Steganografija zasnovana na karakterističnim regijama slike

Bos, Mihaela

Steganografija zasnovana na karakterističnim regijama slike

Bos, Mihaela

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Mihaela Bos

STEGANOGRAFIJA ZASNOVANA NA KARAKTERISTIČNIM REGIJAMA SLIKE

Diplomski rad

Voditelj rada:
prof. dr. sc Andrej Dujella

Zagreb, 2021.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Do or do not,
there is no try.

Sadržaj

Uvod

Cilj ovog diplomskog rada je dati uvid u poznate steganografske i kriptografske tehnike koje se koriste za sakrivanje informacija u slike. Naglasak je na CR-BIS tehnici, odnosno steganografiji zasnovanoj na karakterističnim regijama slike.

Pojavom interneta, masovnom upotrebom računala za prijenos svih vrsta podataka, od videa, slika, običnih tekstualnih datoteka, pojavila se i potreba za zaštitom istih tih podataka. Najčešći pristup su kriptografske tehnike. Kriptografija transformira podatak koji šaljemo u beznačajne bitove upotrebom kriptografskih algoritama.

Za razliku od kriptografije koja samo transformira podatke, steganografija nudi puno više kako bi nadjačala sve slabosti koje nastaju korištenjem kriptiranja. Ona kamuflira postojanje tajnog podatka, tako da eventualni napadač nije ni svjestan da se podaci prenose.

Najčešći medij koji se koristi za sakrivanje poruka jesu slike, na koje ćemo se više usredotočiti u ovom radu.

U prvom poglavlju dajemo kratki pregled povijesti steganografije te općenite informacije o steganografiji i metodama koje se koriste nad slikama, kao što je navedeno u [7]. U drugom poglavlju u središtu je CR-BIS metoda predstavljena u [7], koju podrobnije obrađujemo. Opisujemo algoritme potrebne za izvedbu same metode, Blowfish algoritam, SURF metodu prema [1] te DWT metodu.

Poglavlje 1

Steganografija i steganaliza

1.1 Steganografija

Steganografija je znanstvena disciplina koja se bavi prikrivenom razmjenom informacija, a osnovna joj je zadaća prikrivanje postojanja informacija. Moderna steganografija koristi sve prednosti digitalne tehnologije, tako da informacije sakriva u slikovne, video ili audio datoteke. Koristi se u različite svrhe, kako privatno tako i poslovno.

1.1.1 Steganografija kroz povijest

U prošlosti su ljudi kao i danas imali potrebu sakrivati informacije jedni od drugih i tako pronalazili načine da to isto i ostvare.

Pojam steganografija Grčkog je podrijetla, a dolazi od riječi *steganos* što znači zaštićeno i riječi *graphei* što znači pisanje. Prva steganografska tehnika dolazi iz antičke Grčke, iz petog stoljeća pr. Krista. Miletski tiranin Histiaeus svom je robu obrijao glavu, pa na nju zapisao poruku koju je htio prenijeti. Nakon što je kosa narasla i pokrila tajnu poruku, mogao je poslati roba da ju prenese bez ičije sumnje. U istom tom vremenskom razdoblju, Grci koriste i drvene pločice prekrivene voskom za zapisivanje. Kako bi sakrili tajnu poruku, vosak su skidali s pločica, zapisivali poruku te pločicu ponovno prekrivali voskom. Tom je tehnikom tajna poruka mogla uspješno biti dostavljena bez otkrivanja.

Sljedeća tehnika koja se koristila je nevidljiva tinta. Kao tintu koristili su mlijeko, urin, voćni sok, te time pisali tajne poruke između linija teksta. Kako bi otkrili takvu poruku, koristili su toplinu ili svijetlo.

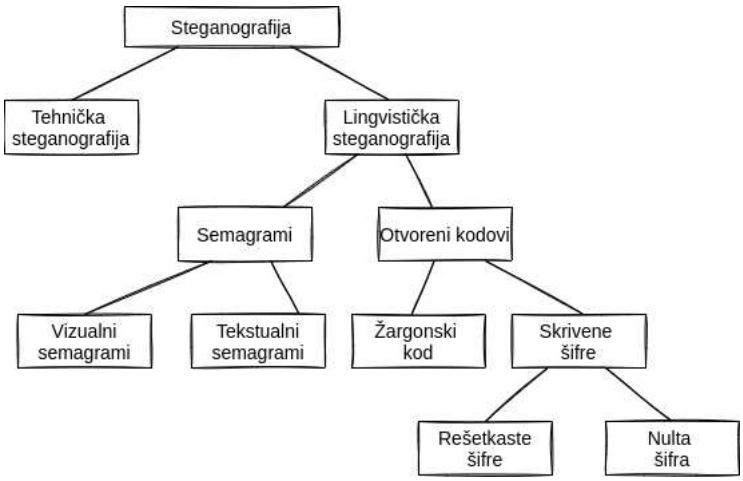
Steganografija se intenzivno koristila i u ratovima, a tijekom Drugog svjetskog rata, osim što su koristili nevidljivu tintu, Nijemci su razvili tehniku mikroteksta/mikrofotografije. To su bili cijeli dokumenti, slike, planovi, smanjeni na veličinu točke i zatim ubačeni

u običan tekst, npr. kao točka na *i* ili *zarez*, obojeni posebnom bojom, kako bi se, kada bi se prinijeli svijetlu mogli uočiti.

Nulta šifra (eng. *null cipher*) predstavlja još jednu tehniku gdje je tajna poruka zamaskirana unutar neke druge poruke koja ne privlači pozornost. Jedan od najpoznatijih primjera primjene te tehnike vezan je uz japansku špijunku Velvalee Dickinson, preprodavačicu lutaka, poznatu kao *Doll Woman* koja je tijekom Drugog svjetskog rata u svoje narudžbe sakrivala informacije o kretanjima brodova.

1.1.2 Steganografske tehnike

Slika 1.1: Taksonomija steganografskih tehnika



Postoje dva osnovna tipa steganografije: tehnička steganografija (eng. *tehnical steganography*) i lingvistička steganografija (eng. *linguistic steganography*) koje se granaju na tehnike kao što je prikazano na slici 1.1.

- **Tehnička steganografija** se koristi metodama kao što su one navedene u potpoglavlju 1.1.1.
- **Lingvistička steganografija** obuhvaća metode koje sakrivaju tajnu poruku u objekt nositelj na način da nositelj djeluje kao bezazleni skup informacija. [2]
  - **Semagrami** sakrivaju informacije koristeći različite simbole i znakove. Dijele se na vizualne i tekstualne semagrame.

- **Otvoreni kodovi** koriste javne kanale tj. neskrivenu komunikaciju za prijenos tajnih informacija. Dijelimo ih na:
  - **Žargonski kod** koristi jezik koji razumije samo određena skupina ljudi.
  - **Skrivene šifre** se odnose na one tajne poruke koje su umetnute u objekt nekom od metoda, a izdvojiti se mogu samo ako je ta metoda poznata. Dijelimo ih na:
    - **Rešetkaste šifre** za koje postoje predlošci pomoću kojih se pišu i kasnije čitaju tajne informacije umetnute u neki tekst.
    - **Nulta šifra** ima predefinirano pravilo, kao na primjer "čitaj svaku petu riječ" i tako ne zahtijeva korištenje kompliciranih algoritama za sakrivanje tajnih informacija.

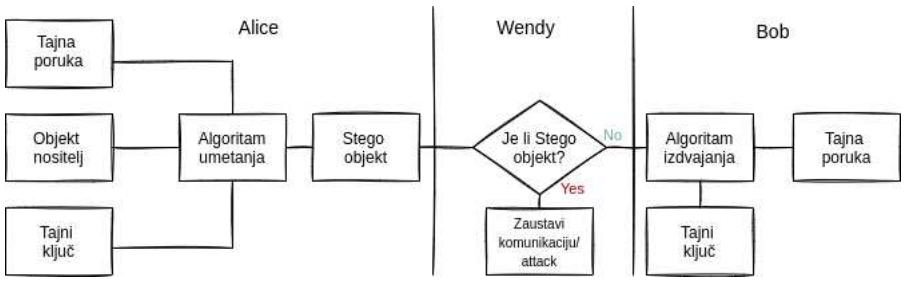
1.1.3 Osnovni principi i svojstva steganografije

Kako bi pobliže opisali osnovne principe moderne steganografije, koristimo primjer *problema zatvorenika* [7].

U opisu problema spominju se pojmovi objekt nositelj (eng. *cover object*), *stego*-objekt, *stego* ključ i steganaliza (eng. *steganalysis*) ili napad (eng. *attack*). Objekt nositelj je taj u koji se tajna poruka sakriva, odnosno služi za prikrivanje tajne poruke, dok je *stego*-objekt pojam koji predstavlja sliku koja sadrži tajnu poruku. *Stego* ključ se odnosi na parametar koji se koristi kako bi se zaštitio *stego*-objekt od neželjenog otkrivanja umetnutih tajnih podataka, a steganaliza je procesiranje i statistička obrada potrebna kako bi se otkrila tajna poruka.

Akteri našeg problema su Alice i Bob, dvoje zatvorenika te Wendy, zatvorski čuvar. Alice i Bob nalaze se u odvojenim ćelijama i žele napraviti plan bijega. Svu komunikaciju koja se odvija između njih nadzire Wendy. Kako Wendy ne bi posumnjala da njih dvoje komuniciraju o nečem tajnom, ne mogu slati kriptirane poruke, jer su one previše očite. Pošiljatelj poruke, algoritmom umetanja sakriva tajnu poruku u objekt nositelj. Dobiveni *stego*-objekt prenosi se komunikacijskim kanalom, u ovom slučaju preko Wendy do primatelja, koji postupkom izdvajanja poruke dobiva tajnu poruku. U slučaju da Wendy (napadač) posumnja na tajnu komunikaciju, ona može aktivno ili pasivno sudjelovati u prenošenju iste. Kao pasivni napadač, samo prisluškuje kanal, ali ako je aktivni napadač, može modificirati *stego*-objekt te prekinuti komunikaciju ili krivotvoreni objekt dalje poslati primatelju.

Slika 1.2: Shematski prikaz steganografskog sustava - Alice i Bob



Svojstva koja steganografski sustav mora zadovoljavati do neke određene razine kako bi bio siguran i uspješan su:

- nezamijećenost (suptilnost) (eng. *undetectability*),
- robusnost (eng. *robustness*),
- pouzdanost (eng. *reliability*),
- nosivost (eng. *payload capacity*).

Definicija 1.1.1. *Nezamijećenost (suptilnost) informacija mjeri koliko je teško uočiti postojanje tajnih informacija u stego-objektu. To je osnovno svojstvo steganografskog sustava.*

Sigurne steganografske metode moraju biti nezamijećene ljudskim okom, ali i ostalim statističkim napadima.

Kako bi se procijenila ta vrijednost, mjeri se "vizualna" razlika između objekta nositelja i stego-objekta uspoređivanjem.

Definicija 1.1.2. *Robusnost se odnosi na otpornost steganografskog sustava, odnosno koliko je teško izdvajanje skrivenih podataka iz stego-objekta ako se dogodi neki napad.*

Definicija 1.1.3. *Pouzdanost je najvažnije svojstvo relevantnog i egzaktnog steganografskog sustava. Nakon napada koji se mogu dogoditi, bitno je da nema gubitka podataka te da sve tajne informacije koje su umetnute u objekt dođu do primatelja u istom obliku kao što ih je pošiljatelj poslao.*

Definicija 1.1.4. *Nosivost je najveća moguća količina informacija koja može biti sigurno i nezamijećeno umetnuta u objekt nositelj*

Nije moguće zadovoljiti sva ova nabrojana svojstva odjednom, no kako bi steganografski sustav bio pogodan za korištenje, mora postojati neki kompromis između robusnosti, nezamijećenosti i nosivosti.

1.1.4 Primjena steganografije

Steganografija ima različitu i široku primjenu u modernom dobu. Neke od primjena su: [5]

- Unaprijeđene strukture podataka (eng. *Enhanced Data Structures*). Poznajemo osnovne strukture podataka, ali s vremenom i razvojem računala, softvera i općenito digitalizacijom, dolazi do potrebe da neke dodatne informacije o npr. slikama sakrijemo odnosno uključimo u samu sliku. To je primjenjivo u medicini, točnije radiologiji. Informacije o pacijentu i komentari ubačeni su u rendgensku snimku i nisu vidljivi golim okom, već pomoću posebnog softvera [7].

- Vodeni žig (eng. *Watermark*). Kreatori i autori digitalnog sadržaja poput filmova, videa, knjiga, glazbe, kako bi zaštitili daljnje neovlašteno širenje i kopiranje ubacuju u datoteke oznake koje nazivamo vodeni žig. Oznaka mora biti otporna na sve vrste napada i dalje se nalaziti na datoteci, bez obzira što je sve primijenjeno da bi se uklonila. Vodeni žigovi koriste se i na novčanicama, na putnim ispravama, poštanskim markama ...

- Privatne komunikacije (eng. *Private Comunications*). Korištene najviše u političke svrhe zbog prisluškivanja.

- Alati za praćenje dokumenata (eng. *Document-Tracking Tools*). Korištenjem steganografije možemo otkriti pravog autora ili vlasnika dokumenta, ako je dokument kruži kod neovlaštenih osoba ili je "procurio".

- Autentifikacija dokumenta (eng. *Document authentication*). Sakrivene informacije u dokumentima mogu sadržavati digitalni potpis, koji kasnije služi kao autentifikacija za pristup dokumentu.

1.2 Steganografske metode nad slikama

Kako se cijeli rad odnosi na steganografiju na slikama u digitalnom obliku, koje su najkorištenije u tu svrhu, a najbitniji dio je nova metoda CR-IBS, najprije je važno predstaviti metode koje se koriste duže vrijeme u svrhu umetanja informacija u slike, kako bi nakon predstavljanja nove metode uočili razlike i njene prednosti.

Slika je u računalu prikazana kao konačni niz brojeva koji predstavljaju piksele. Pikseli su najmanji elementi slike koji sadrže informacije o svjetlini neke boje na određenom mjestu u slici, koja je zapravo reprezentirana matricom piksela (eng. *raster graphics*). Svaki piksel se sastoji od 3 vrijednosti, crvena, zelena i plava (RGB model), koje čine konačnu boju, u rangu između 0 i 255, odnosno, svaka vrijednost ima 8-bita, što piksel čini 24-bitnom vrijednošću. Kako bi se smanjila količina memorije koju slika zauzima, slike se

sažimaju, pa tak imamo 2 osnovne tehnike koje se koriste: bez gubitaka (eng. *lossless*) i s gubitcima (eng. *lossy*).

GIF (eng. *Graphic Interchange Format*), njegova zamjena PNG (eng. *Portable Network Graphics*) te BMP (eng. *bitmap file*) su primjeri lossless tehnike, a JPEG (eng. *Joint Photographic Experts Group*) je primjer lossy tehnike. To su ujedno najkorišteniji formati u steganografiji.

Klasifikaciji metoda koje se koriste može se pristupiti na više načina, ovisno o tome što mijenjamo kod umetanja informacija ili kakav objekt nositelj koristimo, no u nekim slučajevima klasifikacija nije moguća. U ovom radu koristimo klasifikaciju kao u [7]. Prije samog navođenja metoda, slijedi detaljniji opis samog procesa. Slika 1.2 grafički prikazuje proces kojeg možemo opisati i formulom.

Neka C označava objekt nositelj (eng. *cover carrier*) i $C^{\smile}$ stego-objekt. K predstavlja ključ kojim ili kodiramo poruku ili stvaramo pseudo-šum na objektu nositelju, a M predstavlja poruku koju trebamo prenijeti. E_m i E_x će označavati redom ubačenu poruku i izdvojenu poruku.

$$E_m : C \oplus M \oplus K \rightarrow C^{\smile} \tag{1.1}$$

$$E_x\left(E_m\left(c, m, k\right)\right) \approx m, \forall c \in C, m \in M, k \in K \tag{1.2}$$

Steganografske metode koje uključuju modifikaciju slika su sljedeće:

- Metode prostorne domene ili supstitucijske metode (eng. *Spatial domain*)
- Metode transformacije domene (eng. *Transform domain*)
- Metode raspršenog slijeda (eng. *Spread spectrum*)
- Statističke metode (eng. *Statistical methods*)
- Tehnike izobličavanja (eng. *Distortion techniques*)

1.2.1 Supstitucijske metode

Osnovni princip supstitucijskih metoda je zamjena redundantnih dijelova objekta nositelja, odnosno slike, koji su ionako nevidljivi ljudskom oku. Supstitucija bita najmanje važnosti - LSB (eng. *Least Significant Bit*) najčešća je supstitucijska metoda. Bazirana je na činjenici da je bit najmanje važnosti zapravo slučajni šum čijom promjenom se ne stvara neka velika razlika na cijeloj slici.

Postoje dva sustava, uzastopni (eng. *sequential*) i nasumični (eng. *scattered*) koji koriste LSB algoritme. Kod prvog je poruka umetnuta u uzastopne najmanje važne bitove, kao u primjeru 1.2.1, dok kod razbacanog sustava poruku ubacujemo u nasumično odabrane bitove.

Sljedećim jednostavnim primjerom prikazuje se osnovna ideja LSB metode temeljene na uzastopnom sustavu.

Primjer 1.2.1. *Neka je* B *poruka koja treba biti sakrivena u 8 bitni objekt nositelj. ASCII kod poruke je* 01000010 *i uzmimo da je 8 uzastopnih piksela s gornjeg lijevog kuta objekta nositelja* 00100101 11100001 11001000 00100101 11001010 11101000 11001001 00101111. *Rezultat umetanja može biti sljedeći:* 00100100 11100001 11001000 00100100 11001010 11101000 11001001 00101110*, gdje označeni bitovi predstavljaju umetnute vrijednosti poruke.*

1.2.2 Metode transformacije domene

Ove metode baziraju se na sakrivanju informacija pomoću matematičkih funkcija. Osnovni princip je sličan onom kao kod LSB metode, ali su metode robusnije jer sakrivaju podatke u područja slike za koja je manje vjerojatno da će biti kompresirana, rezana ili bilo kako promijenjena. Najčešće se koriste diskretna kosinusna transformacija (eng. *Discrete Cosine Transformation, DCT*), diskretna Fourierova transformacija (eng. *Discrete Fourier Transformation, DFT*) i diskretna valna transformacija (eng. *Discrete Wavelet Transform, DWT*).

U 2-dimenzionalnoj DCT fazi, svaki od 8×8 blokova koji se ne preklapaju se pretvara u DCT domenu pomoću 2-dimenzionalne DCT metode, dane formulom:

$$F(u,v) = \frac{c(u)c(v)}{4} \sum_{i=0}^{7} \sum_{j=0}^{7} \cos\left(\frac{(2i+1)u\pi}{16}\right) \cos\left(\frac{(2j+1)v\pi}{16}\right) f(i,j) \tag{1.3}$$

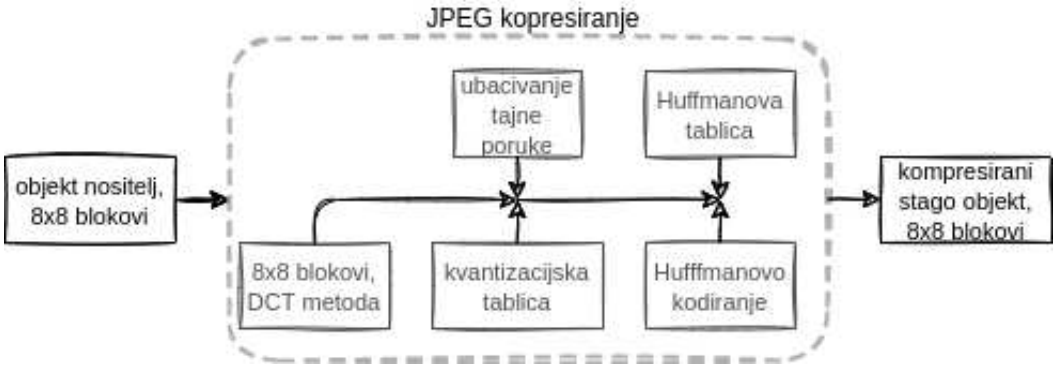
gdje je funkcija $c(e)$ definirana kao:

$$c(e) = \begin{cases} \frac{1}{\sqrt{2}}, & e = 0 \\ 0, & e \neq 0 \end{cases}. \tag{1.4}$$

$F(u,v)$ i $f(i,j)$ predstavljaju redom DCT koeficijent na koordinati (u,v) i vrijednost piksela na koordinati (i,j). $F(0,0)$ naziva se jednosmjernom (DC) komponentom, a ostale $F(u,v)$ se nazivaju naizmjeničnim komponentama (AC). Za redukciju podataka u koraku kvantizacije dobiveni koeficijenti kvantizirani su koristeći kvantizacijsku tablicu.

Format najkorišteniji s ovom metodom je JPEG, a sljedeći graf prikazuje sam proces DCT metode na JPEG slici.

Slika 1.3: Steganografski sistem baziran na DCT metodi



1.2.3 Metode raspršenog slijeda

Raspršeni spektar (SS) je korišten još u 1950-ima u radijskoj komunikaciji. U steganografiji je primijenjen isti princip, poruka se raspriši preko cijelog objekta nositelja i tako ju je teže uočiti. Jačina signala poruke koja je ubačena u objekt nositelj je manja od samog signala objekta nositelja, pa tako ubačeni podatak postane neuočljiv ljudskom oku, ali isto tako i računalnim analizama.

1.2.4 Statističke metode

Kako bi se prenijela poruka, slika se mora podijeliti na blokove, i to na onoliko blokova kolika je i veličina poruke. Princip je opisan formulom:

$$f(B_i) = \begin{cases} 1, & \text{blok } B_i \text{ je izmijenjen u procesu umetanja poruke} \\ 0, & \text{nema izmjena} \end{cases}. \tag{1.5}$$

B_i predstavljaju blokove na koje je slika podijeljena, m_i predstavlja i-ti bit poruke koja se umeće, ako je on jednak 1, dolazi do izmjene i-tog bloka, a ako je 0, blok ostaje nepromijenjen.

Statističke metode podložne su rezanju, rotiranju i skaliranju koji se događaju prilikom napada pa su zato i manje uspješne od ostalih metoda.

1.2.5 Tehnike izobličenja

Tehnike izobličenja ne sakrivaju tajnu poruku direktno u objekt nositelj, već stvaraju neke izmjene na nositelju kako bi se poruka prenijela. Zato je prilikom izdvajanja tajne po-

ruke potrebno imati podatke o originalnom objektu nositelju, jer tijekom procesa dekoder promatra razliku između stego-objekta i originalnog objekta nositelja.

1.2.6 Evaluacija stegnografskih metoda nad slikama

Već ranije navedeno je koja sva svojstva neki steganografski sustav treba imati. Najbitnija i ona koja uspoređujemo za gore navedene metode su: nezamijećenost, robusnost i nosivost.

LSB metoda je praktična za umetanje tajnih poruka, ali je osjetljiva na male promjene nastale procesiranjem slike ili sažimanjem u drugi format. LSB tehnike mogu sakriti veliku količinu podataka, pa imaju veliku nosivost, ali baš zbog toga štete svojstvima slike, pa su neotporne na statističke napade.

DCT, DWT tehnike nisu otporne na napade, pogotovo ako je sakrivena informacija mala. Mijenjaju koeficijente u transformacijskoj domeni i većinom imaju malu nosivost u usporedbi sa supstitucijskim metodama.

Metode raspršenog slijeda su općenito vrlo otporne na statističke napade, pošto je sakrivena poruka raspršena po cijeloj slici, no neke tehnike napada kao što je redukcija šuma omogućuju otkrivanje poruke. Ova je metoda vrlo korištena u vojne svrhe baš zbog robusnosti. Također imaju veliku nosivost, pa su zapravo vrlo pogodne steganografske metode.

Statističke metode su u većini slučajeva neotporne na napade koji uključuju rezanje, rotacije, skaliranje slike, te na napade za otkrivanje vodenog žiga. Nosivost i nezamijećenost ovise o objektu nositelju.

Tehnike izobličavanja su manje sigurne zbog slanja objekta nositelja, kako bi se poruka mogla izdvojiti na kraju. Otporne su na napade koji uključuju rezanje, skaliranje i rotiranje, a primatelj vrlo lako može vratiti stanje slike u ono kakvo je bilo kad je poruka ubačena.

	LSB	**Transformacije domene**	**Metode raspršenog slijeda**	**Statističke metode**	**Tehnike izobličavanja**
Nezamijećenost	Visoka*	Visoka	Visoka	Srednja*	Niska
Robusnost	Niska	Visoka	Srednja	Niska	Niska
Nosivost	Visoka	Niska	Visoka	Niska*	Niska

Tablica 1.1: Usporedba steganografskih tehnika na slikama (*: označava ovisnost o objektu nositelju) [7]

1.3 Steganaliza

Cilj steganografije je izbjeći privlačenje pažnje i sumnji da kod prijenosa postoji sakrivena informacija, tako da ona ostane neotkrivena. Ako i samo postoji sumnja, cilj nije postignut. Za razliku od toga, ciljevi steganalize su identifikacija sumnjivih podataka, utvrđivanje jesu li podaci koji su umetnuti u objekt nositelj kriptirani, utvrđivanje postoji li šum u stego-objektu te samo izdvajanje i dekriptiranje umetnute poruke.

Kod kriptografije znamo da postoji poruka, koja je samo kriptirana, a pomoću kriptoanalize ona se može otkriti, ali kod steganografije postoji samo skup nekih podataka za koje nismo sigurni sadrže li sakrivene podatke. Korištenjem različitih metoda, steganalitičar dolazi do konačne poruke. Koje će metode napada upotrijebiti da dođu do podataka, ovisi i o količini i vrsti dostupnih informacija. Postoji nekoliko vrsta napada u steganalizi:

- Samo steganografska datoteka (eng. *Stego-only attack*). Dostupan je samo konačan stego-objekt za analiziranje.
- Poznati objekt nositelj (eng. *Known cover attack*). Originalan objekt nositelj i stego-objekt su dostupni za analizu.
- Poznata poruka (eng. *Known message attack*). Dostupna je tajna poruka, a napadač može tražiti u stego-objektu dijelove koji odgovaraju poruci te tako ubrzati i pospješiti napad. No ponekad ni poznavanje poruke nije dovoljno i jednako je teško kao i *stego-only attack*.
- Odabrana steganografska tehnika (eng. *Chosen stego attack*). Poznata je steganografska tehnika (algoritam) i stego-objekt.
- Odabrana poruka (eng. *Chosen message attack*). Steganalitičar generira stego-objekt pomoću nekog alata ili algoritma iz odabrane poruke. Cilj ovog napada je odrediti odgovarajuće uzorke u stego-objektu koji mogu ukazivati na korištenje specifičnih alata ili algoritama.
- Poznat nositelj i odabrana steganografska tehnika (eng. *Known stego attack*). Poznat je stego-objekt, odnosno produkt steganografske metode ili algoritma te objekta nositelja koji su također poznati.

Poglavlje 2

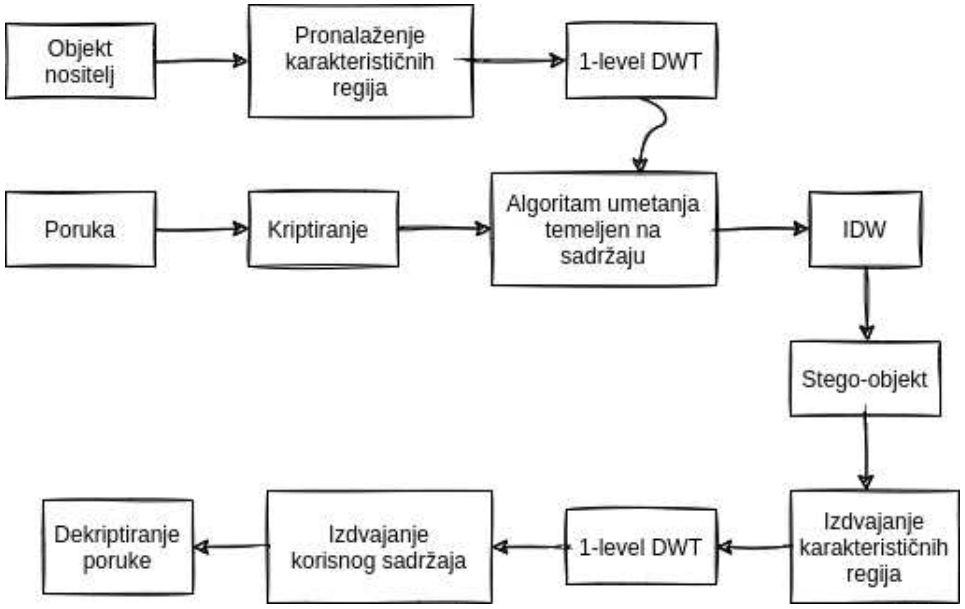
CR-BIS metoda

Steganografija zasnovana na karakterističnim regijama slike (eng. *Characteristic Region-Based image Steganography*) nova je metoda predstavljena u [7]. Metode koje se trenutno koriste, a neke od njih su nabrojane u prijašnjem poglavlju, utječu na kvalitetu slike i povećavaju mogućnost gubitka podatka, nekima je cilj osigurati robusnost, dok je drugima važnija nezamijećenost, što se pokušava izbjeći u novoj metodi, ona osigurava robusnost i nezamijećenost istovremeno.

Kako bi se to ostvarilo, CR-BIS metodom informacije se sakrivaju u robusne lokacije na slici, ali prije toga su kriptirane, a zatim se pronađe najbolji dio slike kako bi se podaci mogli sakriti. Nakon toga, umetanje se izvršava pomoću valne transformacije (DWT) koeficijenata.

2.1 Uvod u CR-BIS metodu

Slika 2.1: Dijagram CR-BIS metode



Dijagram 2.1 prikazuje proces CR-BIS metode koji se sastoji od tri koraka. Svaki od ta tri koraka može funkcionirati zasebno, ne nužno u svrhu steganografije, a kombiniranjem u CR-BIS metodu, daju željene rezultate.

Podaci koje se umeću u objekt nositelj najprije se kriptiraju Blowfish algoritmom, zatim se pomoću SURF algoritma identificiraju područja na slici u koja će kriptirane informacije biti umetnute. Posljednji, treći korak metode je umetanje informacija, koje se izvodi pomoću diskretne valne transformacije (DWT).

2.2 Kriptiranje podataka

2.2.1 Blowfish algoritam

Algoritam je dizajnirao Bruce Scheiner 1993. godine kao alternativu DES algoritmu. Slobodan je za korištenje, a dolazi i kao dio Linuxa. Dizajniran je da bude brz, da se može izvoditi na računalima s malom memorijom, jednostavan je za implementaciju i ključ kojim kriptira varira ovisno o duljini podataka koji se kriptiraju do duljine od 448 bitova. Sastoji se od dvije faze. U prvoj, *key-expansion* fazi, od zadanog ključa koji je maksimalne

duljine 448 bitova, generiraju se podključevi, ukupne duljine 4168 bajtova. Druga faza, kriptiranje podataka, zapravo je 16-ciklusna Feistelova mreža, pri čemu se svaki ciklus sastoji od permutacije ovisne o ključu i supstitucije ovisne o ključu i samom podatku. Sve operacije su XOR operacije i zbrajanje na 32-bitnim riječima, te adresiranje četiri vektora u svakom ciklusu. Dekriptiranje je slično kriptiranju, samo što se podključevi koriste u obrnutom redoslijedu.

2.2.2 Generiranje podključeva

Svi ključevi su 32-bitni, podijeljeni su u P niz te četiri S-tablice (S-box 1, S-box 2, S-box 3, S-box 4). P niz sadrži 18 podključeva, $P_1, P_2, \ldots, P_{18}$, a svaki se koristi u jednoj iteraciji kriptiranja bloka podataka i dodatna dva, za kriptiranje na kraju procesa. Svaka S-tablica sastoji se od 256 zapisa:

$$S_{1,0}; S_{1,1}; \ldots S_{1,255}$$

$$S_{2,0}; S_{2,1}; \ldots S_{2,255}$$

$$S_{3,0}; S_{3,1}; \ldots S_{3,255}$$

$$S_{4,0}; S_{4,1}; \ldots S_{4,255}$$

Kako sam algoritam koristi puno podključeva, oni se moraju izgenerirati unaprijed, prije nego započne kriptiranje ili dekriptiranje. Samo generiranje podključeva odvija se u nekoliko koraka:

- Korak 1: Inicijalizira se polje P, S_1, S_2, S_3, S_4 decimalnim znamenkama zapisa broja π u bazi 16, tako da se P_1 postavi na prvih 8 decimalnih znamenki, P_2 na sljedećih 8 i tako sve dok se ne popuni niz P, a zatim se nastavlja s nizom S. Ukupno je potrebno $18 \times 8 + 4 \times 256 \times 8 = 8336$ znamenki.

$$\pi_{(16)} = 3.243f6a8885a308d313198a2e0370734\ldots$$

$$P_1 = 243f6a88$$

$$P_2 = 85a308d3$$

$$P_3 = 13198a2e$$

$$P_4 = 03707344$$

$$\vdots$$

- Korak 2: Zadani ključ K podijeli se na dijelove od po 32-bita i kombinira na sljedeći način sa podključevima iz P niza:

```
za i = 1 do 18 radi:
    P[i] = P[i] XOR $i$-tih 32 bita od K
```

- Korak 3: Kriptira se zero-string (64 binarne nule) s Blowfish algoritmom koristeći ključeve iz koraka 1 i 2.
- Korak 4: P_1 i P_2 zamijene se s vrijednostima dobivenim u koraku 3.
- Korak 5: Rezultat koraka 3 se kriptira koristeći Blowfish algoritam s novim modificiranim podključevima.
- Korak 6: P_3 i P_4 zamijene se s vrijednostima dobivenim u koraku 5.
- Korak 7: Proces kriptiranja i mijenjanja podključeva nastavlja se dok ne zamijenimo sve vrijednosti P_i za $i = \{5, \ldots, 18\}$ i zatim isti postupak primijenimo na vrijednosti S_1, S_2, S_3, S_4.

Da bi se generirali svi podključevi, potrebno je 521 iteracija.

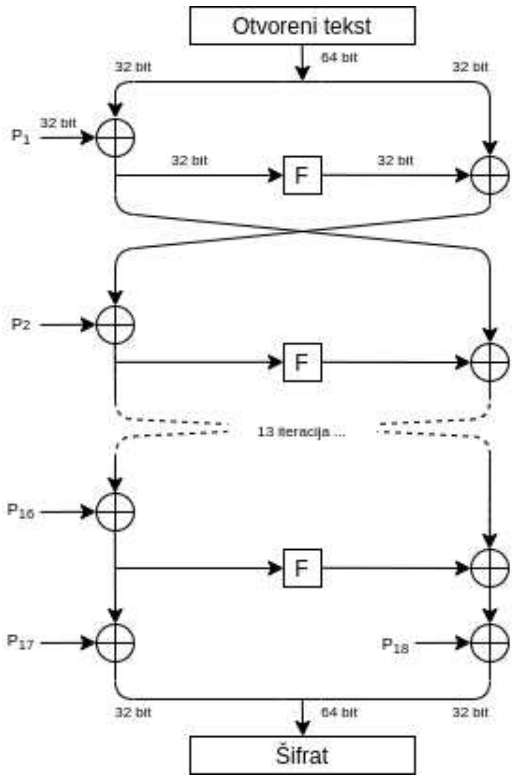
2.2.3 Kriptiranje

Ulaz algoritma je 64-bitni podatak odnosno otvoreni tekst, koji će biti pretvoren u 64-bitni šifrat. Otvoreni tekst podijeljen je na dva 32-bitna segmenta lijevi L_1 i desni R_1. Na dijagramu 2.2 je prikazan princip kriptiranja u Blowfish algoritmu. U svakoj od 16 iteracija ponavlja se sljedeći postupak: Operacija XOR se izvrši između segmenta L_i i podključa P_i, a zatim se rezultat prosljeđuje funkciji F (Feistelova funkcija) da permutira podatak i izbaci novi 32-bitni segment. Operacija XOR se sada izvršava između rezultata funkcije F i desnog segmenta R_i. Tada se lijevi i desni segment zamijene, a postupak se ponavlja.

```
za i = 1 do 16 radi:
    L[i] = L[1] XOR P[1]
    R[i] = F(L[i]) XOR R[i]
    zamijeni L[i] i R[i]
```

Izlaz nakon 16 iteracija su dva 32-bitna segmenta, L i R, koja se opet zamijene da ponište zadnju zamjenu. Zatim se izvršavaju posljednje operacije nad ta dva segmenta, R = R XOR P[17] i L = L XOR P[18]. Dobiveni segmenti L i R se spajaju, a dobiveni 64-bini izlaz predstavlja šifrat.

Slika 2.2: Blowfish algoritam

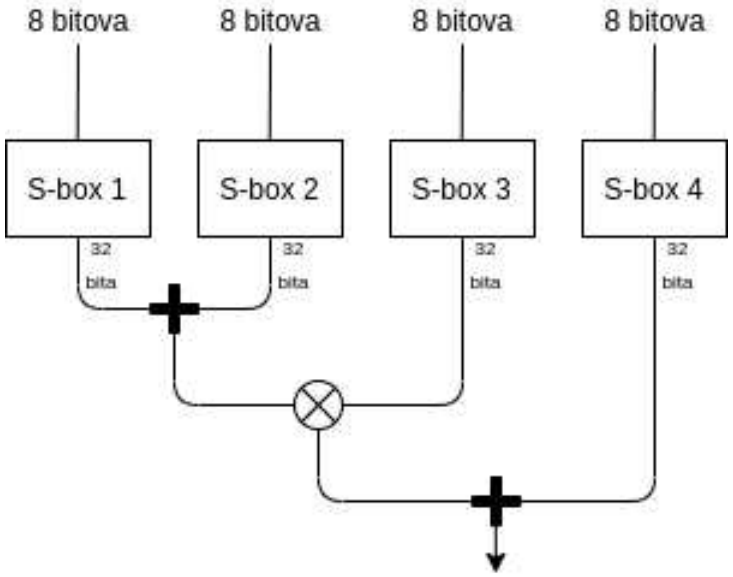


2.2.4 Funkcija enkripcije F

Funkcija F predstavlja najkompliciraniji dio Blowfish algoritma i jedini dio gdje se koriste S-tablice. F podijeli 32-bitni ulaz na četiri 8-bitna dijela, od kojih je svaki transformiran u 32-bitni podatak pomoću odgovarajuće S-tablice. Izlazni podaci S-tablica, koji su 32-bitni, zbrojeni su $\mod 2^{32}$, zatim je izvršena operacija XOR i na kraju zbrajanje $\mod 2^{32}$ koje daje konačni izlaz funkcije F. Funkciju možemo zapisati i formulom:

$$F(L_i) = \left(\left(S_{1,a} + S_{2,b} \mod 2^{32}\right) \text{XOR } S_{3,c}\right) + S_{4,d} \mod 2^{32} \tag{2.1}$$

Slika 2.3: Feistelova funkcija



2.3 Pronalaženje područja za umetanje SURF algoritmom

Većina tehnika koje odabiru područja u koja bi podaci mogli biti umetnuti, kao SIFT detektor, nisu otporne na geometrijske promjene koje se događaju prilikom napada. Podaci su tako izgubljeni ako napadač rotira, izreže ili translatira sliku. Bitno je da poručja koja se odaberu kod umetanja podataka budu jednaka onima kod dekriptiranja, a metoda SURF (eng. *Speeding up Robust Features*) predstavljena 2006. u radu Herberta Baya [1] pruža takvu sigurnost. Podaci su umetnuti u područna slike sa specifičnim statističkim svojstvima, a sama metoda osigurava da se nakon potencijalnih napada podaci ne izgube.

Za razliku od spomenutog SIFT detektora, SURF koristi samo aproksimaciju Hessianove matrice, radi brže i koristi integralne slike koje smanjuju vrijeme izračunavanja.

2.3.1 SURF detektor

2.3.2 Integralne slike

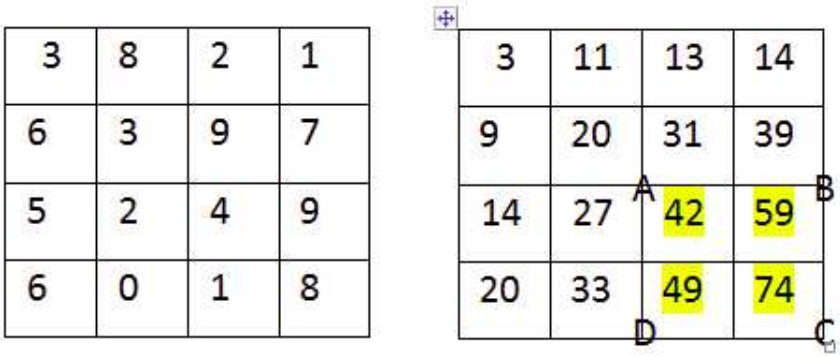
Pojam integralne slike (eng. *integral image* predstavljen je 1984. godine i omogućava brzo izračunavaje konvolucija kvadratnih tipova filtara. Vrijednost integralne slike $I_{\sum}$ na poziciji

$\mathbf{x} = (x, y)^T$ predstavljena je sumom svih piksela početne slike I u kvadratnoj površini koju čini početak slike i pozicija $\mathbf{x}$.

$$I_{\sum}(\mathbf{x}) = \sum_{i=0}^{i \leq x} \sum_{j=0}^{j \leq y} I(i, j) \tag{2.2}$$

Jednom kada je izračunata $I_{\sum}$, vrijeme potrebno da se dobije suma intenziteta bilo koje uspravne kvadratne površine je konstantno, odnosno ne ovisi o veličini kvadratne površine.

Slika 2.4: Lijevo: ulazna slika, desno: integralna slika



Primjer izračuna za sliku 2.4:

$$suma = C + A - B - D.$$

2.3.3 Detekcija točaka interesa pomoću Hessianove matrice

SURF koristi Hessianovu matricu zbog njene točnosti i brzine izračunavanja. Također, pronalazi "grbolike" (eng. *blob-like structures*) strukture na mjestima gdje je vrijednost determinante najveća.

Hessianova matrica $\mathcal{H}(\mathbf{x}, \sigma)$, na poziciji $\mathbf{x}$, sa skalom σ definirana je formulom 2.3.

$$\mathcal{H}(\mathbf{x}, \sigma) = \begin{bmatrix} L_{xx}(\mathbf{x}, \sigma) & L_{xy}(\mathbf{x}, \sigma) \\ L_{xy}(\mathbf{x}, \sigma) & L_{yy}(\mathbf{x}, \sigma) \end{bmatrix} \tag{2.3}$$

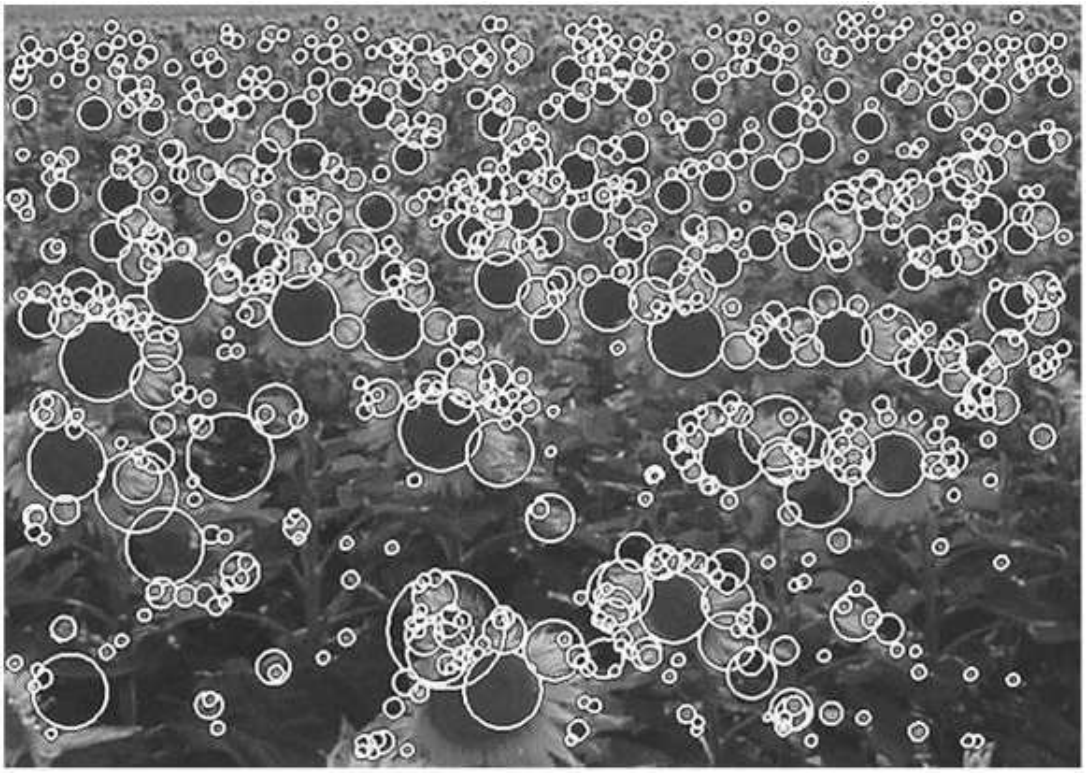
$L_{xx}(\mathbf{x}, \sigma)$ predstavlja konvoluciju Gaussove druge parcijalne derivacije $\frac{\partial}{\partial x^2} g(\sigma)$ sa slikom I na poziciji $\mathbf{x}$ i analogno za L_{xy} i L_{yy}. Na kraju, Hessianova matrica se aproksimira korištenjem box filtera, koji aproksimiraju Gaussovu derivaciju drugog reda i mogu se izračunati jako brzo korištenjem integralnih slika [1]. Determinantu Hessianove matrice

tada dobivamo pomoću formule 2.4, gdje D_{xx}, D_{yy} i D_{xy} redom predstavljaju parcijalne derivacije drugog reda u *x*-smjeru, *y*-smjeru i *xy*-smjeru.

$$\det\left(\mathcal{H}_{approX}\right) = D_{xx}D_{yy} - \left(0.9D_{xy}\right)^2 \tag{2.4}$$

Determinanta aproksimirane Hessianove matrice predstavlja odziv *blob* strukture u slici na poziciji **x**, a ti se odzivi spremaju u mapu odziva *blob* struktura te se unutar tih mapa detektiraju lokalni maksimumi.

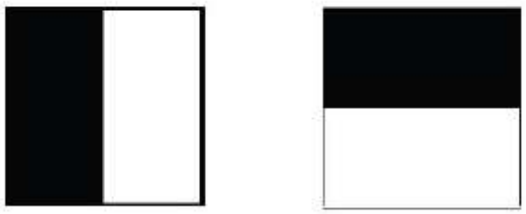
Slika 2.5: Detektirane točke interesa [1]



2.3.4 SURF opisnik

SURF opisnik opisuje distribuciju intenziteta kroz susjedstvo točke interesa, slično kao kod SIFT opisnika. Opisnik je baziran na vrijednostima Haarovih valića prvog reda u *x* i *y* smjeru (slika 2.6).

Slika 2.6: Tipovi Haarovih valića korištenih za SURF

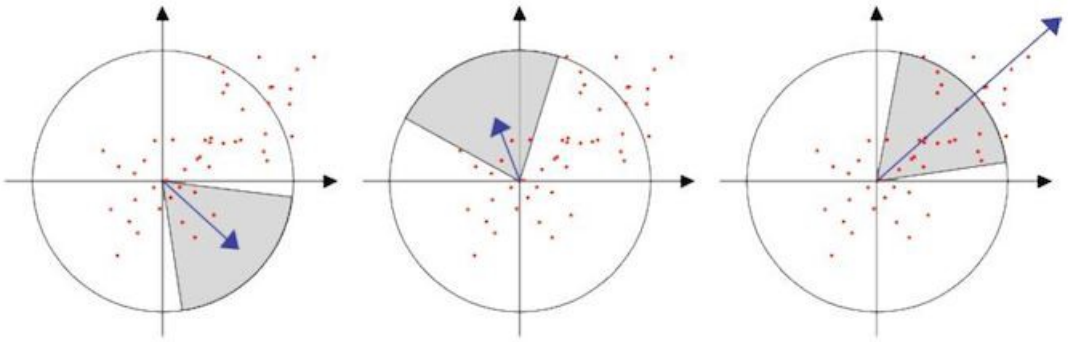


Kako bi deskriptor bio invarijantan na rotacije, prvo se pronalazi reproducibilna orijentacija točke interesa. Za ostvarivanje toga radi se sljedeće:

1. Najprije se dobije rezultat Haarovog valića u x i y smjeru (slika 2.6) i to u radijusu $6s$ oko točke interesa, gdje je s skala na kojoj je ta točka detektirana.

2. Nakon što su dobiveni rezultati Haarovih valića i podijeljeni s Gaussianom ($\sigma = 2.5s$), predstavljeni su kao vektori u prostoru s centrom u točki interesa. Orijentacija vektora dobije se kao suma svih rezultata unutar "prozora" veličine $\frac{\pi}{3}$ kao na slici 2.7.

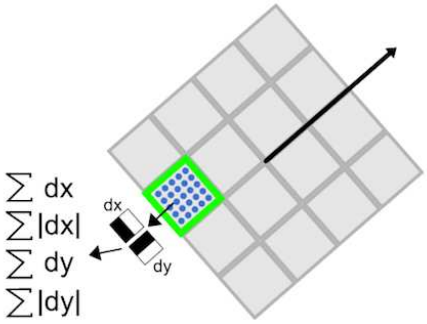
Slika 2.7: Rezultati Haarovih valića predstavljeni kao vektori



Zatim je potrebno izdvojiti deskriptor, također u dva koraka:

1. Započinjemo konstrukcijom kvadratnog područja centriranog oko točke interesa i orijentiranog rotacijom dobivenom u prethodnom koraku. Veličina tog područja je $20s$. Primjer tih područja prikazan je na slici 2.8 (a).

(a)



(b)

Slika 2.8: (a) Različite veličine područja deskriptora (b) Izgled deskriptora

2. Zatim je svako područje podijeljeno na 4×4 podregije kako bi zadržali sve važne informacije. Za svaku podregiju izračunate su jednostavne značajke. Zbrajaju se rezultati Haarovih valića u horizontalnom d_x i vertikalnom d_y smjeru za svaku podregiju, a to je ujedno prvi set podataka u vektoru značajki. Za podatke o polarnosti koristimo apsolutne vrijednosti $|d_x|$ i $|d_y|$ te to čini drugi set značajki. Ilustracija postupka vidljiva je na slici 2.8 (b).

Svaka podregija sada ima četiri-dimenzionalni deskriptor (vektor) v:

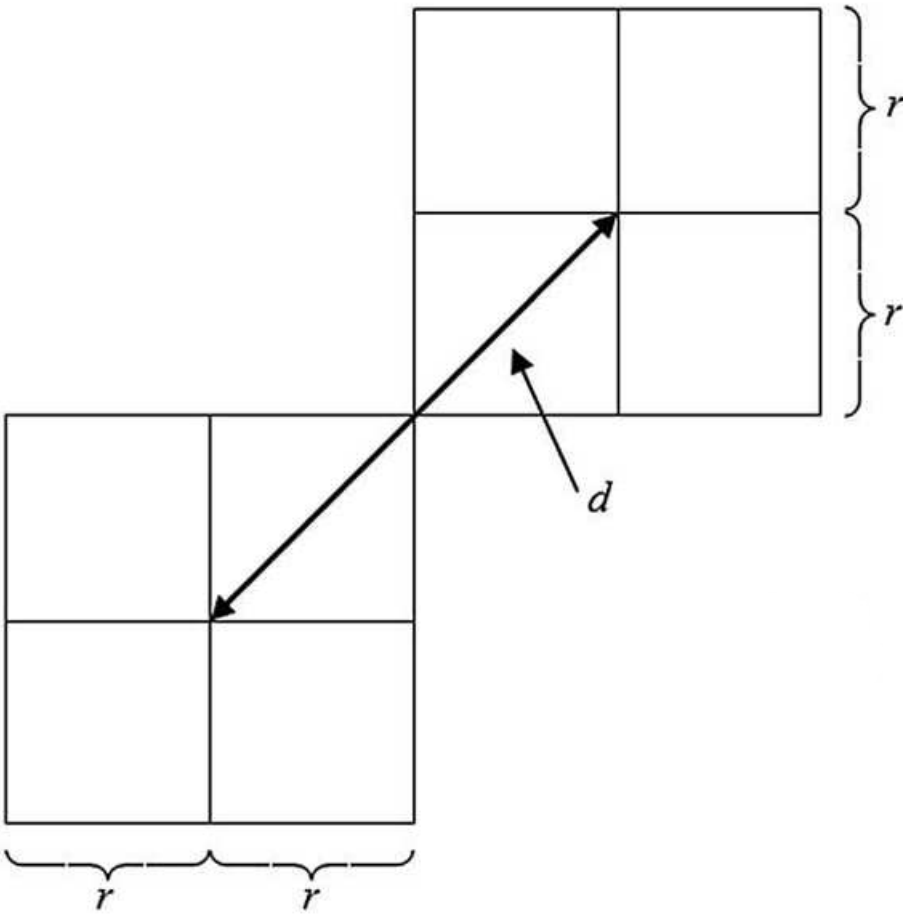
$$v = \sum \Big(d_x + d_y + |d_x| + |d_y| \Big).$$

Spajanjem ovakvog vektora za sve 4×4 podregije dobivamo konačni vektor značajki duljine 64.

Na kraju, deskriptor vektori se uspoređuju za različite slike. Usporedba se temelji na Euklidskoj udaljenosti vektora, samo za značajke s istim tipom kontrasta [1].

Kako bi izbjegli preklapanje područja koja su odabrana SURF algoritmom, mjeri se Euklidska udaljenost d između svih odabranih točaka i ona ne smije prelaziti vrijednost od $2\sqrt{2}r$ (slika 2.9), pošto je veličina područja za umetanje informacija $2r \times 2r$, analogno ako su područja kružnog oblika, d ne smije prelaziti $2r$.

Slika 2.9: Odabir disjunktnih područja



2.4 Umetanje informacija

Nakon što smo kriptirali informacije za umetanje i odredili područja u koja će iste biti sakrivene, posljednji korak je samo umetanje tih informacije DWT metodom.

DWT je popularna metoda kad se govori o procesiranju slika, pogotovo kod sažimanja slika. Zato baš je i koristimo ovdje, pošto je poprilično otporna na JPEG sažimanje i na šumove.

DWT je izabrana i radi dvije bitne karakteristike:

- Valna transformacija bolje modelira model ljudskog vizualnog sustava (HVS), nego DCT.
- Vizualne promjene nakon DWT transformacije manje su očite i manje uočljivije u usporedbi s onima nakon DCT transformacije, jer DWT ne rastavlja sliku u blokove kod samog procesa transformacije.

2.5 Izvođenje opisane metode

2.5.1 Faza umetanja podataka

Slika 2.10: Definiranje područja za ubacivanje informacija

DWT tehnika odabrana je zbog dobrih svojstava navedenih u poglavlju 2.4. Slijedi opis koraka ubacivanja tajnih podataka u objekt nositelj:

1. Karakteristične regije odabiru se na objektu nositelju pomoću SURF tehnike, izbjegavajući preklapanja, a prilikom toga neka su područja odbačena.

2. Koristeći konačnu listu točaka odabranih u prethodnom koraku, područja za umetanje informacija su pozicionirana na objektu nositelju kao krugovi sa $r = 64$. (slika 2.10)

3. Prvi korak diskretne valne transformacije obavlja se na svakom području zasebno, kako bi dobili koeficijente. Za CR-BIS metodu koristi se 9/7 biortogonalni valići, odnosno CDF val.

4. Horizontalni i vertikalni koeficijenti su učitani pomoću raster metode. Zatim su umetnuti bitovi informacije na način da se vrijednosti koeficijenata prilagode, kao na slici 2.11.

5. Za bit b informacije koju ubacujemo, odgovarajući horizontalni i vertikalni valni koeficijenti su odabrani, redom označeni sa $H(x, y)$ i $V(x, y)$. Zatim je bit b ubačen tako da je povećana razlika između $H(x, y)$ i $V(x, y)$ po sljedećim pravilima:

   - Ako je $b = 1$ i $D_1 = H(x, y) - V(x, y) < T$ gdje je T vrijednost kojom se kontrolira nevidljivost informacija, $H(x, y)$ se treba povećati, a $V(x, y)$ smanjiti. Faza je završena umetanjem informacija po formuli:

   $$\hat{H}(x, y) = H(x, y) + \frac{T - D_1}{2}$$

   $$\hat{V}(x, y) = V(x, y) - \frac{T - D_1}{2}$$

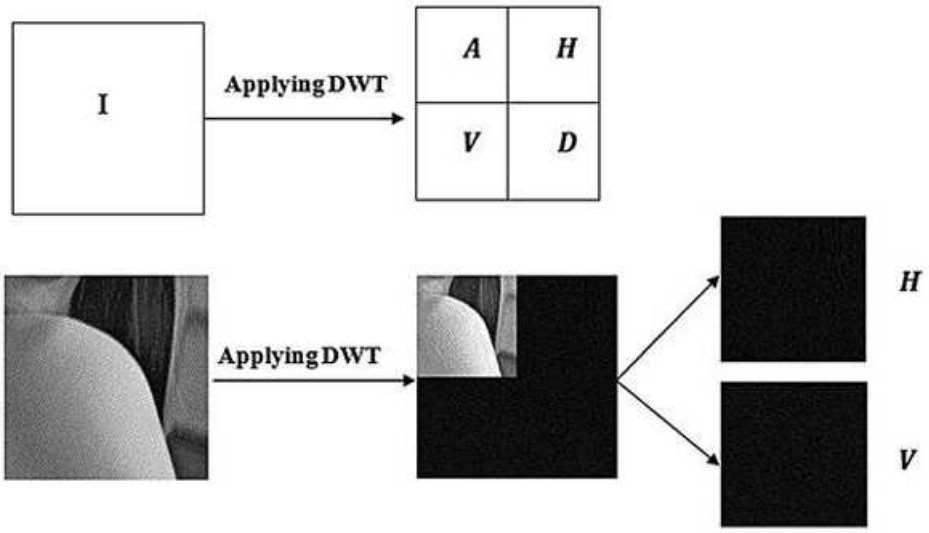
   Ako je $D_1 = H(x, y) - V(x, y) \geq T$, nema sljedećeg koraka.
   - Ako je $b = 0$ i $D_2 = V(x, y) - H(x, y) < T$, primijenjeno je slično kao u slučaju sa $b = 1$.

   $$\hat{H}(x, y) = H(x, y) - \frac{T - D_2}{2}$$

   $$\hat{V}(x, y) = V(x, y) + \frac{T - D_2}{2}$$

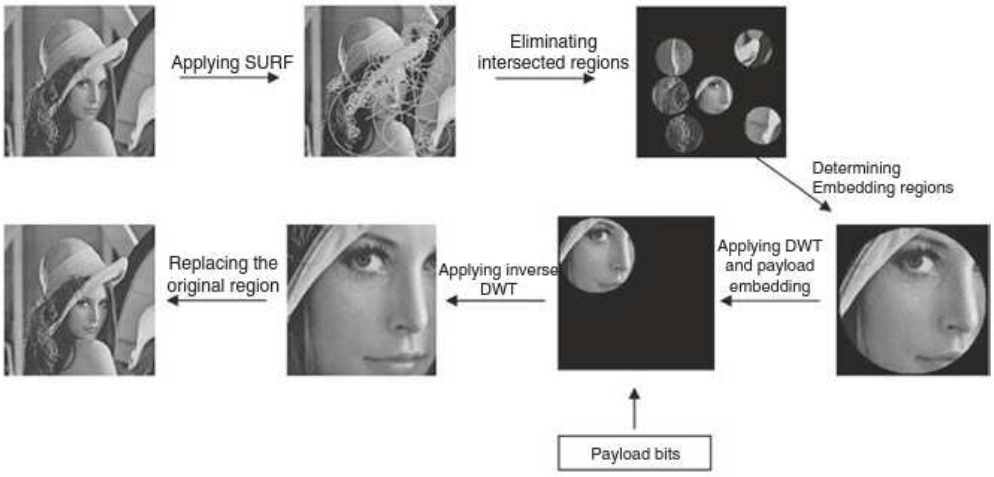
   Ako je $D_2 = V(x, y) - H(x, y) \geq T$, nema sljedećeg koraka.

Slika 2.11: DWT dekompozicija



Na kraju originalna karakteristična regija zamijenjena je sa stego-regijom. Postupak umetanja ponavlja se dok se ne kreira cijeli stego-objekt. Cijeli proces prikazan je na slici 2.12 [7].

Slika 2.12: Umetanje informacija



2.5.2 Izdvajanje podataka

Prve dvije faze izdvajanja podataka iz stego-objekta jednake su kao i prve dvije faze umetanja podataka. Karakteristične regije pronalazimo pomoću SURF algoritma, na možda napadnutoj i deformiranoj slici. Pazi se na disjunktnost točaka interesa kao i kod definiranja područja za umetanje podataka. Nakon toga slijedi izdvajanje korisnih informacija:

1. Pomoću DWT algoritma dobivamo valne koeficijente za svako područje izdvojeno ranije.
2. Određuju se horizontalni i vertikalni koeficijenti, $H(x, y)$ i $V(x, y)$. Izdvajanje bita b korisnih informacije je po formuli:

$$b = \begin{cases} 1, & \text{ako je } H(x,y) > V(x,y) \\ 0, & \text{ako je } H(x,y) < V(x,y) \end{cases}. \tag{2.5}$$

2.6 Prednosti i nedostaci opisane metode

Opisana steganografska metoda osigurava veću robusnost i sigurnost kod prijenosa tajnih informacija. Navedeno je ostvareno uz pomoć sljedećih pristupa u metodi:

- Sigurnost umetnutih informacija postignuta je primjenom Blowfish algoritma za kriptiranje te korištenjem SURF algoritma.
- Otporna je na napade kao što su sažimanje, Gaussov šum te šum ”soli i papra” (eng. *salt and pepper noise*) što je i pokazano primjerima koje se može pronaći u [7].

No, kao i svaka metoda, i ova ima svojih nedostataka:

- Nosivost, odnosno količina informacija koje mogu biti umetnute u objekt nositelj, je ograničena.
- Neće izdržati sve tipove napada.

Bibliografija

[1] Herbert Bay, Tinne Tuytelaars i Luc Van Gool, *SURF: Speeded up robust features*, sv. 3951, srpanj 2006, str. 404–417, ISBN 978-3-540-33832-1.

[2] CARNet CERT, *Steganografija, CCERT-PUBDOC-2006-04-154*, (2006), `https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-04-154.pdf`.

[3] Anurag Jagetiya, *Digital Image Steganography*, The Journal of the Computer Society of India (2014).

[4] Stefan Katzenbeisser i Fabien A. P. Petitcolas, *Information hiding techniques for steganography and digital watermarking*, Artech House, 2000.

[5] Peter Wayner, *Disappearing cryptography Information hiding: Steganography & watermarking*, Morgan Kaufmann, 2008.

[6] Wikipedia, *Steganography*, `http://wikipedia.org/`.

[7] Abid Yahya, *Steganography Techniques for Digital Images*, Springer, 2019.

Sažetak

Cilj ovog rada bio je dati uvid u steganografiju i predstaviti metodu zasnovanu na karakterističnim regijama slike. Na početku rada uveden je pojam steganografije, njenih bitnih karakteristika te osnovnih metoda koje koriste sliku kao objekt nositelj. U drugom dijelu opisana je CR-BIS metoda. U okviru toga dan je opis Blowfish algoritma i SURF metode i na koncu način primjene opisane CR-BIS metode.

Summary

The goal of this thesis was to give an introduction to steganography and describe characteristic region based image steganography. In the first part we defined what steganography is, what are its most important characteristics and we introduced the basic set of methods which use image as the carrier object. In the second part we described CR-BIS method. As a part of it we covered Blowfish algorithm and SURF method and at the end we gave and example of using CR-BIS method.

Životopis

Rođena sam 13.5.1995. u Varaždinu. Osnovno sam obrazovanje završila u Osnovnoj školi Franje Serta u Bednji, a srednjoškolsko obrazovanje u Prvoj gimnaziji Varaždin, gdje pod vodstvom prof. matematike, Anice Sakač, stvaram ljubav prema matematici i brojevima. Nakon završetka srednje škole, teško odlučujem što želim postati i na koncu odabirem PMF - Matematički odsjek te prvu godinu upisujem 2014. Već na prvoj godini rađa se ljubav prema svijetu programiranja, računala i još više prema brojevima. Preddiplomski studij završila sam 2018. godine, a u akademskoj godini 2018./2019. upisujem diplomski studij Matematike i računarstva. Svijet programiranja povukao me sebe, pa tako paralelno sa studijem radim u informatičkoj tvrtci, najprije kao tester softvera, a zatim kao softverski inženjer, skupljajući nova iskustva i upotpunjujući ona dobivena tokom cijelog školovanja. Ovim diplomskim radom završavam još jedno razdoblje, otkrivajući dosad meni poprilično nepoznati, ali vrlo zanimljiv svijet i stvaram temelje za neke daljnje poslovne prilike.