioca. Takođe, izobličenja postoje u znatno užem opsegu što se ogleda u prikazanim opsezima apscise za različite grafikone na slici 39. Razlog zašto su odstupanja za familiju histograma sve

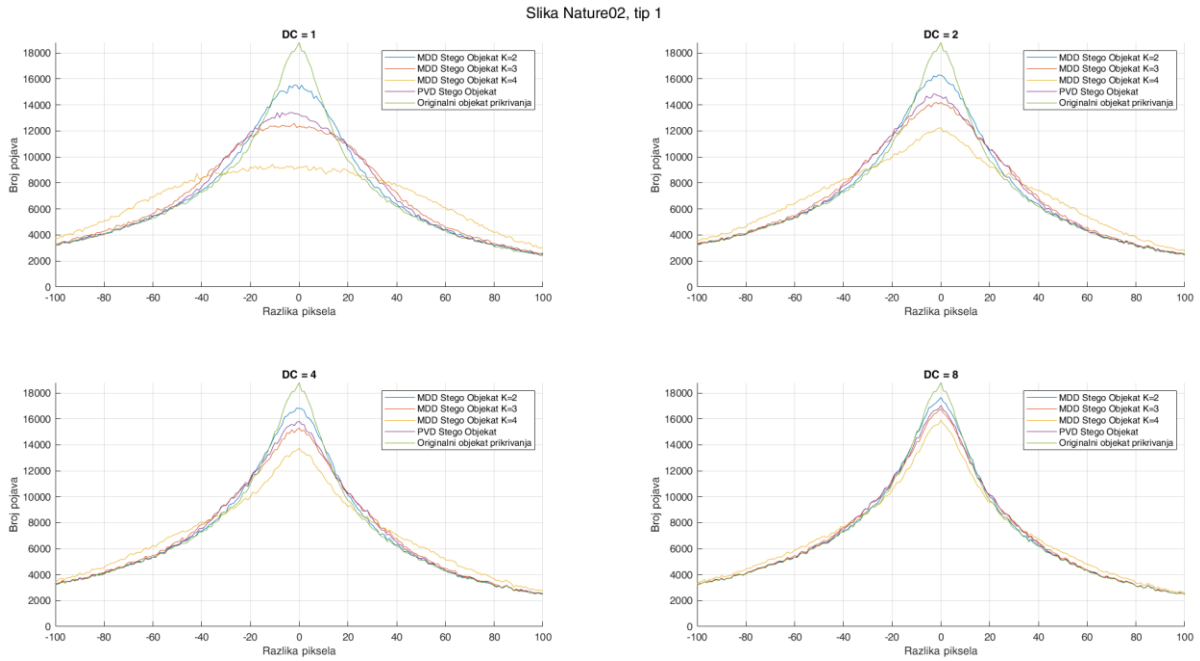
manja kako parametar *DC* raste je u korelaciji sa ponašanjem familije karakteristika na slici 15 i slici 16, gde se karakteristike takođe međusobno približavaju za veće vrednosti parametra *DC*. Kako je to već bilo objašnjeno, razlog takvog ponašanja je manji procenat piksela na koji se utiče sa porastom koeficijenta *DC*. Kao što je bio slučaj i kod steganografske obrade preko cele površine slike, i ovde je situacija takva da se karakteristika za stego-objekat generisan *PVD* metodom nalazi po kvalitetu između karakteristika stego-objekata dobijenih *MDD* metodom za *K*=2 i *K*=3. Četvrti grafikon (*DC*=8) pokazuje da karakteristike stego-objekata verno prate karakteristiku za originalni nosilac uz veoma mala izobličenja.



Slika 40. Komparativni prikaz familija PDH za stego-objekte dobijene obradom nosioca Animals09.jpg

Slika 40 pokazuje familije karakteristika kao na slici 39 ali za nosilac „Animals09.jpg“. Iako je ponašanje karakteristika vrlo slično kao za nosilac „Sport04.jpg“ uočavamo drugačiji opseg vrednosti po apscisi. Razlog većeg opsega prikazane razlike piksela je karakteristika originalne slike, razlike vrednosti po *RGB* kanalima i odnosa svetlih i tamnih nijansi.

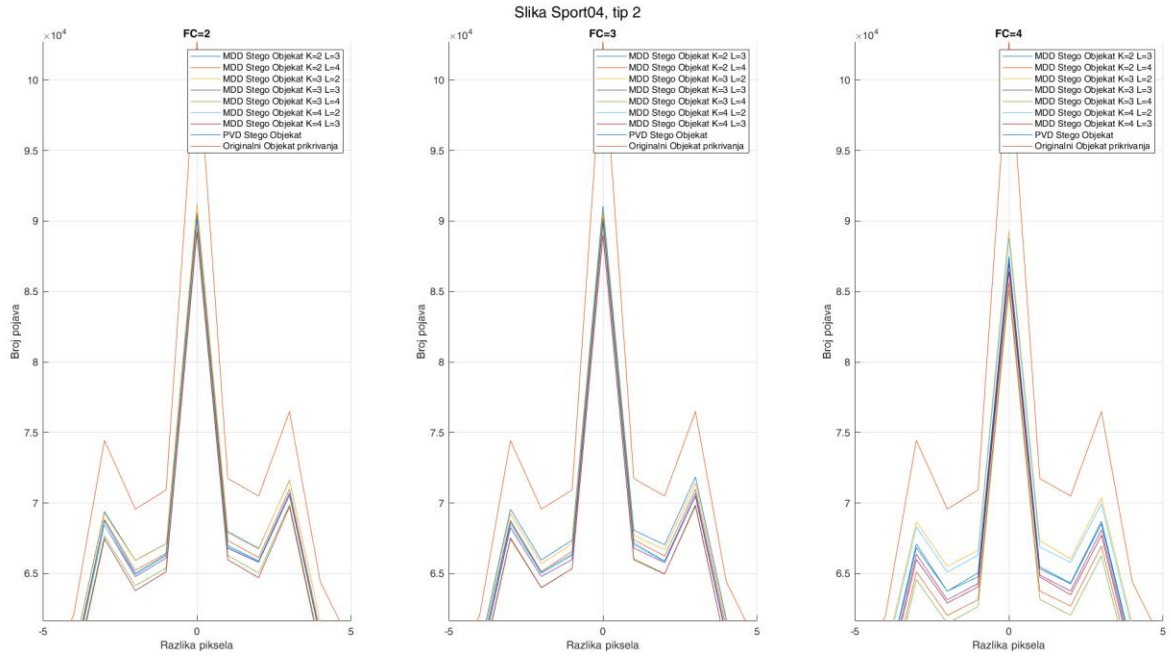
Slika 41 prikazuje istu familiju karakteristika na četiri grafikona, za nosilac „Nature02.jpg“, na širem opsegu po apscisi (od -100 do 100). Zaravnjenje karakteristike uočljivo za stego-objekat dobijen *MDD* metodom za *DC*=1, *K*=4 ukazuje na činjenicu da ukoliko bi, hipotetički, menjali svih 8 bita piksela na svakom od 3 kanala, dobili bi potpuno ravnu karakteristiku u opsegu -255 do 255. Ukoliko *DC* uzima veće vrednosti od 1, što znači da steganografski proces obavljamo u oblastima ovaj efekat ne bi bio moguć jer van stego-oblasti ostaju pikseli sa nepromenjenim vrednostima od originalnih.



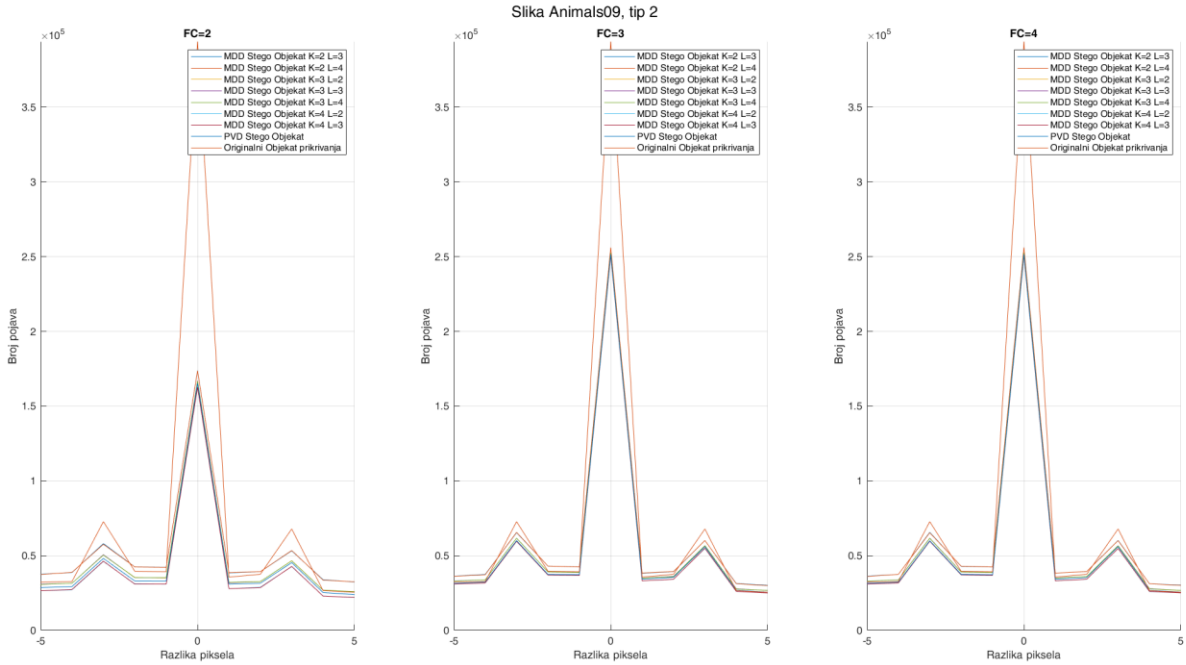
Slika 41. Komparativni prikaz familija PDH za stego-objekte dobijene obradom nosioca Nature02.jpg

Slika 42 predstavlja familiju karakteristika prikazanu na tri grafikona za nosilac „Sport04.jpg“ i stego-objekte dobijene obradom tipa 2, za tri različita koeficijenta filtriranja. Veća odstupanja karakteristika od originalne sa porastom ulaznog parametra *FC* govore o tome da za veće vrednosti faktora *FC* vršimo uticaj na veći broj piksela. Kao što je bilo prikazano na slici 23, kod tipa 2 načina obrade moguće je različito ponašanje procenta piksela na koje vršimo uticaj sa promenom parametra *FC*. Na *PDH* grafikonima to bi se odrazilo tako što bi za različite

nosioce, karakteristike stego-objekata bile više ili manje slične sa originalnom karakteristikom, sa promenom parametra *FC*, bez tačnog pravila ponašanja kao što je to slučaj za tip 1 vrstu obrade.



Slika 42. Komparativni prikaz familija PDH za stego-objekte dobijene obradom nosioca Sport04.jpg, tip 2 vrsta obrade



Slika 43. Komparativni prikaz familija PDH za stego-objekte dobijene obradom nosioca Animals09.jpg

Slika 43 pokazuje familiju karakteristika na *PDH* grafikonima za nosilac „Animals09.jpg“. Uočava se da su drugi i treći grafikon identični što ukazuje na to da je nosilac takav da nije došlo do promene procenta piksela na koje utičemo promenom parametra *FC*.

5.3. Stego-analiza generisanih stego-objekata

Za potrebe stego-analize izdvojena su tri nosioca sa različitim karakteristikama kako bi se napravilo adekvatno poređenje. Nosioci korišćeni za potrebe stego-analize su „Sport04.jpg“, „Nature02.jpg“ i „Animals09.jpg“. Neke od karakteristika stego-objekata generisanih pomoću pomenutih nosilaca date su u tabeli 16 za tip 1 način obrade i tabeli 17 za tip 2 način obrade.

Tabela 16. Vrednosti parametara bpp, PSNR, P_{rs} i P_d za stego-objekte generisane pomoću nosilaca Sport04.jpg, Animals09.jpg i Nature02.jpg, za tip1 vrstu obrade

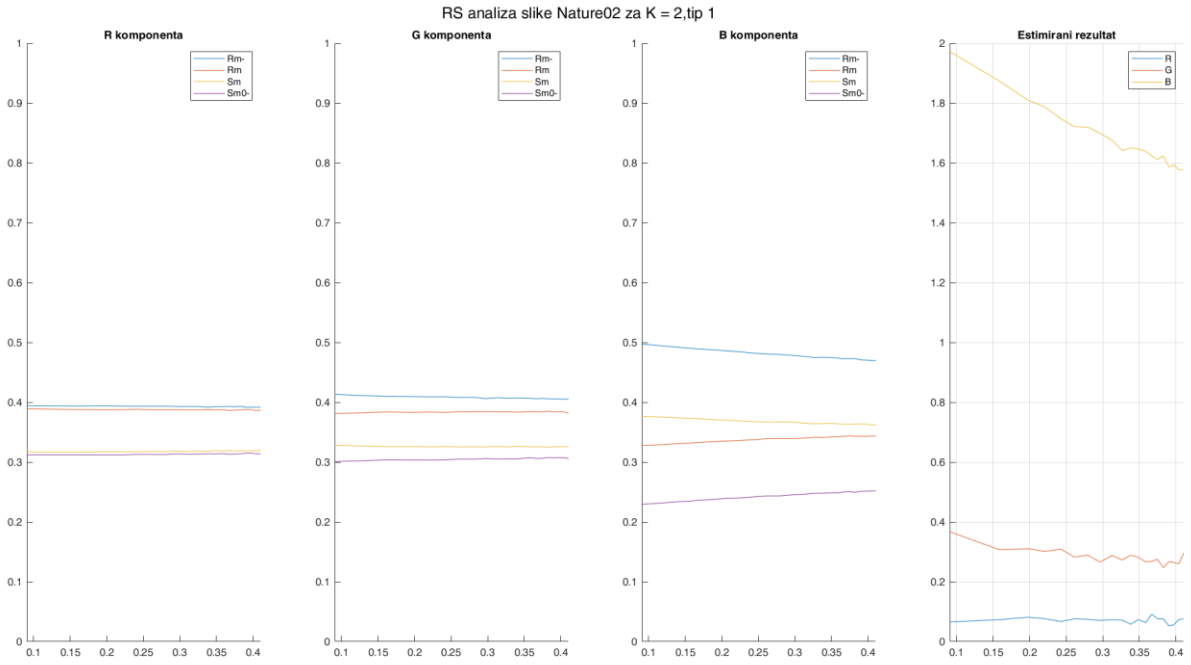
	bpp (srednja vr.)	**PSNR[dB] (sr.vr.)**	**P_{rs} (sr.vr.)**	**P_d(sr.vr.)**
Sport04.jpg	3,25	47,12	0,02	0,01
Animals09.jpg	3,67	44,24	0,23	0,38
Nature02.jpg	4,11	44,38	0,6	0,42

Tabela 17. Vrednosti parametara bpp, PSNR, P_{rs} i P_d za stego-objekte generisane pomoću nosilaca Sport04.jpg, Animals09.jpg i Nature02.jpg, za tip2 vrstu obrade

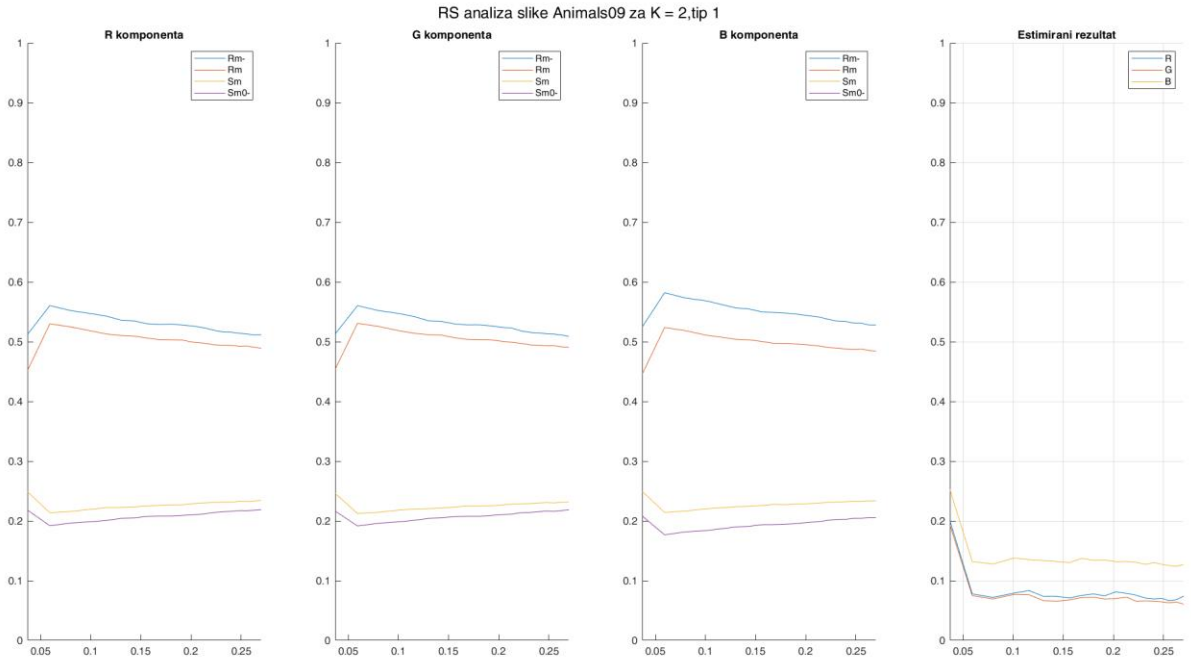
	bpp (srednja vr.)	**PSNR[dB] (sr.vr.)**	**P_{rs} (sr.vr.)**	**P_d(sr.vr.)**
Sport04.jpg	1,05	48,7	0,02	0,02
Animals09.jpg	1,48	46,56	0,16	0,45
Nature02.jpg	2,39	44,64	0,76	0,3

Na osnovu tabele 16 i tabele 17 jasno se zaključuje da srednje vrednosti P_{rs} i P_d ukazuju da stego-objekti dobijeni obradom nosioca „Sport04.jpg“ zadovoljavaju kriterijum stego-analize, definisan tabelom 13 dok to nije slučaj za nosioce „Animals09.jpg“ i „Nature02.jpg“. Iako nosioci „Animals09“ i „Nature02“ imaju nešto veće vrednosti *bpp* (i adekvatno smanjen *PSNR* u tom kontekstu), vrednosti parametara stego-analize se razlikuju za više od reda veličine i postavlja se pitanje zašto se javlja takav efekat? Slika 44, slika 45 i slika 46 predstavljaju

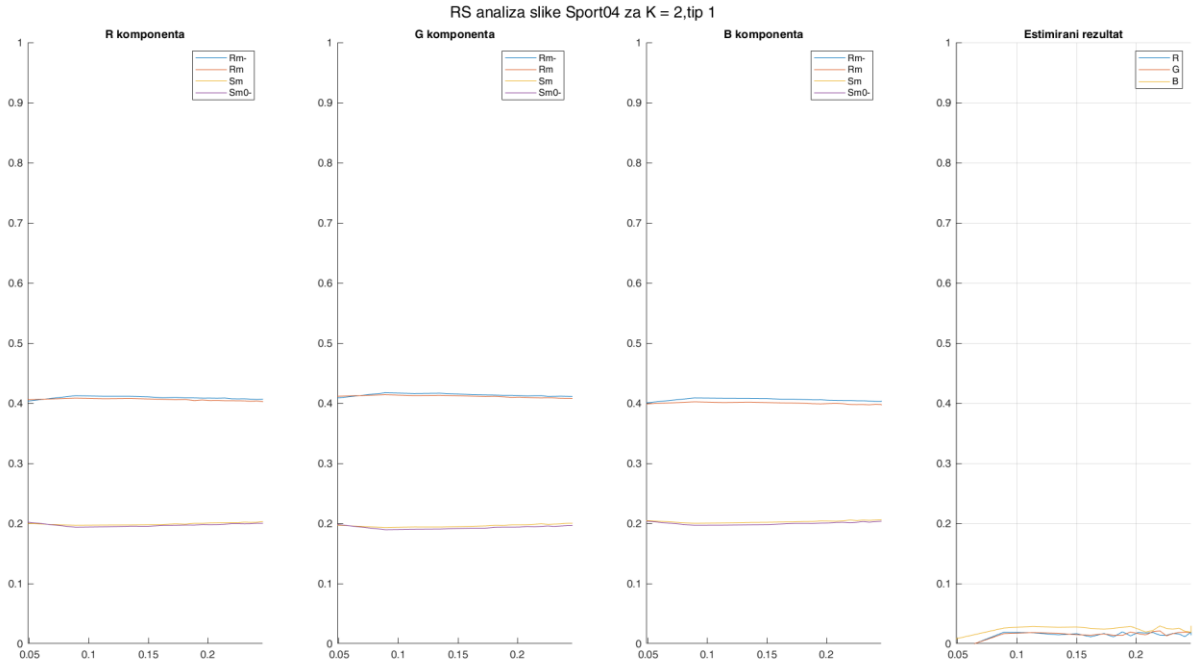
grafikone stego-analize za srednje vrednosti nosilaca „Nature02“, „Animals09“ i „Sport04“ respektivno.



Slika 44. RS analiza stego-objekta dobijenog obradom nosioca Nature02.jpg, tip1 K=2



Slika 45. RS analiza stego-objekta dobijenog obradom nosioca Animals09.jpg, tip1 K=2



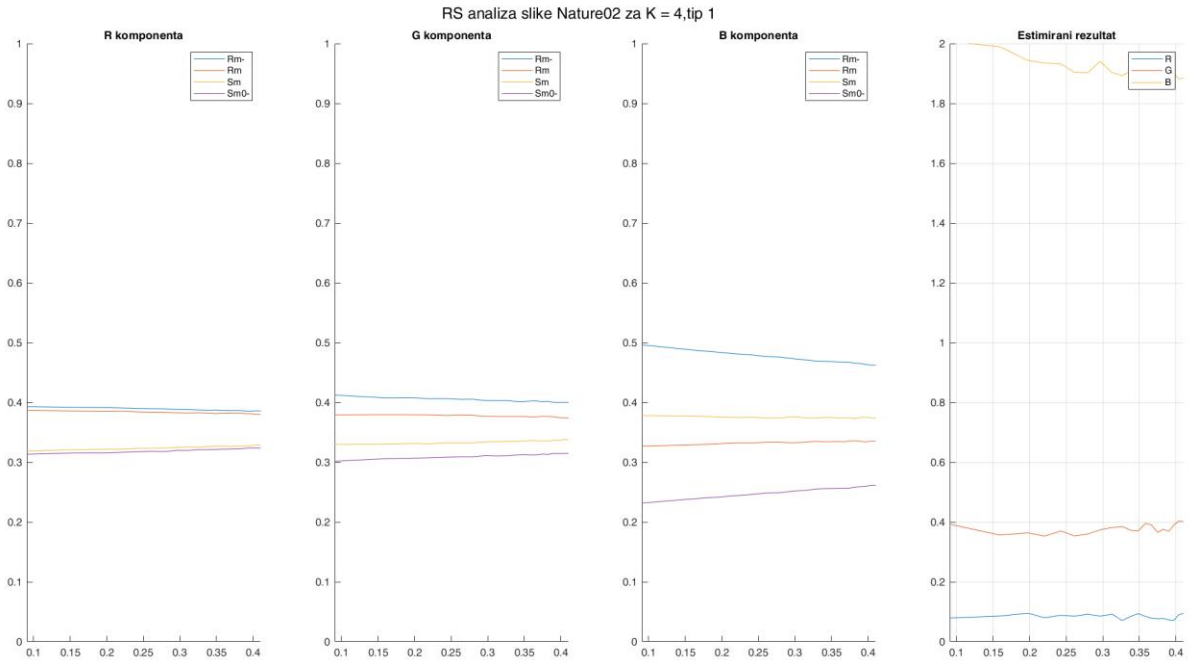
Slika 46. RS analiza stego-objekta dobijenog obradom nosioca Sport04.jpg, tip1 K=2

Na Slici 44 uočljivi su odlični rezultati za stego-analizu tj. procenu utisnutog sadržaja za crvenu komponentu, nešto lošiji rezultati za zelenu komponentu i veoma loši rezultati za plavu komponentu, što u ukupnoj proceni daje veoma loš rezultat.

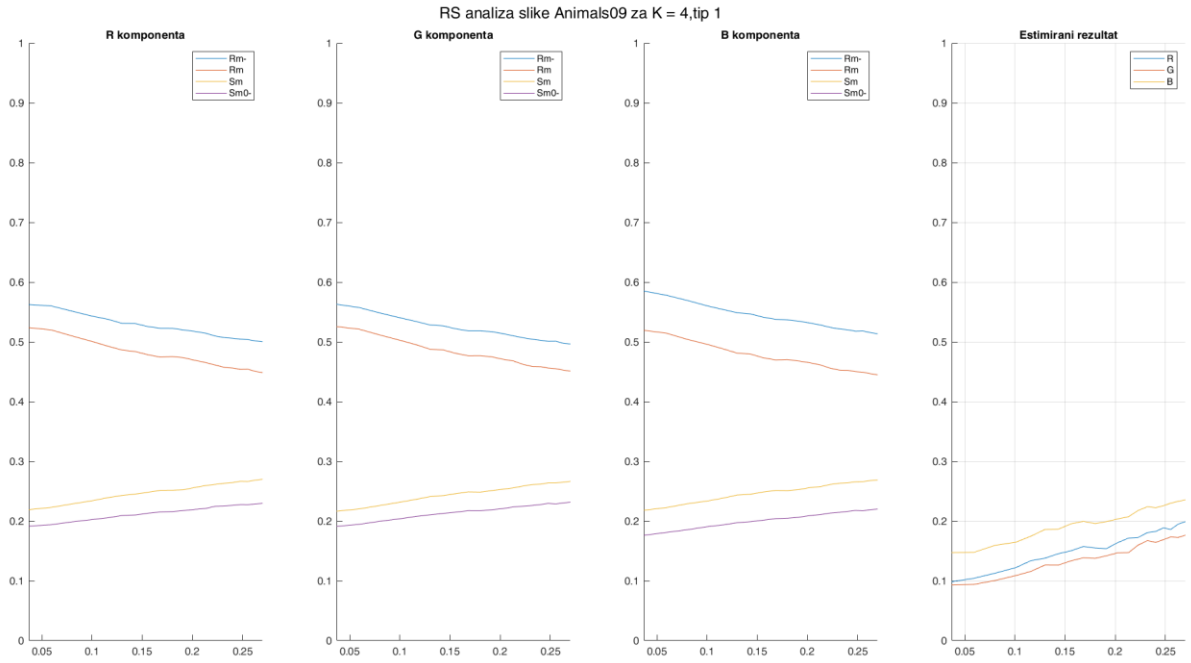
Kada je u pitanju nosilac „Animals09“, na slici 45 vidimo slične procene za količinu izmenjenog sadržaja na crvenom i zelenom kanalu, kao i nešto nepovoljniju procenu na plavom kanalu što u konačnom rezultatu daje procenu nešto lošiju od definisanog praga.

Kada se radi o nosiocu „Sport04“, slika 46 pokazuje odlične vrednosti (loše detekcije) po sva tri kanala (*RGB*) kao i konačnu estimaciju procenta izmenjenih piksela sa vrlo niskim vrednostima. Prethodne tri analize prikazane na Slikama 44-46 obavljene su na nosiocima gde je menjano *K*=2 bita najmanje težine. Postavlja se pitanje da li će rezultat analize biti drugačiji ako, tokom izvođenja *MDD* metode, menjamo više bita najmanje težine? Slika 47, slika 48 i slika 49 predstavljaju rezultat *RS* stego-analize za stego objekte dobijene kao proizvod obrade

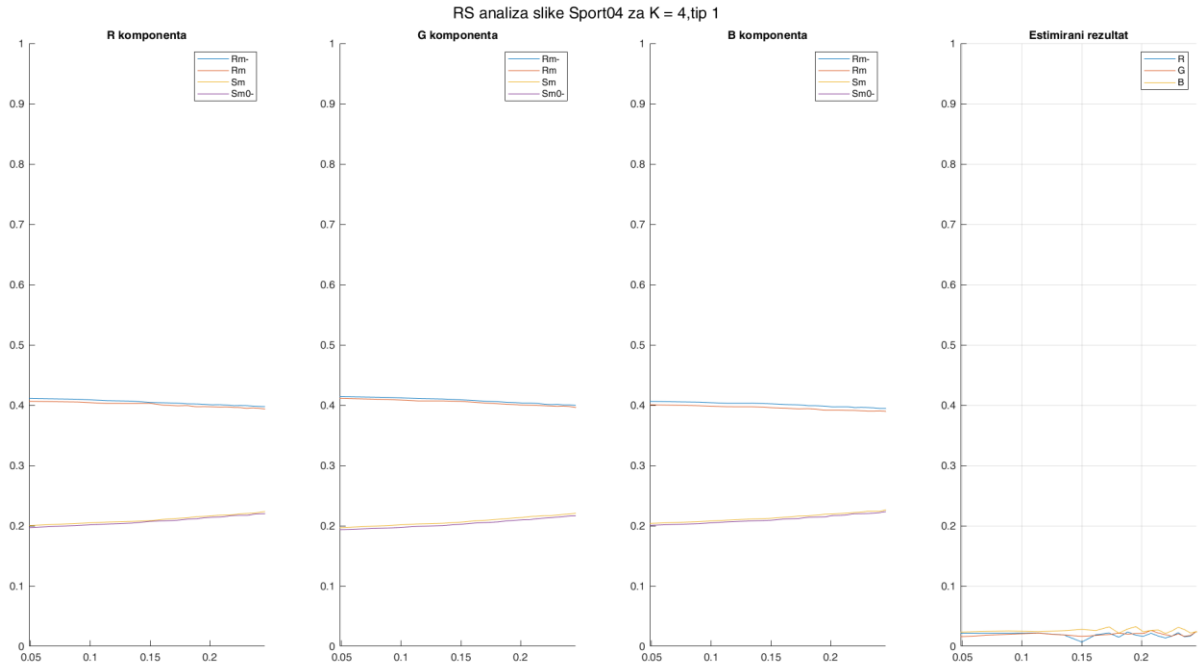
ista tri pomenuta stego-objekta („Nature02“, „Animals09“ i „Sport04“), *MDD* metodom, tipom 1 obrade, gde se sada umesto 2 bita najmanje težine - menja 4 bita.



Slika 47. RS analiza stego-objekta dobijenog obradom nosioca Nature02.jpg, tip1 K=4



Slika 48. RS analiza stego-objekta dobijenog obradom nosioca Animals09.jpg, tip1 K=4

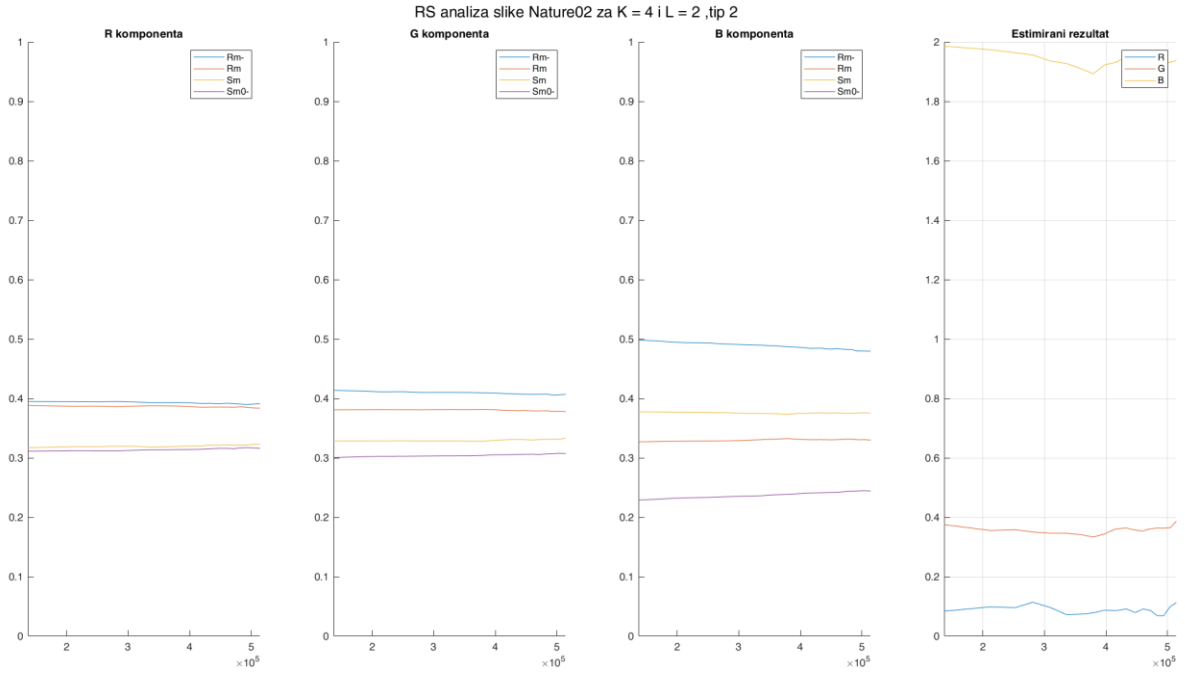


Slika 49. RS analiza stego-objekta dobijenog obradom nosioca Sport04.jpg, tip1 K=4

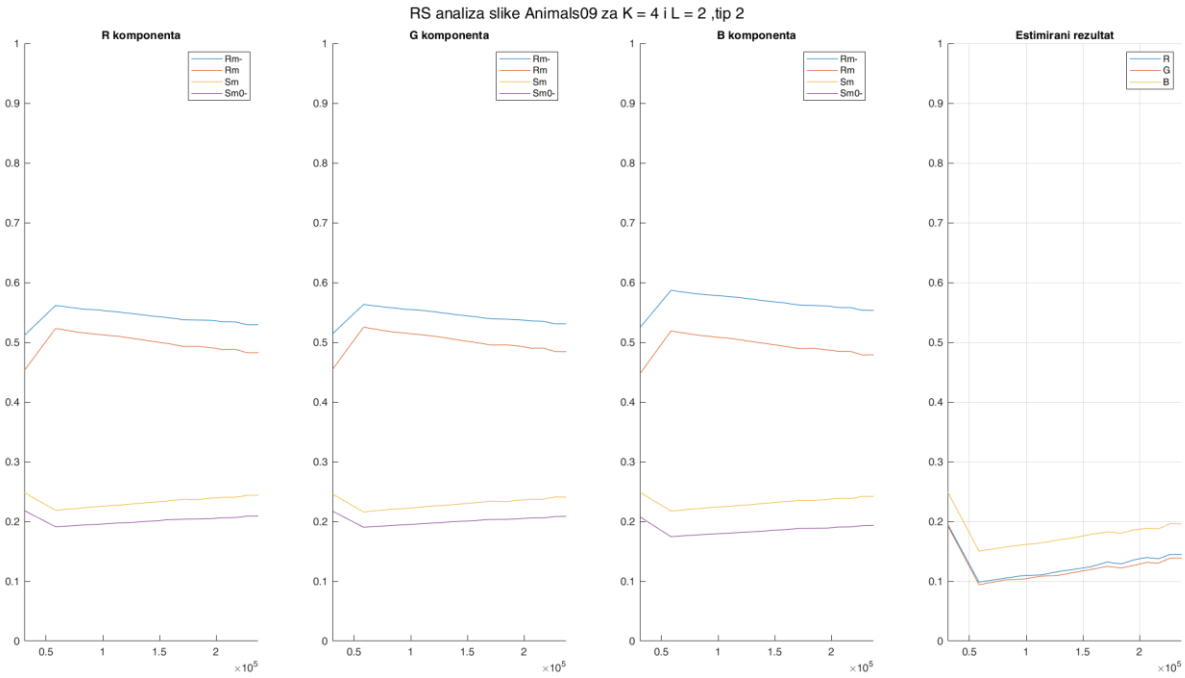
Jasno je da je ponašanje karakteristika stego-analize slično kao u prethodnom slučaju, gde za nosilac „Nature02“ estimacija na plavom kanalu ozbiljno narušava ukupnu procenu, dok kod nosioca „Animals09“ procena za malo prelazi definisani prag detekcije. Ako poredimo ponašanja grafikona analiza stego-objekata gde se uticaj vršio na *K*=4 bita najmanje težine sa slika 47-slika 49 , sa odgovarajućim parnjacima sa slika 44 - slika46 gde se uticaj vršio na *K*=2 bita vidimo nešto lošije ponašanje karakteristika za stego-objekte gde je *K*=4 kod nosilaca „Animals09“ i „Nature02“. Takođe, vidi se identično dobar kvalitet za stego objekte koji su derivat obrade nosioca „Sport04“, bez obzira da li uticaj vršili na 2 ili na 4 bita najmanje težine. Postavlja se pitanje zašto postoji takav efekat i šta je to što nosilac „Sport04“ čini boljim u odnosu na ostale?

Slika 50, slika 51 i slika 52 predstavljaju rezultat stego-analize za stego-objekte dobijene tipom 2 načina obrade. Korišćeni su isti nosioci kao i u prethodnim analizama. Baš kao što je bio slučaj i za analizu stego-objekata dobijenih tipom 1 vrstom obrade, na grafikonima se uočava

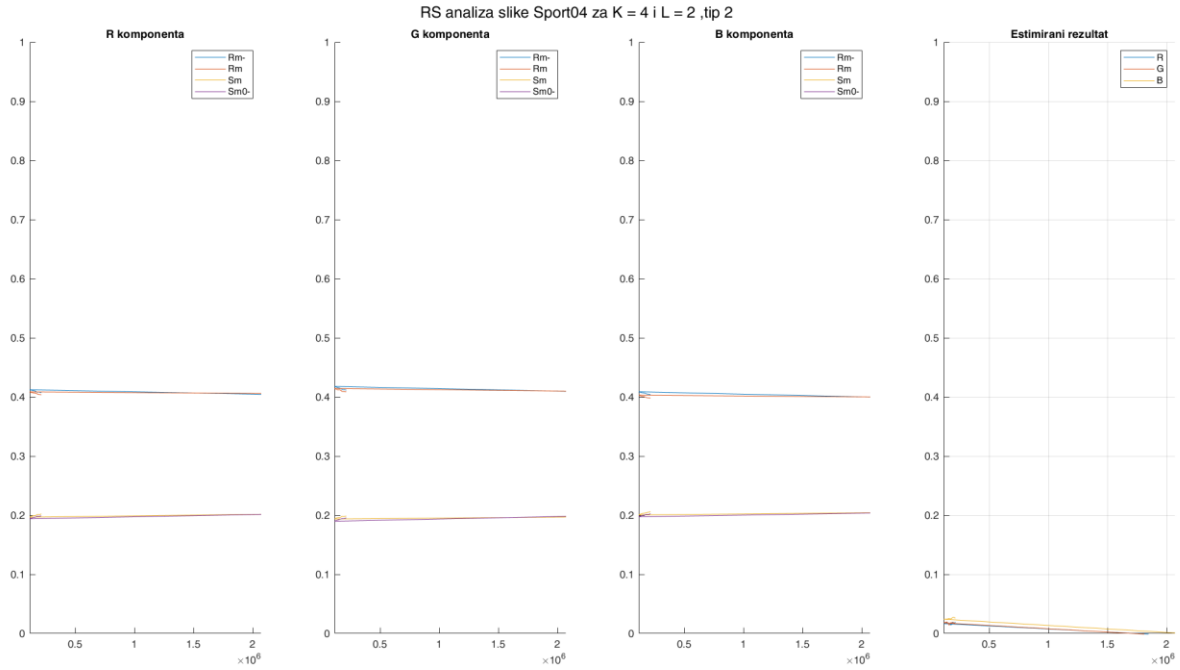
veliki stepen detekcije za nosilac „Nature02“, naročito je kritičan plavi kanal. Takođe, uočava se veoma mali stepen detekcije za nosilac „Sport04“.



Slika 50. RS analiza stego-objekta dobijenog obradom nosioca Nature02.jpg, tip2 K=4, L=2



Slika 51. RS analiza stego-objekta dobijenog obradom nosioca Animals09.jpg, tip2 K=4, L=2



Slika 52. RS analiza stego-objekta dobijenog obradom nosioca Sport04.jpg, tip2 K=4, L=2

Ovim je pokazano da rezultat *RS* stego-analize ne zavisi od tipa obrade nosioca, za predloženi algoritam, bez obzira na ulazne parametre već isključivo zavisi od tipa steganografskog nosioca.

Slika 53. Karakteristični nosioci Animals09, Nature02 i Sport04 nad kojima je vršena RS anlaliza

Cilj kompletne prethodne analize, pored toga što daje smernice kako bi trebalo odabrati ulazne parametre obrade u cilju postizanja željenih performansi, je i način odabira kvalitetnog nosioca.

Da bi napravili adekvatno poređenje rezultata *RS* stego-analize za različite steganografske metode, kreirana je tabela 18 na osnovu ukupnog skupa rezultata datih u Apendix I i Apendix II. Nosioci „Sport04“, „Animals09“ i „Nature02“ su uzeti kao primeri za poređenje.

Tabela 18. Poređenje rezultata RS stego-analize i kapaciteta (bpp) različitih steganografskih metoda, za tip 2 vrstu obrade, za stego objekte dobijene pomoću nosilaca Sport04, Animals09 i Nature02

	bpp (MDD)	**P_{rs} (MDD)**	**P_d (MDD)**	**bpp (PVD)**	**P_{rs} (PVD)**	**P_d (PVD)**
Sport04	1,05	0,02	0,03	0,52	0,02	0,03
Animals09	1,48	0,16	0,45	0,74	0,28	1,13
Nature02	2,39	0,76	0,3	1,29	0,91	0,27

Tabela 18 jasno pokazuje slične pa čak i bolje rezultate (niže vrednosti parametara P_{rs} i P_d) stego-objekata dobijenih *MDD* metodom u odnosu na stego-objekte dobijene *PVD* metodom i pored dvostruko većih kapaciteta u slučaju primene *MDD* metode.

Prethodne analize pokazale su karakteristike i ponašanje stego-objekata generisanih predloženim algoritmom, u zavisnosti od promene ulaznih parametara, odnose kvaliteta i kapaciteta kao i solidan stepen otpornosti stego-objekata na *RS* stego-analizu. Takođe pokazana je dominantnost *MDD* metode u odnosu na originalnu *LSB* metodu, iz koje je nastala, i u odnosu na *PVD* metodu. Kada je reč o poređenju stego-objekata dobijenih predloženim algoritmom sa stego-objektima generisanim metodama adaptivne steganografije drugih autora, rad [62] daje neke komparacije. Komparacija je napravljena sa rezultatima predstavljenim u radu [47] gde je pokazan bolji odnos kapaciteta i kvaliteta stego-objekata dobijenih predloženom metodom. Odnos kvaliteta i kapaciteta je takođe upoređen

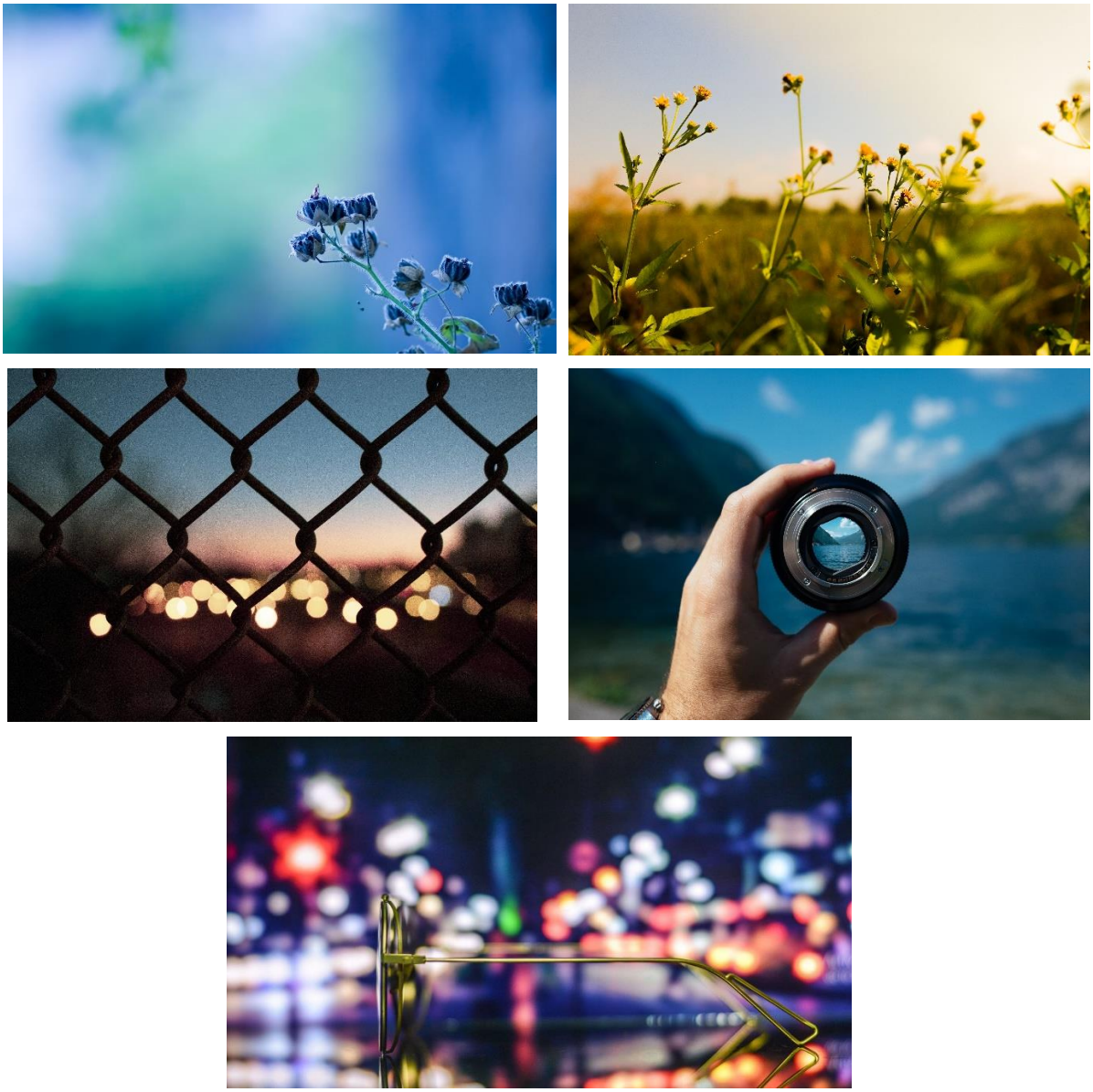
sa rezultatima predstavljenim u radovima [49] i [64] gde se pokazalo da za isti kvalitet stego-objekata izraženih pomoću *PSNR*, stego-objekti predloženog algoritma imaju i do 65% veći kapacitet. Poređenje sa kvalitetom stego-objekata autora radova novijeg datuma obavljeno je komparacijom sa rezultatima autora rada [65]. Pokazan je identičan odnos kvaliteta i kapaciteta generisanih stego-objekata uz činjenicu da je predloženi algoritam znatno jednostavniji i procesorski manje zahtevan od algoritma predloženog u [65] koji za potrebe apriori obrade nosilaca koristi neuralnu mrežu.

5.4. Otpornost predložene metode na moguće stego-napade

Kada je u pitanju otpornost predložene metode na različite vrste napada kao što su izrezivanje, sečenje, kompresija, filtriranje ili dodavanje šuma, treba imati na umu da se kompletan sistem sastoji od dva nezavisna dela: algoritma za odabir stego-oblasti i implementirani stego-metod. Različite steganografske metode daju različite stepene robusnosti stego objekata i otpornosti na procese sterilizacije slike. Neke od tehnika stego-napada i sterilizacije predstavljene su u poglavlju 2.7. Kako *MDD* metoda spada u kategoriju *LSB* steganografije (u prostornom domenu), nije otporna na različite vrste napada ili sterilizaciju stego objekta. S druge strane, ako bi se algoritam za odabir stego područja kombinovao sa drugom steganografskom metodom otpornijom na napade (kao što su metode steganografije u frekvencijskom domenu [41]), za očekivati je da bi takav sistem pokazao poboljšanja u kontekstu sigurnosti, što može biti predmet daljih istraživanja. Međutim, s obzirom na primenu ovog sistema za više nivoe zaštite, svako detektovanje bilo kakvog pokušaja napada podrazumeva i promenu kanala komunikacije.

6. Način izbora kvalitetnog nosioca i optimalnog načina obrade

Pitanje na koje dosadašnja analiza još uvek nije dala odgovor je vezano za pravilan, odnosno optimalan izbor steganografskog nosioca. Fokusiranjem na analizu rezultata iz poglavlja 5.3 jasno se uočava da je nosilac „Sport04“ kvalitetan i dobar izbor. Zašto je ovaj stego-nosilac bolji od ostalih? Posmatranjem nosioca dovelo je do postavljanja hipoteze koju bi trebalo dokazati. Hipoteza je da kvalitet ovog nosioca leži upravo u tome što pored centralne dve figure, koje su u fokusu i izoštrene, postoji velika površina zamućenih boja u pozadini (publika na utakmici). Pretpostavka je da je upravo ta velika zamućena površina idealna zona za utiskivanje skrivenog sadržaja. Raspored različitih boja i oblasti zamućene zone će diktirati koliku količinu informacija je moguće utisnuti i bez obzira na pomenutu količinu izmenjenih piksela, ovakav stego-objekat bi trebalo da je veoma otporan na *RS* stego-analizu. Da bi dokazali predstavljenu hipotezu vrlo pažljivo je odabrano 5 dodatnih nosilaca, nezavisno od uzorka do 100 nosilaca na kojima je vršena kompletna izložena analiza. Zajednička osobina svih 5 dodatnih nosilaca je ta da kod svakog od njih postoji jedna figura koja je u fokusu dok veći deo pozadine je van fokusa i zamućen. Identična obrada, kao i u slučaju uzorka od 100 nosilaca, obavljena je nad pomenutih 5 nosilaca tipom 1 i tipom 2 načinom obrade. Ovim postupkom kreirano je 60 stego-objekata tipom 1 vrstom obrade i 105 stego-objekata vrstom obrade tip 2. Obavljen je proračun svih parametara (kapaciteta, kvaliteta, stego-analize…) novih 165 stego-objekata kako bi rezultati bili poredivi sa rezultatima za slučajno odabranih 100 nosilaca a u cilju potvrđivanja postavljene hipoteze. Na slici 54 prikazani su odabrani nosioci pomenutih osobina.



Slika 54. Primer kvalitetnih nosilaca, balansiranih karakteristika, otpornih na RS anlalizu

Tabela 19 i tabela 20 daju poređenja rezultata generisanih za 100 slučajno odabranih nosilaca i rezultata za 5 odabranih, zamućenih, nosilaca i to za tip 1 i tip 2 vrstu obrade, respektivno.

Tabela 19. Poređenje srednjih vrednosti kapaciteta, PSNR, P_{rs} i P_d za 100 slučajno odabranih nosilaca i 5 zamućenih nosilaca za tip 1 vrstu obrade

	Sr. vr. Kapaciteta[%]	**Sr. vr. PSNR[dB]**	**Sr. vr. P_{rs}**	**Sr. vr. P_d**
Za 100 slučajno odabranih stego -nosilaca	14,27	44,9	0,14	0,34
Za 5 odabranih, zamućenih, stego-nosilaca	17,54	43,94	0,07	0,05

Tabela 20. Poređenje srednjih vrednosti kapaciteta, PSNR, P_{rs} i P_d za 100 slučajno odabranih nosilaca i 5 zamućenih nosilaca za tip 2 vrstu obrade

	Sr. vr. Kapaciteta[%]	**Sr. vr. PSNR[dB]**	**Sr. vr. P_{rs}**	**Sr. vr. P_d**
Za 100 slučajno odabranih stego -nosilaca	13,29	44,05	0,14	0,32
Za 5 odabranih, zamućenih, stego-nosilaca	16,62	42,79	0,07	0,06

Upoređujući vrednosti predstavljene u tabelama 19 i 20 vidi se da su odnosi srednjih vrednosti kapaciteta i *PSNR* međusobno vrlo slične. Osobina da se za nešto veći kapacitet dobija nešto manja vrednost *PSNR* i dalje važi. Ono gde se srednje vrednosti razlikuju je upravo kod parametara P_{rs} i P_d i to tako da u slučaju vrednosti za pet zamućenih nosilaca ovi parametri imaju vrlo male vrednosti, što je potvrda hipoteze sa početka ovog poglavlja. Ako se uzmu u obzir kompletni setovi rezultata dobijenih za 5 zamućenih nosilaca (Apendix III, Apendix IV) vidi se da samo u nekoliko slučajeva stego-objekti dobijeni od nosilaca "BluredFile03" i „BluredFile05" ne zadovoljavaju uslove stego-analize, dok za ostale stego-nosioce svi njihovi produkti zadovoljavaju uslove stego-analize. Takođe je zanimljiva činjenica da stego-objekti koji ne zadovoljavaju uslove stego-analize su oni gde je K=3 i K=4 za nosilac BluredFile05 i gde je K=4 za BluredFile03. Ova činjenica implicira da povećanje vrednosti K može negativno da utiče na zadovoljenje uslova stego-analize.

Tabela 21 pokazuje srednje vrednosti parametara samo za stego-objekte koji su ocenjeni kao odlični, u skladu sa kriterijumima definisanim u tabeli 13, za tip 1 vrstu obrade. Vidi se da je srednja vrednost kapaciteta stego-objekata, dobijenih od zamućenih nosilaca, ocenjenih kao odlični 11,26% dok *PSNR* uzima visoku vrednost od 49,39dB. Posmatranjem svih karakteristika stego-objekata ocenjenih odličnom ocenom kvaliteta uočava se da je pravilnim izborom

nosioca i parametara obrade moguće generisati stego-objekat kapaciteta većeg od 20% sa vrednošću parametra *PSNR* većim od 46dB.

Tabela 21. Srednje vrednosti kapaciteta, PSNR, P_{rs} i P_d za 5 zamućenih nosilaca, ocenjenih odličnom ocenom kvaliteta, za tip 1 vrstu obrade

	Sr. vr. Kapaciteta[%]	**Sr. vr. PSNR[dB]**	**Sr. vr. P_{rs}**	**Sr. vr. P_d**
Za 5 odabranih, zamućenih, stego-nosilaca	11,26	49,39	0,05	0,03

7. Zaključak i pravci daljeg istraživanja

Na osnovu predloženog eksperimenta, izvršenih ispitivanja, dobijenih rezultata i izvršene analize, dokazana je opravdanost izvođenja steganografije u odabranim oblastima stego-nosioca. Osim povećanja sigurnosti samog stego-procesa, pokazano je kako se degradacijom kapaciteta stego-nosioca postiže željeni kvalitet stego-objekata. Dalje, prikazan je način odabira ulaznih parametara algoritma, u zavisnosti od performansi nosioca, kako bi se postigao odgovarajući odnos kapaciteta i kvaliteta. Uvođenje dodatnog filtriranja piksela unutar određenog klastera otvara mnogo širi spektar mogućnosti u načinu odabira vrednosti ulaznih parametara kako bi se postigli željeni efekti. U poglavlju 5, tokom analize dobijenih rezultata, potvrđena je prethodno postavljena hipoteza o opravdanosti izvođenja steganografskog procesa u stego-oblastima. Zapravo, pokazalo se da korišćenjem različitog broja bita za proces steganografije u oblastima sličnih boja i nijansi i u stego-oblastima koja sadrže nekoliko različitih boja mogu imati svoje prednosti za odgovarajuće odabrane ulazne parametre algoritma. Konačno, prikazana je dominacija *MDD* metode nad *PVD* metodom. *MDD* metoda u većini slučajeva daje bolje performanse kao i mogućnost izbora *LS* bita na koje utičemo (*K* i *L*). *PVD* metoda je pokazala da nema razlike u izvođenju stego-procesa u

područjima sličnih boja ili u "šarenim" područjima. Iz tog razloga, *PVD* metodu treba izabrati u situacijama kada je visok kvalitet stego-objekta važan za niske vrednosti kapaciteta, gde pri tome treba uzeti u obzir viši stepen detekcije *RS* stego-analize kod stego-objekata dobijenih *PVD* metodom. Prikazan je visok stepen otpornosti *MDD* stego-objekata na proces stego-analize. Poređenjem parametara kapaciteta i *PSNR* vrednosti sa vrednostima koje su dobili autori sličnih metoda adaptivne steganografije, dokazana je konkurentnost predložene metode.

Važno je napomenuti da je osnovna ideja ovakvog pristupa problemu već našla svoju primenu u nekoliko aktuelnih projekata, odnosno sistemima za sigurnu razmenu fajlova, gde se nakon procesa enkripcije podataka implementira ovakav hibridni proces steganografije kako bi se prevazišao problem zabrane upotrebe šifrovanih datoteka na nekim *mail* servisima i *cloud* servisima (*vPCP-FC*) [66]. Da bi se praktično mogao primeniti u softverskom rešenju, opisani algoritam mora zadovoljiti sledeća ograničenja: mora se definisati maksimalan broj pravougaonika na jednom nosiocu, kao i minimalna veličina stego-oblasti izražena u pikselima ili u procentima od ukupne veličine nosioca, unapred.

Nedostacima ovakvog pristupa mogu se smatrati povećana složenost sistema, vreme potrebno za izvršavanje algoritma za odabir stego-oblasti, smanjen kapacitet nosioca, potreba za dodatnim komunikacionim kanalom za prenos informacija o broju i pozicijama stego-oblasti.

Konačno, ideja za dalji rad i istraživanje mogla bi ići u nekoliko različitih pravaca što otvara veliki spektar mogućnosti. Jedan od pravaca istraživanja može biti implementacija još nekoliko steganografskih metoda različitih kategorija, kao i stvaranje povratne petlje u sistemu (slika 7 pokazuje crveno isprekidanu liniju). Takva povratna sprega bi omogućila sistemu da izabere

parametre stego-oblasti, stego-metode i stego-procesa za odgovarajući nosilac, željeni kapacitet i kvalitet stego-objekata. Drugi pravac istraživanja mogao bi biti kombinovanje predloženog algoritma za odabir stego-oblasti sa robusnijim steganografskim metodama, kako bi se stvorili stego-objekti otporniji na stego-napade kao i na proces sterilizacije. Treća grana pristupa problemu mogla bi se ogledati u razvoju naprednijeg algoritma za odabir stego-područja, gde oblasti nosioca, u koje bi se utisnuo tajni sadržaj, imaju neki drugi pravilan geometrijski oblik ili čak nepravilan geometrijski oblik. Jedan od rezultata predloženog algoritma za izbor stego oblasti, zasnovanog na homogenizaciji delova nosioca, može biti detekcija tipičnih oblika, objekata i kontura. Kako algoritmi zasnovani na tehnikama dubokog učenja predstavljeni u [67] imaju isti cilj, jedan od pravaca daljih istraživanja mogao bi biti kombinovanje ovih tehnika. Četvrti pravac istraživanja mogao bi biti nadogradnja zaključaka iz poglavlja 6, gde je pokazano da je pravilnim izborom nosioca moguće maksimizirati parametre kapaciteta i kvaliteta stego-objekta uz minimiziranje detekcije utisnutog sadržaja metodom *RS* stego-analize. Za ovaj pravac istraživanja, dodatni kvalitet bi se mogao postići uključivanjem naprednijih metoda stego-analize.

8. Apendix

8.1. Apendix I

Apendix I predstavlja kompletne rezultate obrade metodom tipa 1.

- Sheet1 – Sirovi rezultati obrade
- Sheet2 – Statistika dobijena računanjem srednjih vrednosti parametara za 100 izvornih nosilaca
- Sheet3 – Statistički podaci po kriterijumima načina obrade
- Sheet4 - Statistika dobijena računanjem srednjih vrednosti parametara za 100 izvornih nosilaca filtrirana kriterijumima iz tabele 13
- Sheet5 – referentne vrednosti statističkog filtriranja podataka

Naziv fajla u elektronskoj formi: **Tip1_v3_final.xlsx**

Link za online pristup:

https://www.dropbox.com/scl/fi/pikiadpjpp9nglusjtraf/Tip1_v3_final.xlsx?rlkey=o05rrcd9rc8pf9yl4obzn4wvz&dl=0

8.2. Apendix II

Apendix II predstavlja kompletne rezultate obrade metodom tipa 2.

- Sheet1 – Sirovi rezultati obrade
- Sheet2 – Statistika dobijena računanjem srednjih vrednosti parametara za 100 izvornih nosilaca
- Sheet3 – Statistički podaci po kriterijumima načina obrade

- Sheet4 - Statistika dobijena računanjem srednjih vrednosti parametara za 100 izvornih nosilaca filtrirana kriterijumima iz tabele 13
- Sheet5 – referentne vrednosti statističkog filtriranja podataka

Naziv fajla u elektronskoj formi: **Tip2_v5_final.xlsx**

Link za online pristup:

https://www.dropbox.com/scl/fi/752w963th45hs50jbm3p2/Tip2_v5_final.xlsx?rlkey=e1jbkx0uculy7xq06qvftrny8&dl=0

8.3. Apendix III

Apendix III predstavlja kompletne rezultate obrade odabranih zamućenih nosilaca metodom tipa 1.

- Sheet1 – Filtrirani sirovi rezultati obrade
- Sheet2 – referentne vrednosti statističkog filtriranja podataka

Naziv fajla u elektronskoj formi: **Tip1_Blured_v1_final.xlsx**

Link za online pristup:

https://www.dropbox.com/scl/fi/hxdm0ttofjm3j0zg8oo8b/Tip1_Blured_v1_final.xlsx?rlkey=xz50s3j0yng9peox6getiooyq&dl=0

8.4. Apendix IV

Apendix IV predstavlja kompletne rezultate obrade odabranih zamućenih nosilaca metodom tipa 2.

- Sheet1 – Filtrirani sirovi rezultati obrade
- Sheet2 – referentne vrednosti statističkog filtriranja podataka

Naziv fajla u elektronskoj formi: **Tip2_Blured_v1_final.xlsx**

Link za online pristup:

https://www.dropbox.com/scl/fi/x5xyts8fowyx4efonewk3/Tip2_Blured_v1_final.xlsx?rlkey=dox6v22a7a008zyd7irt0dpnj&dl=0

9. Literatura

[1] S. Ramakrishnan, “Cryptographic and Information Security: Approaches for Images and Videos.”

[2] Veinović Mladen and Adamović Saša, “KRIPTOLOGIJA I Osnove za analizu i sintezu šifarskih sistema,” 2013.

[3] D. Kahn, “The history of steganography,” in *UKEssays*, 1996, pp. 1–5. doi: 10.1007/3-540-61996-8_27.

[4] J. C. Judge, “Steganography: Past, Present, Future,” Livermore, CA (United States), Dec. 2001. doi: 10.2172/15006450.

[5] N. Alabdali and S. Alzahrani, “An Overview of Steganography through History,” 2021. [Online]. Available: http://ijses.com/

[6] R. Kaur and B. Kaur, “Volume 4 Issue 4, April 2015 www.ijsr.net Licensed Under Creative Commons Attribution CC BY A Study and Review of Techniques of Spatial Steganography,” 2013. [Online]. Available: www.ijsr.net

[7] A. Dhamade and K. Panchal, “Network Protocols for Steganography: A Glance,” 2014.

[8] T. Ahmad, H. Studiawan, H. S. Ahmad, R. M. Ijtihadie, and W. Wibisono, “Shared secret-based steganography for protecting medical data,” in *2014 International Conference on Computer, Control, Informatics and Its Applications (IC3INA)*, IEEE, Oct. 2014, pp. 87–92. doi: 10.1109/IC3INA.2014.7042606.

[9] M. A. Ahmad *et al.*, “Hiding patients’ medical reports using an enhanced wavelet steganography algorithm in DICOM images,” *Alexandria Engineering Journal*, vol. 61, no. 12, pp. 10577–10592, Dec. 2022, doi: 10.1016/j.aej.2022.03.056.

[10] E. J. Delp, “Digital Watermarking: Algorithms and Applications,” 1998. [Online]. Available: https://www.researchgate.net/publication/277283835

[11] L. K. Saini, V. Shrivastava, M. Tech, and R. Scholar, “A Survey of Digital Watermarking Techniques and its Applications,” *International Journal of Computer Science Trends and Technology*, vol. 2, [Online]. Available: www.ijcstjournal.org

[12] P. Milosav, Z. Banjac, M. Milosavljević, T. Unkašević, and M. Abdelrahman Mohamed Mostafa, “Overview and Classification of Digital Watermarking Algorithms,” Singidunum University, May 2019, pp. 537–545. doi: 10.15308/sinteza-2019-537-545.

[13] U. Sara, “Comparative Study of Different Quality Assessment Techniques on Color Images,” 2019.

[14] V. K. Bhola, T. Sharma, and J. Bhatnagar, “Image Quality Assessment Techniques,” 2014.

[15] V. Azad and P. Sharma, “A Review on Objective Image Quality Assessment Techniques,” *International Journal of Emerging Engineering Research and Technology*, vol. 2, no. 5, pp. 188–192, 2014, [Online]. Available: www.ijeert.org

[16] S. Md. R. Islam, X. Huang, and K. Le, “A Novel Image Quality Index for Image Quality Assessment,” 2013, pp. 549–556. doi: 10.1007/978-3-642-42051-1_68.

[17] Zhou Wang and A. C. Bovik, “A universal image quality index,” *IEEE Signal Process Lett*, vol. 9, no. 3, pp. 81–84, Mar. 2002, doi: 10.1109/97.995823.

[18] W. Xue, L. Zhang, X. Mou, and A. C. Bovik, “Gradient Magnitude Similarity Deviation: A Highly Efficient Perceptual Image Quality Index,” *IEEE Transactions on Image Processing*, vol. 23, no. 2, pp. 684–695, Feb. 2014, doi: 10.1109/TIP.2013.2293423.

[19] K. Seshadrinathan *et al.*, “Image Quality Assessment,” *The Essential Guide to Image Processing*, pp. 553–595, Jan. 2009, doi: 10.1016/B978-0-12-374457-9.00021-4.

[20] S. A. Barman, R. A. Welikala, A. R. Rudnicka, and C. G. Owen, “Image quality assessment,” *Computational Retinal Image Analysis*, pp. 135–155, 2019, doi: 10.1016/B978-0-08-102816-2.00008-3.

[21] Z. Wang, A. C. Bovik, and E. P. Simoncelli, “Structural Approaches to Image Quality Assessment,” *Handbook of Image and Video Processing, Second Edition*, pp. 961–974, Jan. 2005, doi: 10.1016/B978-012119792-6/50119-4.

[22] C. Li and A. C. Bovik, “Three-component weighted structural similarity index,” S. P. Farnand and F. Gaykema, Eds., Jan. 2009, p. 72420Q. doi: 10.1117/12.811821.

[23] U. Sara, M. Akter, and M. S. Uddin, “Image Quality Assessment through FSIM, SSIM, MSE and PSNR—A Comparative Study,” *Journal of Computer and Communications*, vol. 07, no. 03, pp. 8–18, 2019, doi: 10.4236/jcc.2019.73002.

[24] R. Sonar and G. Swain, “Multi-Directional Pixel Difference Histogram Analysis Based on Pixel Blocks of Different Sizes,” *Sens Imaging*, vol. 22, no. 1, p. 11, Dec. 2021, doi: 10.1007/s11220-021-00334-6.

[25] G. Swain, “Digital Image Steganography Using Eight-Directional PVD against RS Analysis and PDH Analysis,” *Advances in Multimedia*, vol. 2018, pp. 1–13, Sep. 2018, doi: 10.1155/2018/4847098.

[26] X.-Z. Xie and C.-C. Chang, “Hiding data in dual images based on turtle shell matrix with high embedding capacity and reversibility,” *Multimed Tools Appl*, vol. 80, no. 30, pp. 36567–36584, Dec. 2021, doi: 10.1007/s11042-021-11368-z.

[27] M. G. S. Sravanthi, M. B. S. Devi, S. M. Riyazoddin, M. J. Reddy, M. B. Sunitha Devi, and & M. J. Reddy, “A Spatial Domain Image Steganography Technique Based on Plane Bit Substitution Method,” 2012.

[28] G. Swain and S. K. Lenka, “Classification of Image Steganography Techniques in Spatial Domain: A Study.”

[29] D. Anandpara, P. D. Scholar, and A. D. Kothari, “Working and Comparative Analysis of Various Spatial based Image Steganography Techniques,” 2015.

[30] R. Chandramouli and N. Memon, “Analysis of LSB based image steganography techniques,” in *IEEE International Conference on Image Processing*, 2001, pp. 1019–1022. doi: 10.1109/icip.2001.958299.

[31] V. Lokeswara Reddy, A. Subramanyam, S. A. Dist DrP Chenna Reddy, and S. A. Dist, “Implementation of LSB Steganography and its Evaluation for Various File Formats,” 2011.

[32] A. Kumar Singh, J. Singh, and H. Vikram Singh, “Steganography in Images Using LSB Technique.”

[33] Avni Aggarwal, Arpit Sanagal, and Aditya Varshney, “IMAGE STEGANOGRAPHY USING LSB ALGORITHM,” 2019. [Online]. Available: http://www.irphouse.com

[34] M. Van Dijk and F. Willems, “Embedding Information in Grayscale Images.”

[35] P. Milosav, Z. Banjac, T. Unkašević, and M. Milosavljević, “Minimal Decimal Difference Method Applied in Spatial Image Steganography.”

[36] P. Milosav, M. Milosavljević, and Z. Banjac, “Stego-Objects Metrics Improvement Using the Method of Minimal Decimal Difference in Spatial Image Steganography.”

[37] D. C. Wu and W. H. Tsai, “A steganographic method for images by pixel-value differencing,” *Pattern Recognit Lett*, vol. 24, no. 9–10, pp. 1613–1626, 2003, doi: 10.1016/S0167-8655(02)00402-6.

[38] J. K. Mandal, “Colour Image Steganography based on Pixel Value Differencing in Spatial Domain,” *International Journal of Information Sciences and Techniques*, vol. 2, no. 4, pp. 83–93, Jul. 2012, doi: 10.5121/ijist.2012.2408.

[39] R. Rojali, I. S. R. Siahaan, and B. Soewito, “Steganography algorithm multi pixel value differencing (MPVD) to increase message capacity and data security,” in *AIP Conference Proceedings*, American Institute of Physics Inc., Aug. 2017. doi: 10.1063/1.4994438.

[40] K. Joshi, S. Gill, and R. Yadav, “A New Method of Image Steganography Using 7th Bit of a Pixel as Indicator by Introducing the Successive Temporary Pixel in the Gray Scale Image,” *Journal of Computer Networks and Communications*, vol. 2018, 2018, doi: 10.1155/2018/9475142.

[41] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, “Digital image steganography: Survey and analysis of current methods,” *Signal Processing*, vol. 90, no. 3. pp. 727–752, Mar. 2010. doi: 10.1016/j.sigpro.2009.08.010.

[42] M. Hussain, A. W. A. Wahab, Y. I. Bin Idris, A. T. S. Ho, and K. H. Jung, “Image steganography in spatial domain: A survey,” *Signal Process Image Commun*, vol. 65, pp. 46–66, Jul. 2018, doi: 10.1016/j.image.2018.03.012.

[43] K. H. Jung, “High-capacity steganographic method based on pixelvalue differencing and LSB replacement methods,” *Imaging Science Journal*, vol. 58, no. 4, pp. 213–221, Aug. 2010, doi: 10.1179/136821910X12651933390584.

[44] T. Dhruw and N. Tiwari, “Different Method Used in Pixel Value Differencing Algorithm,” vol. 18, no. 3, pp. 102–109, doi: 10.9790/0661-180304102109.

[45] M. Khodaei and K. Faez, “New adaptive steganographic method using least-significant-bit substitution and pixel-value differencing,” *IET Image Process*, vol. 6, no. 6, pp. 677–686, Aug. 2012, doi: 10.1049/iet-ipr.2011.0059.

[46] M. Khodaei, B. Sadeghi Bigham, and K. Faez, “Adaptive Data Hiding, Using Pixel-Value-Differencing and LSB Substitution,” *Cybern Syst*, vol. 47, no. 8, pp. 617–628, Nov. 2016, doi: 10.1080/01969722.2016.1214459.

[47] G. Swain, “A Steganographic Method Combining LSB Substitution and PVD in a Block,” in *Procedia Computer Science*, Elsevier B.V., 2016, pp. 39–44. doi: 10.1016/j.procs.2016.05.174.

[48] M. Hussain, A. W. A. Wahab, N. Javed, and K. H. Jung, “Hybrid data hiding scheme using right-most digit replacement and adaptive least significant bit for digital images,” *Symmetry (Basel)*, vol. 8, no. 6, 2016, doi: 10.3390/sym8060041.

[49] A. Ioannidou, S. T. Halkidis, and G. Stephanides, “A novel technique for image steganography based on a high payload method and edge detection,” *Expert Syst Appl*, vol. 39, no. 14, pp. 11517–11524, Oct. 2012, doi: 10.1016/j.eswa.2012.02.106.

[50] N. Hamid, A. Yahya, R. B. Ahmad, and O. M. Al-Qershi, “A Comparison between Using SIFT and SURF for Characteristic Region Based Image Steganography,” 2012. [Online]. Available: www.IJCSI.org

[51] G. Manikandan, R. Bala Krishnan, N. Rajesh Kumar, D. Narasimhan, A. Srinivasan, and N. R. Raajan, “Steganographic approach to enhancing secure data communication using contours and clustering,” *Multimed Tools Appl*, vol. 77, no. 24, pp. 32257–32273, Dec. 2018, doi: 10.1007/s11042-018-6237-5.

[52] Bartel Jim, “Steganalysis: An Overview,” Livermore, 2000. [Online]. Available: http://www.giac.org/registration/gsec

[53] D. A. Shehab and M. J. Alhaddad, “Comprehensive Survey of Multimedia Steganalysis: Techniques, Evaluations, and Trends in Future Research,” *Symmetry (Basel)*, vol. 14, no. 1, p. 117, Jan. 2022, doi: 10.3390/sym14010117.

[54] J. Fridrich, M. Goljan, and R. Du, “Detecting LSB Steganography in Color and Gray-Scale Images,” 2001.

[55] J. Fridrich and M. Goljan, “Practical steganalysis of digital images: state of the art,” E. J. Delp III and P. W. Wong, Eds., Apr. 2002, pp. 1–13. doi: 10.1117/12.465263.

[56] A. D. Ker, “Quantitative evaluation of pairs and RS steganalysis,” in *Security, Steganography, and Watermarking of Multimedia Contents VI*, SPIE, Jun. 2004, p. 83. doi: 10.1117/12.526720.

[57] S. Manoharan, “An Empirical Analysis of RS Steganalysis,” in *2008 The Third International Conference on Internet Monitoring and Protection*, IEEE, 2008, pp. 172–177. doi: 10.1109/ICIMP.2008.15.

[58] S. Geetha, S. Subburam, S. Selvakumar, S. Kadry, and R. Damasevicius, “Steganogram removal using multidirectional diffusion in fourier domain while preserving perceptual image quality,” *Pattern Recognit Lett*, vol. 147, pp. 197–205, Jul. 2021, doi: 10.1016/j.patrec.2021.04.026.

[59] I. Mukherjee and G. Paul, “Double Bit Sterilization of Stego Images.”

[60] A. Jarvis, “Defeating Steganography with Multibit Sterilization using Pixel Eccentricity.”

[61] S. Ganguly and I. Mukherjee, “Image Sterilization through Adaptive Noise Blending in Integer Wavelet Transformation,” in *2022 IEEE 19th India Council International Conference (INDICON)*, IEEE, Nov. 2022, pp. 1–6. doi: 10.1109/INDICON56171.2022.10039861.

[62] P. Milosav, M. Milosavljević, and Z. Banjac, “Steganographic Method in Selected Areas of the Stego-Carrier in the Spatial Domain,” *Symmetry (Basel)*, vol. 15, no. 5, p. 1015, May 2023, doi: 10.3390/sym15051015.

[63] Divya A and S. Thenmozhi, “Steganography: Various Techniques In Spatial and Transform Domain,” *International Journal of Advanced Scientific Research and Management*, vol. 1, no. 3, 2016, [Online]. Available: www.ijasrm.com

[64] W. J. Chen, C. C. Chang, and T. H. N. Le, “High payload steganography mechanism using hybrid edge detector,” *Expert Syst Appl*, vol. 37, no. 4, pp. 3292–3301, Apr. 2010, doi: 10.1016/J.ESWA.2009.09.050.

[65] S. Dhawan and R. Gupta, “High-quality steganography scheme using hybrid edge detector and Vernam algorithm based on hybrid fuzzy neural network,” *Concurr Comput*, vol. 33, no. 24, Dec. 2021, doi: 10.1002/cpe.6448.

[66] “https://www.vlatacominstitute.com/encryption-authentication.”

[67] V. Kumar, S. Sharma, C. Kumar, and A. K. Sahu, “Latest Trends in Deep Learning Techniques for Image Steganography,” *International Journal of Digital Crime and Forensics*, vol. 15, no. 1, pp. 1–14, Feb. 2023, doi: 10.4018/ijdcf.318666.