Steganografija slike

Milošević, Luka

SVEUČILIŠTE SJEVER
SVEUČILIŠNI CENTAR VARAŽDIN

DIPLOMSKI RAD br. 102-MMD-2023

STEGANOGRAFIJA SLIKE

Luka Milošević

Varaždin, Rujan 2024.

SVEUČILIŠTE SJEVER

SVEUČILIŠNI CENTAR VARAŽDIN

Studij Multimedija

DIPLOMSKI RAD br. 102-MMD-2023

STEGANOGRAFIJA SLIKE

Student:
Luka Milošević, 0016123278

Mentor:
izv. prof. dr. sc. Emil Dumić

Varaždin, Rujan 2024.

Sveučilište Sjever
Sveučilišni centar Varaždin
104. brigade 3, HR-42000 Varaždin

UNIVERSITY NORTH

Prijava diplomskog rada

Definiranje teme diplomskog rada i povjerenstva

ODJEL: Odjel za multimediju

STUDIJ: diplomski sveučilišni studij Multimedija

PRISTUPNIK: Milošević Luka | JMBAG: 0016123278

DATUM: 04.09.2023. | KOLEGIJ: Računalni vid

NASLOV RADA: Steganografija slike

NASLOV RADA NA ENGL. JEZIKU: Image steganography

MENTOR: Emil Dumić | ZVANJE: izv.prof.dr.sc.

ČLANOVI POVJERENSTVA:

1. doc. art. dr. sc. Mario Periša - predsjednik
2. izv. prof. art. dr. sc. Robert Geček - član
3. izv. prof. dr. sc. Emil Dumić - mentor
4. doc. dr. sc. Andrija Bernik - zamjenski član
5.

Zadatak diplomskog rada

BROJ: 102-MMD-2023

OPIS

U ovom radu opisat će se algoritmi za steganografiju slike te ispitati neki algoritmi za prikriveno upisivanje informacije (npr. podataka ili slike) u sliku.

Digitalna steganografija može se opisati kao upisivanje prikrivene poruke u digitalni medij, poput teksta, slike, videozapisa, audiozapisa, 3D objekata i drugo, gdje prikrivena poruka ne smije biti vidljiva neautoriziranim korisnicima. U radu će se uglavnom ispitivati upisivanje informacije u sliku. Opisat će se neki klasični algoritmi za ubacivanje informacije u sliku, koji se mogu podijeliti na prostorno bazirane (npr. upisujući informaciju u najmanje značajne bitove, LSB) i frekvencijski bazirane (npr. koristeći DCT, DWT transformacije), koji se mogu koristiti i kao pretkorak prilikom kodiranja. Potom će se opisati noviji algoritmi temeljeni na metodama dubokog učenja za upisivanje informacije poput RoSteALS. Opisat će se mjere usporedbe slika bez i sa prikrivenom informacijom: objektivne mjere kvalitete slike koje koriste referentnu sliku: MSE, PSNR, SSIM, MS-SSIM; objektivne mjere kvalitete slike bez referentne slike: BRISQUE, NIQE, PIQE; TOPIQ mjera s ili bez referentne slike; histogram; te mjera maksimalnog mogućeg kapaciteta za upisivanje informacije. Opisat će se i različiti mogući načini otkrivanja prikrivene informacije, tj. steganaliza.

U praktičnom dijelu rada će se ispitati neki klasični algoritmi ranije navedeni, kao i noviji algoritmi koristeći neuronske mreže. Kvaliteta stvorenih slika ispitat će se koristeći objektivne mjere kvalitete slike navedene ranije, kao i maksimalni kapacitet upisivanja.

ZADATAK URUČEN: 04.09.2023. | POTPIS MENTORA: Emil Dumić

SVEUČILIŠTE SJEVER

Sveučilište
Sjever

SVEUČILIŠTE
SJEVER

IZJAVA O AUTORSTVU

Završni/diplomski/specijalistički rad isključivo je autorsko djelo studenta koji je isti izradio te student odgovara za istinitost, izvornost i ispravnost teksta rada. U radu se ne smiju koristiti dijelovi tuđih radova (knjiga, članaka, doktorskih disertacija, magistarskih radova, izvora s interneta, i drugih izvora) bez navođenja izvora i autora navedenih radova. Svi dijelovi tuđih radova moraju biti pravilno navedeni i citirani. Dijelovi tuđih radova koji nisu pravilno citirani, smatraju se plagijatom, odnosno nezakonitim prisvajanjem tuđeg znanstvenog ili stručnoga rada. Sukladno navedenom studenti su dužni potpisati izjavu o autorstvu rada.

Ja, LUKA MILOŠEVIĆ *(ime i prezime)* pod punom moralnom, materijalnom i kaznenom odgovornošću, izjavljujem da sam isključivi autor/ica ~~završnog~~/diplomskog/~~specijalističkog~~ (*obrisati nepotrebno*) rada pod naslovom STEGANOGRAFIJA SLIKE *(upisati naslov)* te da u navedenom radu nisu na nedozvoljeni način (bez pravilnog citiranja) korišteni dijelovi tuđih radova.

Student/ica:
(upisati ime i prezime)

LUKA MILOŠEVIĆ

(vlastoručni potpis)

Luka Milošević

Sukladno članku 58., 59. i 61. Zakona o visokom obrazovanju i znanstvenoj djelatnosti završne/diplomske/specijalističke radove sveučilišta su dužna objaviti u roku od 30 dana od dana obrane na nacionalnom repozitoriju odnosno repozitoriju visokog učilišta.

Sukladno članku 111. Zakona o autorskom pravu i srodnim pravima student se ne može protiviti da se njegov završni rad stvoren na bilo kojem studiju na visokom učilištu učini dostupnim javnosti na odgovarajućoj javnoj mrežnoj bazi sveučilišne knjižnice, knjižnice sastavnice sveučilišta, knjižnice veleučilišta ili visoke škole i/ili na javnoj mrežnoj bazi završnih radova Nacionalne i sveučilišne knjižnice, sukladno zakonu kojim se uređuje umjetnička djelatnost i visoko obrazovanje.

Sažetak

Ovaj rad predstavlja što je to Steganografija. Definiran je sam pojam steganografije, te kako je ona bila primijenjena u prošlosti. Zašto se danas koristi, te koje su njezine primjene. Predstavljeni su različiti pristupi implementacije steganografije. Pristupi temeljeni na proširenom spektru, na prostornom spektru, adaptivnim tehnikama, na transformaciji i novi način implementacije pod nazivom RoSteALS. Nadalje predstavljena je steganaliza. Definirani je digitalni vodeni žig te je prikazano kako se on razlikuje od digitalne steganografije. Također su definirane objektivne mjere kvalitete slike koje se dijele na koje koriste referentnu sliku, koje koriste značajke referentne slike i one koje ne koriste referentnu sliku. Rad također pokriva dva zadatka. Prvi je bio usporedba LSB, LPS i PVD alata koji implementiraju steganografiju umetanja tekstualne poruke unutar slike. Drugi zadatak je bio usporedba RoSteALS, DCT i LSB alata gdje je poruka bila veličine osam znakova. Stego slike bile su ocijenjene uz pomoć objektivnih mjera za kvalitetu slike koja su opisana u radu.

Popis korištenih kratica

HVS	**Human Visual System**
HSV	**hue, saturation, value**
PN	**pseudonoise**
PVD	**Pixel Value Differencing**
LSB	**Least Significant Bit**
EMD	**Exploiting Modification Direction**
DWT	**Discrete Wavelet Transform**
DCT	**Discrete Cosine Transform**
DFT	**Discrete Fourier Transform**
IWT	**Integer Wavelet Transform**
CWT	**Complex wavelet transform**
JPEG	**Joint Photographic Experts Group**
SPAM	**subctractive pixel adjacency matrix**
SRM	**spatial rich model**
DCTR	**discrete cosine transform residual**
SDSS	**spatial domain steganalytic systems**
FDSS	**frequency domain steganalytic systems**
IQA	**image quality measure**
RS	**regular-singular**
PoV	**pairs of values**
VSS	**visual steganalytic system**
FR	**full-reference**
NR	**no-reference**
SVM	**support vector machines**

QKD	**Quantum key distribution**
QECC	**quantum error-correcting code**
MSE	**Mean Square Error**
PSNR	**Peak Signal to Noise Ratio**
FSIM	**Feature Similarity Indexing Method**
SSIM	**Structural SIMilarity Index**
RMSE	**Root-Mean-Square Deviation**
MSD	**Mean Squared Deviation**
NCC	**Normalized cross correlation**
UQI	**universal image quality index**
BRISQUE	**Blind/Reference less Image Spatial Quality Evaluator**
NIQE	**Naturalness Image Quality Evaluat**
PIQE	**Perception based Image Quality Evaluator**
GM	**gradient magnitude**
CFANet	**coarse-to-fine network**

Sadržaj

1. Uvod

Za početak potrebno je predstaviti samo značenje riječi steganografija te prikazati njezine početke u ljudskoj povijesti. Hassaballah [1] predstavlja kako se steganografija koristi od davnina i vuče korijene iz drevnih civilizacija (npr. Grčka, Egipat). Riječ steganografija složena je od dvije grčke riječi: Steganos što znači "pokriven" i Graphia što znači "pisanje". Primjer rane steganografije nalazimo u 5. stoljeću, gdje je Histajak robu obrijao glavu i tetovirao mu poruku na tjeme, a rob je poslan s porukom nakon što mu je kosa ponovno narasla. Nadalje, Cardan (1501.–1576.) je replicirao Kinesku drevnu metodu tajnog pisanja, gdje se papirnata maska s rupama dijeli između dvije strane, ta maska se stavlja preko praznog papira, a pošiljatelj piše tajnu poruku kroz rupe, zatim skida masku i ispunjava praznine kako bi prikazao poruku kao bezazlen tekst. Nula šifre (engl. *null ciphers*), mikrotočke, i metode nevidljive tinte također su bile vrlo popularne steganografske metode tijekom Drugog svjetskog rata. Ove metode skrivanja tajnih poruka korištene su u različitim oblicima tisućama godina.

Steganografija djeluje na principu čuvanja tajnosti. Na primjer, slikovna datoteka može se mijenjati tako suptilno da su promjene neprimjetne ljudskom oku, a ipak ugrađenu poruku mogu izdvojiti oni koji je znaju potražiti. Slično tome, audio datoteke i video isječci mogu sadržavati skrivene podatke bez utjecaja na njihovu kvalitetu ili upotrebljivost. Ova suptilnost čini steganografiju moćnim alatom u raznim područjima, uključujući kibernetičku sigurnost, upravljanje digitalnim pravima, pa čak i umjetničko izražavanje.

Razumijevanje steganografije ne uključuje samo tehnike koje se koriste za skrivanje i vraćanje informacija, već i etičke i pravne implikacije povezane s njezinom upotrebom. Iako nudi legitimne prednosti u zaštiti privatnosti i osiguravanju digitalnih komunikacija, također predstavlja rizik ako se koristi u nedopuštene svrhe. Kako tehnologija napreduje, praksa steganografije vjerojatno će se razvijati, predstavljajući nove mogućnosti i izazove u potrazi za sigurnom i neprimjetljivom komunikacijom.

2. Steganografija

U današnje vrijeme steganografija se također koristi, a Hassaballah ju je definirao kao umjetnost skrivanja tajnih poruka iza digitalnih medija nevinog izgleda. Nadalje steganografija je umjetnost prikrivene komunikacije gdje je postojanje poruke tajno. Drugi istraživači definiraju digitalnu steganografiju kao zadatak skrivanja digitalnih informacija u prikrivenim kanalima na takav način da se neke informacije mogu sakriti i da se spriječi otkrivanje tih skrivenih informacija. Steganografija se može definirati kao znanost o prikrivanju poruke u nositelju (eng. *host*) s namjerom da se ne povuče sumnja o kontekst na koji se način poruka prenosi. Općenito, postoji nekoliko vrsta digitalnih medija koji se mogu koristiti za skrivanje tajnih informacija kao što su slika, video, audio, tekst, 3D modeli. Ovi digitalni mediji imaju različite karakteristike za umetanje tajnih informacija, gdje najbolji medij za ugrađivanje tajnih informacija mora imati dvije značajke: medij bi trebao biti popularan, a izmjena u tom nositelju poruke bi trebala biti nevidljiva bilo kojoj neovlaštenoj trećoj strani. Odnosno, trebalo bi biti nemoguće zapaziti poruku i uopće postojanje poruke u tom medijskom objektu.

Hassaballah predstavlja da je u literaturi digitalne steganografije slika najpopularniji medij koji je privukao steganografe. Razlozi za ovu popularnost su obilje digitalnih slika na Internetu, slika pruža dovoljno redundantnosti za manipuliranje steganografijom, a HVS značajke ljudskog vizualnog sustava (eng. *Human Visual System*) motiviraju istraživače da iskoriste te značajke u sustavima za skrivanje podataka. Iako su slike popularne u steganografiji, drugi mediji kao što je tekst također su izbor za izvođenje steganografije. Postoji nekoliko aplikacija za skrivanje podataka vezanih uz tekst. Na primjer, u kontekstu zaštite autorskih prava, tekstualni vodeni žig se može koristiti, a steganografija se može koristiti za dodavanje kriptografskog sažetka (eng. *hash*) u tekstualnu datoteku za zaštitu od izmjena. Nažalost, nedostatak redundancije u tekstovima u usporedbi s digitalnim slikama čini steganografiju, korištenjem teksta, netrivijalnim izazovom. Obično je svaki pristup steganografiji slike sastavljen od dva algoritma:

- jedan za ugrađivanje, što je zapravo postupak ili algoritam koji se koristi za skrivanje tajne poruke unutar bazne slike,
- a drugi, algoritam za izdvajanje, koji se jednostavno može koristiti kako bi obnovio (vratio) tajnu poruku sa (iz) stego slike.

Tako stego slika, kao konačna izlazna slika, sadrži tajne podatke.

2.1. Primjena steganografije

Hassaballah navodi kako se steganografija može koristiti kad god se želi prikriti neki podatak. Postoji mnogo razloga za skrivanje podataka, ali svi u srži žele spriječi neovlaštenim pojedincima da dođu do podataka ili da postanu svjesni postojanja poruke. Steganografija se može vrlo učinkovito koristiti u automatskom praćenju radijske reklame ili glazbe. Automatizirani sustav može se postaviti da prati određene stego poruke.

Nadalje, Hassaballah predstavlja da suvremena računalna i mrežna tehnologija omogućuje pojedincima osnovne primjene steganografije vezane uz tajne komunikacije. Grupe i tvrtke mogu imati pristup web stranici koja može sadržavati tajne informacije namijenjene drugoj strani. Svatko može preuzeti web stranicu; međutim, skrivene informacije su nevidljive i ne privlače pozornost. Neke moderne primjene steganografije se koriste u medicinskim slikovnim sustavima, gdje se odvajanje smatra nužnim za povjerljivost između slikovnih podataka pacijenata ili sekvenci DNK i njihovih naslova, kao što su Liječnik, ime pacijenta, adresa i drugi podaci. Korištenje steganografije može pomoći kako bi se izbjeglo curenje osobnih podataka pacijenata u neovlaštene ruke.

Hassaballah predstavlja kako japanska tvrtka Fujitsu, nadahnuta idejom da se steganografija može ugraditi kao dio normalnog procesa ispisa, razvija tehnologiju za kodiranje podatka u ispisanoj slici koji su nevidljivi ljudskom oku i kasnije se mogu dohvatiti pomoću kamere mobilnih telefona. Proces traje manje od jedne sekunde jer ugrađeni podaci imaju samo 12 bajtova. Stoga korisnici mogu koristiti svoje mobitele za snimanje kodiranih podataka. Osnovna ideja je transformacija sheme boja slike prije ispisa u njezinu komponentu nijanse, zasićenosti i vrijednosti (HSV – hue, saturation, value), zatim njezino ugrađivanje u domenu nijanse na koju ljudske oči nisu osjetljive. Mobilne kamere mogu vidjeti i dekodirati kodirane podatke. Postoji nekoliko drugih područja gdje se steganografiju može primijeniti za tajnu komunikaciju, a to su:

- Obavještajne usluge ili intelektualno vlasništvo.
- Osiguranje multimodalnih biometrijskih podataka.
- Korporacije s poslovnim tajnama koje treba zaštititi.
- Vlade su tvrdile da kriminalci mogu koristiti steganografiju za komunikaciju. Dakle, može postati ograničeno zakonom.
- Vojna i obrambena komunikacija.

Nadalje, u poslovnom svijetu steganografija se može koristiti za skrivanje tajne kemijske formule ili planova za nove izume. Također se može koristiti za korporativnu špijunažu slanjem poslovnih tajni. Također, može se koristiti u nekomercijalnom sektoru za skrivanje informacija koje netko želi ostaviti privatnim.

2.2. Izazovi steganografije

Hassaballah navodi kako se pri tehnikama steganografije bazna slika koristi za umetanje tajne informacije u nju bez promjene njezinih svojstava. Rezultirajuća slika naziva se stego slika. Stego slika mora biti bez vidljivih promjena, tako da bilo koja treća strana ne može otkriti te promjene i želi rukovati tom slikom kao normalnom slikom, dok tajni podaci preneseni putem ove slike ostaju sigurni. Bilo koji steganografski sustav koji koristi sliku kao medij, suočava se sa sljedećim velikim izazovima:

- Veličina nosivosti: kako se može postići maksimalni kapacitet ugradnje? Steganografija ima za cilj osigurati dovoljno veliki kapacitet ugradnje. Čim je više digitalnog prostora dostupno poruka može biti veća ili može biti kompleksnije kriptirana. Zahtjevi za veću nosivost i sigurnost komunikacije često su kontradiktorne.
- Kvaliteta vizualne slike: koliko je stego slika perceptivno identična baznoj sliici? Stoga bi tehnike steganografije slike trebale proizvesti visoku neprimjetnost stego slika. Čim je kvaliteta bazne slike veća, čovjek lakše može uočiti promjenu koja nastaje dodavanjem tajne poruke, što ne znači da bi cilj trebao biti slika niže kvalitete, jer se time gubi smisao koji bazna slika želi prenesti, te promatraču može dati do znanja da je došlo do izmjene slike.
- Robusnost: kako se stego slika može oduprijeti različitim napadima detekcije steganalize? Stego slika trebala bi pružiti otpornost na tehnike obrade slike kao što je kompresija, obrezivanje, promjena veličine i tako dalje; to jest, kada se bilo koja od ovih tehnika steganalize izvodi na stego slici, tajne informacije ne bi trebale biti potpune uništene.

Hassaballah navodi kako bi zbog toga idealna steganografska metoda morala istovremeno ispunjavati gornje ciljeve kao što su visok kapacitet, dobra vizualna kvaliteta slike i neprimjetnost. Ali najčešće, steganografski pristupi s velikim korisnim opterećenjem uvode artefakte izobličenja u stego slike koji su osjetljivi na stega-analizu. Steganografske metode koje imaju dobru vizualnu kvalitetu slike, kao suprotnost, imaju mali kapacitet nosivosti, odnosno tajna poruka mora zauzimati manje digitalni prostora. Prema tome, kako postići istodobno visoku nosivost, dobru vizualnu kvalitetu i neprimjetnost pravi je izazov za istraživanje zbog proturječja među njima. Cilj je naći optimalnu ravnotežu između ta tri zahtjeva.

2.3. Pristupi implementacije steganografije

Potrebno je razmotriti različite pristupe primjene steganografije nad slikovnim medijem, kako funkcioniraju te koje su im razlike. Hassaballah navodi kako na temelju prirode ugradnje postoje različiti steganografske tehnike dostupne nad slikovnim medijima koji se dijele na prostorne, tehnike korištenjem proširenog spektra, tehnike korištenjem transformacija i adaptivne

tehnike. Pri tehnikama baziranim na proširenom spektru tajni podaci se množe sa slijedom pseudo-šuma (eng. *pseudonoise*, PN), a zatim se moduliraju prije ugrađivanja u glavni objekt. Tehnike prostorne ili slikovne domene koriste metode operacija nad bitovima koje primjenjuju umetanje bitova i manipulaciju šuma pomoću jednostavnih mehanizama, dok je domena transformacije definirana kao transformacija slike u njenu frekvencijsku reprezentaciju nakon čega slijedi promjena spektralne komponente slike. Adaptivan pristup može se uvesti u sheme ugrađivanja podataka na nekoliko načina kao što je odabir ciljanih piksela bazne slike, prirodu promjene koju treba izvršiti, te broj bitova koji su ugrađeni u piksel. Nadalje će biti predstavljen svaki pristup zasebno.

2.3.1. Pristup temeljen na proširenom spektru

Hassaballah predstavlja kako ti sustavi skrivaju i vraćaju poruku značajne duljine unutar digitalnih slika zadržavajući izvornu veličinu slike i dinamički raspon. Ugrađena tajna poruka može se vratiti korištenjem odgovarajućih ključeva bez ikakvog znanja o izvornoj slici. Poruka ugrađena ovom metodom može biti u obliku teksta, slike ili bilo kojeg drugog digitalnog signala. Primjene za takve sheme uključuju titlove unutar same slike ili videozapisa, prikrivene komunikacije, zaštitu od neovlaštenog mijenjanja slike, autentifikaciju ugrađenu kontrolu i revizijsko praćenje.

2.3.2. Pristup temeljen na prostornoj domeni

Hassaballah navodi kako su sheme prostorne domene više prilagođene ljudskom vizualnom sustavu (HVS) i mogu pružati veći kapacitet ugradnje od shema transformacije domene s prihvatljivom kvalitetom slike. To je najjednostavniji način ugrađivanja podataka u digitalne slike u kojem se vrijednosti piksela mogu izravno modificirati za kodiranje bitova tajne poruke. Glavne steganografske sheme koje potpadaju pod tehniku prostorne domene uključuju razliku vrijednosti piksela (eng. *Pixel Value Differencing*, PVD), zamjenu najmanje značajnog bita (eng. *Least Significant Bit substitution*, LSB), iskorištavanje smjera promjene (eng. *Exploiting Modification Direction*, EMD), sheme zasnovane na kvantizaciji, modifikaciji razine sive boje, više bitovnih ravnina i steganografske sheme temeljene na paletama boja.

Modifikacija razine sive boje. Vrijednosti razine sivih piksela se provjeravaju i uspoređuju s protokom bitova koji trebaju biti mapirani na slici. Prvo, vrijednosti razine sive odabranih piksela unutar kojih pohranjujemo poruku se postavljaju na parne vrijednosti, odnosno neparne vrijednosti se povećavaju za jedan. Kada svi odabrani pikseli imaju parnu razinu sive boje,

uspoređuju se s tokom bitova koji se mora mapirati. Glavni bit iz toka bitova se uspoređuje s inicijalno odabranim pikselom. Kada je primarni bit paran (tj. nula), primarni piksel se ne mijenja budući da svi odabrani pikseli imaju parnu vrijednost razine sive. Kad god je bit neparan (tj. jedan), vrijednost razine sivih piksela smanjuje se za jedan. Ovo se radi za sve bitove u toku bitova, a svaki pojedini bit se preslikava posljedičnom promjenom vrijednosti razine sive. Ova metoda nam pomaže da pružimo kvalitetnije stego slike u usporedbi s drugim metodama.

Razlika vrijednosti piksela (PVD). Ova tehnika dijeli banzu sliku na blokove koji se ne preklapaju i koji se sastoje od dva povezana piksela. Skriva podatke mijenjajući razliku između ta dva piksela. Razlika piksela određuje kapacitet skrivanja ove tehnike. Na primjer, ako je odabrano područje s rubom, razlika je velika između povezanih piksela, dok je u glatkim područjima razlika mala. Stoga je najbolji izbor odabrati područja s rubom za ugradnju tajne poruka koja ima veći kapacitet ugradnje.

Zamjena bitova najmanjeg značaja (LSB). Ova metoda je jedna od temeljnih i konvencionalnih metode koje mogu sakriti velike tajne informacije u baznu sliku. Ova tehnika uključuje zamjenu svih LSB bitova piksela unutar bazne slike tajnim bitovima. Nadalje, ugrađuje tajne bitove fiksne duljine u iste LSB-ove fiksne duljine piksela. Iako je ova tehnika jednostavna, općenito uzrokuje primjetna izobličenja kada broj ugrađenih bitova za svaki piksel premaši četiri.

Iskorištavanje smjera promjene (EMD). Ova metoda koristi n piksela kao grupu tako da može uspostaviti skrivene znamenke u (2n + 1)-narnom sustavu za smanjenje izobličenja stego slike. Nadalje, ugrađivanje zahtijeva smanjenje ili povećanje vrijednosti određenog piksela unutar skupa. Za ovu metodu potrebno je izračunati vrijednost n prije ugrađivanja. Najveća kvaliteta slike postiže se kada je vrijednost n jednaka 2, gdje je ugrađivanje predstavljeno samo jednom tajnom znamenkom unutar svaka dva piksela.

Pristupi temeljeni na kvantizaciji. Steganografski sustav ove kategorije koristi bilo koju vrstu sustava kodiranja za skrivanje tajnih bitova podataka. Sustav kodiranja je bilo koji standardni kompresijski kodek kao što je JPEG, vektorska kvantizacija i tako dalje. Tajni podaci podijeljeni su u male dijelove podataka, a ti su mali dijelovi podataka ugrađeni zajedno s kodiranom baznom slikom. Ovi se sustavi koriste za povećanje kapaciteta uz smanjenje izobličenja stego slike. Nažalost, ovi sustavi nisu dovoljni da se nose s geometrijskim napadima i steganalizom.

Pristupi koji se temelje na više bitovnih ravnina. Ova metoda je uvedene kao proširenje metode LSB supstitucije, gdje se bitovne ravnine koriste za skrivanje bitova tajnih podataka. Obično se stego pristupi bitne ravnine koriste zajedno s drugim metodama za poboljšanje performansi cjelokupnog sustava. Prošireno kodiranje više bitovnih ravnina donosi dvije

prednosti: može ugraditi više tajnih bitova nego 8-bitne LSB tehnike, a stupanj slučajnosti ugrađivanja je visok.

2.3.3. Pristup temeljen na adaptivnim tehnikama

Hassaballah navodi kako je adaptivna steganografija poznata kao ugrađivanje koristeći statistiku (eng. *statistics-aware embedding*) ili maskiranje (eng. *masking*). Drugim riječima, statistika bazne slike koristi se za ugrađivanje tajnih informacija bez mijenjanja njihovih svojstava. Ovo ugrađivanje može se izvršiti nasumičnim adaptivnim odabirom piksela prema baznoj slici i odabirom piksela u bloku s velikom lokalnom standardnom devijacijom. Pikseli koji nose tajne bitove odabiru se adaptivno ovisno o sadržaju bazne slike.

2.3.4. Pristup temeljeni na transformaciji

Hassaballah predstavlja kako se nekoliko metoda domene transformacije koristi u polju steganografije, a najpopularnije sheme uključuju: diskretnu valićnu transformaciju (eng. *Discrete Wavelet Transform*, DWT), diskretnu kosinusnu transformaciju (eng. *Discrete Cosine Transform*, DCT), diskretnu Fourierovu transformaciju (eng. *Discrete Fourier Transform*, DFT), cjelobrojnu valićnu transformaciju (eng. *Integer Wavelet Transform*, IWT) i kompleksnu valićnu transformaciju (eng. *Complex wavelet transform*, CWT). U osnovi, ova vrsta tehnike je robusnija s obzirom na uobičajene operacije obrade slike i kompresiju s gubitkom. Steganografija temeljena na DCT-u prikladno se primjenjuje u standardima kompresije Joint Photographic Experts Group (JPEG), dok se steganografija temeljena na DWT-u prikladno primjenjuje u standardima kompresije Joint Photographic Experts Group 2000 (JPEG2000).

2.3.5. RoSteALS

Bui i sur. [33] predstavljaju RoSteALS, kao jednostavnu, ali učinkovitu steganografsku tehniku koja koristi 'besplatno znanje' iz zaključanog (zamrznutog) autoenkodera. Tehnički doprinosi RoSteALS su trostruki:

1. **Latentno steganografsko umetanje.** Predlaže se nova metoda za umetanja tajne poruke izravno u latentni kod zaključanog autoenkodera, omogućavajući robusno označavanje vodenim žigom uz ograničeni trening i bez specijalizacije sadržaja. Koder je male

veličine, jednostavan za trening, generalizira daleko izvan podataka za trening i može se prilagoditi najnaprednijim autoenkoderima do sada.

2. **Robustan tajni oporavak.** Pokazalo se da takav pristup tajnom umetanju može izdržati ozbiljne promjene slike, što je ključno za slučaj upotrebe postojanih identifikatora putem redistribucije sadržaja na internetu.
3. **Steganografija bez omota (eng. *cover-less*).** Pokazuju da se RoSteALS može lako prilagoditi za upotrebu bez omota (tj. gdje se omot sintetizira u hodu za tajno ugrađivanje) i za nove steganografske aplikacije temeljene na tekstu. S RoSteALS-om proširuju ideju steganografije bez omota na latentni prostor autoenkodera, gdje je cilj generirati latentni pomak koji može jedinstveno predstavljati tajnu. S obzirom na autoenkoder, naučeni pomak može se dodati bilo kojem slučajnom latentnom kodu (generiranom pomoću slike ili teksta pomoću difuzijskog modela) tog autoenkodera da bi se proizvela stego slika.

2.4. Analiza sigurnosti

Robusnost steganografskih metoda nije trivijalan ili jednostavan zadatak zbog nekoliko čimbenika. Nadalje će biti predstavljeno nekoliko tradicionalnih metoda steganalize.

Kao prvu metodu Hassaballah predstavlja alizu histograma razlike piksela. Histogram je mjera broja pojavljivanja piksela s obzirom na određenu vrijednost piksela. Svaka vrijednost piksela na baznoj slici mijenja se tijekom procesa ugrađivanja, a te se promjene mogu koristiti za otkrivanje steganografije. Stoga mala razlika histograma između bazne i njezine stego slike rezultira time da je napadači teže otkrivaju. Histogram razlike piksela može biti potencijalna karakteristika za razotkrivanje skrivene poruke tih poruka pomoću steganografskih metoda temeljenih na PVD-u. Dokazano je da izvorna PVD shema neizbježno uvodi neke neželjene korake u histogramu razlika između dva kontinuirana piksela u svakoj jedinici ugradnje zbog svoje fiksne podjele jedinica ugradnje i svojih fiksnih koraka kvantizacije. Otkrivanjem i analizom takvih izobličenja moguće je procijeniti veličinu skrivene poruke, osobito kada je stopa ugradnje visoka.

Nadalje Hassaballah predstavlja univerzalnu steganalizu. Univerzalna steganaliza je metoda metadetekcije u smislu da se može prilagoditi nakon treninga na baznim i stego slikama za otkrivanje bilo koje steganografske metode bez obzira na domenu ugradnje. Trik je u pronalaženju odgovarajućeg skupa osjetljivih statističkih veličina (vektor značajki) s

mogućnostima "razlikovanja". Neuronske mreže, algoritmi klasteriranja i drugi alati mekog računarstva mogu se koristiti za pronalaženje pravih pragova i konstruiranje modela detekcije iz prikupljenih podataka. Univerzalna steganaliza je također poznata kao slijepa steganaliza, što je moderan pristup za napad na stego slike bez ikakvog prethodnog znanja o vrsti korištenog steganografskog algoritma. Ovi slijepi detektori izrađeni su korištenjem strojnog učenja kao što je korištenje klasifikatora treniranog na izdvojenim značajkama s baznih i stego slika za prepoznavanje razlika između baznih stego značajki. Postoje mnoge značajke steganalize koje su prikladne za detekciju prostorne i JPEG steganografije. Među skupovima značajki prostorne domene, predložena je subtraktivna matrica susjedstva piksela drugog reda (eng. *subctractive pixel adjacency matrix,* SPAM) i prostorno obogaćeni model (eng. *spatial rich model,* SRM). U skup značajki nazvan rezidual diskretne kosinusne transformacije (eng. *discrete cosine transform residual,* DCTR) predložen je za steganalizu JPEG slika gdje se točnost detekcije mjeri korištenjem minimalne ukupne vjerojatnosti pogreške pod jednakim prethodnim vrijednostima i dan je izrazom

$$P_E = \min_{P_{FA}} \frac{1}{2}(P_{FA} + P_{MD}) \tag{2.1}$$

gdje su P_{FA} i P_{MD} vjerojatnosti lažnog alarma i propuštene detekcije.

Sljedeće, i zadnja metode koje Hassaballah predstavlja su redovna i singularna steganaliza. Nije lako otkriti i kvantificirati slab odnos između nekih pseudoslučajnih komponenti stego slike i bazne slike. Pretpostavimo da je bazna slika s M × N piksela i s vrijednostima piksela iz skupa P = {0,..., 255} za 8-bitnu sliku u sivim tonovima. Prostorna korelacija se bilježi pomoću diskriminacijske funkcije f koja dodjeljuje realni broj f $(x_1,..., x_n) \in$ R skupini piksela G = $(x_1,..., x_n)$. Funkcija f je definirana kao jednadžba 2.2:

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{n-1}(|x_{i+1} - x_i|) \tag{2.2}$$

koja mjeri glatkoću G: G s većim šumom ima veću vrijednost diskriminacijske funkcije f. U LSB algoritmu za ugradnju, kako se šum povećava na slici, vrijednost f će se povećati nakon ugradnje. U tipičnim slikama, permutacija grupe G češće će dovesti do povećanja diskriminacijske funkcije f umjesto smanjenja. Označimo relativni broj regularnih grupa za nenegativnu masku m kao R_m (u postocima svih grupa), a neka je S_m relativni broj singularnih grupa. Vrijednost R_m približno je jednaka onoj od R_{-m}, a isto bi trebalo vrijediti za S_m i S_{-m} u

slučaju pretpostavke metode steganalize za baznu sliku bez upisivanja tajne poruke LSB ugrađivanjem:

$$R_m \cong R_{-m} \ i \ S_m \cong S_{-m} \tag{2.3}$$

Nakon upisivanja, razlika Rm i Sm bi trebala biti blizu 0, dok razlika R-m i S-m raste s porastom duljne ugrađene poruke. Pomoću tih pretpostavki, RS-steganaliza može procijeniti duljinu upisane poruke računajući kvadratnu jednadžbu (ovisnu o Rm, Sm, R-m i S-m). Glavna ideja RS-steganalize iskorištava korelaciju slika u prostornoj domeni i primjenjiva je na većinu komercijalnih steganografskih softverskih proizvoda. Također, principi RS-steganalize mogu se proširiti na varijante LSB ugradnje u indekse paletnih slika i kvantizirane DCT koeficijente u JPEG datotekama.

2.5. Steganaliza

Shih [2] navodi kako se poput digitalnog vodenog žiga, digitalni steganalitički sustavi mogu kategorizirati u dvije klase: steganalitički sustavi prostorne domene (eng. *spatial domain steganalytic systems,* SDSS) i steganalitički sustavi frekvencijske domene (eng. *frequency domain steganalytic systems,* FDSS). SDSS-ovi usvojeni su za provjeru komprimiranih slika bez gubitaka analizom statističkih značajki u prostornoj domeni. Najjednostavniji SDSS je LSB supstitucija. Ova tehnika smatra LSB nasumičnim šumom, tako da njegova modifikacija neće utjecati na cjelokupnu vizualizaciju slike. Za slike s kompresijom s gubitkom kao što su JPEG, FDSS se koriste za analizu statističkih značajki u frekvencijskoj domeni. Postoje dva SDSS-a temeljena na vizualnim i χ-kvadrat napadima. Vizualni napadi koriste ljudski vid za pregled stego slika provjeravajući njihove LSB ravnine. χ-kvadrat napadi mogu automatski detektirati specifične karakteristike generirane LSB steganografskom tehnikom. Avcibas i sur. [8] su bili predložili mjeru kvalitete slike (eng. *image quality measure*, IQM), koja se temelji na hipotezi da steganografski sustavi ostavljaju statističke dokaze koji se mogu iskoristiti za detekciju korištenjem multivarijatne regresijske analize. Fridrich i sur. [3] predstavili su FDSS za otkrivanje JPEG stego slika analizirajući njihov DCT s izrezanim slikama.

U srži Shih predstavlja kako je Stegaanaliza proces otkrivanja steganografije. U osnovi, postoje dvije metode otkrivanja modificiranih datoteka. Jedna se zove vizualna analiza, koja uključuje usporedbu sumnjive datoteke s izvornom kopijom. Namjerava otkriti prisutnost tajne komunikacije pregledom, bilo očima ili uz pomoć računalnog sustava, tipično rastavljajući sliku na bitovne ravnine. Iako je ova metoda vrlo jednostavna, nije vrlo učinkovita; većinu vremena

izvorna kopija nije dostupna. Drugi se zove statistička analiza, koja otkriva promjene u uzorcima piksela i frekvencijskoj distribuciji intenziteta. Može otkriti je li slika modificirana provjerom da li odstupaju njezina statistička svojstva od norme. Stoga namjerava pronaći čak i male promjene u statističkom ponašanju uzrokovane steganografskim ugrađivanjem.

Shih navodi kako se steganalitičke tehnike moraju često ažurirati i kontinuirano razvijati kako bi se borile protiv novih i sofisticiranijih steganografskih metoda. Čak ni američke agencije za provođenje zakona nemaju dostupne steganografske smjernice. Međutim, postoje određena pravila koja istraživači usvajaju kada traže naznake koje bi mogle sugerirati korištenje steganografije. To uključuje tehničke mogućnosti vlasnika računala, softverske tragove, programske datoteke, multimedijske datoteke i vrstu zločina.

Nadalje ću predstaviti neke od navedenih pojmova za bolje shvaćanje teme. Predstavit će se sustave vizualne steganalize, sustave bazirane na IQM-u, strategije učenja i FDSS.

2.5.1. Statistička svojstva slike

Za bolje shvaćanje metoda analize valja razmotriti koja su statistička svojstva slike. Shih definira kako postoje statistička svojstva za ljudsku percepciju prirodnih slika. Valna duljina svjetlosti stvara vizualne podražaje. Kada se valna duljina dinamički mijenja, percipirana boja varira od crvene, narančaste, žute, zelene, plave do ljubičaste. Ljudska vizualna osjetljivost usko je povezana s bojom; na primjer, ljudi su osjetljiviji na zelenu nego na crvenu i plavu. Sastav boje možemo podijeliti na tri komponente: svjetlinu, nijansu i zasićenost. Prilagodba oka na određenu nijansu iskrivljuje percepciju drugih nijansi; na primjer, siva nakon zelene ili na zelenoj pozadini izgleda ljubičasto. Stoga je potrebno imati na umu da će se manje promjene na zelenom dijelu slike puno brže uočiti od strane čovjeka promatrača za razliku od promjena na plavom dijelu. To nužno ne mora biti isto kao kada računalni sustav analizira tu istu sliku.

Shih navodi kako su istraživači u statističkoj steganalizi uložili trud u unapređenje svojih metoda zbog sve većeg očuvanja statistike prvog reda u steganografiji kako bi se izbjeglo otkrivanje. Enkripcija skrivene poruke također otežava otkrivanje jer šifrirani podaci općenito imaju visok stupanj slučajnosti, a jedinice i nule postoje s jednakom vjerojatnošću. Osim detekcije, vraćanje skrivenih poruka čini se kompliciranim problemom, budući da zahtijeva poznavanje kripto-algoritma ili ključa za šifriranje. Umetanje LSB-a u sliku temeljenu na paleti proizvest će veliku količinu dvostrukih boja. Neke identične (ili gotovo identične) boje mogu se pojaviti dva puta u paleti. Neke steganografske tehnike koje preuređuju redoslijed palete boja za skrivanje poruka mogu uzrokovati strukturne promjene, koje će generirati potpis steganografskog algoritma.

Shih predstavlja kako slične boje imaju tendenciju grupiranja zajedno. Promjena LSB-a piksela boje ne degradira cjelokupnu vizualnu percepciju. Na primjer, u LSB steganografiji. Postoje četiri druge steganalitičke metode, uključujući metodu regular-singular (RS), metodu parova vrijednosti, metodu analize parova i metodu parova uzoraka, koje iskorištavaju prednosti statističkih promjena modeliranjem promjena u određenim vrijednostima kao funkciji postotka piksela s ugrađenom steganografijom. Nadalje ću navesti metode koje je Shih predstavio.

RS metodu razvili su Fridrich i sur. [3]. Opisanu ranije.

Metodu parova vrijednosti razvili su Pfitzman i Westfeld [4]. Oni koriste fiksni skup parova vrijednosti (eng. *pairs of values*, PoV) za preokret za ugrađivanje bitova poruke. Oni konstruiraju PoV-ove pomoću kvantiziranih DCT koeficijenata, vrijednosti piksela ili indeksa palete i raširе dvije vrijednosti iz svakog para nepravilno na baznoj slici prije ugrađivanja poruke. Pojavljivanja vrijednosti u svakom paru su sklona biti jednaka nakon ugrađivanja. Zbroj pojavljivanja para boja na slici ostaje isti ako jednu vrijednost zamijenimo drugom. Ovaj se koncept koristi u izradi statističkog chi-square testa.

Metodu analize parova razvili su Fridrich i sur [5]. Može detektirati steganografiju s razrijeđenim promjenama koje su ravnomjerno raspoređene po cijelom mediju nositelja. Također može procijeniti duljinu ugrađene poruke. Parovi boja koji se izmjenjuju tijekom LSB ugradnje odgovaraju prethodnom rasporedu palete pomoću LSB steganografije.

Metodu parova uzoraka razvili su Dumitrescu i sur. [6]. Slika je predstavljena kao skup parova uzoraka, koji su podijeljeni u sub-multiskupove prema razlici između vrijednosti piksela i vrijednosti nakon LSB ugradnje. Oni pretpostavljaju da je vjerojatnost da parovi uzoraka imaju veliku parnu komponentu jednaka onoj koja ima veliku neparnu komponentu za prirodne slike. Stoga točnost njihove metode ovisi o točnosti ove pretpostavke. Oni koriste automate stanja za statističko mjerenje kardinaliteta od tragova multiskupova prije i poslije LSB ugradnje.

Shih navodi kako steganografske tehnike općenito modificiraju statistička svojstva nositelja; duža skrivena poruka izmijenit će nositelja više nego kraća. Statistička analiza se koristi za otkrivanje skrivenih poruka, posebno u slijepoj steganografiji. Statističkom analizom slika može se utvrditi odstupaju li njihova svojstva od očekivane norme. To uključuje srednje vrijednosti, varijance i χ-kvadrat testove.

2.5.2. Sustavi vizualne steganalize

Kessler [7] definira strategije steganografije kako obično slijede metodu koju koristi algoritam steganografije. Jednostavan način je vizualni pregled nositelja i medija za steganografiju. Mnoge jednostavne steganografske tehnike ugrađuju tajne poruke u prostornu

domenu i odabiru bitove poruke u nositelja neovisno o njegovom sadržaju. Većina steganografskih sustava ugrađuje bitove poruke na sekvencijalni ili pseudoslučajni način. Ako slika sadrži određena povezana područja jednolične boje ili zasićene boje (tj. 0 ili 255), možemo upotrijebiti vizualni pregled kako bismo pronašli sumnjive artefakte. Ako se artefakti ne pronađu, provodi se inspekcija LSB bitovne ravnine. Westfeld i Pfitzmann predstavili su sistem za vizualnu steganalizu (eng. *visual steganalytic system,* VSS) koji koristi funkciju dodjele zamjene boja koja se naziva vizualni filtar. Ideja je ukloniti sve dijelove slike koji sadrže potencijalnu poruku. Proces filtriranja oslanja se na pretpostavljeni steganografski alat i može napasti steganogram nositelja medija, izdvojiti potencijalne bitove poruke i proizvesti vizualnu ilustraciju.

2.5.3. Sustavi temeljeni na kvaliteti slike

Shih predstavlja kako se kvaliteta slike može karakterizirati korelacijom između zaslona i ljudskog vidnog sustava (eng. *human visual system*, HVS). Širi pojam, iskustvena kvaliteta (eng. *quality of experience*, QoE), definira se kao stupanj zadovoljstva ili smetnje korisnika aplikacijom ili uslugom, a na što utječe i HVS [30]. S pojavom objektivnih ocjena kvalitete slike (eng. *image quality measure,* IQM), cilj nam je smanjiti subjektivna ispitivanja za procjenu kvalitete slike. Računalna analiza kvalitete slike usmjerena je prema razvoju točnog računalnog modela za opisivanje kvalitete slike. Postoje tri vrste: s referentnom slikom (eng. *full-reference*, FR), sa značajkama referentne slike (eng. *reduced-reference*) i bez referentne slike (eng. *no-reference*, NR). IQM s referentnom slikom ima izvornu (tj. neiskrivljenu) sliku dostupnu kao referencu za usporedbu s iskrivljenom slikom. Primjenjuje različite vrste mjerenja udaljenosti za mjerenje njihove bliskosti. IQM bez reference uzima samo iskrivljenu sliku za analizu. Koristi operatore za obradu slike, kao što su detektori rubova, za izračunavanje indeksa kvalitete ili novije metode dubokog učenja..

Shih navodi kako su Avcibas i sur. [8] razvili tehniku temeljenu na IQM-u za steganalizu slika koje su potencijalno bile podvrgnute steganografskim algoritmima, unutar pasivnog i aktivnog upraviteljskog okvira. Oni pretpostavljaju da steganografske sheme ostavljaju statističke dokaze koji se mogu iskoristiti za otkrivanje uz pomoć značajki kvalitete slike i multivarijatne regresijske analize. U tu svrhu identificirane su mjere kvalitete slike, temeljene na tehnikama analize varijance, kao skupovi značajki za razlikovanje baznih slika i stego slika. Klasifikator između baznihslika i stego slika izgrađen je korištenjem multivarijatne regresije na odabranim ocjenama mjera kvalitete i trenira se na temelju procjene izvorne slike. Općenito,

IQM-ove možemo kategorizirati u tri vrste, IQM-ovi temeljeni na udaljenosti piksela, temeljeni na korelaciji i temeljeni na srednjoj kvadratnoj pogrešci.

2.5.4. Strategije učenja

Shih navodi kako postoje mnoge vrste strategija učenja, uključujući statističko učenje, neuronske mreže i strojevi potpornih vektora (eng. *support vector machines, SVM*). SVM je namijenjen za generiranje optimalne razdvajajuće hiperravnine minimiziranjem pogreške generalizacije bez korištenja pretpostavke vjerojatnosti klase kao što su Bayesovi klasifikatori. Hiperravnina SVM-a određena je najinformativnijim instancama podataka, zvanim potporni vektori (eng. *support vectors,* SV). U praksi, ti SV-ovi su podskup cjelokupnih podataka o treningu. Primjenom smanjenja značajki i u ulazu i u prostoru značajki, može se dizajnirati brzi nelinearni SVM bez primjetnog gubitka performansi. Procedura traninga SVM-ova obično zahtijeva ogroman memorijski prostor i značajno vrijeme računanja zbog velikih količina podataka za trening i problema kvadratnog programiranja. Neki su istraživači predložili inkrementalni trening ili aktivno učenje kako bi se skratilo vrijeme treninga. Cilj je odabrati podskup uzoraka za obuku uz očuvanje izvedbe korištenja svih uzoraka. Umjesto učenja iz nasumično odabranih uzoraka, SVM koji aktivno uči ispituje informativne uzorke u svakom inkrementalnom koraku.

Syed i sur. [9] razvili su inkrementalni postupak učenja dijeljenjem skupa podataka o treningu u podskupove. U svakom inkrementalnom koraku, samo SV-ovi se dodaju skupu za trening u sljedećem koraku. Campbell i sur. [10] predložili su strategiju učenja upita iterativnim traženjem oznake uzorka koji je najbliži trenutnoj hiperravnini. Schohn i Cohn [11] predstavili su pohlepnu optimalnu strategiju izračunavanjem vjerojatnosti klase i očekivane pogreške. Jednostavna heuristika koristi se za odabir uzoraka za obuku prema njihovoj blizini u odnosu na razdjelnu hiperravninu. Štoviše, An i sur. [12] su razvili inkrementalni algoritam učenja izdvajanjem početnih uzoraka obuke kao marginalnih vektora dviju klasa, odabirom novih uzoraka prema njihovoj udaljenosti od trenutne hiperravnine i odbacivanjem uzoraka treninga koji ne doprinose ravnini razdvajanja. Nguyen i Smeulders su istaknuli su je prethodna distribucija podataka korisna za aktivno učenje, a novi podaci o treningu odabrani iz uzoraka imaju maksimalan doprinos trenutnoj očekivanoj pogrešci. Većina postojećih metoda aktivnog učenja mjeri blizinu razdvajajuće hiperravnine. Mitra i sur. [13] predstavili su probabilističku strategiju aktivnog učenja koristeći distribuciju određenu trenutnom razdvajajućom hiperravninom i faktorom pouzdanosti. Nažalost, nisu dali kriterije za odabir ispitnih uzoraka. Postoje dva problema u njihovom algoritmu. Prvo, početni uzorci za trening odabiru se

nasumično, što može generirati početnu hiperravninu koja je daleko od optimalnog rješenja. Drugo, korištenje samo SV-ova iz prethodnog skupa treninga može dovesti do lošeg rješenja.

2.5.5. Sustavi frekvencijske domene

Shih predstavlja kako slično vodenom žigu, steganografija može ugraditi skrivene poruke u frekvencijsku domenu koristeći redundanciju. Najjednostavnija metoda je LSB supstitucija. Postoje različite metode mijenjanja koeficijenata frekvencije za smanjenje statističkih izobličenja u procesu ugrađivanja—na primjer, algoritmi F5 i OutGuess. Pfitzmann i Westfeld [14] razvili su F5 algoritam za postizanje robusne JPEG steganografije velikog kapaciteta. Oni ugrađuju poruke modificiranjem DCT koeficijenata. Algoritam F5 ima dvije važne karakteristike; prvo, permutira DCT koeficijente prije ugradnje, i drugo, koristi ugrađivanje matrice. Prva operacija, mijenjanje DCT koeficijenata, ima učinak ravnomjernog širenja promijenjenih koeficijenata po cijeloj slici. Druga operacija je umetanje matrice. Oni koriste ne-DC koeficijente koji su različite od nule i duljinu poruke za izračunavanje prikladnog ugrađivanja matrice koje će smanjiti broj promjena na baznoj slici. Iako algoritam mijenja histogram DCT koeficijenata, oni su potvrdili da su neke karakteristike, kao što je monotonost inkremenata i histograma, zapravo sačuvane.

Fridrich i sur. [15] predstavili su steganalitičku metodu koja otkriva skrivene poruke u JPEG slikama koristeći F5 algoritam. Procjenjuje histogram bazne slike iz stego slike. To se može postići dekomprimiranjem stego slike, obrezivanjem slike za četiri piksela u oba smjera i ponovnim sažimanjem stego slike s istim faktorom kvalitete. OutGuess je steganografski sustav dostupan u UNIX-u. Prva verzija, OutGuess 0.13b, ranjiva je na statističku analizu. Druga verzija, OutGuess 0.2, uključuje očuvanje statističkih svojstava. OutGuess ugrađuje poruku u odabrane DCT koeficijente pomoću generatora pseudoslučajnih brojeva. Generator pseudoslučajnih brojeva i šifra toka stvoreni su korisnički definiranom zaporkom. U osnovi, postoje dva koraka u OutGuessu za umetanje poruke. Prvo detektira redundantne DCT koeficijente s najmanjim učinkom na baznu sliku. Zatim odabire bitove u koje će ugraditi poruku prema dobivenim informacijama.

Shih navodi kako nedavne novinske priče ukazuju na to da teroristi mogu komunicirati tajne informacije jedni drugima koristeći steganografiju, skrivajući poruke u slikama na Internetu. Kako bi analizirali postoje li steganografske poruke na internetu, Provos i Honeyman [16] predstavili su nekoliko alata za dohvaćanje i automatsku analizu internetskih slika. Alturki i Mersereau [17] predložili su kvantiziranje koeficijenata u frekvencijskoj domeni za ugrađivanje tajnih poruka. Oni prvo promjene sliku nasumičnim šifriranjem piksela, što zapravo izbjeljuje frekvencijsku domenu slike i povećava broj koeficijenata transformacije u frekvencijskoj

domeni, čime se povećava kapacitet ugradnje. Frekvencijski koeficijenti se zatim kvantiziraju na parne ili neparne višekratnike veličine koraka kvantizacije kako bi se ugradile jedinice ili nule. Zatim se uzima inverzna Fourierova transformacija i dekodira. Dobivena slika vizualno je neusporediva s izvornom slikom.

2.6. Kvantna steganografija

Za bolje shvaćanje ovog poglavlja potrebno je predstaviti razlike između steganografije i kriptografije. Hassaballah navodi kako u kriptografiji pošiljatelj (Alice) šifrira tajnu poruku korištenjem zajedničkog tajnog ključa, a dobiveni šifrirani tekst se zatim šalje primatelju (Bob) na dekodiranje. Ako prisluškivač (Eve promatra šifrirani tekst, onda ga ne može dekodirati bez tajnog ključa. Međutim, znat će da postoji tajna poruka, budući da Alice Bobu šalje očito brbljanje. Tajnovitost steganografije proizlazi iz prikrivanja činjenice da uopće postoji poruka. U mnogim slučajevima, ako Eve postane svjesna da tajna poruka postoji, tada je može pročitati bez poteškoća.

Nadalje te dvije paradigme također daju različitu ulogu prisluškivaču ili protivniku. U standardnoj kriptografiji pretpostavlja se da prisluškivač djeluje tajno i (možda) nelegitimno. U steganografiji prisluškivač može djelovati otvoreno i često je u poziciji vlasti. Ako je Eve upraviteljica zatvora, onda bi mogla spriječiti tajnu komunikaciju tako da zabrani svu komunikaciju. Ali općenito, ona želi dopustiti određene vrste odobrene komunikacije dok druge zabranjuje. Kriptografija je obrana protiv špijuna, a steganografija, protiv cenzora i tajne policije.

Hassaballah predstavlja kako je kvantna kriptografija naširoko proučavana. Proučavanje kvantne steganografije je, međutim, još uvijek u relativno ranoj fazi. Generalizirajući ideju steganografije kvantna informacija može imati više različitih oblika. Mogla bi se poslati tajna klasična poruka kroz kvantni kanal, skrivena u kvantnom komunikacijskom protokolu. Na sličan način se mogu slati tajne kvantne poruke (tj. kvantna stanja) kroz kvantni kanal. Kvantna steganografija također može uključivati korištenje kvantnih resursa (kao što je isprepletenost, eng. *entanglement*) osim kanala za slanje tajnih klasičnih ili kvantnih poruka. Ove mogućnosti zahtijevaju razvoj novih metoda kodiranja, prikladnih za kvantne komunikacijske kanale, i razumnog pojma za bezazlenu kvantnu poruku.

Curty i sur. [18] predložili su tri različita kvantna steganografska protokola. Međutim, niti jedan od ovih protokola nije se bavio pitanjem priopćavanja bezazlene poruke preko klasičnog kanala sa šumom ili općeg kvantnog kanala, niti je dao stope potrošnje ključa. Natori [19] je pružio jednostavan tretman kvantne steganografije koja je modifikacija supergustog kodiranja. Martin [20] je također uveo pojam kvantne steganografske komunikacije. Njegov protokol je

varijacija Bennettovog i Brassardovog protokola kvantne distribucije ključa (eng. *Quantum key distribution,* QKD), u kojem on skriva steganografski kanal u QKD protokolu. Banerjee [21] je dao klasičnu steganografsku metodu inspiriranu uporabom reverzibilnih kvantnih vrata.

Za shvaćanje nadolazećih sustava potrebno je razmotriti protokol GeaBanaclochea. GeaBanacloche [23] je dao protokol za skrivanje tajnih klasičnih poruka u obliku kvantnih sindroma pogreške namjernom primjenom ispravljivih pogrešaka na kvantno stanje kodirano u tri-kubit kvantnom kodu za ispravljanje pogrešaka (eng. *quantum error-correcting code,* QECC).

Hassaballah predstavlja kako postoje dva glavna cilja kvantne steganografije. Komunikacija: Alice želi poslati klasične ili kvantne informacije Bobu preko kvantnog kanala. Većina protokola koji su predloženi za kvantnu steganografiju su za slanje klasičnih informacija, ali Shaw i Brun [22] su pokazali da je također moguće slati kvantne informacije, s obzirom na određene pretpostavke o ponašanju prisluškivača. Evene bi trebala moći otkriti prisutnost tajne poruke. U idealnom slučaju, protokol bi trebao maksimizirati brzinu komunikacije, u skladu sa zahtjevom tajnosti. Sigurnost kao treći zahtjev može, ali i ne mora biti nametnut. U nekim slučajevima možemo zahtijevati da Eva ne može pročitati steganografsku poruku čak i ako zna da je prisutna. Ovaj zahtjev je u određenom smislu odvojen od samih metoda steganografije i može se postići kombinacijom steganografije i kriptografije.

Shaw i Brun su predstavili skup protokola koji postižu gore navedene ciljeve. Ovi protokoli imaju sljedeću strukturu. Alice je bezazlenu kvantnu poruku (ili stanje) kodirala u QECC. Alice zatim izvodi drugu operaciju na kodiranom baznom tekstu, koja ugrađuje steganografsku poruku u kodnu riječ. Jedan bit ili kubit stegoteksta naziva se stego bit ili stego kubit. Modificirana kodna riječ šalje se preko kvantnog kanala Bobu, koji je (s velikom vjerojatnošću) može dekodirati i izdvojiti stegotekst. Kodiranje se vrši na takav način da ako prisluškivač Eve presretne kodnu riječ, ona će izgledati točno kao kodirano stanje nakon što je prošla kroz kanal a šumom. Drugim riječima, Eve ne može razlikovati kodiranu steganografsku poruku od šuma u kanalu.

Hassaballah mnogo je otvorenih pitanja o kvantnoj steganografiji. Na primjer, postoji kvalitativna razlika između dijeljenog tajnog ključa i zajedničkog isprepletanja. Protokoli temeljeni na tajnom ključu mogu se simulirati korištenjem zajedničkog ispreplitanja; ali općenito, očekivali bismo da je isprepletenost snažnija. Trebao bi dati veću mogućnost zavaravanja Eve i zaštite tajnih informacija od intrinzičnog šuma u kanalu.

Slučaj u kojem je temeljni fizički kanal bešuman prilično je jednostavan i nije ga teško razumjeti. Kodiranja koja se temelje na pretpostavci da se koriste nedegenerirani QECC-ovi, mogu se gotovo sigurno lako generalizirati na degenerirani slučaj. Slučaj s kanalom sa šumom mnogo je kompliciraniji, budući da Alice i Bob moraju zadovoljiti kriterije tajnosti i mogućnosti

povrata, gdje je mogućnost povrata mnogo manje trivijalna u prisutnosti šuma. Kvantna steganografija je moguća preko kanala sa šumom barem za neke kanale i neke QECC-ove. Ali trebalo bi se napraviti šire istraživanje, koja povezuju specifična kodiranja s nekim kanalima i dokazuju asimptotička ograničenja za moguće stope tajne komunikacije.

Drugi smjer istraživanja je u kontradiktornom slučaju kvantne steganografije, gdje Alice i Bob koriste nepouzdanu komunikacijsku opremu koja bi mogla pokušati prenijeti informacije prisluškivaču.

Kao sažetak kvantne steganografije Hassaballah predstavlja kako je to skup protokola koji skrivaju klasične ili kvantne informacije u naizgled bezazlenoj kvantnoj komunikaciji. Postoji posebno dobro razvijen pristup, u kojem su poruke maskirane kao pogreške na kvantnom kodu za ispravljanje pogrešaka iz bučnog kvantnog kanala. Uz pomoć zajedničkog tajnog ključa, poruke mogu biti kodirane od strane pošiljatelja Alice na takav način da odgovaraju učincima kanala koje očekuje prisluškivač Eve i da ih može dekodirati primatelj Bob. Specifična kodiranja i brzine komunikacije razrađeni su za brojne kanale za nedegenerirane kvantne kodove, ali mnogo toga ostaje nepoznato. Iako su razvijene mnoge osnovne ideje, samo je započeto proučavanje kvantne steganografije.

3. Digitalni vodeni žig (Watermarking)

Zbog uske povezanosti digitalnog vodenog žiga (eng. *digital watermarking*) korisno je razmotriti sličnosti i razlike između žiga i steganografije. Ovo poglavlje će predstaviti digitalni vodeni žig te po kojim aspektima se on razlikuje od steganografije.

Shih predstavlja kako vodeni žig nije nova pojava, već kako su gotovo tisuću godina vodeni žigovi na papiru korišteni za vidljivo označavanje određenog izdavača i za odvraćanje od krivotvorenja novca. Vodeni žig je dizajn utisnut na komad papira tijekom proizvodnje i koji se koristi za identifikaciju autorskih prava. Dizajn može biti uzorak, logotip ili neka druga slika. U modernom dobu, budući da se većina podataka i informacija pohranjuje i prenosi u digitalnom obliku, dokazivanje autentičnosti igra sve važniju ulogu. Kao rezultat toga, digitalni vodeni žig je proces u kojem se proizvoljne informacije kodiraju u sliku na takav način da budu neprimjetne promatračima.

Nadalje Shih predstavlja kako je digitalni vodeni žig predložen kao prikladan alat za identifikaciju izvora, kreatora, vlasnika, distributera ili ovlaštenog korisnika dokumenta ili slike. Također se može koristiti za otkrivanje dokumenta ili slike koji su ilegalno distribuirani ili modificirani. Druga tehnologija, enkripcija, je proces prikrivanja informacija kako bi bile nečitljive promatračima bez posebnih ključeva ili znanja. Ova se tehnologija ponekad naziva šifriranjem podataka (eng. *data scrambling*). Vodeni žig, kada je nadopunjen enkripcijom, može poslužiti u puno slučajeva, uključujući zaštitu autorskih prava, praćenje emitiranja i provjeru autentičnosti podataka. U digitalnom svijetu, vodeni žig je uzorak bitova umetnutih u digitalni medij koji može identificirati kreatora ili ovlaštene korisnike. Digitalni vodeni žigovi - za razliku od tradicionalnih tiskanih, vidljivih vodenih žigova - dizajnirani su da budu nevidljivi gledateljima. Bitovi ugrađeni u sliku razbacani su posvuda kako bi se izbjegla identifikacija ili modifikacija. Stoga digitalni vodeni žig mora biti dovoljno robustan da preživi detekciju, kompresiju i druge operacije koje se mogu primijeniti na dokument. Poruka s vodenim žigom W ugrađena je u medijsku poruku, koja je definirana kao bazna slika H. Rezultirajuća slika je slika s vodenim žigom H*. U procesu ugrađivanja, tajni ključ K—to jest, generator nasumičnog broja—ponekad je uključen za generiranje sigurnijeg vodenog žiga. Slika s vodenim žigom H* zatim se prenosi duž komunikacijskog kanala. Primatelj kasnije može detektirati ili izdvojiti vodeni žig.

Neprimjetnost, sigurnost, kapacitet i robusnost među mnogim su aspektima dizajna vodenog žiga. Slika s vodenim žigom ne smije se razlikovati od izvorne slike; ako sustav za označavanje vodenim žigom iskrivi baznu sliku do te mjere da je vidljiva, nema koristi. Idealan sustav vodenih žigova trebao bi savršeno sigurno ugraditi veliku količinu informacija, ali bez vidljive

degradacije bazne slike. Ugrađeni vodeni žig trebao bi biti robustan, otporan na namjerne (npr. šum) ili nenamjerne (npr. poboljšanje slike, obrezivanje, promjena veličine ili kompresija) napade. Mnogi su se istraživači usredotočili na sigurnost i robusnost, ali rijetko na sposobnost označavanja vodenim žigom. Količina podataka koju algoritam može ugraditi u sliku utječe na to kako se vodeni žig može primijeniti. Doista, i sigurnost i robusnost su važni jer se očekuje da ugrađeni vodeni žig bude neprimjetan i neuklonjiv. Unatoč tome, ako se veliki vodeni žig može ugraditi u baznu sliku, postupak bi mogao biti koristan za mnoge druge primjene. Druga shema je korištenje ključeva za generiranje nasumičnih nizova tijekom procesa ugrađivanja. U ovoj shemi, bazna slika nije potrebna tijekom procesa otkrivanja vodenog žiga. Također je cilj da sustav vodenog žiga koristi asimetrični ključ, kao u kriptografskim sustavima s javnim ili privatnim ključem. Javni ključ koristi se za provjeru slike, a privatni ključ je potreban za ugradnju sigurnosnih značajki. Poznavanje javnog ključa ne pomaže u izračunavanju privatnog ključa niti dopušta uklanjanje vodenog žiga.

U svrhu korisničkog ugrađivanja, vodeni žigovi mogu se kategorizirati u tri vrste: robusni, polulomljivi i lomljivi. Robusni vodeni žigovi dizajnirani su da izdrže proizvoljne, zlonamjerne napade kao što su skaliranje slike, savijanje, obrezivanje i kompresija s gubitkom. Obično se koriste za zaštitu autorskih prava kako bi se deklariralo pravo vlasništva. Polulomljivi vodeni žigovi dizajnirani su za otkrivanje bilo kakvih neovlaštenih izmjena, dok u isto vrijeme omogućuju neke operacije obrade slike. Drugim riječima, selektivna provjera autentičnosti otkriva nelegitimno izobličenje dok zanemaruje primjene legitimnog izobličenja. U svrhu provjere autentičnosti slike, lomljivi vodeni žigovi usvojeni su kako bi se uopće otkrila bilo kakva neovlaštena izmjena.

Općenito, vodene žigove možemo ugraditi u dvije vrste domena: prostornu domenu ili frekvencijsku domenu. U prostornoj domeni možemo zamijeniti piksele na baznoj slici s pikselima na slici vodenog žiga. Treba se pripaziti da sofisticirani računalni program može lako otkriti umetnuti vodeni žig. U frekvencijskoj domeni možemo zamijeniti koeficijente transformirane slike s pikselima na slici s vodenim žigom. Transformacije frekvencijske domene koje se najčešće koriste su diskretna kosinusna transformacija, diskretna Fourierova transformacija i diskretna valična transformacija. Ovu vrstu ugrađenog vodenog žiga općenito je teško otkriti. Međutim, kapacitet ugradnje obično je nizak, budući da će velika količina podataka značajno iskriviti sliku glavnog računala. Vodeni žig mora biti manji od bazne slike.

3.1. Razlike između steganografije i vodenog žiga

Shih predstavlja kako je vodeni žig usko povezan sa steganografijom, međutim, postoje neke razlike između njih. Vodeni žig se uglavnom bavi provjerom autentičnosti slike, dok se

steganografija bavi skrivanjem podataka. Poruke ugrađenog vodenog žiga obično se odnose na informacije o baznoj slici kao što su autorska prava, tako da su povezane sa baznom slikom. Vodeni žig se često koristi kad god je bazna slika dostupna korisnicima koji su svjesni postojanja skrivenih informacija i možda ih namjeravaju ukloniti. Skrivene poruke u steganografiji obično nisu povezane s baznom slikom. One su dizajnirane kako bi izuzetno važne informacije učinili neprimjetnim za presretače.

Nadalje pri vodenom žigu, ugrađena informacija povezana je sa značajkama nositelja i prenosi dodatne informacije o ili svojstvima nositelja. Primarni objekt komunikacijskog kanala je sam nositelj. U steganografiji, ugrađena poruka obično nema nikakve veze s nositeljem, koji se jednostavno koristi kao mehanizam za prijenos poruke. Objekt komunikacijskog kanala je skrivena poruka. Kao i kod primjene vodenog žiga, održava se ravnoteža između percepcijske kvalitete slike i robusnosti. Ograničenja u održavanju kvalitete slike imaju tendenciju smanjenja kapaciteta ugrađenih informacija. Kako je primjena steganografije drugačija, koja se bavi tajnim prijenosom poruka, ugrađeni kapacitet često se smatra jednako važnim kao i robusnost i kvaliteta slike.

4. Objektivne mjere kvalitete slike

4.1. Kapacitet

Kako bi se mogla predstaviti mjere potrebno je definirati što je to kapacitet ugradnje. Hassaballah navodi kapacitet ugradnje (ili kapacitet reprodukcije) ovisi o steganografijskoj shemi i prirodi odabrane bazne slike. Kapacitet se može definirati kao najveća veličina tajnih podataka koji se mogu ugraditi u baznu sliku bez oštećenja cjelovitosti bazne slike. Drugim riječima, kapacitet je broj ugrađenih bitova u svakom pikselu i predstavljen je bitovima po pikselu (bpp) ili u relativnom postotku što se može predstaviti na sljedeći način prikazan jednadžbom 2.1:

$$Kapacitet\ (bpp) = \frac{broj\ ugrađenih\ bitova}{ukupnan\ broj\ piksela\ bazne\ slike} \tag{4.1}$$

4.2. Mjere koje koriste referentnu sliku

Sara i sur. [24] predstavljaju kako je kvaliteta vrlo važan parametar za sve objekte i njihove funkcionalnosti. U prepoznavanju objekata temeljenom na slici, kvaliteta slike je glavni kriterij. Za autentičnu procjenu kvalitete slike potrebna je referentna slika (eng. *full-reference, FR*). Ali u praksi je ponekad teško prenijeti referentnu sliku, pa se razvijuaju i mjere koje ne trebaju referentnu sliku (eng. *no-reference ,NR*). Obično se kvaliteta slike mjerama koje koriste referentni sliku, kao što su MSE (srednja kvadratna pogreška, eng. *Mean Square Error*) i PSNR (vršni omjer signala i šuma, eng. *Peak Signal to Noise Ratio*). Za razliku od MSE i PSNR, razvijene su još mjere SSIM (eng. *Structural SIMilarity Index*) i FSIM (eng. *Feature Similarity Indexing Method*) s ciljem usporedbe strukturnih i značajnih mjera sličnosti između procesiranih i izvornih slika na temelju percepcije. Sara i sur. navode kako su sve mjere dale dosljedne rezultate. Ipak, kada se koristi veća baza slika s više različitih izobličenja i razina izobličenja, FSIM i SSIM će bolje korelirati s HVS od PSNR (i MSE) [26]. Međutim, iz perspektive reprezentacije, SSIM i FSIM su normirani, ali MSE i PSNR nisu; i iz semantičke perspektive, MSE i PSNR daju samo apsolutnu pogrešku; s druge strane, SSIM i PSNR daju pogrešku temeljenu na percepciji i upadljivosti. Dakle, SSIM i FSIM mogu se tretirati razumljivije nego MSE i PSNR.

4.2.1. MSE

Sara i sur. predstavljaju kako je MSE najčešća metoda procjene kvalitete slike. To je mjera koja koristi referentnu sliku i vrijednosti bliže nuli su bolje. Varijanca procjenitelja i njegova pristranost uključeni su sa srednjom kvadratnom pogreškom. MSE je varijanca procjenitelja u slučaju nepristranog procjenitelja. Ima iste mjerne jedinice kao kvadrat količine koja se izračunava kao varijanca. MSE uvodi srednju kvadratnu pogrešku (eng. Root-Mean-Square Error, RMSE) ili srednju kvadratnu devijaciju (eng. *Root-Mean-Square Deviation*, RMSD) i često se naziva standardnom devijacijom varijance. MSE se također može reći kao srednje kvadratno odstupanje (eng. *Mean Squared Deviation*, MSD) procjenitelja. Estimator se naziva postupak za mjerenje neopažene količine slike. MSE ili MSD mjeri prosjek kvadrata pogrešaka. Pogreška je razlika između procjenitelja i procijenjenog ishoda. To je funkcija rizika, uzimajući u obzir očekivanu vrijednost gubitka kvadrata pogreške ili kvadratnog gubitka. Srednja kvadratna pogreška (MSE) između dvije slike kao što su g(x,y) i g'(x,y) definirana je kao što je prikazano jednadžbom 4.2.

$$MSE = \frac{1}{MN}\sum_{n=0}^{M}\sum_{m=1}^{N}\left[g'^{(n,m)} - g(n,m)\right]^2 \tag{4.2}$$

4.2.2. PSNR

Sara i sur. navode kako se PSNR koristi za izračunavanje omjera između najveće moguće snage signala i snage šuma koji utječe na kvalitetu njegovog prikaza. Ovaj omjer između dvije slike izračunava se u obliku decibela. PSNR se obično izračunava kao logaritam skale decibela zbog signala koji imaju vrlo širok dinamički raspon. Ovaj dinamički raspon varira između najvećih i najmanjih mogućih vrijednosti koje su promjenjive svojom kvalitetom. Omjer vršnog signala i šuma najčešće je korištena tehnika procjene kvalitete za mjerenje kvalitete rekonstrukcije kodeka za kompresiju slike s gubitkom. Signal se smatra izvornim podacima, a šum je pogreška nastala kompresijom ili izobličenjem. PSNR je približna procjena kvalitete rekonstrukcije prema ljudskoj percepciji u usporedbi s kompresijskim kodecima. U degradaciji kvalitete kompresije slike i videa, vrijednost PSNR varira od 30 do 50 dB za 8-bitni prikaz podataka i od 60 do 80 dB za 16-bitne podatke (iako mogu biti i druge vrijednosti). U bežičnom prijenosu, prihvaćeni raspon gubitka kvalitete je približno 20 - 25 dB. PSNR se izražava kao što je prikazano jednadžbom 4.3:

$$PSNR = \frac{10\log_{10}(peakval)^2}{MSE} \tag{4.3}$$

Ovdje je peakval (eng. *Peak Value*, vršna vrijednost) maksimum u podacima slike. Ako je to 8-bitni tip podataka bez predznaka, peakval je 255.

4.2.3. NCC

Mjera kosinusne sličnosti ili normirana križna korelacija (eng. *Normalized cross correlation, NCC*) ilustrira koliko je stego slika u korelaciji sa baznom slikom. Vrijednost NCC-a se nalazi između 0 i 1. Ako su NCC vrijednosti između stego slike i napadnute stego slike jednake 1, to znači da su stego slike potpuno otporne na različite napade obrade slike. NCC je predstavljena jednadžbom 4.4:

$$NCC = \frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(S(i,j)\times C(i,j))}{\sqrt{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}S(i,j)^2}\sqrt{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}C(i,j)^2}} \tag{4.4}$$

4.2.4. UQI

Univerzalni indeks kvalitete slike(eng. *universal image quality index, UQI*) [27] koristi se za procjenu vizualne kvalitete slike. Visoke vrijednosti za Q znače da su stego i bazna slika u visokoj korelaciji i razlike među njima su vrlo male. Univerzalni indeks kvalitete Q može se izračunati pomoću jednadžbe 4.5:

$$Q = \frac{4\sigma_{xy}\overline{x}\overline{y}}{(\sigma_x^2+\sigma_y^2)[(\overline{x})^2+(\overline{y})^2]} \tag{4.5}$$

Gdje su:

$$\overline{x} = \frac{1}{M\times N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(x_{ij}) \tag{4.6}$$

$$\overline{y} = \frac{1}{M\times N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(y_{ij}) \tag{4.7}$$

$$\sigma_x^2 = \frac{1}{(M\times N)-1}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(x_{ij}-\overline{x})^2 \tag{4.8}$$

$$\sigma_y^2 = \frac{1}{(M\times N)-1}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(y_{ij}-\overline{y})^2 \tag{4.9}$$

$$\sigma_{xy}^2 = \frac{1}{(M\times N)-1}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(x_{ij}-\overline{x})(y_{ij}-\overline{y}) \tag{4.10}$$

gdje je x vrijednost piksela naslovne slike, y je vrijednost piksela stego slike, $\overline{x}$ je srednja vrijednost x, $\overline{y}$ je srednja vrijednost y, a σ_x^2 , σ_y^2 i σ_{xy}^2 su varijanca i kovarijanca x odnosno y slika.

4.2.5. SSIM

Sara i sur. navode kako je metoda indeksa strukturne sličnosti (SSIM) model koji [27] se temelji na percepciji. U ovoj se metodi degradacija slike smatra promjenom percepcije strukturnih informacija. Također surađuje s nekim drugim važnim činjenicama koje se temelje na percepciji, kao što je maskiranje svjetline, maskiranje kontrasta, itd. Pojam strukturne informacije naglašava jako međuovisne piksele ili prostorno zatvorene piksele. Ovi međusobno ovisni pikseli upućuju na neke važnije informacije o vizualnim objektima u domeni slike. Maskiranje svjetline (eng. *Luminace masking*) je pojam gdje je dio slike s izobličenjem manje vidljiv na rubovima slike. S druge strane maskiranje kontrasta je pojam gdje su izobličenja također manje vidljiva u teksturi slike. SSIM procjenjuje percipiranu kvalitetu slika i videa. Mjeri sličnost između dvije slike: izvorne i porcesirane. Postoji napredna verzija SSIM-a pod nazivom Metoda indeksa strukturne sličnosti nad više skala (eng. *Multiscale SSIM, MS-SSIM*) koja [28] procjenjuje različite slike strukturne sličnosti na različitim skalama. U MS-SSIM-u, dvije slike se uspoređuju na ljestvici iste veličine i rezolucije. Kod MS-SSIM, konstrast i struktura se računa na svim skalama, a luminancija na frekvencijski najnižoj skali. Ponekad daje bolje performanse u odnosu na SSIM koristeći subjektivne ocjene slika i videozapisa. Druga verzija SSIM-a, nazvana trokomponentni SSIM (3-SSIM) koja [29] odgovara činjenici da ljudski vizualni sustav točnije opaža razlike u teksturiranim regijama nego u glatkim regijama. 3-komponentni SSIM model rastavlja sliku na tri važna svojstva kao što su rub, tekstura i glatko područje. Rezultirajuća mjera izračunava se kao težinski prosjek strukturne sličnosti za ove tri kategorije. Predložene procjene težine su 0,5 za rubove, 0,25 za teksturu i 0,25 za glatka područja.

Metoda indeksa SSIM, mjera mjerenja kvalitete izračunava se na temelju izračuna tri glavna aspekta koja se nazivaju svjetlina, kontrast i struktura. Ovaj indeks je kombinacija množenja ova tri aspekta. Metoda indeksa strukturne sličnosti može se izračunati kao što je prikazano na formuli:

$$SSIM(x,y) = [l(x,y)]^{\alpha} \times [c(x,y)]^{\beta} \times [s(x,y)]^{\gamma}$$

Ovdje je l svjetlina (koristi se za usporedbu svjetline između dviju slika), c je kontrast (koristi se za razlikovanje usporedbe lokalnog kontrasta), a s je struktura (koristi se za usporedbu lokalne strukture između dviju slika kako bi se pronašla sličnost i različitost slika), a α, β i γ su pozitivne konstante.

Opet, svjetlina, kontrast i struktura slike mogu se zasebno izraziti kao:

$$l(x,y) = \frac{2\mu_x\mu_y + C_1}{\mu_x^2 + \mu_y^2 + C_1}$$

$$c(x,y) = \frac{2\sigma_x\sigma_y + C_2}{\sigma_x^2 + \sigma_y^2 + C_2}$$

$$s(x,y) = \frac{\sigma_{xy} + C_3}{\sigma_x\sigma_y + C_3}$$

gdje su μ_x i μ_y lokalne srednje vrijednosti, σ_x i σ_{xy} standardne devijacije, a σ_{xy} križna kovarijanca za slike x i y. Ako je α=β=γ=1, tada se indeks pojednostavljuje kao sljedeći oblik pomoću jednadžbi:

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

4.3. Mjere koje ne koriste referentnu sliku

4.3.1. BRISQUE

Procjenitelj prostorne kvalitete slijepe/referentne slike (eng. *Blind/Reference less Image Spatial Quality Evaluator*, BRISQUE). Abbadi i sur. [25] predstavljaju kako je BRISQUE model koji koristi samo piksele slike za izračunavanje značajki (ostale metode temelje se na transformaciji slike kao što je valićna ili diskretna kosinusna transformacija). Dokazano je da je vrlo učinkovit jer ne treba nikakvu transformaciju da bi se izračunale njegove značajke. BRISQUE se koristi za mjerenje kvalitete slike usporedbom ulazne slike s modelom iste vrste izobličenja. BRISQUE je treniran na bazi podataka slika stvorenih od slika prirodnih scena s poznatim izobličenjima. BRISQUE je svjestan mišljenja (eng. *opinion aware*), što znači da

subjektivne ocjene kvalitete prate slike na kojima se vršio trening. Bolja perceptivna kvaliteta može se postići s manjom vrijednošću BRISQUE.

4.3.2. NIQE

Procjenitelj kvalitete slike prirodnosti (eng. *Naturalness Image Quality Evaluator*, NIQE). Abbadi i sur. navode kako NIQE izračunava rezultat kvalitete slike bez reference za ulaznu sliku koristeći Naturalness Image Quality Evaluator. NIQE ima mogućnost odrediti kvalitetu slike s proizvoljnim izobličenjem, unatoč tome što je NIQE uvježban na netaknutim slikama visoke kvalitete. percepcijska kvaliteta se povećava kada se smanji vrijednost NIQE. NIQE nije svjestan mišljenja (eng. *opinion unaware*) i ne koristi subjektivne ocjene kvalitete.

4.3.3. PIQE

Procjenitelj kvalitete slike na temelju percepcije (eng. *Perception based Image Quality Evaluator*, PIQE). Abbadi i sur. navode kako PIQE izračunava ocjenu kvalitete slike bez reference za ulaznu sliku pomoću evaluatora kvalitete slike koji se temelji na percepciji. PIQE algoritam ne treba model treninga, a to znači da nije svjestan mišljenja. PIQE u većini slučajeva radi slično NIQE-u uz mogućnost određivanja kvalitete slike s proizvoljnim izobličenjem. PIQE procjenjuje izobličenje za blokove i određuje lokalnu varijancu osjetno izobličenih blokova za izračunavanje ocjene kvalitete. Algoritmi BRISQUE i NIQE izračunavaju ocjenu kvalitete slike s računalnom učinkovitošću, te su računalno učinkovitije od PIQE u fazi testiranja (tj. nakon treninga)., nakon što se model uvježba. PIQE je računalno manje učinkovit, ali pruža lokalne mjere kvalitete uz globalnu ocjenu kvalitete. Sve mjere koje ne koriste referentnu sliku (NR) obično nisu bolje od mjera koje koriste referentu sliku (FR) u smislu slaganja sa subjektivnom ljudskom ocjenom kvalitete.

4.3.4. FSIM

Indeks sličnosti značajki (eng. *feature-similarity, FSIM*) za punu referentnu IQA na temelju činjenice da HVS razumije sliku uglavnom prema njezinim značajkama niske razine. Konkretno, fazna podudarnost (eng. *phase congruency, PC*), koja je bezdimenzionalna mjera značaja lokalne strukture, koristi se kao primarna značajka u FSIM-u. Uzimajući u obzir da je računalo kontrastno nepromjenjivo dok informacije o kontrastu utječu na HVS-ovu percepciju kvalitete slike, veličina gradijenta slike (eng. *gradient magnitude, GM*) koristi se kao sekundarna značajka

u FSIM-u. PC i GM igraju komplementarne uloge u karakterizaciji lokalne kvalitete slike. Nakon dobivanja lokalne karte kvalitete, ponovno koristimo PC kao težinsku funkciju za izvođenje jedinstvene ocjene kvalitete. Opsežni eksperimenti provedeni na šest referentnih IQA baza podataka pokazuju da FSIM može postići mnogo veću konzistentnost sa subjektivnim procjenama od najsuvremenijih IQA metrika. [31]

4.4. TOPIQ

Chen i sur. [32] predlažju pristup odozgo prema dolje koji koristi semantiku visoke razine za vođenje IQA mreže da se usredotoči na semantički važna lokalna područja iskrivljenja, nazvana TOPIQ. Njihov pristup IQA-u uključuje dizajn heurističke „od grubog do glatkog“ mreže (eng. *coarse-to-fine network, CFANet*) koja koristi značajke više razmjera i progresivno širi semantičke informacije na više razina do prikaza niske razine na način odozgo prema dolje. Ključna komponenta njihovog pristupa je predloženi mehanizam pažnje na više razina, koji izračunava mape pažnje za značajke niže razine vođene značajkama više razine. Ovaj mehanizam naglašava aktivna semantička područja za izobličenja niske razine, čime se poboljšava izvedba. TOPIQ se može koristiti za IQA s punom referencom (FR) i bez reference (NR). Koristiju ResNet50 kao bazu i pokazuju da TOPIQ postiže bolje ili konkurentne performanse na većini javnih FR i NR referentnih vrijednosti u usporedbi s najsuvremenijim metodama temeljenim na transformatorima vida.

5. Usporedba različitih implementacija steganografije

5.1. Zadatak – usporedba lsb, lps i pvd

Cilj zadatka je testirati tri različita alta koja implementiraju lsb steganografiju na različite načine. Kao bazne slike odabrane su tri različite slike. Kodim02 prikazuje drvena vrata. Slika je odabrana zbog veliko udjela jedne (crvene) boje, te slika ima pravilne linije i oblike. Druga odabrana slika je kodim13 koja prikazuje krajolik, zbog mnogih detalja kao što su krošnje drveća i prelijevanja vode kvaliteta slika je osjetljiva na povećanje šuma. Te treća slika kodim15 je slika osobe. Odabrana je jer veliki postotak slika prikazuje ljude su ljudi osjetljivi na promjene detalja na licima, te predstavlja dobar odabir na kojem bi se lakše mogle uočiti promijene. Za svaku različitu implementaciju steganografije pridodano je više različitih veličina tajne poruke koje se protežu od 2,5 % do 20 % veličine bazne slike u koju se umeće poruka. Poruke su nasumični niz znakove odgovarajuće veličine. Kvaliteta dobivenih stego slika je testirana metodama bez referentne slike (BRSQUE, NIQE, PIQE i TOPIQ) i metodama koje zahtijevaju referentnu sliku (PSNR, SSIM i TOPIQ).

5.2. Izvedba

Kao početak potrebno je bilo generirati tajne poruke te su one bile generirane putem online alata Online FILE Tools. Alat omogućuje kreirane nasumičnih znakova precizne veličine koje se mogu spremiti kao .txt datoteka. Tako je kreirano šest datoteka za svaku sliku veličine 2,5 %, 5 %, 7,5 %, 10 %, 15% i 20 %.

Svi od programa za implementaciju steganografije koriste tekstualno sučelje te su bazirani na Python programskom jeziku. Prvi alat, pod nazivom SecretPixel, implementira klasičnu LSB (*eng. Least Significant Bit*) metodu, ali osim samog skrivanja podataka kriptira te podatke, te omogućuje generaciju privatnog i javnog para ključa za šifriranje. Alat zahtijeva putanju bazne slike, putanju gdje se nalazi .txt datoteka, putanju gdje će spremiti novonastalu stego sliku, putanju javnog ključa, ako sakrivamo poruku. Drugačiji su zahtjevi pri dešifriranju slike, odnosno „vađenju“ tajne poruke, ali to nije bio fokus ovog zadatka. Kreirane su četiri stego slike za svaku kodim02 i kodim15 sliku, te 3 stego slike za kodim13 sliku. Kodim13 slika je veličine 800 KB što je za kojih 25 % veće od druge dvije bazne slike. Te provedbom zadatka ustanovljeno je da ovaj alat uzima u obzir apsolutnu veličinu tajne poruke ili ju nekako uzima u obzir, a ne veličinu u odnosu na veličinu bazne slike, te je time generirana jedna stego slika manje za kodim13 čija najveća tajna poruka nije bila veća od 7,5 % veličine bazne slike, dok je kod druge dvije bazne slike najveća tajna poruka bila 10 % veličine bazne slike.

Drugi alat pod nazivom Linked-Pixel-Steganography koristi isto imenu LPS metodu. LPS ne skriva podatke redom na slici. Inspiriran je povezanim popisom u algoritmu. Baš kao i povezani popisi, svaki „blok“ sadrži dijelove podataka i pokazivač na sljedeći piksel koji drži ostatak podataka. Svaki piksel slike sastoji se od najmanje tri kanala (R, G, B). LPS koristi LSB svakog kanala za različitu upotrebu. LPS koristi samo jedan kanal za pohranu stvarnih podataka, te zbog toga zauzima najmanje tri puta više prostora za pohranu od klasičnog LSB-a. Alat koristi sličan pristup korištenju tekstualnog sučelja, ali ovaj puta bez korištenja javnih i tajnih ključeva. Provedbom zadatka ustanovljeno je da također koristi apsolutnu veličinu tajne poruke te je jednako kao i u prethodnoj metodi generirana jedna slika manje za kodim13. Generirane su 3 stego slike za svaku kodim02 i kodim15, te dvije za kodim13.

Treći alat je koristi PVD (*eng. Pixel Value Diffrencing*). U PVD-u se na rasterski način koriste adaptivni ne preklapajući blokovi piksela 3x3 ili kombinacija blokova 3x3 i 2x2. Korištenje alat je slično prethodnicima kroz tekstualno sučelje. Provedbom zadatka je ustanovljeno da ovaj alat koristi relevantnu veličinu tajne poruke u odnosu na baznu sliku, te su generirane stego slike koje sadrže veličinu tajne poruke od 20 % veličine bazne slike. Te su time generirane 6 slika za svaku od triju baznih slika.

Pošto alati koriste LSB metodu koja mijenja bitove najmanjeg značaja vizualno stego slike izgledaju identično baznoj slici te se ne može zamijetiti distorzija slike ili šum.

Ocjena kvalitete slika koje provedena pomoću IQA-PyTorch alata koji je također baziran na Python programskom jeziku te se koristi pomoću tekstualnog sučelja. Postoji razlika u primjeni ovisno o tome da li se koristi metoda bez ili s referentnom slike. Alat zahtjeva putanju na sliku ili datoteku sa slikama nad kojima se vrši evaluacija, vrstu metode koju želimo primijeniti i putanju gdje želimo spremiti dobivene rezultate. Ako želimo primijeniti metodu koja koristi referentnu sliku potrebno je i navesti putanju na traženu baznu sliku.

5.3. Prikaz dobivenih slika

5.3.1. LSB

Veličina tajne poruke	kodim02

2,5%	 *Slika 5.1 lsb_kodim02_025*
5%	 *Slika 5.2 lsb_kodim02_05*

7,5%	 *Slika 5.3 lsb_kodim02_075*
10%	 *Slika 5.4 lsb_kodim02_10*

Veličin	kodim13

a tajne poruke	
2,5%	 *Slika 5.5 lsb_kodim13_025*
5%	 *Slika 5.6 lsb_kodim13_05*

7,5%	 *Slika 5.7 lsb_kodim13_075*

Veličina tajne poruke	kodim15
2,5%	 *Slika 5.8 lsb_kodim15_025*

5%	 *Slika 5.9 lsb_kodim15_05*
7,5%	 *Slika 5.10 lsb_kodim15_075*

10%	 *Slika 5.11 lsb_kodim15_10*

5.3.2. LPS

Veličina tajne poruke	kodim02

2,5%	 *Slika 5.12 lps_kodim02_025*
5%	 *Slika 5.13 lps_kodim02_05*

7,5%	 *Slika 5.14 lps_kodim02_075*

Veličina tajne poruke	kodim13
2,5%	 *Slika 5.15 lps_kodim13_025*

5%	 *Slika 5.16 lps_kodim13_05*

Veličina tajne poruke	kodim15
2,5%	 *Slika 5.17 lps_kodim15_025*

5%	 *Slika 5.18 lps_kodim15_05*
7,5%	 *Slika 5.19 lps_kodim15_075*

5.3.3. PVD

Veličin	kodim02

a tajne poruke	
2,5%	 *Slika 5.20 pvd_kodim02_025*
5%	 *Slika 5.21 pvd_kodim02_05*

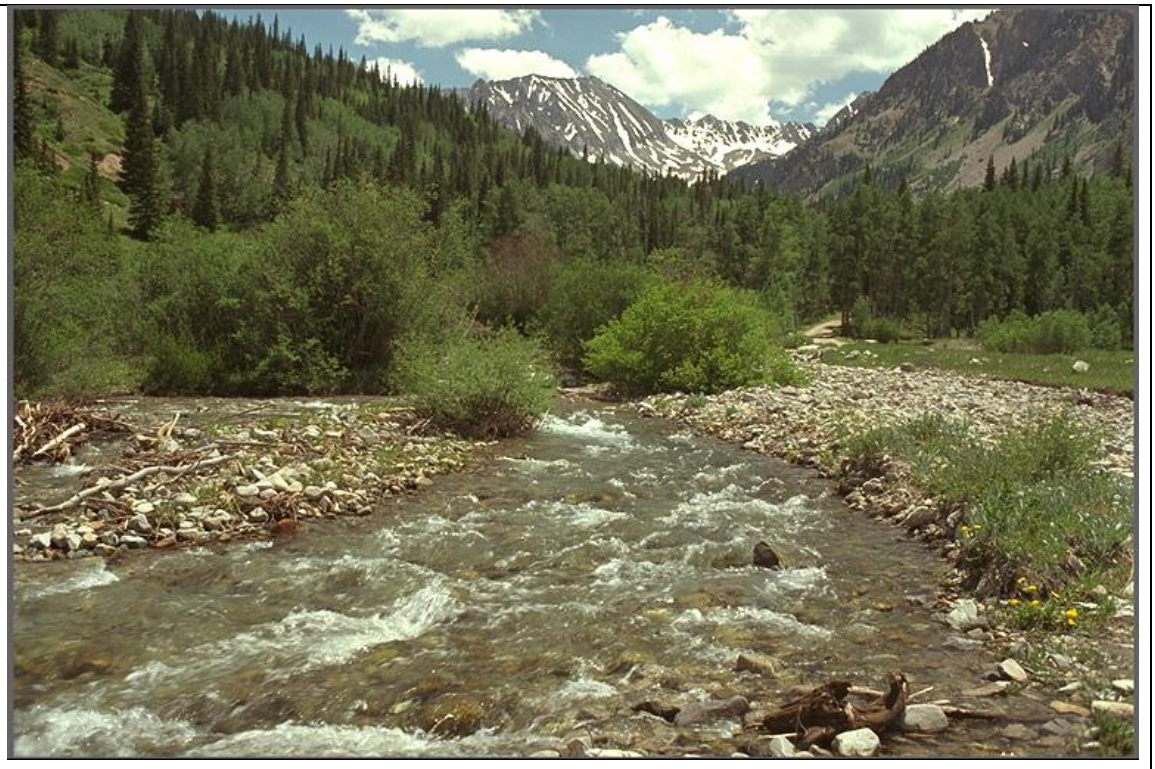
7,5%	 *Slika 5.22 pvd_kodim020_075*
10%	 *Slika 5.23 pvd_kodim02_10*

15%	 *Slika 5.24 pvd_kodim02_15*
20%	 *Slika 5.25 pvd_kodim02_20*

Veličina tajne poruke	kodim13

2,5%	 *Slika 5.26 pvd_kodim13_025*
5%	 *Slika 5.27 pvd_kodim13_05*

7,5%	 *Slika 5.28 pvd_kodim13_075*
10%	 *Slika 5.29 pvd_kodim13_10*

15%	 *Slika 5.30 pvd_kodim13_15*
20%	 *Slika 5.31 pvd_kodim13_20*

Veličina tajne poruke	kodim15

2,5%	 *Slika 5.32 pvd_kodim15_025*
5%	 *Slika 5.33 pvd_kodim15_05*

7,5%	 *Slika 5.34 pvd_kodim15_075*
10%	 *Slika 5.35 pvd_kodim15_10*

15%	 *Slika 5.36 pvd_kodim15_15*
20%	 *Slika 5.37 pvd_kodim15_20*

5.4. Rezultati bez referentne slike

5.4.1. BRISQUE

Bolja ocjena je ona s nižom vrijednosti.

LPS	bazna	2.5%	5%	7.5%
kodim02	14.95135	15.07147217	15.21209717	15.47625732
kodim13	15.38348	15.43572998	15.49969482	
kodim15	2.649597	2.776550293	2.574401855	2.422058105

LSB	bazna	2.5%	5%	7.5%	10%
kodim02	14.95135	15.08807373	15.06365967	15.21405029	15.19744873
kodim13	15.38348	15.47186279	15.46209717	15.39666748	
kodim15	2.649597	2.710632324	2.438171387	2.667663574	2.844421387

PVD	bazna	2.5%	5%	7.5%	10%	15%	20%
kodim02	14.95135	15.10418701	15.15985107	15.44256592	15.23895264	15.33953857	15.11151123
kodim13	15.38348	15.45477295	15.28338623	15.20721436	15.34979248	15.15350342	15.28289795
kodim15	2.649597	2.669128418	2.596374512	2.692565918	2.312683105	2.156433105	2.009460449

Najbolju ocjenu ima slika kodim15 koja prikazuje lice, te možemo pretpostaviti da je BRISQUE treniran nad podacima slika ljudi. Ocjene između različitih stego metoda su poprilično podjednake. Interesantno za napomenuti je da su stego slike s poprilično velikom tajnom porukom u nekim slučajima dobile bolje ocjene od bazne slike.

5.4.2. NIQE

Bolja ocjena je ona s nižom vrijednosti.

LPS	bazna	2.5%	5%	7.5%
kodim02	3.467986	3.475862951	3.481721937	3.491587527
kodim13	2.107902	2.092222765	2.084162026	
kodim15	3.818861	3.916183384	3.97484267	3.962506736

LSB	bazna	2.5%	5%	7.5%	10%
kodim02	3.467986	3.46193418	3.457616485	3.451373537	3.461604588
kodim13	2.107902	2.107202756	2.105134098	2.099866029	
kodim15	3.818861	3.848046988	3.869363415	3.864837326	3.86282876

PVD	bazna	2.5%	5%	7.5%	10%	15%	20%
kodim02	3.467986	3.476326963	3.471239937	3.468724123	3.481678083	3.476738578	3.491817653
kodim13	2.107902	2.11128196	2.113446336	2.118419244	2.13763299	2.144796721	2.189757346
kodim15	3.818861	3.796960257	3.751280512	3.772165404	3.795181687	3.821613997	3.939599496

Ocjene se ponovo podjednake između stego metoda. Najbolju ocjenu ima kodim13 slika prirode s LPS metodom, dok ostale dvije slike bolje rezultate dobivaju s PVD metodom.

5.4.3. PIQE

Bolja ocjena je ona s nižom vrijednosti.

LPS	bazna	2.5%	5%	7.5%
kodim02	23.80293	22.69560623	20.40195656	19.51696014
kodim13	40.68229	39.88775253	39.31287384	
kodim15	25.1578	24.2931366	23.66781044	22.7603054

LSB	bazna	2.5%	5%	7.5%	10%
kodim02	23.80293	23.41748238	23.30394173	23.21183205	23.5435257
kodim13	40.68229	40.64327621	40.71202087	40.84592819	
kodim15	25.1578	25.19157028	24.87385941	24.55168915	24.66230774

PVD	bazna	2.5%	5%	7.5%	10%	15%	20%
kodim02	23.80293	21.80114746	21.23748207	21.18581772	20.65806389	19.56175995	18.73634529
kodim13	40.68229	39.4644165	39.14890289	39.24770737	39.19240952	39.2776413	38.74436188
kodim15	25.1578	23.15724754	22.28051567	21.94527435	21.65107727	20.91656685	20.87272072

Slika prirode je ovom provjerom dobila znatno lošiju ocjenu neovisno o korištenoj stego metodi. PVD s velikom tajnom porukom ostvaruje najbolje rezultate. LPS ostvaruje bolje rezultate kada se uspoređuje s PVD-om na istoj veličini tajne poruke.

5.4.4. TOPIQ_NR

Bolja ocjena je ona s višom vrijednosti.

LPS	bazna	2.5%	5%	7.5%
kodim02	0.728282	0.727880955	0.727665365	0.726862431
kodim13	0.706918	0.706223786	0.705541432	

kodim15	0.708685	0.708091557	0.7066347	0.705946386

LSB	bazna	2.5%	5%	7.5%	10%
kodim02	0.728282	0.728280723	0.728097856	0.727732956	0.727883458
kodim13	0.706918	0.706807792	0.706660748	0.706939399	
kodim15	0.708685	0.708765209	0.709120333	0.708439767	0.708532333

PVD	bazna	2.5%	5%	7.5%	10%	15%	20%
kodim02	0.728282	0.727527499	0.726652086	0.725911379	0.726431012	0.725221455	0.723451674
kodim13	0.706918	0.70605725	0.705696166	0.705535054	0.704760611	0.701417327	0.699322641
kodim15	0.708685	0.708450019	0.708333194	0.708456218	0.708638132	0.707107365	0.703630686

Ocjene između različitih stego metoda i različitih slika su podjednake. Najbolju ocjenu postiže slika prirode kodim13i to ponovo PVD s velikom tajnom porukom.

5.5. Rezultati s referentnom slikom

5.5.1. PSNR

Bolja ocjena je ona s višom vrijednosti.

LPS	2.5%	5%	7.5%
kodim02	56.13676453	53.16842651	51.39711761
kodim13	54.91670227	51.90468597	
kodim15	56.18669128	53.19262695	51.43024826

LSB	2.5%	5%	7.5%	10%
kodim02	62.65739059	59.75110626	58.04043579	56.82099152
kodim13	61.46837234	58.54224777	56.81318283	
kodim15	62.66532898	59.79824829	58.08866119	56.85324097

PVD	2.5%	5%	7.5%	10%	15%	20%
kodim02	55.33583832	52.13656616	50.22679138	48.75606155	46.91164398	45.73799133
kodim13	50.2955246	47.31598282	45.40299225	44.22119522	42.32386017	41.07330704
kodim15	55.78034973	52.41217041	50.13631439	48.32915497	46.62678528	45.7546196

Najbolje ocjene postiže LSB metoda. PVD metoda ostvaruje značajno lošiji rezultat. Čim je manja tajna poruka veće je ocjena.

5.5.2. SSIM

Viša ocjena reprezentira veću sličnost s referentnom slikom.

LPS	2.5%	5%	7.5%
kodim02	0.998912599	0.997858782	0.996823908
kodim13	0.999641595	0.999295553	
kodim15	0.998868931	0.997802221	0.996824136

LSB	2.5%	5%	7.5%	10%
kodim02	0.999749728	0.999511858	0.999288169	0.999061227
kodim13	0.999907728	0.999819922	0.999731708	
kodim15	0.999681876	0.999385996	0.999095767	0.998810291

PVD	2.5%	5%	7.5%	10%	15%	20%
kodim02	0.999424677	0.998846601	0.998240021	0.997715707	0.996593719	0.995364013
kodim13	0.999641614	0.999275213	0.998904605	0.998506517	0.997804684	0.997122801
kodim15	0.999110071	0.998374952	0.997931507	0.997512675	0.996549468	0.995140326

Prema SSIM slike su iznimno slične. Ovog puta LSB postiže najveće ocjene, ali s razlikama tek pri trećoj decimali.

5.5.3. TOPIQ_FR

Viša ocjena reprezentira veću sličnost s referentnom slikom.

LPS	2.5%	5%	7.5%
kodim02	0.927234709	0.928403437	0.929220378
kodim13	0.91224438	0.91301477	
kodim15	0.9230721	0.924301088	0.925469935

LSB	2.5%	5%	7.5%	10%
kodim02	0.926097631	0.926483035	0.926806152	0.92713809
kodim13	0.911283016	0.911589801	0.911866963	
kodim15	0.921623766	0.922074378	0.922441304	0.922871172

PVD	2.5%	5%	7.5%	10%	15%	20%
kodim02	0.925386429	0.926144898	0.926914573	0.927625477	0.931791902	0.934750021
kodim13	0.911341488	0.91240555	0.91330713	0.914248407	0.91662991	0.921109021
kodim15	0.921088517	0.921540201	0.921868861	0.924197376	0.926507533	0.931369781

Ponovo najbolje ocjene dobiva PVD s velikom tajnom porukom. Najmanju ocjenu dobiva kodim13 slika prirode.

5.6. Zadatak – usporedba RoSteALS, DCT i LSB

Cilj je usporediti različite implementacije steganografije. Zbog ograničenja korištenih alata, tajna poruka je iznimno mala, sadrži osam znakova. Kao u prethodnom zadatku kvaliteta dobivenih stego slika će biti ocijenjena na isti način.

5.7. Izvedba

Za DCT i LSB metodu je korišten isti alat goji omogućuje obje, alat se koristi kroz tekstualno sučelje. Za RoSteALS korišten alat putem web preglednika, kojim se koristi kroz grafičko sučelje. U principu sučelja su jednaka, potrebno je priložiti baznu sliku te tajnu poruku najveće duljene osam znakova. Na dobivenim slikama vidimo vizualnu promjeni tamo gdje je primijenjena metoda DCT i RoSteALS. Primjenom DCT metode stego slika dobiva plavu nijansu, a primjenom RoSteALS metode vidimo blagu distorziju slike koja je najmanje primjetna na kodim15 slici koja prikazuje ljudsko lice.

5.8. Prikaz dobivenih slika

kodim02	
bazna	

Slika 5.38 kodim02

DCT	 *Slika 5.39 dct_kodim02_8c*
LSB	 *Slika 5.40 lsb_kodim02_8c*

RoSteALS	

Slika 5.41 RoSteALS_kodim02_8c

kodim13	
bazna	

Slika 5.42 kodim13

DCT	 *Slika 5.43 dct_kodim13_8c*
LSB	 *Slika 5.44 lsb_kodim13_8c*

RoSteALS	

Slika 5.45 RoSteALS_kodim13_8c

kodim15	
bazna	

Slika 5.46 kodim15

DCT	 *Slika 5.47 dct_kodim15_8c*
LSB	 *Slika 5.48 lsb_kodim15_8c*

RoSteALS	

Slika 5.49 RoSteALS_kodim15_8c

5.9. Rezultati bez referentne slike

5.9.1. BRISQUE

	bazna	RoSteALS	DCT	LSB
kodim02	14,95135	16,34832764	9,682312012	14,95428467
kodim13	15,38348	20,72674561	16,37322998	15,37908936
kodim15	2,649597	1,721862793	0,274597168	2,648620605

Ponovo vidimo da slika lica ostvaruje najveće ocjene, te stego slike postižu bolje ocjene od bazne. Dok to nije slučaj s ostale dvije slike. Plavi sloj na slikama izgleda ide u korist BRISQUE metode koja je korištena za ocijene dobivene u ovom zadatku.

5.9.2. NIQE

	bazna	RoSteALS	DCT	LSB
kodim02	3,467986	3,95942969	3,523479141	3,468020685
kodim13	2,107902	2,991011473	2,496215592	2,107406815
kodim15	3,818861	4,75414008	4,003452327	3,819237754

LSB postiže najbolje ocijene koje su vrlo bliske baznoj slici, a RoSteALS postiže najlošije.

5.9.3. PIQE

	g bazna	RoSteALS	DCT	LSB
kodim02	23,80293	19,94633293	19,64784813	23,80233002
kodim13	40,68229	41,78477478	38,48839951	40,6818428
kodim15	25,1578	24,7582016	27,12336731	25,1574192

U dva slučaja DCT i RoSteALS metoda postiže bolje ocjene od baznih slika.

5.9.4. TOPIQ_NR

	bazna	RoSteALS	DCT	LSB
kodim02	0,728282	0,71764046	0,624657929	0,728293121
kodim13	0,706918	0,671020567	0,556503952	0,706964374
kodim15	0,708685	0,707753181	0,579867005	0,708683848

Ponovo DCT postiže bolje ocjene.

5.10. Rezultati s referentnom slikom

5.10.1. PSNR

	RoSteALS	DCT	LSB
kodim02	32,63683701	12,95949554	68,6018066406
kodim13	26,50601578	15,3094635	68,6018066406
kodim15	31,80846024	13,85436249	68,6018066406

DCT postiže iznimno lošije rezultate od ostalih metoda. Dok LSB ima iznimno dobru ocjenu.

5.10.2. SSIM

	RoSteALS	DCT	LSB
kodim02	0,974277011	0,973908077	0,999999999776040
kodim13	0,936356528	0,979117442	0,999999999939091
kodim15	0,972206978	0,956805232	0,999999999977070

LSB ostvaruje daleko najbolji rezultat dok su ostale dvije metode podjednake.

5.10.3. TOPIQ_FR

	RoSteALS	DCT	LSB
kodim02	0,750055015	0,378762811	0,925124943
kodim13	0,744126976	0,391179174	0,910483658
kodim15	0,77832371	0,425528705	0,920462966

DCT s niskim rezultatom potvrđuje ta TOPIQ metoda dobro ocjenjuje razliku iz perspektive ljudskog oka. LSB s najvišim rezultatom.

6. Zaključak

Zaključno, steganografija je fascinantno i višestruko polje koje ispreplićе tehnologiju, umjetnost i sigurnost na složene i intrigantne načine. Njezini korijeni sežu duboko u povijest, odražavajući upornu želju čovječanstva da komunicira tajno i sigurno. Kako prolazimo kroz digitalno doba, važnost steganografije postaje sve izraženija. Moderne aplikacije, u rasponu od sigurne komunikacije do digitalnog vodenog žiga, ističu njegovu važnost u zaštiti informacija i očuvanju privatnosti u svijetu koji je uvijek povezan.

Evolucija steganografije od drevnih tehnika do suvremenih digitalnih metoda ilustrira njezinu prilagodljivost i trajni značaj. Sofisticiranost trenutnih steganografskih tehnika pokazuje sposobnost ovog područja da drži korak s naprednom tehnologijom, nudeći inovativna rješenja za suvremene izazove. Međutim, ovo također otvara važna pitanja o etici i potencijalnoj zlouporabi. Dok nastavljamo razvijati i implementirati steganografske tehnologije, ključno je uravnotežiti inovacije s odgovornošću, osiguravajući da se ti alati koriste za poboljšanje sigurnosti i zaštitu privatnosti, a ne za olakšavanje opakih aktivnosti.

Nadalje, proučavanje steganografije nudi vrijedan uvid u šira pitanja sigurnosti podataka i kriptografije. Razumijevanjem mehanizama i potencijalnih ranjivosti steganografskih metoda, možemo se bolje pripremiti za buduće izazove u informacijskoj sigurnosti. Kako istraživanje napreduje, interdisciplinarna suradnja bit će ključna u rješavanju ovih izazova, kombinirajući stručnost iz različitih područja kako bi se unaprijedila i teorija i praksa steganografije.

U konačnici, kontinuirano istraživanje i usavršavanje steganografskih tehnika nastavit će oblikovati krajolik digitalne sigurnosti. Cijeneći njezin povijesni kontekst, trenutačne primjene i budući potencijal, možemo bolje razumjeti i iskoristiti moć steganografije za zaštitu informacija u sve digitalnijem i međusobno povezanom svijetu.

7. Literatura

[1] Mahmoud Hassaballah, "Digital Media Steganography: Principles, Algorithms, and Advances", 1st Edition, Academic Press, 2020,

[2] Frank Y. Shih, "Digital Watermarking and Steganography: Fundamentals and Techniques", 2nd Edition, Taylor & Francis Group, 2017,

[3] J. Fridrich, M. Goljan i R. Du, "Reliable detection of LSB steganography in color and grayscale images", Proc. ACM Workshop Multimedia Security, Ottawa, ON, Kanada, str. 27–30, 2001., doi: 10.1145/1232454.1232466

[4] A. Westfeld i A. Pfitzmann, "Attacks on steganographic systems", Lecture Notes in Computer Science, Springer, Berlin, vol. 1768, str. 61-76, 2000., doi: 10.1007/10719724_5

[5] J. Fridrich, M. Goljan i D. Soukal, "Higher-order statistical steganalysis of palette images", Security and Watermarking of Multimedia Contents V, vol. 5020, str. 178–190, 2003., doi: 10.1117/12.473140.

[6] S. Dumitrescu, X. Wu i Z. Wang , "Detection of LSB Steganography via Sample Pair Analysis", Information Hiding (IH 2002), Lecture Notes in Computer Science, vol 2578., Springer, Berlin, Heidelberg, str. 355–372, 2002., doi: 10.1007/3-540-36415-3_23

[7] G. C. Kessler, "An overview of steganography for the computer forensics examiner", Forensic Science Communications, vol. 6, no. 3, str. 1-27, 2004.

[8] Avcibas, N. Memon i B. Sankur, "Steganalysis using image quality metrics", EEE Transactions on Image Processing, vol. 12, no. 2, str. 221-229, 2003., doi: 10.1109/TIP.2002.807363

[9] N.A. Syed, S. Huan, L. Kah i K. Sung, "Incremental learning with support vector machines", Proceedings of the 16th International Joint Conference on Artificial Intelligence, Stockholm, Švedska, str. 161–168, 1999.

[10] C. Campbell, N. Cristianini i A. J. Smola, "Query Learning with Large Margin Classifiers", Proceedings of the Seventeenth International Conference on Machine Learning (ICML '00), San Francisco, CA, SAD, str.111–118, 2000.

[11] Schohn, G. and Cohn, D., Less is more: Active learning with support vector machines, in Proc. Int. Conf. Machine Learning, Stanford University, CA, 2000, 839.

[12] J.-L. An, Z.-O. Wang i Z.-P. Ma, "An incremental learning algorithm for support vector machine", Proceedings of the 2003 International Conference on Machine Learning and Cybernetics (IEEE Cat. No.03EX693), Xi'an, Kina, vol. 2, str. 1153-1156, 2003., doi: 10.1109/ICMLC.2003.1259659

[13] P. Mitra, C. A. Murthy i S. K. Pal, "A probabilistic active support vector learning algorithm", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 26, no. 3, str. 413-418, 2004., doi: 10.1109/TPAMI.2004.1262340

[14] A. Westfeld , F"5—A Steganographic Algorithm", Information Hiding (IH 2001), Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, vol 2137., str. 289-302, 2001., doi: 10.1007/3-540-45496-9_21

[15] J. Fridrich, M. Goljan i D. Hogea, "Steganalysis of JPEG Images: Breaking the F5 Algorithm", Information Hiding (IH 2002), Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, vol 2578., str. 310-323, 2002., doi: 10.1007/3-540-36415-3_20

[16] N. Provos i P. Honeyman, "Detecting Steganographic Content on the Internet", Network and Distributed System Security Symposium, San Diego, SAD, str. 1-13, 2002.

[17] F. Alturki i R. Mersereau, "A novel approach for increasing security and data embedding capacity in images for data hiding applications", Proceedings International Conference on Information Technology: Coding and Computing, Las Vegas, NV, SAD, str. 228-233, 2001., doi: 10.1109/ITCC.2001.918796

[18] M. Curty i D. J. Santos, "Quantum Steganography", 2nd Bielefeld Workshop on Quantum Information and Complexity, Bielefeld, Njemačka, str. 12-14, 2000.

[19] S. Natori, "Why Quantum Steganography Can Be Stronger Than Classical Steganography", Quantum Computation and Information: Topics in Applied Physics, Springer, Berlin, Heidelberg, vol 102., str. 235-240, 2006., doi: 10.1007/3-540-33133-6_9

[20] K. Martin, "Steganographic Communication with Quantum Information", Information Hiding (IH 2007), Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, vol 4567., str. 32-49, 2007., doi: 10.1007/978-3-540-77370-2_3

[21] I. Banerjee, S. Bhattacharyya i G. Sanyal, "A Procedure of Text Steganography Using Indian Regional Language", International Journal of Computer Network and Information Security(IJCNIS), vol.4, no.8, str. 65-73, 2012., doi: 10.5815/ijcnis.2012.08.08

[22] B.A. Shaw i T.A. Brun, "Hiding quantum information in the perfect code", arXiv:1007.0793, 2010.

[23] J. Gea-Banacloche, "Hiding messages in quantum dana", Journal of Mathematical Physics, vol. 43, no. 9, str. 4531–4536, 2002., doi: 10.1063/1.1495073

[24] U. Sara, M. Akter i M. Uddin, "Image Quality Assessment through FSIM, SSIM, MSE and PSNR—A Comparative Study", Journal of Computer and Communications, vol. 7, no. 3, str. 8-18, 2019., doi: 10.4236/jcc.2019.73002

[25] N. K. El Abbadi, E. A. Al-Zubaidi, " Image Quality Assessment Tools", Journal of Xi'an University of Architecture & Technology, vol. 12, no. 3, str. 1260-1276, 2020., doi: 10.37896/JXAT12.03/10

[26] C. Chen et al., "TOPIQ: A Top-Down Approach From Semantics to Distortions for Image Quality Assessment", IEEE Transactions on Image Processing, vol. 33, str. 2404-2418, 2024., doi: 10.1109/TIP.2024.3378466

[27] Z. Wang, A. C. Bovik, H. R. Sheikh i E. P. Simoncelli, "Image quality assessment: from error visibility to structural similarity", IEEE Transactions on Image Processing, vol. 13, no. 4, str. 600-612, 2004., doi: 10.1109/TIP.2003.819861

[28] Z. Wang, E.P. Simoncelli i A.C. Bovik, "Multiscale Structural Similarity for Image Quality Assessment", The Thirty-Seventh Asilomar Conference on Signals, Systems & Computers, Pacific Grove, CA, SAD, str. 1398–1402., 2003., doi: 10.1109/ACSSC.2003.1292216

[29] Chaofeng Li i Alan C. Bovik "Three-component weighted structural similarity index", Proc. SPIE 7242, Image Quality and System Performance VI, 72420Q, 2009., doi: 10.1117/12.811821

[30] Recommendation ITU-T P.10/G.100: Vocabulary for performance, quality of service and quality of experience, 2017.

[31] L. Zhang, L. Zhang, X. Mou and D. Zhang, "FSIM: A Feature Similarity Index for Image Quality Assessment," in IEEE Transactions on Image Processing, vol. 20, no. 8, pp. 2378-2386, Aug. 2011, doi: 10.1109/TIP.2011.2109730.

[32] C. Chen et al., "TOPIQ: A Top-Down Approach From Semantics to Distortions for Image Quality Assessment," in IEEE Transactions on Image Processing, vol. 33, pp. 2404-2418, 2024, doi: 10.1109/TIP.2024.3378466.

[33] Bui, S. Agarwal, N. Yu i J. Collomosse, "RoSteALS: Robust Steganography using Autoencoder Latent Space", 2023 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Vancouver, BC, Kanada, str. 933-942, 2023., doi: 10.1109/CVPRW59228.2023.00100

Popis slika