Univerzitet u Nišu, Elektronski fakultet
Katedra za računarstvo

Steganografija u slikama

Digitalna forenzika

Seminarski rad

Mentor:

Prof. dr Bratislav Predić

Student:

Milica Vacić 1440

Niš, 2022.

Sadržaj

1. Uvod

Osnovno sredstvo za komunikaciju danas je računar i s razvojem računarskih mreža, razvile su se i informaciono-komunikacione tehnologije. Prilikom slanja kroz mrežu, poruka prolazi kroz više računara, pa podaci mogu da budu izloženi neautorizovanom pristupu. Zbog toga je potrebno zaštititi podatke tako da šanse za njihovu zloupotrebu budu minimalne. Jedno od rešenja jeste primena steganografije.

Steganografija je nauka koja se bavi zaštitom podataka tako što ih ugrađuje u druge, tj. omogućava sakrivanje poruke unutar neke datoteke. Od ključnog značaja je da prisustvo poruke bude neprimetno. U tu svrhu razvijene su različite tehnike.

Objašnjenje steganografije se nalazi u poglavlju broj 2, dok je detaljan opis steganografskih sistema dat u poglavlju 3. Poglavlje 4 je posvećeno podeli steganografije, a u poglavlju 5 se nalazi lista sa objašnjenjima steganografskih tehnika. U poglavlju 6 je opisan PVD algoritam. Za potrebe ovog rada implementirana je steganografija u slikama pomoću PVD algoritma i detalji implementacije prikazani su u poglavlju 7. Poglavlje 8 sadrži zaključak, a poglavlje 9 spisak korišćene literature.

2. Steganografija

Steganografija je koncept skladištenja podataka na takav način da je postojanje takvih podataka skriveno. Ova nauka skriva podatke u drugim podacima. Reč steganografija je kovanica od dve reči grčkog porekla, στεγανοσ (steganos) i γραφο (grafo), što u prevodu znači pisati skriveno. Cilj steganografije je da se onemogući neovlašćen pristup poverljivim podacima i da se informacija prenese od pošiljaoca do primaoca tako što podatak utisne u nosioca podatka, koji mora da bude čitljiv i razumljiv za odredište.

Steganografija se koristila još u doba Antičke Grčke. Pojam steganografije prvi put se konkretno pominje u 15. veku nove ere u knjizi Džona Tritemiusa "Steganografija: umetnost koja zahteva otkrivanje skrivenog pisanja misaonim aktivnostima čoveka". U srednjem veku steganografija je korišćena za sakrivanje sadržaja pisama koje su razmenjivali vladari, a prva konkretna tehnika razvijena je za vreme Drugog svetskog rata i zasniva se na korišćenju mikrotačaka. Mikrotačke su delovi filma uvećani oko 200 puta unutar kojih su umetane informacije. Tada se koristila i bešifrarna tehnika koja podrazumeva umetanje jedne poruke u drugu na neki jednostavan način. Krajem 20. veka počeo je naučni razvoj steganografije i razvijeni su različiti algoritmi.

Pored steganografije, zarad ovog cilja koristi se i kriptografija koja šifruje podatke i pretvara ih u oblik koji je čitljiv samo onome kome su podaci i namenjeni. Osnovna razlika izmedju kriptografije i steganografije je to što je kod kriptografije moguće presretanje poruke i narušavanje integriteta, dok je kod steganografije samo postojanje poruke neprepoznatljivo. Podaci su najbezbedniji ukoliko se kombinuju steganografija i kriptografija.

3. Steganografski sistem

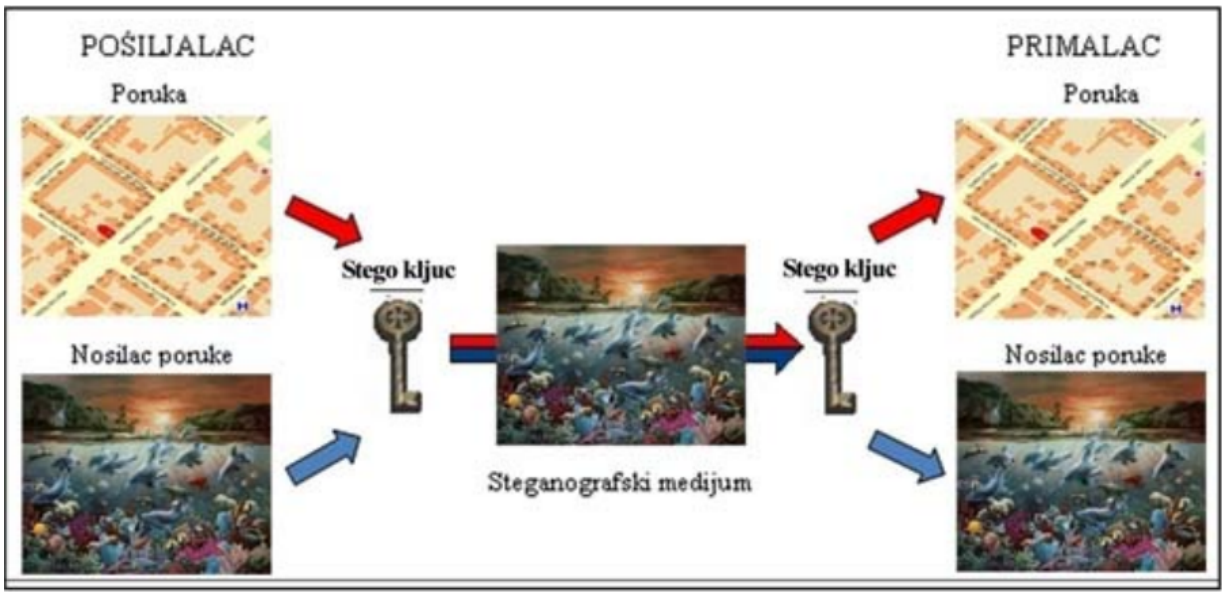
Steganografija podrazumeva prenos informacija kroz skriveni kanal. Taj kanal se naziva steganografski kanal i on zajedno sa porukom koja se prenosi, formira steganografski medijum (eng. steganography medium). Nosilac poruke može da bude bilo koja informacija u vidu teksta, slike, audio ili video formata. Poruka koju treba preneti se ugrađuje u nosioca. Prikaz steganografskog procesa dat je na slici 1.

Stego ključ se koristi za šifrovanje, kako bi se dodatno osigurala bezbednost podataka i on nije obavezan. Pomoću njega se poruka šifruje, tako da i u slučaju da se izdvoji iz nosioca poruke biće u nečitljivom formatu za primaoce koji nemaju ključ.

Steganografski sistemi se u zavisnosti od toga da li je ključ javni ili tajni, dele na

- Simetrične
- Asimetrične

Simetrični steganografski sistemi koriste samo tajni ključ, dok asimetrični koriste i tajni i javni ključ. Kod simetričnih sistema isti ključ se koristi i za šifrovanje i za dešifrovanje, dok se kod asimetričnih sistema javni ključ koristi za šifrovanje, a tajni za dešifrovanje.



Slika 1: Steganografski process

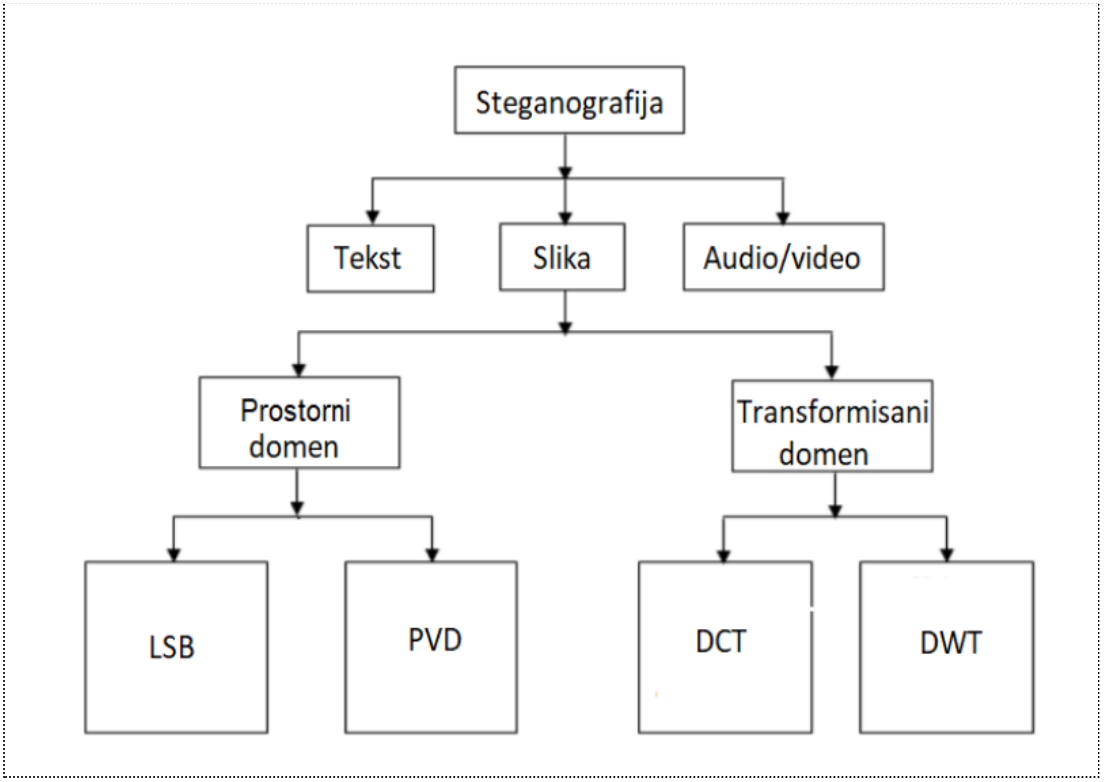
Pošiljalac bira nosioca poruke i ugrađuje skrivenu poruku u njega koristeći neku od tehnika ugrađivanja. Tako kreiran steganografski medijum se prenosi do primaoca koji, da bi pročitao poruku, treba da izvrši inverzan proces.

Kada se kao medijum za prenos sakrivene poruke koristi slika, obično se unutar nje smešta tekst ili neka druga slika. Poruku je potrebno sakriti tako da u originalnoj slici ne dođe do većih distorzija i promena. Sa stanovišta računara, slika je matrica piksela od kojih je svaki predstavljen određenim brojem bitova koji određuju boju i intenzitet svetlosti. Broj bitova kojim je predstavljena boja piksela je dubina bita i minimalna vrednost za nju je 1, što je slučaj kod binarnih ili monohromatskih slika. Pomoću 8 bitova može da se prikaže 256 različitih boja ili nijansi sive. Digitalne slike mogu da se pamte tako da dubina bita iznosi 24, što znači da je za svaku komponentu boje iskorišćeno po 8 bitova, čime se postiže najveći kvalitet slike. Takve slike su pogodni kandidati za sakrivanje informacija zbog njihove visoke rezolucije Razlog je što one sadrže veliku količinu informacija, pa promene koje nastaju sakrivanjem poruke ne utiču značajno na kvalitet slike. Ipak, ako je poruka koju treba sakriti veoma velika, može doći do deformacija slike.

Uslov da postojanje poruke u nosiocu ne bude vidljivo je da postoji dovoljan broj redundantnih bitova koji mogu da se iskoriste za umetanje poruke. Takođe, nephodno je da digitalni format nosioca poruke bude takav da promena redundantnih delove ne izaziva greške (što je slučaj sa npr. exe fajlovima).

Ugrađivanje poruke u sliku može da se odvija kroz vrednosti piksela (prostorni domen) ili kroz vrednosti koeficijenata (frekventni domen). U fizičkom svetu, svaka veličina koja se meri vremenom u prostoru ili nekom drugom višom dimenzijom može se uzeti kao signal. Signal je matematička funkcija i on prenosi neke informacije i može biti jednodimenzionalni, dvodimenzionalni ili viši dimenzionalni. Jednodimenzionalni signal je signal koji se meri vremenom (npr. zvuk). Dvodimenzionalni signali su oni koji se mere preko nekih drugih fizičkih veličina. Digitalna slika nije ništa drugo do dvodimenzionalni signal. Definisana je matematičkom funkcijom f(x, y) gde su x i y horizontalna i vertikalna koordinata. Vrednost f(x, y) u bilo kojoj tački je vrednost piksela u toj tački slike. Iz tog razloga, nad slikama mogu da se vrše transformacije za prelazak u frekventni domen (DCT, DWT). U nastavku će biti opisane različite tehnike koje su operativne u prostornom ili frekventnom domenu.

Pregled najčešće korišćenih tehnika u digitalnoj steganografiji prikazan je na slici 2.



Slika 2: Pregled najkorišćenijih tehnika

Tri važne karakteristike steganografskog sistema

1. *Kapacitet*
Količina informacija koja se može sakriti u stego medijumu.

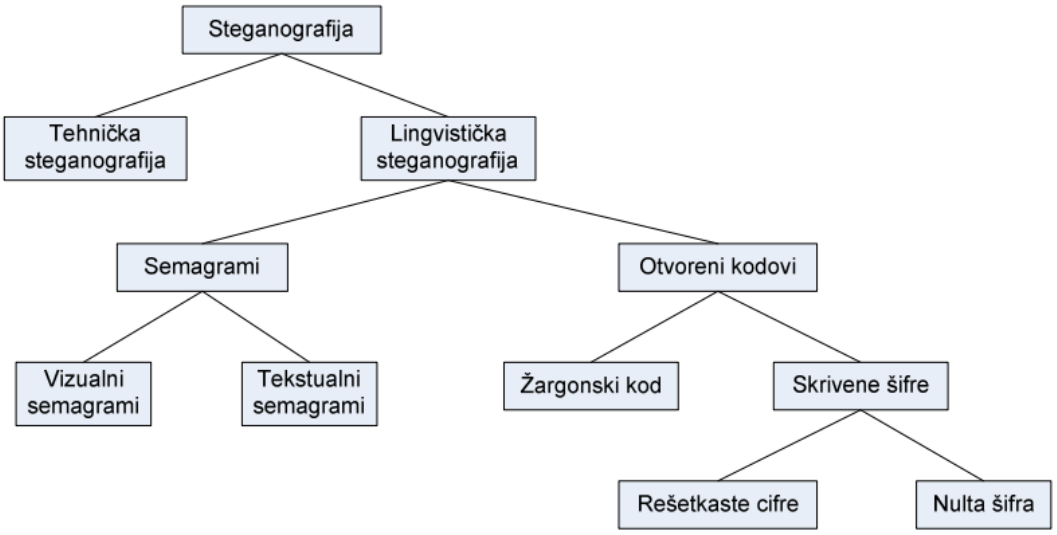
2. *Bezbednost*
Zaštita podataka od neautorizovanog pristupa, tj. nemogućnost presretanja podataka i otkrivanja poruke.

3. *Robusnost*
Sposobnost steganografskog sistema da se odupre izdvajanju poruke, tj. otpornost medijuma kojim se poruka prenosi na napade.

4. Podela steganografije

Na slici 3 je prikazana podela steganografije. Steganografija se deli na tehničku i lingvističku steganografiju. Tehnička steganografija odnosi se na ugrađivanje i ekstrakciju poruke iz pisanog teksta ili mikrofilma i u te svrhe koristi naučne metode poput metode mikrotačaka i drugih metoda koje redukuju veličinu tajne poruke. Lingvistička steganografija

obuhvata tehnike skrivanja podataka u datoteci tako da razlike između stego datoteke i originalne datoteke budu neprimetne.



Slika 3: Podela steganografije

Lingvistička se dalje deli na semagrame i otvorene kodove.

Semagrami koriste simbole i znakove za sakrivanje informacija i mogu biti vizuelni ili tekstualni. Kod vizuelnih semagrama se koriste svakodnevni fizički oblici za prenos poruka koji su naizgled bezopasni, poput detalja na nekom veb-sajtu. Tekstualni semagrami modifukuju tekst nosioca dodavanjem razmaka, promenom veličine ili boje fonta i sl.

Otvoreni kodovi koriste različite metode za neprimentno sakrivanje poruka. Dele se na žargonski i skriveni kod. Žargonski kodovi se baziraju na korišćenju predefinisanih fraza koje su poznate samo učesnicima komunikacije (unapred dogovoreni pojmovi i sl.). Kod skrivenih kodova se skrivena poruka može izdvojiti iz stego-datoteke samo u slučaju ako je poznata metoda kojom je skrivena informacija utisnuta u datoteku. U skrivene kodove se ubrajaju rešetkasti i nulti kodovi. Rešetkasti kodovi rade na principu šablona koji se koriste za skrivanje poruke u nosiocu, dok se kod nultog koda usvaja skup pravila za umetanje poruke u nosiocu podataka (izuzimanje neparnih redova, čitanje svake treće reči i sl.).

Savremena steganografija koristi mogućnosti digitalne tehnologije i uglavnom je usmerena na skrivanje tajne poruke unutar sadržaja nekog multimedijalnog fajla npr. slike, audio ili video zapisa. Multimedijalni fajlovi u sebi sadrže veliki broj bitova od manjeg značaja čija promena ne utiče značajno na sam fajl, pa je moguće iskoristiti ih za sakrivanje poruke.

5. Steganografske tehnike

5.1. Tehnike supstitucije

- Delovi nosioca poruke koji nisu od velike važnosti koriste se za sakrivanje poruke. Primer ovakve tehnike je LSB (Least Significant Bit). Kod ove tehnike, delovi poruke smeštaju se u najniže bitove nosioca poruke jer njihova promena najmanje dovodi do vidljive promene. najjednostavnija i najkorišćenija steganografska tehnika. Najniži bitovi slike koja se koristi kao medijum služe za prenos skrivene poruke. Slika obično sadrži određen broj bitova koji ne nosi značajne informacije, tj. ne utiču mnogo na njen izgled. U ovoj tehnici se upravo ti bitovi modifikuju tako da predstavljaju bitove tajne poruke. LSB metoda je najpogodnija za slikovne datoteke koje imaju visoku rezoluciju uz upotrebu različitih boja. Primenom ove metode ne povećava se veličina datoteke, ali zavisno od veličine informacije koja se skriva, može doći do primetnih distorzija. Zato su najbolji kandidati za ovu metodu 24-bitne slike, zbog njihove veličine.Bitna karakteristika ovog metoda je da se konverzijom slike u drugi format gubi skrivena informacija. Jos jedan primer ovakve tehnike je PVD algoritam o kome ce biti reči u nastavku.

5.2. Tehnike transformacije domena

- Kod ovih tehnika, pre sakrivanja poruke vrši se transformacija domena, a onda se u novom, transformisanom domenu vrši sakrivanje. Ovde se ubraja diskretna kosinusna tranformacija (eng. Discrete Cosine Transform), diskretna Furijeova transformacija (eng. Discrete Fourier Transform) i diskretna talasna transformacija (eng. Discrete Wavelet Transform). Kad se podaci sakrivaju u prostornom domenu, gubici mogu da budu vidljivi ako se slika iseče i sl. Zbog toga je bolje pre promene slike preći u frekventni domen, za šta se koristi DCT algoritam. Ovom transformacijom izdvajaju se komponente visoke, srednje i niske frekvencije. Nakon primene algoritma poruka se sakriva po LSB metodi, ali se umesto realnih vrednosti piksela koriste dobijeni DCT koeficijenti. DWT (eng. Discrete Wavelet Transformation) ili diskretna talasna transformacija konvertuje prostorni u frekventni domen. Koristi se u steganografiji zato što se ovom transformacijom jasno odvajaju visoke od niskih frekvencija. Visoke frekvencije označavaju ivične komponente i one su pogodne za ugrađivanje poruke jer je ljudsko oko manje osetljivo na promene u ivicama.

5.3. Tehnike proširenog spektra

- Poruka koja se prenosi se modifikuje signalom šuma, tako da i sama izgleda kao slučajan šum, a ne informacija. Ove tehnike se obično koriste u bežičnim sistemima jer povećavaju otpornost na smetnje i omogućavaju nesmetanu komunikaciju između više učesnika. Najčešće korišćene tehnike ovog tipa su proširenje spektra metodom direktne sekvence (eng. Direct Sequence Spread Spectrum) i proširenje spektra metodom frekvencijskog skakanja (eng. Frequency Hopping Spread Spectrum). Tehnika proširenog spektra (eng. Spread Spectrum) radi na principu ubacivanja, a bazira se na proširenju frekvencijskog spektra signala u određenom domenu. Koristi slabosti koje imaju ljudska čula. Ima primenu u kontroli bezbednosti komunikacionog kanala, povećanju otpornosti na prirodne smetnje i u ograničavanju snage određenih prenosnih linkova. Funkcioniše tako što dodaje šumove u slučajne odabrane signale. Informacije se kriju unutar nosioca i šire se preko frekvencijskog spektra. Šum može da bude sam nosilac poruke, tj. slika, ili neki pseudo-šum. Kad se slika koristi kao šum, onda se može preneti jedna vrednost ispod nivoa šuma. Praktično, na taj način može da se prenese samo 1 bit. Da bi se prenelo više, potrebno je sliku podeliti na manje delove. Varijanta sa dodavanjem pseudo-šuma je mnogo teža za detekciju zato što se poruka prenosi kroz nosioca, tj. sliku. Tehnika proširenog spektra ugrađuje poruku u sliku u vidu Gausovog šuma. Na nižim nivoima energije šuma, degradacija slike nije primetna ljudskom oku, dok se na višim nivoima manifestuje u vidu „pega“. Poruka koja treba da se prenese se konvertuje u binarni zapis i generiše se pseudo-slučajna sekvenca šuma. Vrši se modulacija pseudo-šuma pomoću poruke čime se dobija šum koji će da se kombinuje sa nosiocem poruke, tj. sa slikom. Za inverzni proces nije neophodna originalna slika. Nad stego-slikom se primenjuju filteri za izdvajanje šuma, što rezultuje slikom koja je aproksimacija originalne slike. Što su filteri bolji, to je aproksimacija verodostojnija, pa će manje grešaka biti u izdvojenoj poruci. Međutim, da bi poruka mogla da se izdvoji, neophodno je da odredišnoj strani bude poznata pseudo-slučajna sekvenca šuma. Vrši se demodulacija izdvojenog šuma upoređivanjem sa pseudo-šumom, čime se dobija sakrivena poruka.

5.4. Statističke tehnike

- Poruka koju treba sakriti se deli na bitove, a nosilac poruke na onoliko delova koliko bitova poruke ima. Ako je bit poruke 1, odgovarajući blok se menja tako da primalac može statističkim testiranjem da otkrije da li je blok promenjen, u suprotnom blok se ne menja. Statističke metode, poznate kao tehnike zasnovane na modelu (eng. Model based techniques), moduliraju ili modifikuju statistička svojstva slike pored njihovog

očuvanja u procesu ugrađivanja. Ta modifikacija je obično mala i na taj način je u stanju da iskoristi ljudsku slabost u detekciji promene osvetljenosti. Ovaj postupak se vrši jednostavnim modifikovanjem slike koja je nosilac poruke pravljenjem neke značajne promene u statističkim karakteristikama ako se prenosi „1“, a u suprotnom ne dolazi do promena. Da bi se poslalo više bitova, slika se deli na manje, od kojih će svaka da prenese 1 bit poruke.Međutim, statističke steganografske metode u njihovom najjednostavnijem obliku, za koje su delovi slike (eng. sub-images) jednostavno pravougaonici originalne slike, osetljivi su na odsecanje, rotiranje i skaliranje, zajedno sa napadima koji rade protiv tehnike vodenog žiga. Da bi se to izbeglo, sliku treba deliti na „pod-slike“ (eng. sub-images) na osnovu elemenata slike (npr. lica u gužvi) uz korišćenje koda za ispravljanje grešaka u poruci.

5.5. Tehnike distorzije

- Umesto da se poruka sakriva direktno u medijum, sam medijum menja oblik kako bi mogao da sakrije i prenese poruku. Da bi poruka mogla da se ekstrahuje na prijemnoj strani, neophodno je da bude poznat originalni oblik medijuma. Tehnike distorzije zahtevaju poznavanje originalne slike tokom procesa dekodiranja, gde dekoder proverava razlike između originalne slike i stego-slike kako bi se izdvojila tajna poruka. Poruka se ugrađuje tako što se originalna slika modifikuje sekvencom funkcija, tako da poruku u stvari krije distorzija signala. Modifikacije se biraju tako da se poklapaju sa tajnom porukom koja se prenosi. Poruka se smešta u pseudo-slučajno izabranim pikselima. Ako se stego-slika razlikuje od originalne slike na određenom pikselu, onda je bit poruke 1. U suprotnom, bit poruke je 0. Modifikacije mogu da se izvrše tako da se statističke karakteristike slike ne menjaju. Prednost ove tehnike je što, ukoliko dođe do napada i napadač izvrši odsecanje, skaliranje ili rotaciju slike, primalac to može lako da detektuje. U nekim slučajevima, ako se poruka kodira sa informacijom za ispravljanje grešaka, modifikacije napadača mogu da se invertuju i da se izdvoji cela poruka bez grešaka.

5.6. Tehnike stvaranja medijuma pomoću skrivene poruke

- Kod ovog metoda se na osnovu poruke formira medijum.

Sve pomenute tehnike, nakon što izvrše neophodne transformacije, ugrađuju poruku u medijum koristeći jedan od sledeća tri principa:

- *Ubacivanje* se koristi za sakrivanje podataka u delovima medijuma koji su od manjeg značaja za potencijalnog napadača. Zasniva se na dodavanju bitova u datoteke tako da površinski deo medijuma ostane savršeno čist. Umetanjem određenog broja dodatnih bezopasnih bitova u medijum njegova struktura se ne menja značajno, tako da krajnji korisnik ne može da detektuje prisustvo skrivenog podatka u medijumu. Mana ovog pristupa je što u zavisnosti od veličine poruke koja se ugrađuje raste i veličina medijuma, tj. datoteke koja se prenosi. U slučaju da je poruka velika, veličina medijuma može da naraste tako da izazove sumnju kod potencijalnih napadača.

- *Supstitucija* ili zamena podrazumeva zamenu najmanje značajnih (najnižih) bitova datoteke, tako da promene datoteke budu što manje vidljive. Prednost ovog pristupa je što se ne menja veličina datoteke, a mane to što ipak dolazi do degradacije datoteke i što je veličina poruke koja može da se ugradi u datoteku ograničena brojem najmanje značajnih bitova datoteke.

- *Generisanje* ne zahteva originalnog nosioca poruke, već se nosilac poruke, tj. datoteka generiše na osnovu poruke koja se šalje. Rezultat generisanja je originalna datoteka, imuna na komparaciju sa drugim datotekama. To je glavna prednost generisanja u odnosu na ubacivanje i supstituciju, kod kojih je moguće uočiti promene u datoteci upoređivanjem sa originalom.

6. PVD

PVD ili metoda razlike vrednosti piksela (eng. Pixel Value Difference) je tehnika koja se koristi za sakrivanje poruka u slikama u prostornom domenu. Koristi sive slike kao nosioce signala, a stego-slike koje nastaju primenom ove tehnike odlikuje neuočljivost razlika u odnosu na originalnu sliku. Promene u glatkom region slike znatno su primetnije od promena u ivičnom region slike, pa se upravo u ivičnom regionu čuva veći deo tajne poruke

Inicijalno, slika se deli u uzastopne, nepreklapajuće objekte veličine 1x2 rasterskim skeniranjem. Neka su dva uzastopna piksela u i-tom bloku označena sa P_i i P_{i+1}. Za svaki blok, vrednost d_i jednaka je apsolutnoj vrednosti razlike dva piksela u bloku $|P_i - P_{i+1}|$. Mala vrednosti d_i označava da se radi o glatkom regionu, a velika vrednost da je u pitanju ivični region. Pošto piksel može da ima vrednost između 0 i 255, razlika uzima vrednosti od -255 do 255, a njena apsolutna vrednost, tj. d_i, od 0 do 255. Vrednost d_i može da se kvantizuje u nekoliko opsega. Broj bitova koji može da se sakrije u dva uzastopna piksela zavisi od tabele kvantizacionog opesega. Ona se sastoji od n opsega iste dužine, čija je ukupna dužina 255. Ako je gornja granica opsega R_i jednaka $upper_i$, a donja granica $lower_i$, onda je širina opsega jednaka $(upper_i – lower_i + 1)$, tj. broj bitova poruke koji može da se smesti u okviru jednog bloka iznosi $t = \lfloor \log2(upper_i – lower_i + 1) \rfloor$. Tabela kvantizacionih opsega prikazana je na slici 4.

R_1	R_2	R_3	R_4	R_5	R_6
8	8	16	32	64	128

0 7 8 15 16 31 32 63 64 127 128 255

Slika 4: Tabela kvantizacionih opsega za PVD

Po izračunavanju parametra t, uzima se toliko bitova iz poruke i konvertuju se u decimalnu vrednost b, a onda se razlika između piksela ažurira na vrednost $d_i = b + lower_i$. Nova razlika treba da bude u istom opsegu kao stara. Nakon toga, računaju se nove vrednosti piksela po sledećoj formuli:

$$If\ (P_i \geq P_{i+1}\ and\ d_i' > d_i), (P_i', P_{i+1}') = (P_i + \left\lceil \frac{m}{2} \right\rceil, P_{i+1} - \left\lceil \frac{m}{2} \right\rceil)$$

$$If\ (P_i < P_{i+1}\ and\ d_i' > d_i), (P_i', P_{i+1}') = (P_i - \left\lceil \frac{m}{2} \right\rceil, P_{i+1} + \left\lceil \frac{m}{2} \right\rceil)$$

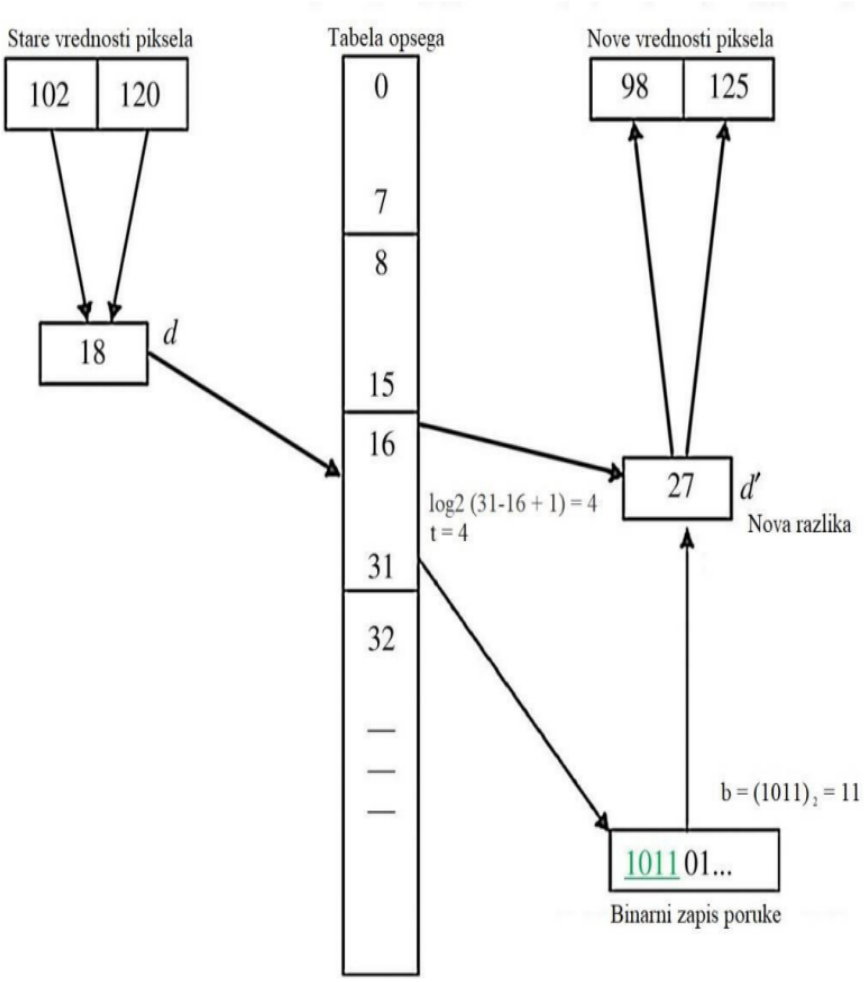
$$If\ (P_i \geq P_{i+1}\ and\ d_i' \leq d_i), (P_i', P_{i+1}') = (P_i - \left\lceil \frac{m}{2} \right\rceil, P_{i+1} + \left\lceil \frac{m}{2} \right\rceil)$$

$$If\ (P_i < P_{i+1}\ and\ d_i' \leq d_i), (P_i', P_{i+1}') = (P_i + \left\lceil \frac{m}{2} \right\rceil, P_{i+1} - \left\lceil \frac{m}{2} \right\rceil),$$

gde je m = | d’ – d |.

Na prijemnoj strani poruka može da se izdvoji identičnim postupkom. Slika se ponovo deli na uzastopne, nepreklapajuće blokove od po 2 piksela. Za svaki blok se računa razlika piksela (d_i’) i preko tabele kvantizaonih opsega određuje se broj bitova poruke koji je sakriven u tom bloku. Sami bitovi poruke dobijaju se konverzijom razlike d_i – $lower_i$ u binarnu vrednost.

Ilustracija rada ove tehnike na primeru prikazana je na slici 5. PVD metod može da se iskoristi i za RGB slike, s tim što se svaki RGB „blok“ deli na dva koja se preklapaju (jedan se sastoji od R i G, a drugi od G i B komponente) i onda se opisani postupak vrši nad njima.



Slika 5: Ilustracija PVD tehnike

7. Implementacija steganografije u slikama pomoću PVD tehnike

Slika 6: Original i slika sa ugrađenom porukom

Za potrebe ovog rada implementirana je steganografija u slikama korišćenjem PVD tehnikeu programskom jeziku *python*. Kao nosilac poruke korišćena je siva slika, dok je poruka u tekstualnom formatu. Tekstualna poruka se najpre pretvara u binarni zapis. Računa se apsolutna vrednost razlike za svaka dva uzastopna piksela slike. Ukoliko je ta vrednost mala, znači da se radi o glatkom regionu, a ukoliko je velika radi se o ivičnom regionu. Zatim se na osnovu te razlike i kvantizacione tabele, određuje broj bitova koji može da se sakrije u dva uzastopna piksela. Broj tih bitova se računa po sledećoj formuli

$$t = \lfloor \log_2(upper_i - lower_i + 1) \rfloor$$

8. Zaključak

Razvoj računarskih mreža, a kasnije i informacionih tehnologija zanačajno je unapredio i ubrzao komunikaciju. Istovremeno, informacije koje se prenose kroz mrežu postale su mnogo osetljivije na napade, pa je potrebno zaštiti ti ih od neovlašćenog pristupa. U tu svrhu se, osim kriptografije, koristi i steganografija. Steganografija je nauka koja se bavi sakrivanjem informacija u drugim podacima. Neki njen primitivni vid koristio se još u doba Antičke Grčke, a značajnu primenu imala je i tokom ratova. Naučni razvoj steganografije uznapredovao je krajem 20. veka. Vremenom su razvijene različite grane steganografije, kao i tehnike za njenu primenu.

Mrežom se prenose digitalni podaci, pa se digitalna steganografija upravo bazira na sakrivanju podataka u digitalne formate. Jedan od najčešćih tipova datoteka koje se koriste jesu slike. Najbolji kandidati za nosioce poruka su 24-bitne slike zbog svog kvaliteta jer se u njima deformacija najmanje vidi, ali se zbog njihove velike rezolucije često koriste i 8-bitne slike. Ugrađivanje poruke u sliku može da se odvija u prostornom domenu, kroz vrednosti piksela, ili u frekventnom domenu, kroz vrednosti koeficijenata. Tehnike prostornog domena koje se često koriste su LSB, PVD i tehnike distorzije. U frekventnom domenu najviše se koriste diskretna kosinusna i diskretna talasna transformacija. Originalna slika se deformiše ugrađivanjem poruka, a suština jeste iskoristiti tehniku kod koje će promene da budu najmanje vidljive. Svaka od ovih tehnika ima prednosti i mane, a one se ogledaju kroz njihov kapacitet, bezbednost i robusnost.

9. Literatura

[1] M. Ćajić, B. Brkić, M. Veinović, *Analiza, steganografskih tehnika*, (2010), https://www.researchgate.net/publication/265003223_ANALIZA_STEGANOGRAFSKIH_TEHNIKA_I_METODA

[2] D. Veljarević, M. Veinović, *DIGITALNA STEGANOGRAFIJA JPEG SLIKA PRIMENOM DCT TRANSFORMACIJE*

[3] N. Hamid, A. Yahua, R. Ahmad, O. Al-Qershi, *Image Steganography Techniques: An Overview*, (2012), https://www.cscjournals.org/manuscript/Journals/IJCSS/Volume6/Issue3/IJCSS-670.pdf

[4] T. Eriik, *STEGOTE - STEGANOGRAPHY TOOL FOR HIDING INFORMATION IN JPEG AND PNG IMAGES*, (2019), Tallin

[5] A. Sahu, M. Sahu, *DIGITAL IMAGE STEGANOGRAPHY TECHNIQUES IN SPATIAL DOMAIN*, https://www.researchgate.net/publication/312826532_Digital_image_steganography_techniques_in_spatial_domain_A_study

[6] S. Goel, A. Rana, m. Kaur, *A DCT-Based Robust Methodology for Image Steganography*, (2013), Karnal: Doon Valley Institute of Engg. & Technology

[7] O. Foaud, H. Hamed, *Hiding data in images using DCT steganography techinuque with compression algorithms*, (2019), https://www.researchgate.net/publication/330565811_Hiding_data_in_images_using_DCT_steganography_techniques_with_compression_algorithms

[8] H. Sheisi, J. Mesgerian, M. Rahmani, *Steganography: Dct Coefficient Replacement Method and Compare With JSteg Algorithm*, (2012), http://www.ijcee.org/papers/533-P0025.pdf

[9] S. Zagade, *S. Boshale, Secret Data Hiding in Images by using DWT Technique*, (2014), https://www.ijeat.org/wp-content/uploads/papers/v3i5/E3215063514.pdf

[10] M. Tushara, K. Navas, *Image Steganography Using Discrete Wavelet Transform – A Review*, (2016), https://ijireeice.com/wp-content/uploads/2016/07/nCORETech-38.pdf

[11] C. Boncelet, *Spread Spectrum Image Steganography*, (1999), University of Delaware

[12] *Discrete Cosine* Transform, (januar 2021), https://www.mathworks.com/help/images/discrete-cosine-transform.html