Implementiranje steganografskih metoda

Stojanović, Stjepan

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Stjepan Stojanović

IMPLEMENTIRANJE STEGANOGRAFSKIH METODA

ZAVRŠNI RAD

Varaždin, 2022.

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Stjepan Stojanović

Matični broj: 0016138909

Studij: Poslovni sustavi

IMPLEMENTIRANJE STEGANOGRAFSKIH METODA

ZAVRŠNI RAD

Mentor:

Doc. dr. sc. Nikola Ivković

Varaždin, srpanj 2022.

Stjepan Stojanović

Izjava o izvornosti

Izjavljujem da je moj završni/diplomski rad izvorni rezultat mojeg rada te da se u izradi istoga nisam koristio drugim izvorima osim onima koji su u njemu navedeni. Za izradu rada su korištene etički prikladne i prihvatljive metode i tehnike rada.

Autor/Autorica potvrdio/potvrdila prihvaćanjem odredbi u sustavu FOI-radovi

_____

Sažetak

Steganografski postupci skrivaju poruku unutar nekog objekta. U ovom radu se razmatraju isključivo digitalne poruke koje su skrivene unutar nekog digitalnog objekta (sadržaja). Primjerice, poruke se mogu sakriti unutar slike, zvukovnog zapisa, videa i drugih digitalnih sadržaja. Opisani su različiti postupci i tehnike skrivanje tajnih informacija unutar objekta. Skrivena poruka može biti komprimirana i/ili kriptirana. Steganografski su objekti podložni i napadima, točnije steganalizi. U programskom jeziku *Python* je implementiran program koji može umetati i čitati skriveni sadržaj u druge datoteke korištenjem algoritma najmanje značajnog bita. Program je testiran na ispitnim primjerima.

Ključne riječi: sigurnost, programiranje, steganografija

Sadržaj

1. Uvod

Danas se sve više spominje informatička tj. Informacijska sigurnost u komunikaciji. Sve većim i bržim razvojem moderne tehnologije ljudi su izloženi u smislu da privatna komunikacije nije baš više toliko privatna. Ponekad se radi o izrazito rizničnim informacijama koje je potrebno na neki način prikriti ili zaštiti. Stoga postavlja se pitanje kako riješiti taj problem, pojavile su se razne metode i tehnologije. Široj populaciji je uglavnom poznat pojam kriptografije, dok su s druge strane uglavnom programeri i informatičari upoznati sa steganografijom. Obje tehnologije se koriste za skrivanje podataka, no postoji bitna razlika. Kriptografija se koristi za zaštitu podataka kodiranjem tako da nitko ne može pročitati tajnu poruku bez određenih metoda ili ključeva. Dok s druge strane steganografija skriva podatke unutar nekog objekta koji ni na koji način ne izaziva sumnju u postojanje tajne komunikacije.

Termin steganografija potječe od grčkih riječi *steganos*, što znači “pokriven” i *graphein*, što znači “pisati”. Namjera je sakriti informaciju u mediju na način da nitko osim očekivanog primatelja ne zna za njihovo postojanje [1].

Steganografija se danas koristi tako što se podaci skrivaju unutar elektroničke datoteke kao što su slike, zvukovnih zapisa pa čak i unutar video zapisa. Moguće je npr. čitav word ili knjigu sakriti unutar jedne slikovne datoteke. Najčešće se to radi na način da se koristi najmanje značajan bit (eng. *Least Significant Bit*, LSB) algoritam točnije zamjenom najmanje važnog bita u originalnoj datoteci da bi se stvorila datoteka sa steganografskim sadržajem tj. skrivenim sadržajem, no to će biti opširnije obrađeno u radu. Postoje mnogi softveri i alati koji omogućuju steganografiju, a pažnju je privuklo raznim vojnim ili vladinim organizacijama, iako se koristi još i u komercijalne svrhe.

Svrha steganografije je izbjegavanje sumnje u prijenos tajne poruke preko datoteke unutar koje je skrivena. Osnovni princip je taj da objekt koji sadrži skrivenu poruku treba biti jednak originalnom objektu tj. da razlike budu neprimjetne između datoteka. Otkrivanje tajne poruke unutar datoteka se zove steganaliza, a ono podrazumijeva da se mijenjanju karakteristike nositelja poruke i da poprima na neki način vrstu izobličenja. Analizom različitih karakteristika stego objekta i objekta koji ne sadrži skrivenu poruku razvija se steganalitički sustav za otkrivanje skrivenih informacija.

2. Steganografija

Steganografija je vrsta skrivene komunikacije koja doslovno znači "skriveno pisanje". Poruka je na otvorenom, često na uvid svima, ali ostaje neotkrivena jer je samo postojanje poruke tajno. Još jedan popularan opis steganografije je "skriven na vidiku (eng. *Hidden in plain sight*)". Nasuprot tome, kriptografija je kada je poruka kodirana, nečitljiva, a postojanje poruke je često poznato [2].

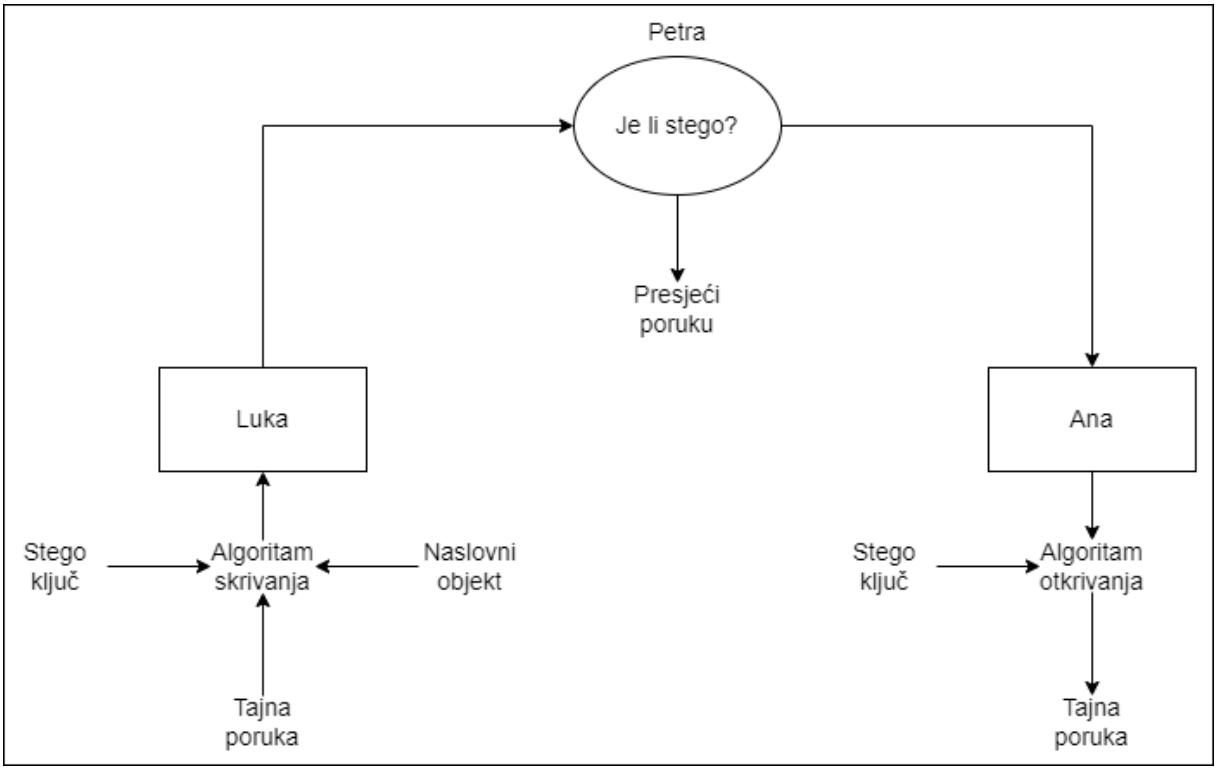
2.1. Problem zatvorenika

Kao jedan od klasičnih primjera steganografije koristi se zatvorenikov problem ili problem zatvorenika. U tom primjeru su dva izmišljena zatvorenika Ana i Luka. Njihov je cilj napraviti plan kako pobjeći iz zatvora, ali su smješteni u različite ćelije. Jedini način komunikacije između njih je preko upraviteljice zatvora Petre. Naime, problem je taj što će Petra pokušati presrest i njihovu tajnu komunikaciju, te im tako neće dopustiti da pobjegnu iz zatvora jer će u protivnome završiti u samici. Stoga, zatvorenici Ana i Luka moraju komunicirati na način da to nije oku vidljivo, što znači da će komunicirati koristeći steganografiju.

Način na koji bi komunicirali je takav da bi npr. Luka nacrtao šarenu kuću u šumi pored rijeke, te bi upraviteljica Petra prenijela tu sliku do Ane. No, ono što upraviteljica ne zna je da boje na slici prenose tajnu poruku za Anu. Tu može doći do dvije vrste napada od strane upraviteljice. Aktivni napad bi značio da je upraviteljica namjerno izmijenila sliku što bi uništilo skrivenu poruku. Dok s druge strane zlonamjerni napad bi značio da upraviteljica mijenja poruku ili stvara svoju poruku te ju šalje do jednog od zatvorenika.

Zatvorenikov problem se koristi kao glavni primjer za objašnjavanje rada komunikacije pomoću steganografije. Postoje dvije strane, a to su zatvorenici koji žele komunicirati i upraviteljica koja prisluškuje tu komunikaciju.

Na slici 1 su prikazane glavne komponente koje čine neki osnovni okvir komunikacije pomoću steganografije. Naslovni objekt je u principu slika ili ono što je oku vidljivo, koji se koristi za prijenos tajne poruke. Stego ključ je kod koji pošiljatelj koristi za ugradnju tajne poruke unutar naslovnog objekta, a taj isti stego ključ koristi i primatelj za izvlačenje tajne poruke. Stego objekt je skup naslovnog objekta, stego ključa i tajne poruke, kombinaciju navedena tri elementa stvara se objekt koji na naslovnici nosi tajnu poruku što čini komunikaciju pomoću steganografije.



Slika 1: Primjer steganografije (Problem zatvorenika) [autorski rad]

2.2. Steganografija kroz povijest

Steganografija se koristi od davnina i vuče korijene iz drevnih civilizacija (npr. Grčka, Egipat). U 5. stoljeću prije Krista, Histaiacus je obrijao glavu roba i tetovirao poruku na njegovu lubanju, a rob je poslan s porukom nakon što mu je kosa ponovno izrasla. Cardan (1501. – 1576.) ponovno je izumio kinesku drevnu metodu tajnog pisanja, gdje se papirna maska s rupama dijeli između dvije strane, ova se maska stavlja na prazan papir, a pošiljatelj upisuje tajnu poruku kroz rupe, a zatim skida masku i ispunjava praznine kako bi se poruka teme prikazala kao bezopasan tekst. Nulta šifra, mikrotisak 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 [3].

U Prvom svjetskom ratu Nijemci su koristili mikrotisak skriven u kutovima razglednica koje su bile otvorene nožem i ponovno zapečaćene škrobom. Moderni mikrotisak dvadesetog stoljeća mogle su sadržavati do jedne stranice teksta, pa čak i fotografije. Saveznici su 1941. otkrili upotrebu mikrotiska. Nedavno je predložena moderna verzija koncepta mikrotiska za skrivanje informacija u DNK (Deoksiribonukleinska kiselina) u svrhu označavanja važnog genetskog materijala. Nedavno je predložen i mikrotisak u obliku prašine za identifikaciju dijelova automobila [4].

Možda je najpoznatiji oblik steganografije pisanje nevidljivom tintom. Prve nevidljive tinte bile su organske tekućine, kao što su mlijeko, urin, ocat, razrijeđeni med ili otopina šećera. Poruke ispisane takvom tintom bile su nevidljive nakon što se papir osušio. Da bi bila uočljiva, slovo je jednostavno zagrijano iznad svijeće. Kasnije su izumljene sofisticiranije verzije zamjenom algoritma za ekstrakciju poruka sigurnijim alternativama, kao što je korištenje ultraljubičastog svjetla [4].

Steganografija u modernom vremenu i svom modernom obliku je relativno mlada. Sve do početka 1900-ih ovaj način komunikacije koristili su uglavnom samo špijuni. U tom vremenu to su bili samo snalažljivi trikovi s gotovo nimalo teorijske osnove kako bi se omogućilo da se steganografije razvija na današnji način. S naglim prijelazom komunikacije na digitalnu s analogne, steganografija je doživjela eksplozivno moderniziranje. Naime, došlo je do razvoja skrivanja poruka u elektroničkim dokumentima, a sve u svrhu tajne komunikacije, no to je ipak bilo najlakše programerima. Uskoro su se na internetu pojavili steganografski programi koji su omogućili široj masi skrivanje tajnih poruka unutar digitalnih slika, zvuka, videa i slično.

3. Vrste steganografskih postupaka

U svim metodama steganografije nešto se radi kako bi se poruka prikrila, naravno, te se radnje ili tehnike mogu odvojiti i analizirati kako bi se naučilo što se događa tijekom cijelog procesa. Šest kategorija steganografije su:

1) Tehnika supstitucijskog sustava,
2) Tehnika transformacije domene,
3) Tehnike širenja spektra,
4) Tehnika statističke metoda,
5) Tehnika distorzije,
6) Tehnika generiranja naslovnica [2].

3.1. Tehnika supstitucijskog sustava

U steganografiji koja koristi tehniku supstitucijskog sustava zamjenjuju se nepotrebni ili viškovi bitova naslovnog objekta s bitovima tajne poruke. Najčešće se koristi metoda najmanje značajnog bita ili *LSB* algoritam za kodiranje tajne poruke. Ukratko *LSB* funkcionira na sljedeći način: u naslovnom objektu, recimo da se radi o slici postoji veća količina suvišnog prostora. Taj prostor će program za steganografiju iskoristiti kako bi sakrio tajnu poruku, ali na razini bita u naslovnom objektu.

Dolje navedeni niz bajtova u *Tablici 1* predstavlja dio neke slike točnije naslovnog objekta:

Tablica 1:Primjer promjene u nizu bajtova

10011001	00110110	10100110
01110101	10010100	00100110

Svaki se bajt sastoji od osam bitova, a ti bitovi čine vrijednosti boje na naslovnom objektu tj. slici (crvena, plava, zelena…). Bitovi koji čine jedan bajt po važnosti se gledaju s lijeva na desno. Kad bi se promijenio prvi bit u prvom bajtu (10011001) iz 1 u 0 došlo bi do velike promjene boje za razliku od promjene zadnjeg bita iz 1 u 0. Najlakše se može shvatiti na način da se binarni pretvori u dekadski, dakle **1**0011001=153, promjenom prvog bita **0**0011001=25, a promjenom zadnjeg bita 1001100**0**=152. U radu će biti detaljnije objašnjen *LSB* algoritam.

3.2. Tehnika transformacije domene

Ova tehnika je također vrlo učinkovita i malo je teže objasniti. U osnovi, tehnike transformacijske domene skrivaju podatke poruke u "prostoru transformacije" signala. Svakodnevno na internetu ljudi šalju slike naprijed-natrag, a najčešće koriste *JPEG* (eng. *Joint Photographic Experts Group*) format. *JPEG*-ovi su zanimljivi po tome što se sami komprimiraju kada se zatvore. Da bi se to dogodilo, moraju se riješiti viška podataka, viška bitova koji bi ih inače spriječili da se komprimiraju. Tijekom kompresije, *JPEG* će napraviti aproksimaciju samog sebe kako bi postao manji; ta promjena, ta aproksimacija, je prostor transformacije i ta se promjena može koristiti za skrivanje informacija [2].

3.3. Tehnike širenja spektra

U širem spektru izravnog niza, tok informacija koji se prenosi podijeljen je na male dijelove. Svaki od dijelova je dodijeljen frekvencijskom kanalu spektra. Podatkovni signal, u točki prijenosa, kombinira se s nizom bitova veće brzine prijenosa koji dijeli podatke prema unaprijed određenom omjeru širenja. Redundantni kod bitova brzine prijenosa podataka pomaže signalu da se odupre smetnjama i omogućuje obnavljanje izvornih podataka ako se bilo koji od bitova podataka ošteti tijekom prijenosa [2].

Tehnika frekvencijskih skokova dijeli široki dio spektra širine pojasa na mnoge moguće frekvencije emitiranja. Općenito, uređaji za skakanje frekvencije troše manje energije i jeftiniji su, ali izvedba sustava s proširenim spektrom izravnog niza obično je bolja i pouzdanija [2].

3.4. Tehnika statističke metode

Statističke steganografske tehnike iskorištavaju postojanje "1 bita", gdje je gotovo dio podataka ugrađen u digitalni nosač. Ovaj proces se izvodi jednostavnom modifikacijom naslovne slike kako bi se napravila neka vrsta značajne promjene u statističkim karakteristikama ako se prenese "1", u suprotnom ostaje nepromijenjena. Za slanje više bitova, slika se dijeli na podslike, od kojih svaka odgovara jednom bitu poruke [16].

Predložena je druga tehnika koja se naziva maskiranje podataka. Prema ovoj tehnici, signal poruke se obrađuje tako da vidi svojstva proizvoljnog pokrivnog signala. U radu autori predlažu metodu u kojoj se transformirani koeficijenti slike raščlanjuju na dva dijela kako bi signal kodirane poruke zamijenio perceptivno beznačajnu komponentu. Stoga je statistika kvantiziranih (ne-nultih) diskretnih kosinusnih transformacija (eng. *Discrete Cosine Transform,* DCT*)* koeficijenata modificirana uzimajući u obzir parametarsku funkciju gustoće. Ovaj proces zahtijeva nisku preciznost histograma svakog frekvencijskog kanala uz usklađivanje modela sa svakim histogramom određivanjem odgovarajućih parametara modela [17].

3.5. Tehnika distorzije

Poruka je kodirana u pseudo-slučajno odabranim pikselima. Ako se stego-slika razlikuje od naslovne slike u danom pikselu poruke, tada je bit poruke "1". Inače, bit poruke je "0". Koder može modificirati piksele vrijednosti "1" na takav način da to ne utječe na statistička svojstva slike (što se razlikuje od mnogih *LSB* metoda). Međutim, potreba za slanjem naslovne slike ograničava prednosti ove tehnike. Kao i u svakoj steganografskoj tehnici, naslovna slika se nikada ne smije koristiti više od jednom. Ako napadač mijenja stego-sliku izrezivanjem, rotiranjem ili skaliranjem, primatelj može lako otkriti modifikaciju. U nekim slučajevima, ako je poruka kodirana informacijama za ispravljanje pogrešaka, promjena se može čak i poništiti, a izvorna poruka može se u potpunosti oporaviti [2].

Prvi rani pristup skrivanju informacija bio je u tekstu. Većina tehnika skrivanja temeljenih na tekstu je tipa distorzije. Na primjer, izgled dokumenta ili raspored riječi mogu pokazati ili odražavati prisutnost informacija. Uzimajući u obzir jednu od ovih tehnika, može prikazati podešavanje položaja redaka i riječi gdje se tekstu dodaju razmaci i "nevidljivi" znakovi, pružajući način slanja skrivenih informacija.

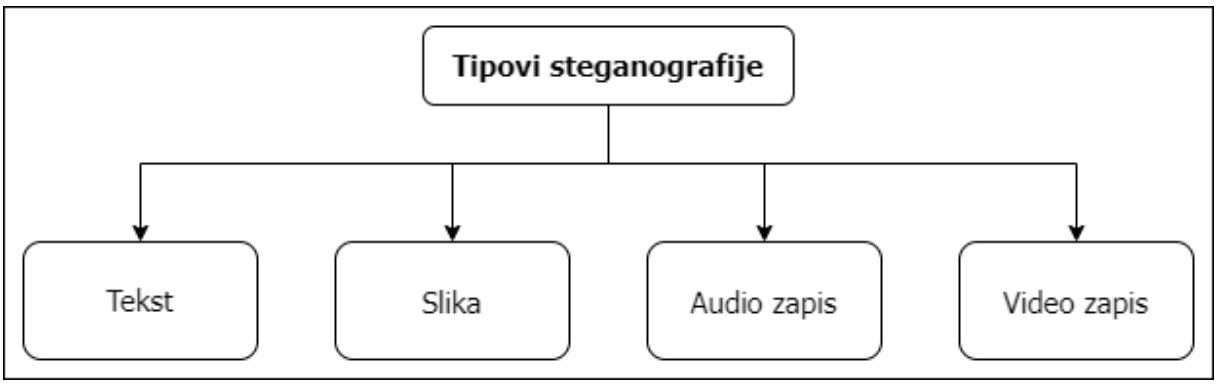
3.6. Tehnika generiranja naslovnica

Ova tehnika ili metoda je vrlo vjerojatno jedinstvena od svih 6 navedenih tehnika. Razlog tome je taj što ona radi na obrnuti način steganografiju. U klasičnoj steganografiji se odabire naslovni objekt za skrivanje poruke, no ovdje ne ide tako.

Naime, tu se stvara naslovni objekt s jednom jedinom svrhom, a to je skrivanje informacija. *Spammimic* je odličan primjer toga, a program radi na način da prvo unesete tajnu poruku i onda se generira poruka u obliku spama u koji se skrije tajna poruka.

4. Steganografija u elektroničkim dokumentima

Internet se uvelike koristi za razmjenu različitih vrsta informacija (tekst, slike, audio i video). No, temeljni protokoli ne podrazumijevaju nikakva stroga pravila za sigurnost podataka osim nekih kriptografskih protokola. Stoga je na krajnjim korisnicima da budu oprezni u pogledu sigurnosti svojih podataka tijekom tranzita. Iako ove kriptografske tehnike olakšavaju značajke kao što su provjera autentičnosti, povjerljivost, integritet i neporicanje, ne osiguravaju tajnost. Dakle, svaka treća strana koja promatra prenesene podatke može lako shvatiti da se prenosi nešto važno. Kako bi se prevladalo ovo ograničenje, prilagođene su tehnike skrivanja podataka poput steganografije. Steganografija izbjegava takvu privlačnost izvodeći komunikaciju na tajan način [5].



Slika 2: Tipovi steganografije [autorski rad]

4.1. Steganografija teksta

Steganografija se može klasificirati na slikovnu, tekstualnu, audio i video steganografiju ovisno o naslovnom mediju koji se koristi za umetanje tajnih podataka. Steganografija teksta može uključivati bilo što, od promjene oblikovanja postojećeg teksta, do promjene riječi unutar teksta, do generiranja nasumičnih nizova znakova ili korištenja gramatika bez konteksta za generiranje čitljivih tekstova [6].

Općenito mišljenje, a i činjenica je ta da je steganografija teksta najzahtjevnija, ponajviše zbog nedostatka viška informacija koje su prisutne u npr. slikama, audio ili video zapisima. Sama struktura tekstualnih datoteka je slična onome što se promatra, dok je u drugim vrstama, kao što je slika struktura datoteke drukčija od onog što se

promatra. Dakle, u takvim dokumentima se mogu sakriti informacije uvođenjem promjena u strukturu datoteke bez bitnije promjene u navedenom izlazu.

Na slikama ili audio zapisima se mogu napraviti neprimjetne promjene, no u slučaju tekstualnih datoteka obični čitatelj može označiti čak dodatno slovo ili interpunkcijski znak. Ipak nije sve tako loše u steganografiji teksta, naime pohranjivanje tekstualne datoteke zahtijeva manje memorije, a ono što ju čini poželjnom je njena brža i lakša komunikacija u odnosu na druge vrste steganografskih metoda. Steganografija teksta se može svrstati u tri tipa, a to su:

1) Metode na temelju formata,
2) Slučajno i statističko generiranje,
3) Lingvističke metode.

4.1.1. Metode na temelju formata

Metode temeljene na formatu uključuju fizičku promjenu formata teksta kako bi se sakrile informacije. Ova metoda ima određene nedostatke. Ako se stego datoteka otvori programom za obradu teksta, otkrit će se pravopisne pogreške i dodatni razmaci. Promijenjene veličine fontova mogu izazvati sumnju kod ljudskog čitatelja. Osim toga, ako je izvorni otvoreni tekst dostupan, usporedba ovog otvorenog teksta sa sumnjivim steganografskim tekstom učinila bi manipuliranim dijelovima teksta prilično vidljivima [6].

4.1.2. Slučajno i statističko generiranje

Kako bi izbjegli usporedbu s poznatim otvorenim tekstom, steganografi često pribjegavaju generiranju vlastitih naslovnih tekstova. Jedna metoda je prikrivanje informacija u nasumičnom slijedu znakova. U drugoj metodi, statistička svojstva duljine riječi i učestalosti slova koriste se kako bi se stvorile riječi za koje će se činiti da imaju ista statistička svojstva kao stvarne riječi u danom jeziku [7].

4.1.3. Lingvističke metode

Lingvistička steganografija posebno razmatra jezična svojstva generiranog i modificiranog teksta, te u mnogim slučajevima koristi jezičnu strukturu kao prostor u kojem su poruke skrivene. Gramatika bez konteksta (eng. *Context-Free Grammar,* CFG) kreira strukturu stabla koja se može koristiti za prikrivanje bitova gdje lijeva grana

predstavlja '0', a desna grana odgovara '1'. Gramatika u Greibachovoj normalnoj formi (eng. *Greibach Normal Form*, GNF) također se može koristiti gdje prvi izbor u produkciji predstavlja bit 0, a drugi izbor predstavlja bit 1. Ova metoda ima neke nedostatke. Prvo, mala gramatika će dovesti do puno ponavljanja teksta. Drugo, iako je tekst sintaktički besprijekoran, nedostaje mu semantička struktura. Rezultat je niz rečenica koje nemaju nikakve veze jedna s drugom [6].

4.2. Steganografija slike

4.2.1. Definicija slike

Uobičajeni način predstavljanja slika unutar memorije računala je kao matrica bitova (u engleskom jeziku poznata pod nazivom *bitmap*). Bitmapa je dvodimenzionalni niz malih točaka poznatih kao pikseli, a memorija računala (ili prostor unutar računalne datoteke) se koristi za pohranjivanje statusa svakog pojedinačnog piksela [8].

- U jednobojnoj bitmapi koristi se 1 bit memorije po pikselu, a to jednostavno pohranjuje je li piksel uključen (obično 1) ili isključen (obično 0).
- U bitmap prikazu u boji koristi se nekoliko bitova memorije po pikselu i u kombinaciji oni sadrže binarni broj ili brojeve. U nekim slučajevima, brojevi pohranjuju stvarnu boju piksela (često kao kombinacija vrijednosti intenziteta crvene, zelene i plave). U drugim slučajevima, ti brojevi mogu pohraniti referencu na tablicu boja ("paleta") [8].

Broj se bitova nazvan dubina bita ustvari odnosi na broj bitova koji se koriste za svaki piksel unutar svake slike. Trenutno najmanja dubina bita u shemama boja je 8, a to znači da se za opisivanje boje svakog piksela koristi 8 bitova. Obično slike sa sivim tonovima ili jednobojne slike koriste 8 bitnu shemu za svaki piksel što znači da svaki piksel može prikazati 256 različitih boja ili nijansi sive. S druge strane digitalne slike u boji se pohranjuju u 24 bitne datoteke i koriste crveni, zeleni i plavi (eng. *Red Green Blue*, RGB) model boja. Za piksele 24 bitne slike izvedene su iz tri primarne boje: crvene, zelene i plave, a svaka od boja je posebno predstavljena s 8 bitova. Stoga, u samo jednom pikselu može biti 256 različitih količina crvene, zelene i plave, što rezultira s više od 16 milijuna boja.

4.2.2. Kompresija slike

Kada se radi s većim slikama veće dubine bita, slike imaju tendenciju da postanu prevelike za prijenos putem standardne internetske veze. Kako bi se slika prikazala u razumnom vremenu, moraju se uključiti tehnike za smanjenje veličine datoteke slike. Ove tehnike koriste matematičke formule za analizu i kondenzaciju slikovnih podataka, što rezultira manjim veličinama datoteka. Taj se proces naziva kompresija. Na slikama postoje dvije vrste kompresije: s gubicima i bez gubitaka. Obje metode štede prostor za pohranu, ali se postupci koje provode razlikuju. Kompresija s gubitkom stvara manje datoteke odbacivanjem viška slikovnih podataka iz izvorne slike. Uklanja detalje koji su premali da ih ljudsko oko može razlikovati, što rezultira bliskim aproksimacijama izvorne slike, iako nije točan duplikat. Primjer formata slike koji koristi ovu tehniku kompresije je JPEG (*Joint Photographic Experts Group*) [9].

4.2.3. Steganografija slike JPEG formata

S obzirom da slike u *JPEG* formatu koriste kompresiju s gubicima vladalo je mišljenje da je nemoguće koristiti steganografiju jer bi dolazilo do promjena slikovnih podataka. Činjenica je naravno da je glavna karakteristika steganografije skrivanje informacija u suvišnim bitovima objekta nositelja, ali postojao je strah kada se koristi *JPEG* jer su redundantni bitovi izostavljeni da će tajna poruka biti uništena. Pa čak kada bi se i uspjelo sačuvati poruku bez oštećenja bilo bi teško ugraditi poruku, a da promjene nisu vidljive zbog primijenjene grube kompresije. Ipak, svojstva kompresijskog algoritma su iskorištena kako bi se razvio steganografski algoritam za *JPEG*. Jedno od tih svojstava se iskorištava kako bi se napravile promjene na slici koje kako bi bile nevidljive ljudskom oku. U procesu faze *DCT* transformacije algoritma kompresije se pojavljuju pogreške u zaokruživanju unutar podatak koeficijenata koje nisu uočljive. Ovo se može koristiti za skrivanje poruka iako ga algoritam klasificira kao s gubicima.

Nije ni izvedivo ni moguće ugraditi informacije u sliku koja koristi kompresiju s gubicima, budući da bi kompresija uništila sve informacije u procesu. Stoga je važno prepoznati da je algoritam kompresije *JPEG* zapravo podijeljen na faze s gubicima i bez gubitaka. *DCT* i faza kvantizacije čine dio faze s gubicima, dok je Huffmanovo kodiranje korišteno za daljnje kompresiranje podataka bez gubitaka. Steganografija se može odvijati između ove dvije faze. Koristeći iste principe *LSB* umetanja, poruka se

može ugraditi u najmanje značajne bitove koeficijenata prije primjene Huffmanovog kodiranja. Ugrađivanjem informacije u ovoj fazi, u transformacijskoj domeni, iznimno ju je teško otkriti, budući da nije u vizualnoj domeni [9].

4.3. Steganografija audio zapisa

Većina audio datoteka sastoji se od dugog niza brojeva (ili dva duga toka u slučaju stereo datoteke), pri čemu svaki broj odgovara amplitudi zvuka u bilo kojem trenutku. Obično postoje tisuće ili deseci tisuća brojeva za svaku sekundu zvuka. To je poznato kao pulsna kodna modulacija (eng. *Pulse Code Modulation*, PCM). Ako ima dovoljno brojeva u sekundi, a raspon brojeva je dovoljno širok, promjena na najmanje značajan bit nekih ili svih brojeva vjerojatno bi bila neprimjetna ili gotovo neprimjetna. Kao i kod slika, šifriranje skrivenih podataka prije dodavanja u audio tok učinilo bi ga gotovo nerazlučivim od nasumične buke. Također, kao i kod slika, postoje neki formati audio datoteka koji koriste kompresiju s gubicima, pa ova vrsta stenografije nije prikladna u takvim slučajevima [8].

U steganografiji audio zapisa se također koristi mnoštvo raznih metoda koje su malo detaljnije opisane u nastavku, s tim da *LSB* algoritam ovdje nije naveden, već je u nastavku obrađen u posebnom odjeljku.

4.3.1. Paritetno kodiranje

Paritetno kodiranje je jedna od robusnih steganografskih tehnika za audio zapise. Ova metoda razbija signal u posebne uzorke i ugrađuje svaki bit skrivene poruke iz bita parnosti. Proces invertira *LSB* jednog od uzoraka unutar odabrane regije ako paritetni bit ne odgovara tajnom bitu koji se kodira. Stoga, pošiljatelj ima više izbora u kodiranju tajnog bita.

4.3.2. Fazno kodiranje

Tehnika faznog kodiranja radi zamjenom faze početnog audio segmenta s referentnom fazom koja predstavlja tajnu informaciju. Faza preostalih segmenata se prilagođava kako bi se očuvala relativna faza između segmenata. Što se tiče omjera signala i šuma, fazno kodiranje je jedna od najučinkovitijih metoda kodiranja. Kada dođe do drastične promjene u faznom odnosu između svake komponente frekvencije, doći će do primjetne disperzije faze. Međutim, sve dok je modifikacija faze dovoljno

mala, može se postići nečujno kodiranje. Ova metoda se oslanja na činjenicu da fazne komponente zvuka nisu toliko uočljive ljudskom uhu kao buka [10].

4.3.3. Metoda proširenog spektra

Metoda proširenog spektra pokušava po frekventnom spektru audio signala proširiti tajne informacije ili poruke. Ova metoda je najsličnija sustavu koji koristi LSB implementaciju koji nasumično širi bitove poruke preko cijelog audio zapisa. Premda, za razliku od *LSB* algoritma metoda širenja spektra širi tajne poruke preko frekvencijskog spektra audio zapisa koristeći koji nije ovisan o stvarnom signalu. U odnosu na *LSB* algoritam ili fazno kodiranje, metoda proširenog spektra je sposobna pridonijeti boljoj izvedbi u nekim područjima jer nudi umjerenu brzinu prijenosa podataka i visoku razinu otpornosti na tehnike uklanjanja. Ipak, metoda proširenog spektra ima jedan veliki nedostatak, a to je da može unijeti šum u audio zapis.

4.3.4. Metoda skrivanja jeke

Kao što i samo ime govori može se pretpostaviti način rada ove metode, a to je da skriva tajnu poruku tako što doda jeku u diskretni signal. Prednosti ove metode su što omogućuje visoku brzinu prijenosa podataka, te vrhunsku robusnosti u usporedbi s ranije navedenim metodama. Jedan bit tajne poruke bi se mogao kodirat ako bi se iz izvornog objekta tj. audio zapisa proizvela samo jedan jeka. Dakle, izvorni signal se razbija u blokove prije početka procesa kodiranja. Blokovi se ponovno spajaju nakon što se proces kodiranja završi, te se tako u konačnici stvara gotov signal s tajnom porukom.

4.4. Steganografija videozapisa

U moderno vrijeme sve većim razvojem različitih tehnologija za obradu videa dalo je povoda za se video sve više smatra dobrim medijem za skrivanje informacija. Glavna prednost je u tome što video ima volumen ponavljanja podataka što se u principu može iskoristiti za pohranu podataka. Videozapis se sastoji od dva dijela, dekodera i kodera, koji automatski dekompresira i komprimira video, te spremnik koji sadrži stvarne okvire podataka. Kompresija videozapisa može biti s gubicima koji imaju osjetno manju veličinu od izvornog videozapisa, no kvaliteta i razlučivost su ugroženi.

Kvaliteta se zadržava kod kompresije bez gubitka, ali problem je onda ogromna veličina datoteke.

4.4.1. Tehnika DCT

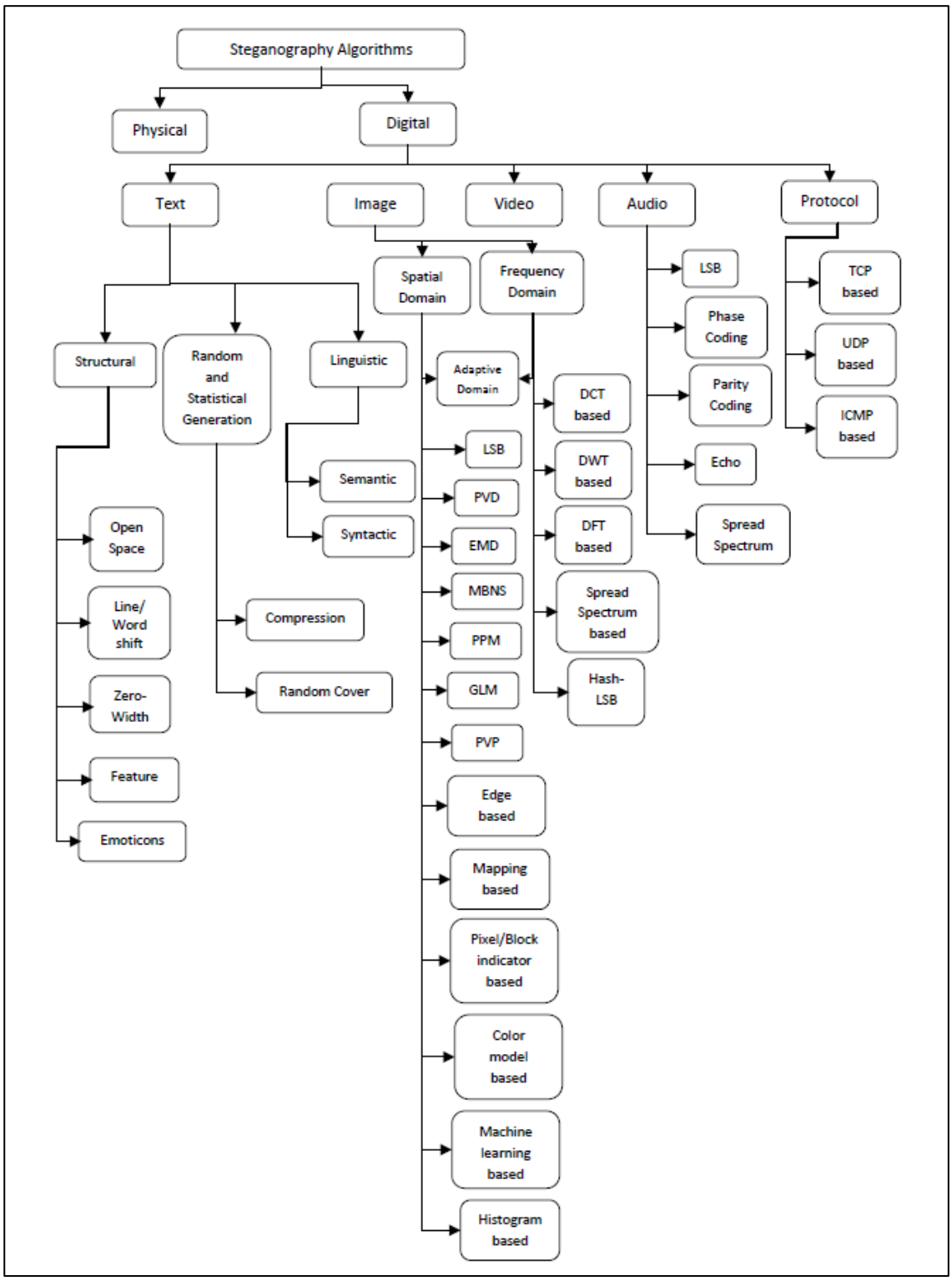
U tehnici baziranoj na *DCT*, slika je segmentirana u nisko, srednje i visokofrekventne pojaseve. Prednosti ove metode su visoki omjer kompresije i vrlo niska stopa pogreške. Neke od tehnika temeljenih na *DCT*-u su *Bose-Chaudhuri-Hocquenghem* (*BCH*) kodovi za ispravljanje pogrešaka, algoritam za skrivanje podataka bez širenja pogrešaka unutar okvira, shema perturbacije temeljena na *DCT*-u, formulacija tajne poruke i koeficijenti praćenja [11].

4.4.2. Tehnika DWT

Valić je mali val i valna oscilacija temelji se na vremenskoj domeni. Diskretna transformacija valića (eng. *Discrete Wavelet Transform*, DWT) je najnovija i učinkovita metoda za skrivanje podataka. Prednost *DWT* tehnike je u tome što obavlja i lokalnu i multirezolucijsku analizu. Inverzna valna transformacija koristi se za davanje izvornog formata objekta. Neke od tehnika temeljenih na *DWT*-u koje se koriste za skrivanje podataka su inverzni dvodimenzionalni *DWT*, algoritam praćenja Kanade, Lucasa i Tomasija, Transformacija cjelobrojnog vala, Arnoldova transformacija i skrivanje kanala [11].

4.5. Algoritam LSB

Prije samoga opisa *LSB* algoritma koji je više puta spomenut u radu, potrebno je prikazati podjelu svih steganografskih algoritama koji se koriste u moderno doba.



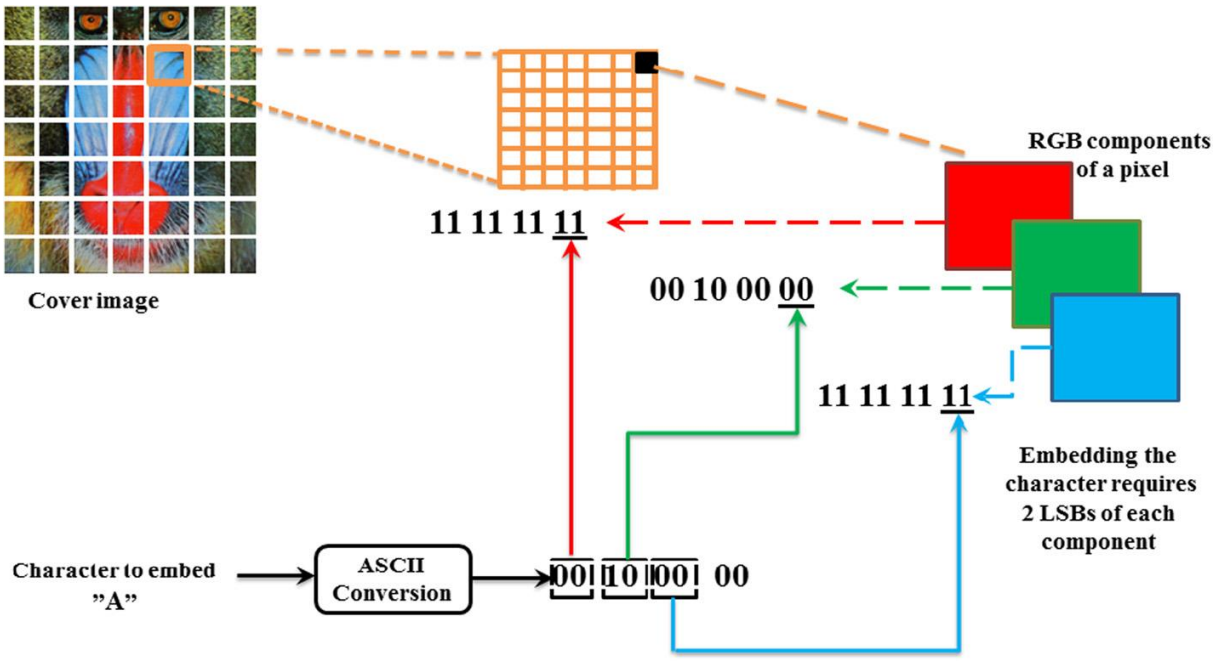
Slika 3: Steganografski algoritmi [12]

Iz slike 3 se vidi da tu postoji mnoštvo različitih algoritama, od tekstualnih pa do video datoteka. S obzirom da će kroz rad biti prikazan praktični primjer koji koristi *LSB* algoritam onda je jedini podrobnije opisan.

LSB algoritam je vjerojatno najjednostavniji steganografski algoritam. Može se primijeniti na bilo koju zbirku brojčanih podataka predstavljenih u digitalnom obliku. Pretpostavka da je x[*i*] ∈ X = $\{0, \ldots, 2^{n_c} - 1\}$ je niz cijelih brojeva. Na primjer, x[*i*] može biti intenzitet svjetla na i-tom pikselu u 8-bitnoj slici u sivim tonovima ($n_c = 8$), indeks palete u *GIF* (eng. *Graphic Interchange Format*) datoteci ($n_c = 8$) ili kvantizirani *DCT* koeficijent u *JPEG* datoteku ($n_c = 11$). Ovisno o formatu slike i dubini bita odabranoj za predstavljanje pojedinačnih vrijednosti, svaki x[*i*] može se predstaviti pomoću n_c bitova b[*i*, 1], . . . , b[*i*, n_c] [4].

$$x[i] = \sum_{k=1}^{n_c} b[i,k]\, B^{n_c-k}$$

Stoga se o slijedu (b[*i*, 1], . . ., b[*i*, n_c]) može razmišljati kao o binarnom prikazu x[*i*] u obliku velikog broja (najznačajniji bit b[*i*, 1] je prvi). *LSB* je posljednji bit b[*i*, n_c]. *LSB* ugrađivanje, kao što mu ime sugerira, radi zamjenom *LSB*-ova od x[*i*] s bitovima poruke m[*i*], dobivajući u tom procesu stego sliku y[*i*] [4].



Slika 4: Skrivanje podataka pomoću LSB-a u slikama [3]

Laički objašnjeno u svom najosnovnijem obliku *LSB* steganografija znači jednostavnu zamjenu najmanje značajnijih bitova kanala boja u svakom pikselu na naslovnom objektu s bitovima steganografske poruke. Zamjena se bitova izvodi sekvencijalno ili na podskupu piksela, npr. odabranom upotrebom generatora pseudoslučajnih brojeva. Iako prisutnost steganografije na slici nije sasvim očita ljudskom oku osim ako promatrač ne zna za postojanje steganografije ipak je relativno laka za detekciju različitim metodama analize ponajviše zbog svoje jednostavnosti.

Jednostavan primjer *LSB* steganografije je najlakše prikazati kroz binarni zapis: Pretpostavka je da se slovo S želi sakriti u sljedećem zapisu:

01101011	11010001	00101101	11100100
10110010	00100011	10101001	01010011

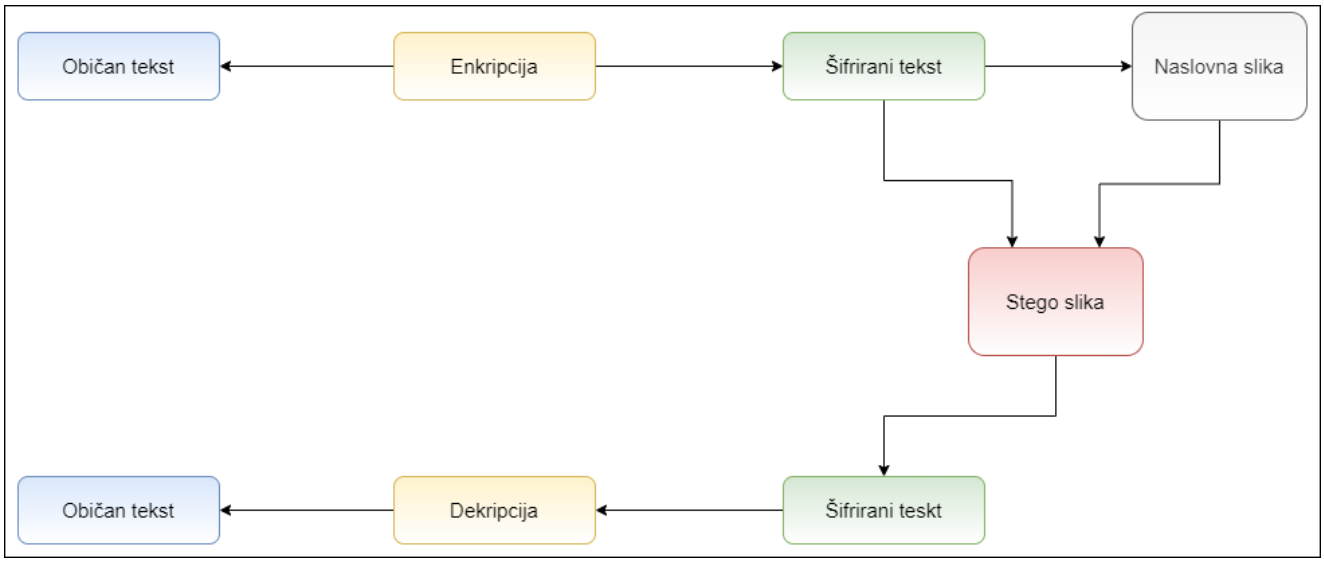
Slovo S u binarnom zapisu prema Američkom standardnom znakovniku za razmjenu informacija (eng. *American Standard Code for Information Interchange*, ASCII) je sljedeće **01010011**. Ovih se 8 bitova zapisuje na mjesto bitova najmanje važnosti ranije navedenog zapisa, te stoga dolazi do promjene u zapisu:

0110101**0**	1101000**1**	0010110**0**	1110010**1**
1011001**0**	0010000**1**	1010100**1**	0101001**1**

4.6. Kriptografija i steganografija

Za razliku od steganografije, kriptografija mijenja tajnu poruku iz jednog oblika u drugi, gdje je često samo postojanje poruke poznato, ali sadržaj poruke ne jer je poruka kodirana i nečitljiva. Šifrirane poruke se ne mogu baš lako dekodirati dok se uglavnom nerijetko mogu presresti i locirati. Ovaj pristup skrivanja informacija u šifri štiti poruku, no presretanje poruke može biti isto štetno jer daje trag neprijatelju ili protivniku da netko komunicira s nekim drugim. Steganografija daje suprotan pristup i pokušava sakriti sve moguće dokaze tijekom komunikacije.

Steganografija nije isto što i kriptografija, tehnike skrivanja podataka naširoko su korištene za prijenos skrivenih tajnih poruka dugo vremena. Osiguravanje sigurnosti podataka veliki je izazov za korisnike računala. Poslovni ljudi, profesionalci i kućni korisnici imaju neke važne podatke koje žele zaštititi od drugih. Iako obje metode pružaju sigurnost, za dodavanje više slojeva sigurnosti uvijek je dobra praksa koristiti kriptografiju i steganografiju zajedno. Kombiniranjem se šifriranje podataka može obaviti softverom, a zatim šifrirani tekst ugraditi u sliku ili bilo koji drugi medij uz pomoć stego ključa. Kombinacija ove dvije metode poboljšat će sigurnost ugrađenih podataka [11].



Slika 5:Kombinacija kriptografije i steganografije [autorski rad]

Tablica 2: Steganografija, kriptografija i njihova kombinacija

Rb	**Steganografija**	**Kriptografija**	**Kombinacija**
1.	Tajna poruka je skrivena unutar neke datoteke tj. naslovnog objekta, te stvara stego datoteku.	Poruka je u nečitljivom formatu pretvorena u niz šifriranih znakova.	Običan se tekst pretvara u šifriranu poruku, a zatim se šifrirana poruka pretvara u stego datoteku.
2.	Tajna poruka se ne može lako otkriti jer je skrivena unutar druge datoteke.	Svatko može lako otkriti i izmijeniti poruku.	Poruka je šifrirana i zaštićena od napadača ili presretača.
3.	Cilj je osigurati postojanje skrivene tajne poruke od napadača.	Cilj je spriječiti neovlašten pristup.	Sprječava neovlašten napad i sprječava čitanje poruka od strane napadača.
4.	Vađenje i otkrivanje tajne poruke je jako složen proces.	Podaci se mogu lako otkriti, ali vađenje podataka je jako složeno.	Otkrivanje kao i vađenje tajne poruke su složeni proces.
5.	Podaci razmjene se redovito analiziraju i prate.	Provodi se obrnuti inženjering kako bi se udvostručila ili poboljšala sigurnost.	Sigurnost se poboljšava obrnutim inženjeringom kao i redovitim praćenjem podataka.

4.7. Primjena steganografije u moderno doba

Iako relativno još mnogima nepoznat pojam i tehnologija na internetu postoji mnoštvo programa za skrivanje podataka u elektroničkim medijima, čak štoviše mnogi od njih su i besplatni. Većina njih ima poprilično jednostavna korisnička sučelja koja su laka za korištenje koja omogućuju skrivanje podataka u različitim formatima na različitim operacijskim sustavima. Osim besplatnih programa postoji određen broj programa koji se koriste u komercijalne svrhe, što ustvari govori da postoji tržište za steganografiju, te je to isto tržište spremno platiti za korištenje. Tradicionalno gledajući steganografiju su uglavnom koristile kriminalne organizacije i vojske. Trend u usponu je taj da dolazi do povećanja upotrebe steganografije u komercijalnom sektoru.

Stvarnost je da tajnu komunikaciju koriste iz raznih razloga i od strane raznih ljudi, od poslovnih ljudi koji štite poslovne tajne tvrtke dok putuju do kriminalaca koji prenose dječju pornografiju. Vlade skrivaju informacije od drugih vlada, a tehnofili se zabavljaju slanjem tajnih poruka jedni drugima samo iz zabave. Jedina veza koja veže sve te ljude je želja da se nešto sakrije od nekog drugog. Nažalost, u svijetu uzbune, metode dostupne svakome tko želi sakriti informacije sigurno će postati sofisticiranije kako bi odgovarale vremenu i bit će zlouporabljene [15].

Poduzeća danas žele pod svaku cijenu zaštiti svoje podatke, kao i podatke svojih korisnika ako ih imaju naravno. Ipak, mnoga poduzeća zaostaju za kriminalnim organizacijama pod čijim se napadom nerijetko nalaze. Velik broj tvrtki misli da mogu koristiti samo jednu tehnologiju tipa sigurnosni sloj utikača (eng*. Secure Sockets Layer*, SSL) za online transakcije ili softver s vatroštitom ili virtualnom privatnom mrežom (eng. *virtual private network*, VPN), što je za današnje doba u esenciji pogrešno razmišljanje. Iako, jednostavna zaštita funkcionira dobro unutar tvrtke, ona je praktički nepostojeća dok se mediji razmjenjuju putem interneta. Stoga, steganografija dolazi sve više do izražaja kao i samo skrivanje podataka i neprimjetno tajno komuniciranje. Primjenu je čak dobilo i u nezamjenjivim tokenima (eng. *Non-fungible Token*, NFT)

Korištenje vodenog žiga u medicinskoj dokumentaciji kao metode točne identifikacije odmah je vidljivo. S obzirom na to da medicinska industrija sve više migrira prema digitalnim zapisima, vodeni žig postaje obvezan dodatak za sprječavanje zabune u kartonima pacijenata. Zbog različitih protokola i različitih platformi koje se koriste u svijetu računala, podaci se ponekad mogu oštetiti kada se pretvore iz jednog formata u drugi. Trenutno, većina slikovnih formata odvaja slikovne podatke od teksta; rendgenski snimak je odvojen od imena pacijenta, datuma rendgenske snimke i imena liječnika; ako bi se veza između slike i teksta ikada prekinula, stvari bi se mogle pogoršati. Način da se to spriječi je da se u sliku ugradi ime pacijenta i sve druge relevantne informacije. Svaki pacijent ima elektronički karton pacijenta (eng. *Electronic Patient Records*, EPR) koji se sastoji od pregleda, dijagnoza, recepata itd., u osnovi glavna datoteka koja sadrži zapis o tome što je učinjeno s pacijentom [2].

Danas postoji mnoštvo programa i aplikacija za implementaciju steganografije, a mnoge od njih su besplatne. Par najboljih su:

- *Image Steganography* – jedan u nizu besplatnih alata za izvođenje robusne steganografije slika.
- *Steghide* – ovaj program može sakriti slikovne i audio datoteke. Glavne karakteristike ovog programa su da uključuje kompresiju, šifriranje i automatski integritet. Formati koji su podržani su *JPEG, BMP, WAV, AU*. Tajni podaci nisu ograničeni samo na tekst, nego može biti bilo koja vrsta podataka. Za šifriranje se koristi algoritam Rijndael s ključem od 128 bita tj. AES (eng. *Advanced Encryption Standard*) enkripcija. Preporuka je da je najbolji softver za Linux i Mac operacijske sustave.
- *RSteg* – alat razvijen u programskom jeziku Java, stoga je za pokretanje programa potrebno imati instaliranu Javu na računalu. Moguća je samo steganografija slike koja se šifrira, što znači da je za dešifriranje tajne poruke potrebno postaviti i upisati lozinku. Format u kojemu program radi je PNG (eng. *Portable Network Graphic*) ekstenzije.

Naravno postoje još mnoge druge aplikacije i alati, ali iznad su navedeni neki od trenutno dostupnih i besplatnih. Između ostalog postoje i razni softveri otvorenog koda (eng. *Open source*) programi, posebice na GitHub-u.

5. Steganaliza

U ranije spomenutom problemu zatvorenika, Ani i Luki je dopušteno komunicirati, ali sve poruke koje razmjenjuju pažljivo prati upraviteljica zatvora Petra koja traži tragove tajnih poruka koje bi mogle biti skrivene u predmetima koje dvoje zatvorenika razmjenjuje. Petrina aktivnost se naziva steganaliza i ona je komplementaran zadatak steganografiji. U principu, steganalitičar je uspješan u napadu na steganografski kanal ako može razlikovati objekte za prikrivanje i stego s vjerojatnošću boljom od samo slučajnog pogađanja. Za razliku od kriptoanalize nije potrebno biti u stanju pročitati tajnu poruku da bi se razbio steganografski sustav. Bitan zadatak izdvajanja tajne poruke iz slike nakon što je poznato da sadrži tajnu poruku ili podatke pripada forenzičkoj steganalizi.

Steganalizom napadač može identificirati prisutnost skrivenog teksta u digitalnim medijima. Glavni cilj steganalitičara je identificirati je li tajni tekst prisutan ili ne u stego medijima. Mnogi istraživači pokušali su kategorizirati napade steganalizom, na temelju pristupa steganalize kao što su statistička steganaliza i steganaliza temeljena na značajkama. Postoje različiti načini na koje se može napraviti analiza slike za koje su dostupne različite metode i alati za otkrivanje steganografije. Steganaliza slike podijeljena je u dvije široke kategorije:

a) Ciljna steganaliza
b) Slijepa steganaliza [12].

S obzirom da steganografija postaje sve sofisticiranija, njena otpornost da bude analizirana pa čak i prepoznata će se poboljšati. Trenutno stanje stego tehnologije je da ako postoji sumnja da se koristi steganografija relativno je lako otkriti postojanje same poruke. Nakon što se otkrije da postoji onda se može uz primjenu pravih metoda otkriti i dohvatiti sadržaj koji može biti zaštićen samo enkripcijom ako postoji. Kroz neku bližu budućnost će se nastojati da stego bude neprimjetan i nepovratan osim onima kojima je namijenjen. Puno toga ovisi i o vrstama nositelja i dostupnim vrstama komunikacije, npr. mogu li se velike video datoteke lako poslati putem osobne bežične mreže s nekim oblikom bežičnog protokola koji uspješno štiti podatke od otkrivanja.

5.1. Vizualni napad

Vizualni napad je najjednostavniji oblik steganalize koji uključuje analiziranje stego slike ili objekta golim okom u svrhu identifikacije bilo kakve moguće degradacije. Steganografije obično ne ostavlja nekakvu vrstu vizualnog izobličenja na slici zbog modifikacije bitova. Iako, kada se uklone dijelovi slike koji nisu promijenjeni kao rezultat ugradnje obično je onda moguće uočiti znakove manipulacije. Ljudski je vid osposobljen za prepoznavanje poznatih stvari, te je sposoban prepoznati promjene, a takva se sposobnost koristi za vizualne napade. Vizualni napad omogućuje ljudima da razlikuju slikovnu buku i vizualne obrasce.

Vizualni napad se može implementirati na mnogo načina provjeravanjem različitih svojstava slike. Mogao bi se uspostaviti vizualni napad na prikaz prostorne domene slike provjeravanjem njenog *LSB*-a. Slike uglavnom sadrže onoliko 1 koliko 0 u svojoj najmanjoj ravnini, dok s druge strane tekst često ima više 0 nego 1, te to stvara vizualnu nedosljednost. Osobe koje se bave steganalizom traže takvu nedosljednost kako bi klasificirale sliku kao stego sliku ili kao sasvim normalnu sliku.

5.2. Statistički napad

Kod ove vrste napada ili analize statistička analiza slika se provodi uz pomoć neke matematičke formule, te se otkriva prisutnost skrivenih podataka. Jednim je dijelom čak i sličan vizualnom napadu. Općenito, skrivena je poruka slučajnija od izvornih podataka slike, stoga pronalaženje formule za poznavanje slučajnosti otkriva postojanje podataka.

Izradila bi se teorija koja naizgled objašnjava zašto se fenomen događa, a statističke metode se tada mogu koristiti da se dokaže da je ova teorija ili istinita ili netočna. Ako se struktura podataka razmatra za stego-sliku, tada statistika može biti korisna za steganalizu kada se dokazuje sadrži li slika skrivenu poruku ili ne. Statistički testovi mogu otkriti da je slika modificirana steganografijom utvrđivanjem da statistička svojstva slike odstupaju od norme. Neki testovi su neovisni o formatu podataka i samo mjere entropiju suvišnih podataka. Najjednostavniji test mjeri korelaciju prema jednoj i ne može automatski odlučiti sadrži li slika skrivenu poruku [13].

5.3. Strukturni napad

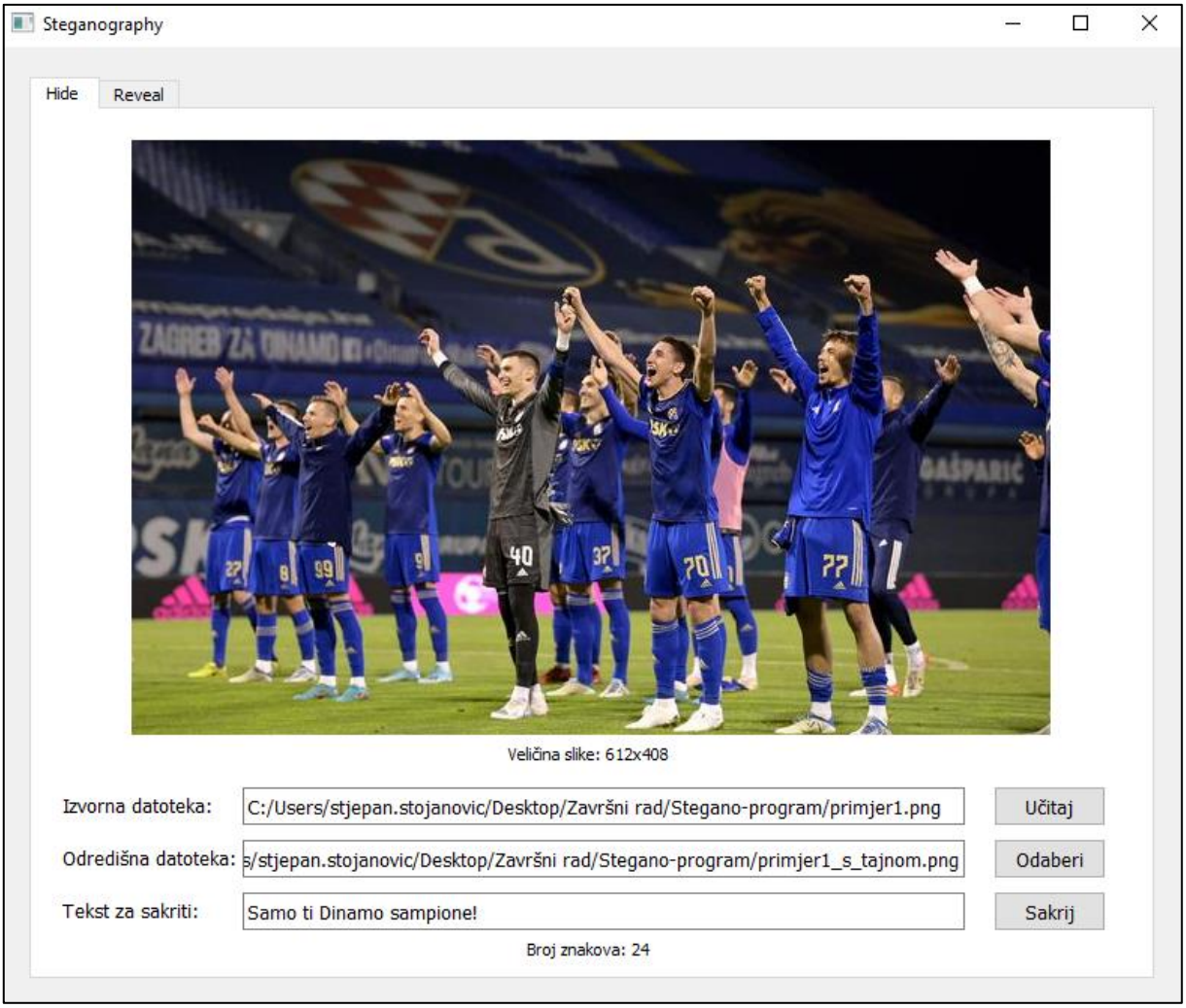
Strukturni napadi su dizajnirani da iskoriste svojstva visoke razine za koja se zna da postoje za određeni steganografski algoritam. Steganografske metode ostavljaju za sobom karakterističnu strukturu podataka. Napadač može otkriti postojanje tajne poruke ispitivanjem statističkog profila bitova ili identificiranjem ovih karakterističnih promjena strukture. Strukturni napadi rijetko analiziraju svaku sliku prema njezinim vrijednostima. Umjesto toga, slike se skeniraju kako bi se vidjelo sadrže li neke od poznatih nuspojava za različite steganografske algoritme. Slike koje sadrže ta svojstva često su podvrgnute daljnjoj istrazi. Postoje neki slučajevi u kojima slika može imati znakove steganografije kada može biti potpuno nevina. Zbog toga strukturalni napad obično slijedi temeljitiju istragu [14].

Za steganalitičare je bez imalo dvojbe strukturni napad poprilično važniji u odnosu na vizualni napad iz razloga što se može primijeniti na širi raspon tehnika implementacije. Napad uglavnom najbolje funkcionira kada steganalitičar već ima pristup poznatoj stego slici ili stego objektu. U principu se strukturni napad ne koristi kao neko sredstvo za dokaz da slika sadrži steganografiju, nego istražuje sadrži li slika znakove ugradnje što ustvari omogućuje steganalitičaru da zaključi je li netko petljao sa slikom ili ne. Strukturni napadi su RS analiza i analiza para.

6. Praktični rad

U nastavku će biti prikazan praktični primjer steganografije slike, primjer aplikacije je napisan u programskom jeziku *Python*, a za grafičko korisničko sučelje (eng. *Graphical user interface*, GUI) je korišten *PyQt5*. Korisničko sučelje aplikacije je poprilično jednostavan, prilikom pokretanja otvara se glavni zaslon koji se sastoji od dva prozorčića *hide* i *reveal*. U *hide* dijelu se nalaze tri gumba učitaj koji otvara preglednik datoteka za odabir slike, odaberi za odabir gdje će se stego slika spremiti, te najbitniji gumb sakrij kojemu je funkcionalnost sakriti tajnu poruku u sliku, te se nakon toga otvara *popup* prozor ako je uspješno odrađena steganografija slike.

GUI kao što je spomenuto je napravljen pomoću modula *PyQt5*, a većim dijelom Qt Designerom. Klasa *MainWindow* nasljeđuje objekte učitane iz ui datoteke. Prilikom inicijalizacije objekta klase *MainWindow* se dodaju, povezuju signali koji se šalju



Slika 6:Korisničko sučelje Hide [autorski rad]

pritiskom tipke na korisničkom sučelju. Pritiskom svake tipke pokreću se određene metode definirane u klasi kao što su odabir datoteka i slično.

U nastavku slijedi opis samog koda i funkcionalnosti aplikacije. Kao što je kroz rad nekoliko puta spomenuto za skrivanje teksta u slici koristi se algoritam *Least Significant Bit* (LSB). S obzirom da je boja piksela definirana *RGB* komponentama (3-osam bitne vrijednosti), binarni zapis teksta (uključujući i *breakpoint* na kraju teksta) se sprema na najmanje značajan bit crvene boje. Što znači da veličina slike (broj piksela) mora biti veća ili jednaka duljini skrivenog teksta u bitovima (svaki znak je 7 bitova + 7 bitova za *breakpoint* na kraju poruke). Skrivena poruka u slici se čita tako da se uzima najmanje značajan bit crvene boje sve dok zadnjih sedam bitova ne budu jednaki vrijednosti *breakpointa*.

```
def __img2binary(self, img_path):

    # Provjeri ispravnost slike
    if not os.path.exists(img_path):
        raise Exception("Ne postoji putanja izvorne slike!")
    elif not img_path.endswith(".png"):
        raise Exception("Izvorna slika mora biti .png ekstenzije!")


    # Otvori sliku i saznaj njenu veličinu
    img = Image.open(img_path)
    self.size = img.size


    # Provjeri je li slika RGB
    if img.mode != 'RGB':
        raise Exception("Izvorna slika nije u RGB formata!")


    # Pretvori RGB (dekadske vrijednosti) u binarni zapis i dodaj u listu kao tuple-ove
    binary_data = []
    for r, g, b in img.getdata():
        binary_data.append((bin(r), bin(g), bin(b)))

    return binary_data
```

Slika 7:Prikaz koda pretvorbe slike u binarni zapis [autorski rad]

Aplikacija ima 5 privatnih metoda, a jedna od njih je *__img2binary*, a ona pretvara sliku (objekt tipa *Image*) u binarni zapis. Aplikacija prihvaća samo slike koje su u *RGB* formatu .png ekstenzije. Također postoji još i funkcija *__binary2img* koja pretvara binarni zapis u sliku tj. u objekt tipa *Image*.

```python
def __text2binary(self, text):

    # Provjeri je li upisan tekst
    if text == "":
        raise Exception("Nije upisan tekst za skrivanje!")


    # Kodiraj zadani tekst u ASCII
    byte_obj = text.encode('ascii')


    # Čitaj znak po znak u binarnom zapisu
    # Ignoriraj '0b' na početku zapisa
    # Ako znak koristi manje od 7 (toliko ih može biti maksimalno) nadopuni prazna mjesta s nulama
    # Svaki uređeni zapis znaka nadodaj na string varijablu 'binary_data'
    binary_data = ""
    for b in byte_obj:
        temp = bin(b)[2:]
        temp = '0' * (7 - len(temp)) + temp
        binary_data += temp

    # Dodaj točku završetka na kraj kako bi znali prilikom čitanja slike gdje skrivena poruka završava
    binary_data += self.breakpoint

    return binary_data
```

Slika 9:Prikaz koda pretvorbe stringa u binarni zapis [autorski rad]

Nadalje funkcija *__text2binary* služi za pretvorbu znakovnog niza (eng. *String*) u binarni zapis. Za program je korištena *ASCII* notacija, što znači da nije moguće upisati u tajnu poruku slova s kvačicom. Funkcija čita znak po znak u binarnom zapisu s tim da se ignorira 0b na početku zapisa. U slučaju da znak koji se koristi za skrivanje koristi manje od 7 bitova onda se nadopune prazna mjesta s nulama.

```python
def __return_secret_text_binary(self, binary_image):
    # Dohvaćaj zadnji bit crvene boje sve dok zadnjih sedam znamenki ne bude jednaka točki završetka
    # Vrati sve dohvaćene bitove kao string bez zadnjih sedam (oni su točka završetka koja se odbacuje)
    binary_text = ""
    for r, b, g in binary_image:
        binary_text += r[-1]
        if binary_text[-7:] == self.breakpoint:
            return binary_text[:-7]

    # Vrati 'None' ako nije pronađen uzorak jednak točki završetka (znači da nema skrivene poruke u slici)
    return None
```

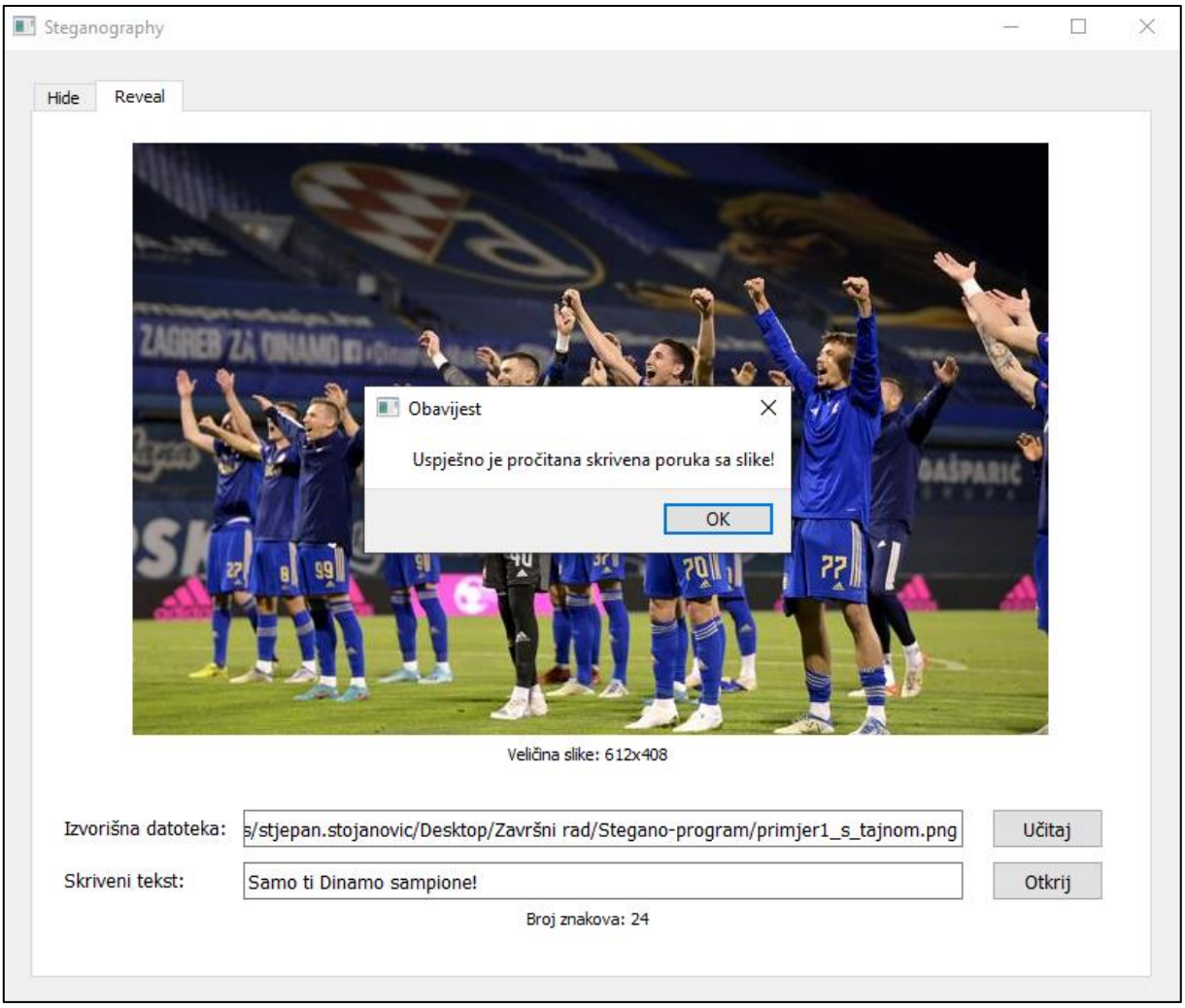
Slika 8:Prikaz koda metode za pronalazak skrivenog teksta u binarnom obliku i u binarnom obliku slike [autorski rad]

Za skrivanje tajne poruke koriste se bitovi piksela crvene boje, a funkcija *__return_secret_text_binary* pronalazi skriveni tekst u binarnom obliku. Funkcija dohvaća zadnji bit crvene boje sve dok zadnjih sedam znamenki ne bude jednako točki završetka. Dohvaćeni se bitovi vraćaju kao *string* bez zadnjih sedam jer su oni točka završetka koji se odbacuju.

```python
    def hide(self, text, img_src, img_dest):
        """
        Metoda kao argumente prima tekst koji će se sakriti, putanju slike u koju će se sakriti
        te putanju na koju će biti pohranjena nova slika sa skrivenim tekstom.
        Metoda vraća None vrijednost
        """
        binary_image = self.__img2binary(img_src)
        binary_text = self.__text2binary(text)


        # Provjeri ima li slika manje binarnih tuple-ova nego tekst binarnih znamenki
        if len(binary_image) < len(binary_text):
            raise Exception("Slika je premala da mi se u nju sakrio zadani tekst")


        # Svaki bit teksta zapiši na mjesto bita najmanje značajnosti (LSB algoritam) crvene boje
        binary_image_new = []
        for i, bin_value in enumerate(binary_text):
            r, g, b = binary_image[i]
            r = r[:-1] + bin_value
            binary_image_new.append((r, g, b))

        # Ostatak tuple-ova (nepromjenjenih) dodaj u novi binarni zapis slike
        for i in range(len(binary_text), len(binary_image)):
            binary_image_new.append(binary_image[i])

        self.__binary2img(binary_image_new, img_dest)


    def reveal(self, img_path):
        """
        Metoda kao argument prima putanju slike i vraća string ako se u njoj nalazi skriveni tekst
        ili None ako ga nema skrivenog teksta
        """
        binary_image = self.__img2binary(img_path)
        binary_text = self.__return_secret_text_binary(binary_image)
        return self.__binary2text(binary_text)
```

Slika 10:Prikaz koda javnih metoda [autorski rad]

Jedine javne metode su dvije koje su u principu srž dvije glavne funkcionalnosti aplikacije, jedna *hide* koja služi za skrivanje teksta, te druga *reveal* koja služi za otkrivanje skrivenog teksta ako ga ima. Ako slika ima manje binarnih uređenih N-torki (eng. *Tuple*) nego tekst binarnih znamenki onda nije moguće skrivanje tekst u suprotnom je moguće. Također kroz rad više puta spomenuti *LSB* algoritam je metodi *hide*, koji radi na način da se svaki bit teksta zapiše u bit najmanje značajnosti piksela crvene boje. Ostatak nepromijenjenih *tuple*-ova se dodaje u novi binarni zapis slike.



Slika 11:Korisničko sučelje Reveal [autorski rad]

Korisničko sučelje za otkrivanje teksta je još jednostavnije, u principu traži samo da se učita slika iz koje želimo iščitati tajnu poruku. U slučaju da se u slici nalazi tajna poruka *popup* prozor izbacuje obavijest o uspješno pročitanoj tajnoj poruci ili obavijest o pogrešci ako nema skrivenog tekst u slici.

6.1. Korištene tehnologije

Za praktični rad su korištene sljedeće tehnologije:

- *Python* – U programskom jeziku Python je napisan čisti program, što znači da je to bez korisničkog sučelja. Python je objektno orijentirani, programski jezik visoke razine s dinamičkom semantikom. Jedan je od najjednostavnijih i najefikasnijih programskih jezika za brzi razvoj aplikacija.

- *PIL* biblioteka – Python Imaging Library dodaje mogućnosti obrade slika Python interpretatoru. Ova datoteka je krucijalan dio same aplikacije s obzirom da se radi o steganografiji slika, te ne bi bilo moguće raditi sa slikama bez ove biblioteke.
- *Image* modul – Modul Image pruža klasu s istim imenom koja se koristi za predstavljanje PIL slike. Modul također nudi brojne tvorničke funkcije, uključujući funkcije za učitavanje slika iz datoteka i stvaranje novih slika.
- *PyQt5* – PyQt5 je korišten za razvoj i implementaciju korisničkog sučelja.
- *PyCharm* – PyCharm je integrirano razvojno okruženje (IDE) koje se koristi u računalnom programiranju, posebno za programski jezik Python. Poprilično je jednostavan za korištenje i omogućuje pokretanje programa izravno.
- *QtDesigner* – Qt Designer je Qt alat za projektiranje i izgradnju grafičkih korisničkih sučelja (GUI) s Qt Widgetima. Program se inače plaća, ali za studente je besplatan za korištenje.

Slika iz praktičnog dijela preuzeta s Večernji.hr, „Čak i kada je loš i nudi postolje protivnicima, u HNL-u naslov osvaja – Dinamo“ (https://www.vecernji.hr/sport/i-kada-je-los-i-nudi-postolje-protivnicima-u-hnl-u-i-dalje-naslov-osvaja-dinamo-1586674), Igor Soban, PIXSELL

7. Zaključak

Svjedoci smo da danas više ništa nije privatno, pa tako niti komunikacija s najbližim prijateljem. Razvojem IT industrije i tehnološkom eksplozijom naša aktivnost na internetu postaje sve ranjivija, a naša komunikacija više nije samo između dvije osobe. Danas postoji mnogo aplikacija i programa koje široj masi omogućuje tajno komuniciranje. Ipak, s pojmom steganografije i tehnologijom su uglavnom upoznati informatičari ili osobe koje vole same istraživati.

Samim razvojem steganografije dolazi i do razvoja steganalize, koja kontrira steganografiji. Danas je veliki problem taj što steganografiju koriste terorističke grupe za komunikaciju. Za razliku od kriptografije za koju se između ostalog zna da postoji i da je prisutna, u steganografiji to nije slučaj. Naime, ono što može djelovati kao samo nevino slanje slika može skrivati iza sebe tamnu pozadinu, slike ispod kojih mogu biti osjetljive informacije i podaci. Zbog toga je došlo do velikih programa koji prikupljaju veliki broj slika koje onda prolaze razne tehnike steganalitičkih napada u slučaju da se odvija tajna komunikacija.

U svakom slučaju steganografija je moćan alat ako se koristi na pravilan način. Iako ima svoje mane, prednosti su ipak brojnije i važnije od nedostataka. Ljudi su danas osjetljivi na svoju privatnost, ponajviše zbog brzog razvoja tehnologija koje istu tu privatnost narušavaju. Stoga je bitno uraditi sve kako bi barem imali jedan mali dio privatnosti, a to se može postići korištenjem raznih tehnologija, između ostalog i steganografije.

Popis literature

[1] Frank Y. Shih: Digital Watermarking and Steganography: Fundamentals and Techniques (Second Edition), CRC Press, (2020)

[2] Greg Kipper: Investigator's Guide to Steganography, Auerbach Publications, (2004)

[3] Mahmoud Hassaballah: Digital Media Steganography Principles, Algorithms and Advances, Academic Press, (2020)

[4] Jessica Fridrich: Steganography in Digital Media Principles, Algorithms, and Applications, Cambridge University Press, (2010)

[5] R.Bala Krishnan, Prasanth Kumar Thandra, M. Sai Baba: An Overview of Text Steganography, IEEE Xplore, pristupljeno 8.6.2022., (https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8085643)

[6] K. Benett: Linguistic steganography - survey, analysis and robustness concerns for hiding information in text, Purdue University, (2004)

[7] L.Y. Por i B. Delina: Information hiding - a new approach in text steganography, WSEAS, (2008)

[8] Sunil Tanna: Codes, Ciphers, Steganography & Secret Messages, Answers 2000 Limited, (2020)

[9] T. Morkel, J.H.P. Eloff, M.S. Olivier: An overview of image steganography., Proceedings of the ISSA 2005 New Knowledge Today Conference, (Eds. J. H. P. Eloff, L. Labuschagne, M. M. Eloff, H. S. Venter), pp. 1-11, ISSA, Pretoria, South Africa, 2005

[10] Nedeljko Cvejic, Tapio Seppben: Increasing the capacity of LSB-based audio steganography, University of Oulu, (2002)

[11] Neetha Francis: Information Security using Cryptography and Steganography, Pazhassi Raja College, pristupljeno 13.6.2022., (https://www.ijert.org/research/information-security-using-cryptography-and-steganography-IJERTCONV3IS28029.pdf)

[12] Dipti Kapoor Sarmah, Anand J. Kulkarni, Ajith Abraham: Optimization Models in Steganography Using Metaheuristics, Springer, (2020)

[13] N. Provos, P. Honeyman: Detecting steganographic content on the internet, Ann Arbor, (2001)

[14] Shamim Ahmed Laskar, Kattamanchi Hemachandran: A Review on Image Steganalysis techniques for attacking Steganography, Assam University, pristupljeno

14.6.2022., (https://www.ijert.org/research/a-review-on-image-steganalysis-techniques-for-attacking-steganography-IJERTV3IS11136.pdf)

[15] Eric Cole: Steganography and the Art of Covert Communication, Wiley Publishing, (2003)

[16] S.C. Katzenbeisser: Principles of Steganography, Information Hiding Techniques for Steganography and Digital Watermarking, S. Katzenbeisser and F. Petitcolas, Ed. London: Artech House, pp. 43-78, 2000.

[17] P. Sallee: Model-based steganography, Proc. the 2nd International Workshop on Digital Watermarking, LNCS, pp. 254-260, 2004.

Popis slika

Popis tablica

Popis kratica

LSB – Least Significant Bit (najmanje značajan bit)

DNK – Deoksiribonukleinska kiselina

JPEG – Joint Photographic Experts Group

CFG – Context-Free Grammar (Gramatika bez konteksta)

GNF – Greibach Normal Form (Greibachova normalna forma)

RGB – Red Green Blue (crvena zelena plava)

DCT – Discrete Cosine Transform (Diskretna kosinusna transformacija)

PCM – Pulse Code Modulation (Pulsna kodna modulacija)

BCH – Bose–Chaudhuri–Hocquenghem

DWT – Discrete Wavelet Transform (Diskretna valovna transformacija)

GIF – Graphic Interchange Format (Format grafičke razmjene)

ASCII – American Standard Code for Information Interchange (Američki standardni kod za razmjenu informacija)

RS – Regular-Singular

NFT – Non-fungible tokens (Nezamjenjivi tokeni)

EPR – Electronic Patient Record (Elektronički karton bolesnika)

BMP – Bitmap

WAV – Waveform Audio File (Audio datoteka valnog oblika)

DES – Data Encryption Standard (Standard šifriranja podataka)

PNG – Portable Network Graphics (Prijenosna mrežna grafika)