Steganografija - praktični primjeri

Jelić, Ana

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA

Sveučilišni studij

STEGANOGRAFIJA – PRAKTIČNI PRIMJERI

Diplomski rad

Ana Jelić

Osijek, 2023.

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA
I INFORMACIJSKIH TEHNOLOGIJA **OSIJEK**

Obrazac D1: Obrazac za imenovanje Povjerenstva za diplomski ispit

Osijek, 06.07.2023.

Odboru za završne i diplomske ispite

Imenovanje Povjerenstva za diplomski ispit

Ime i prezime Pristupnika:	Ana Jelić
Studij, smjer:	Diplomski sveučilišni studij Elektrotehnika, smjer Komunikacije i informatika'
Mat. br. Pristupnika, godina upisa:	D-1218, 06.10.2019.
OIB studenta:	76100190004
Mentor:	izv. prof. dr. sc. Krešimir Grgić
Sumentor:	,
Sumentor iz tvrtke:	
Predsjednik Povjerenstva:	doc. dr. sc. Višnja Križanović
Član Povjerenstva 1:	izv. prof. dr. sc. Krešimir Grgić
Član Povjerenstva 2:	mr. sc. Anđelko Lišnjić
Naslov diplomskog rada:	Steganografija - praktični primjeri
Znanstvena grana diplomskog rada:	**Telekomunikacije i informatika (zn. polje elektrotehnika)**
Zadatak diplomskog rada:	Steganografija je tehnika prikrivanja tajnih poruka na način da nitko osim predajne i prijemne strane nije niti svjestan da postoji komunikacija (obično se za prikrivanje koristi neka druga datoteka). Potrebno je detaljno opisati i analizirati različite pristupe i metode koji se koriste u području steganografije, te ih ilustrirati na praktičnim primjerima. (Studentica: Ana Babić)
Prijedlog ocjene pismenog dijela ispita (diplomskog rada):	Izvrstan (5)
Kratko obrazloženje ocjene prema Kriterijima za ocjenjivanje završnih i diplomskih radova:	Primjena znanja stečenih na fakultetu: 3 bod/boda Postignuti rezultati u odnosu na složenost zadatka: 3 bod/boda Jasnoća pismenog izražavanja: 3 bod/boda Razina samostalnosti: 3 razina
Datum prijedloga ocjene od strane mentora:	06.07.2023.

Potvrda mentora o predaji konačne verzije rada:	*Mentor elektronički potpisao predaju konačne verzije.*
	Datum: 13.07.2023.

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA
I INFORMACIJSKIH TEHNOLOGIJA **OSIJEK**

IZJAVA O ORIGINALNOSTI RADA

Osijek, 14.07.2023.

Ime i prezime studenta:	Ana Jelić
Studij:	Diplomski sveučilišni studij Elektrotehnika, smjer Komunikacije i informatika'
Mat. br. studenta, godina upisa:	D-1218, 06.10.2019.
Turnitin podudaranje [%]:	5

Ovom izjavom izjavljujem da je rad pod nazivom **: Steganografija - praktični primjeri**

izrađen pod vodstvom mentora izv. prof. dr. sc. Krešimir Grgić

i sumentora ,

moj vlastiti rad i prema mom najboljem znanju ne sadrži prethodno objavljene ili neobjavljene pisane materijale drugih osoba, osim onih koji su izričito priznati navođenjem literature i drugih izvora informacija.
Izjavljujem da je intelektualni sadržaj navedenog rada proizvod mog vlastitog rada, osim u onom dijelu za koji mi je bila potrebna pomoć mentora, sumentora i drugih osoba, a što je izričito navedeno u radu.

Potpis studenta:

SADRŽAJ

1. UVOD

Steganografija je tehnika koja omogućava skrivanje postojanja komunikacije, tj. prikrivanja tajnih poruka. Steganografske su se tehnike koristile još u dalekoj povijesti od strane Grka i Rimljana, a prvi zapisi o korištenju ovih tehnika sežu u daleko 5. stoljeće. Izumom računala i razvojem tehnologije, razvile su se i moderne steganografske tehnike za digitalnu primjenu. Cilj steganografskih tehnika je da treća, neovlaštena strana nije svjesna postojanja komunikacije. Ukoliko je taj cilj ostvaren, steganografija je uspješna. Za prikrivanje tajne komunikacije, potrebno je odabrati objekt nositelj u koji će se poruka ugraditi, a on može biti tekstualna, slikovna, zvukovna, video datoteka i dr. Važno je odabrati odgovarajuću tehniku i odgovarajući objekt nositelj kako bi rezultat steganografije bio zadovoljavajući. Za dodatnu sigurnost koriste se stego ključevi kojima se kriptira tajna poruka kako njen sadržaj ne bi bio otkriven, ukoliko dođe do otkrivanja postojanja tajne komunikacije. Za otkrivanje postojanja tajnih poruka zadužena je steganaliza. Steganaliza služi i kao test sigurnosti steganografskih tehnika jer, osim otkrivanja tajne poruke, procjenjuje i njenu veličinu, dešifrira ju, izmjenjuje ili uništava.

Danas su dostupni razni besplatni alati koji se temelje na nekoj od steganografskih tehnika i omogućuju njihovu primjenu. Steganografske se tehnike mogu koristiti u razne svrhe, legalne i ilegalne. Koriste se za osiguravanje povjerljivosti podataka, očuvanja podataka od neovlaštenih strana, ali i za kibernetički kriminal, pornografiju, terorizam i dr. Nažalost, sve je veća primjena steganografskih tehnika u ilegalne svrhe.

U ovom diplomskom radu opisana su osnovna načela steganografije, povijest razvoja i podjela steganografije. Nakon toga navedene su različite steganografske tehnike i opisan je njihov način rada. Zatim su opisani oblici napada steganalize i tehnike koje se koriste u toj znanosti. Kao glavni dio, navedene je primjena korištenja steganografskih tehnika i prikazani su različiti praktični primjeri steganografije.

1.1 Zadatak diplomskog rada

Steganografija je tehnika prikrivanja tajnih poruka na način da nitko osim predajne i prijemne strane nije niti svjestan da postoji komunikacija (obično se za prikrivanje koristi neka druga datoteka). Potrebno je detaljno opisati i analizirati različite pristupe i metode koji se koriste u području steganografije, te ih ilustrirati na praktičnim primjerima.

2. STEGANOGRAFIJA

Steganografija (engl. *steganography*) je znanstvena disciplina koja proučava načine prikrivanja tajnih poruka u smislu da nitko osim predajne i prijemne strane nije svjestan da se komunikacija zapravo odvija. Sama riječ dolazi od grčkih riječi *steganos* i *graphein* što u prijevodu znači „*skriveno pisanje*“, [1]. Primjenom steganografije moguće je umetnuti tajnu poruku unutar informacije koja ni na koji način nije sumnjiva u smislu da bi netko pomislio da u sebi skriva tajnu poruku.

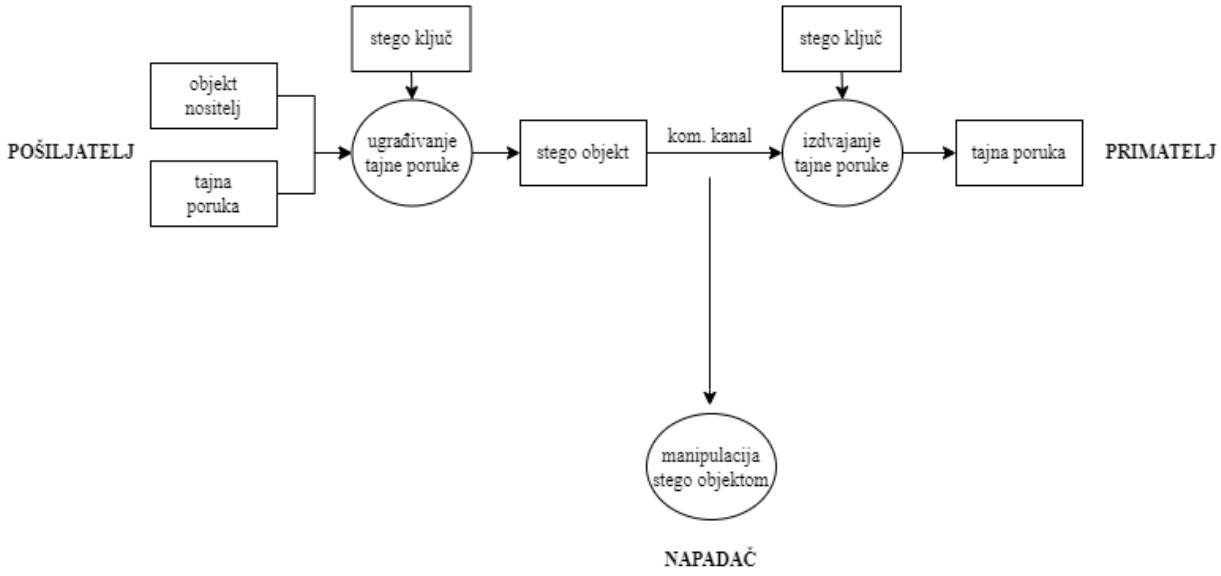
Steganografija se često povezuje s kriptografijom, što je razumljivo s obzirom na to da je kod obje discipline cilj sakriti poruku, tj. informaciju od treće strane. No važno je istaknuti ključne različitosti ovih dviju disciplina. Kriptografija je znanstvena disciplina koja se bavi očuvanjem tajnosti informacija na način da se informacija transformira u oblik koji je nerazumljiv bilo kome tko ne posjeduje ključ za dekripciju. Dakle, kriptografija prikriva sadržaj poruke, dok steganografija prikriva postojanje same poruke. Obje discipline imaju svojih prednosti i nedostataka kada se samostalno koriste. Korištenjem obje discipline zajedno moguće je povećati sigurnost tajnih informacija i tajne komunikacije. Čak štoviše, neke steganografske metode kombiniraju elemente steganografije s elementima kriptografije što potencijalnim napadačima dodatno otežava otkrivanje informacije, [2].

2.1. Steganografski sustav i načela

Za razumijevanje steganografskog sustava potrebno je definirati osnovne pojmove od kojih se on sastoji [1, 7]:

- objekt nositelj (engl. *cover-object*) – objekt u koji se ugrađuje tajna poruka i koji služi za prikrivanje iste; odabire se na način da ne smije privlačiti pozornost
- stego objekt (engl. *stego-object*) – objekt koji nastane umetanjem tajne poruke u objekt nositelj
- stego ključ (engl. *stego-key*) – steganografski ključ omogućava dodatnu zaštitu i kontrolu skrivanja tajne poruke; najčešće se koristi kako bi se tajna poruka kriptirala prije nego što se ugradi u objekt nositelj

S obzirom na definirane pojmove, na slici 2.1. prikazan je model steganografskog sustava.



Slika 2.1. Model steganografskog sustava

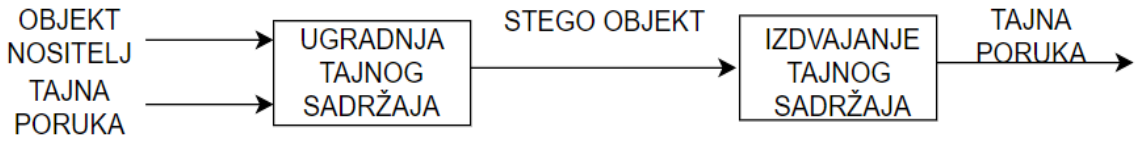
Kada pošiljatelj želi poslati tajnu poruku, uz korištenje stego ključa tajna se poruka ugrađuje u odabrani objekt nositelj (npr. zvučni zapis, video zapis i dr.) i time nastaje stego objekt. Koristeći određeni komunikacijski kanal, stego objekt se prenosi do primatelja. Na drugoj strani, primatelj uz korištenje stego ključa izdvaja tajnu poruku iz stego objekta i iščitava njezin sadržaj. Također, postoji i treća strana, a to je potencijalni napadač koji može manipulirati stego objektom. Napadač pokušava otkriti sadrži li poslani stego objekt neke skrivene i tajne informacije i pritom može izvršiti pasivan ili aktivan napad nad stego objektom. Ukoliko napadač samo promatra i prisluškuje komunikaciju ne poduzimajući pritom nikakve druge akcije, radi se o pasivnom napadu. S druge strane, napadač može promijeniti dio stego objekta i time upropastiti pokušaj prijenosa tajne poruke između primatelja i pošiljatelja – takav napad naziva se aktivan napad. Napad može biti i zlonamjeran. U tom bi slučaju napadač otkrio sadržaj tajne poruke, izdvojio ga i izmijenio.

S obzirom na sigurnost skrivene poruke, steganografiju možemo podijeliti na tri osnovna tipa, a to su: [5]

- Čista steganografija (engl. *Pure Steganography*)
- Steganografija tajnog ključa (engl. *Secret key Steganography*)
- Steganografija javnog ključa (engl. *Public key Steganography*)

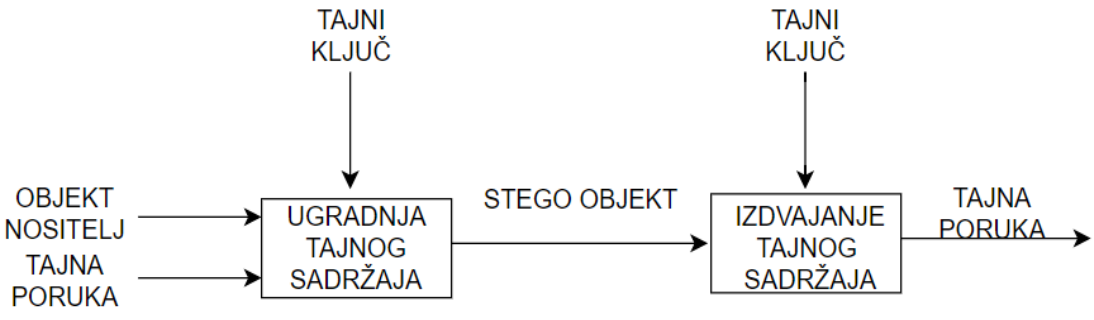
Čista steganografija temelji se na principu da sigurnost cijelog sustava ovisi isključivo o njegovoj tajnosti. U ovom slučaju steganografski sustav ne zahtijeva korištenje stego ključeva

za ugradnju tajnih informacija u objekt nositelj. Pretpostavka je da za razmjenu poruka znaju samo pošiljatelj i primatelj te je upravo u tome i najveća mana ovog sustava. Ukoliko bi neki korisnik posumnjao na sadržaj poruke, tajne informacije bile bi lako otkrivene, dakle sustav ne pruža sigurnost. Na slici 2.2. prikazan je proces rada sustava temeljnog na čistoj steganografiji.



Slika 2.2. Proces čiste steganografije [5]

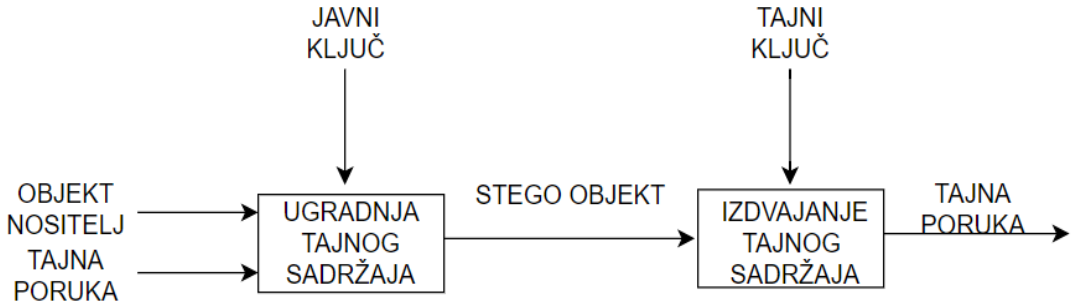
Za razliku od čiste steganografije, steganografija tajnog ključa zahtijeva razmjenu tajnog ključa prije same komunikacije. Tajni steganografski ključ može predstavljati neku lozinku koju određena strana mora unijeti ukoliko želi otkriti ili prikriti tajni sadržaj. Pošiljatelj postavlja tajni ključ prilikom ugradnje tajne poruke u objekt nositelj. Ukoliko je tajni ključ poznat primatelju, on može izdvojiti tajnu poruku. U tome je i prednost ovog sustava, samo ona strana kojoj je tajni ključ poznat može izdvojiti tajni sadržaj iz stego objekta. S druge strane, s obzirom na to da je nužno razmijeniti tajni ključ, sustav time može privući pažnju te može doći do presretanja tajnog ključa od strane potencijalnih napadača. Na slici 2.3 prikazan je je proces rada sustava temeljnog na steganografiji tajnog ključa.



Slika 2.3. Proces steganografije tajnog ključa [5]

Steganografija javnog ključa zahtijeva korištenje javnog i tajnog ključa. Prilikom šifriranja poruke koristi se javni ključ, koji se pohranjuje u javnim bazama podataka, dok se prilikom rekonstruiranja poruke koristi tajni ključ. Ovakav se sustav može koristiti kada se šalje neki

sadržaj koji bi bio dostupan više različitih strana, a nije od velikog značaja za potencijalne napadače. Na slici 2.4. prikazan je proces rada sustava temeljnog na steganografiji javnog ključa.



Slika 2.4. Proces steganografije javnog ključa [5]

Sam proces probijanja sigurnosti steganografskog sustava sastoji se od otkrivanja, izdvajanja i modificiranja ugrađenih tajnih informacija. Međutim, može se reći da je sigurnost sustava ugrožena u trenutku kada napadač može dokazati postojanje tajne poruke. Steganografski je sustav potrebno graditi s pretpostavkom da potencijalni napadač ima neograničenu moć i sposobnost za izvođenje napada i ugrožavanje tajnih informacija.

2.2 Povijest steganografije

Različiti primjeri steganografije prisutni su u čovječanstvu već tisućljećima iako nisu odmah definirani pod tim pojmom. Povijest razvoja steganografije možemo podijeliti na onu do izuma osobnog računala 1985. godine i na suvremenu, modernu steganografiju od izuma osobnog računala. Najstariji zapisani primjeri pripadaju dalekom 5. stoljeću, a zabilježio ih je grčki povjesničar Herodot. Prema njemu, postoje dvije priče vezane uz ovu temu. Prva priča odnosi se na prijenos poruka preko voštanih pločica. U to vrijeme komadi drveta prelili bi se voskom i tako nastale pločice koristile bi se za pisanje. Upravo su te pločice Grcima dale ključnu informaciju da ih Perzija planira napasti. Tajna poruka prenesena je tako što je vosak oguljen s pločice, tekst je urezan u drvo i zatim se vosak ponovo prelio preko drveta. Na taj način voštana pločica nije privlačila nikakvu pozornost jer je djelovala kao obična prazna pločica za pisanje, a poruka je uspješno prenesena, [3]. Druga priča također je vezana uz Grčku i Perziju, a poruka se prenosila preko tijela robova. Obrijali bi robovu glavu i tetovirali poruku na nju. Kada bi robova kosa narasla, poruka bi bila skrivena, a ponovnim brijanjem glave, poruka je bila prenesena, [1].

Osim voštanih pločica s kojima su Grci započeli povijest steganografije, poznato je da su se u povijesti Kinezi koristili i voštanim kuglicama. Na komadiće svile napisali bi poruku, svilu bi savili u kuglicu i uronili u tekući vosak. Kada bi se kuglice ohladile, nosile bi se na raznim vidljivim dijelovima odjeće. Smatrali su da što su kuglice vidljivije, bit će manje sumnjive da se u njima nešto skriva, [4].

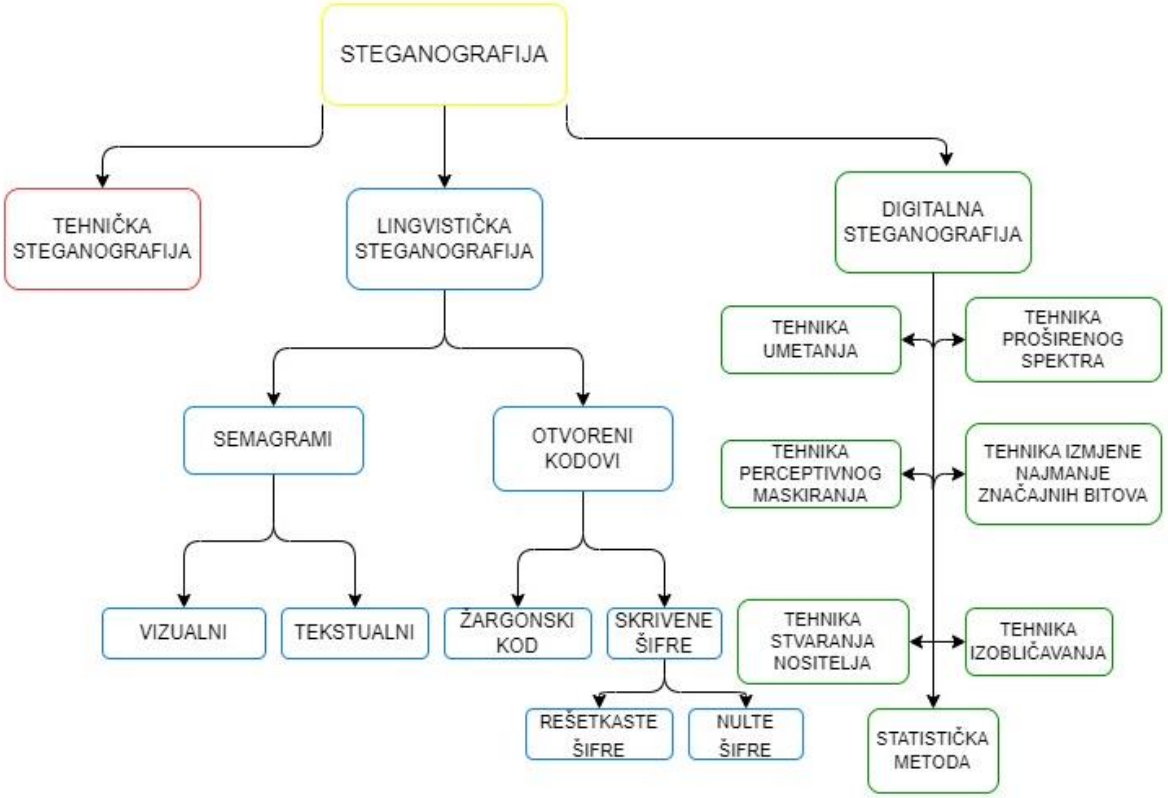
Sljedeći primjer odnosi se na korištenje nevidljive tinte za prijenos tajnih poruka. Ova metoda koristila se još kod starih Rimljana i Grka. Oni su se za stvaranje tinte koristili organskim tekućinama poput mlijeka, urina, octa, voćnih sokova i sl. Sve te supstance imale su zajedničko to da prilikom laganog zagrijavanja tamne i postaju vidljive, na taj način bi se skrivene poruke mogle pročitati. Postoje i naprednije vrste nevidljive tinte koje se prave od određenih sintetskih kemikalija. Takve tinte bezbojne su kada se osuše, a u reakciji s drugim određenim kemikalijama ponovno postaju vidljive. Sintetske tinte korištene su u raznim oblicima tijekom Drugog svjetskog rata za prenošenje ratnih informacija, a u nekim naprednijim oblicima koriste se i danas, [3].

Tijekom Prvog i Drugog svjetskog rata razvile su se razne steganografske metode. Jedna od tih metoda je korištenje mikrotočke i mikrofotografije za prijenos tajnih informacija. Skrivene poruke nastajale su složenim metodama i bile bi veličine i oblika točke. Tajna poruka bi se fotografirala, smanjila na određenu veličinu, izradila i zatim bi se posebnom iglom i emulzijom utisnula u tekst na mjesto interpunkcijskog znaka točke, na točkama koje se nalaze na slovima i, j i sl. Na taj su način poruke bile neuočljive i mogle su se iščitati samo korištenjem optičkih povećala, [3]. Tijekom ovog razdoblja razvila se i metoda „nulte šifre“ gdje bi se unutar naizgled obične poruke sakrila tajna informacija, a otkrila bi se npr. čitanjem svakog trećeg slova u tekstu. Poznat je primjer japanske špijunke zvane *Doll Woman,* žene koja se bavila proizvodnjom lutaka. Ona je tijekom Drugog svjetskog rata slala tajne poruke na način da bi poslala pisma s narudžbama za lutke, a koja su u sebi zapravo sadržavala informacije o rutama ratnih brodova, [1].

S pojavom digitalizacije i Interneta, slanje, primanje i pohranjivanje raznih podataka i informacija odvija se putem računalnih i informacijskih sustava te je tako došlo i do potrebe za razvojem puno naprednijih steganografskih metoda i pristupa koji bi bili u skladu s današnjim dobom.

2.3 Podjela steganografije

S obzirom na upravo navedene primjere, steganografske tehnike možemo podijeliti u tri osnovne skupine, a to su: tehnička, lingvistička i digitalna steganografija. Tehnička steganografija (engl. *technical steganography*) podrazumijeva upotrebu različitih uređaja, alata i općenito znanstvenih metoda za skrivanje poruke. Lingvistička steganografija (engl. *linguistic steganography*) prenosi informacije koje su jezičnog sadržaja na način da ih prikrije unutar nekog naizgled beznačajnog skupa informacija. Digitalna je steganografija moderni oblik steganografije gdje se informacije skrivaju unutar računalnih datoteka, [4].



Slika 2.5. Podjela steganografije [4]

Na slici 2.5. prikazana je podjela steganografije na osnovne skupine i njihove podskupine. Može se vidjeti da tehnička steganografija nema neke točno izražene podskupine, no u nju pripadaju razni prethodno spomenuti primjeri iz povijesti kao što su voštane pločice i kuglice, nevidljiva tinta, urezivanje na tijelo, skrivanje informacija u skrovitim mjestima (npr. pete obuće, dvostruka dna drvenih bačvi) i sl.

Lingvistička steganografija može se podijeliti na semagrame i otvorene kodove. Semagrami (engl. *semagrams*) koriste tehniku premještanja simbola, objekata ili znakova kako bi prenijeli

skrivenu informaciju – svaka promjena predstavlja određenu informaciju. Dodatno, semagrami imaju i svoju podjelu na podskupine, a to su: [4]

- vizualni semagrami - koriste se svakodnevni fizički objekti za skrivanje poruke, npr. specifičan razmještaj predmeta na radnom stolu (računalo, pribor za pisanje, mobilni uređaj, rokovnik i dr.). Svaka specifična promjena u razmještaju predmeta prenosila bi određenu informaciju.

- tekstualni semagrami – informacije se skrivaju modificiranjem teksta, npr. promjeni se veličina fonta ili sami font teksta, koriste se dodatni suvišni razmaci i sl.

Otvoreni kodovi (engl. *open codes*) mogu se podijeliti na žargonske kodove i skrivene šifre. Kod žargonskog koda (engl. *jargon code*) je princip taj da sama poruka nije skrivena, vidljiva je svakom čitatelju, ali pisana je upotrebom određenog žargona tako da samo određena skupina ljudi tu poruku uistinu može razumjeti. Znakovni kod, koji je podskup žargonskog koda, koristi unaprijed definirane fraze koje označavaju točno određene pojmove. Skrivene šifre (engl. *covered ciphers*) temelje se na tome da je tajnu poruku moguće otkriti samo ako je poznato koja je metoda korištena za umetanje te poruke u medij koji ju prenosi, tj. mogu ju iščitati samo oni koji ju znaju dešifrirati. Skrivene šifre dijele se na sljedeće dvije podskupine: [1]

- rešetkaste šifre (engl. *grille ciphers*) – temelj ove metode su predlošci u čijim se otvorima skrivaju poruke

- nulta šifra (engl. *null cipher*) – princip rada ove metode je jednostavan – definira se skup pravila, npr. čitanje svake treće riječi u rečenici. Primjenom tog pravila, istaknute pročitane riječi predstavljale bi tekst skrivene poruke. Ovakav princip omogućava skrivanje poruka u uobičajenim, svakodnevnim tekstovima (npr. novine).

Pojavom računala i razvojem tehničkih znanosti, razvila se potreba za stvaranjem novih, suvremenijih steganografskih metoda i došlo je do razvoja digitalne steganografije. Informacije se skrivaju preko digitalnih medija, tj. različitih računalnih datoteka. Prilikom korištenja digitalnih steganografskih metoda, kao transportni sloj mogu se koristiti audio i video zapisi, tekstualne i slikovne datoteke, programi, protokoli i sl. Tekstualni dokumenti najmanje su korisni za ove tehnike zbog male količine podataka koja automatski znači da je poruku puno teže sakriti. S druge strane, multimedijske datoteke najprikladnije su za steganografske metode upravo zbog svoje veličine. Veličina multimedijskih datoteka omogućava iskorištavanje suvišnih podataka za skrivanje informacija. Postoje različite metode digitalne steganografije,

ovisno i o mediju u kojem će informacije biti prikrivene. Sa sve većim brojem korisnika računalnih sustava i informacija koje se razmjenjuju preko elektroničkih sustava, dolazi do zloporabe steganografskih metoda, ali istovremeno i do primjene steganografije s ciljem zaštite autorskih prava i privatnosti. U sljedećim poglavljima ovog diplomskog rada bit će opisane i analizirane razne tehnike digitalne steganografije koje se koriste danas te će biti ilustrirane na odgovarajućim primjerima.

3. STEGANOGRAFSKE TEHNIKE

Postoji nekoliko različitih pristupa kada je riječ o klasifikaciji tehnika steganografskih sustava. Jedan je način podjela prema tipu odabranog objekta nositelja u koji se ugrađuje tajna informacija. U tablici 3.1. prikazana je osnovna podjela prema tipu odabranog objekta nositelja, [7].

Tablica 3.1. Podjela steganografskih tehnika prema tipu objekta nositelja

Steganografska tehnika	**Objekt nositelj**	**Karakteristike**	**Ugradnja tajnih informacija**
tehnike binarnih datoteka	binarna datoteka	jednostavna implementacija	unošenje promjena u binarni kod
tehnike teksta	dokument	nedostatak suvišnih podataka za skrivanje tajnih informacija	fizička promjena formata teksta, skrivanje informacija unutar niza znakova
tehnike slikovnih datoteka	slikovna datoteka	najrašireniji medij koji služi kao objekt nositelj; različiti formati koriste različite algoritme	transformacije, filtriranje, metode najmanje značajnog bita itd.
tehnike zvukovnih datoteka	zvukovna datoteka (npr. wav, mp3)	veliki raspoloživi prostor unutar kojeg se mogu sakriti tajne informacije; tajna informacija može biti tekstualna datoteka, slikovni ili zvučni zapis	mijenjanje binarnog slijeda originalne zvukovne datoteke
tehnike video datoteka	video datoteka	veliki raspoloživi prostor unutar kojeg se mogu sakriti tajne informacije	kombinacije zvukovnih i slikovnih tehnika

Drugi se način odnosi na podjelu prema modifikacijama primijenjenim na objektu nositelju prilikom ugradnje tajnih informacija. U ovom će se diplomskom radu detaljno objasniti steganografske tehnike prema drugom načinu klasifikacije. S obzirom na to, steganografske se tehnike mogu podijeliti u šest osnovnih skupina, a to su:

- tehnike supstitucije (engl. *substitution systems*)

- tehnike transformacije domene (engl. *tranform domain techniques*)
- tehnike proširenog spektra (engl. *spread spectrum techniques*)
- statističke tehnike (engl. *statistical techniques*)
- tehnike izobličenja (engl. *distortion techniques*)
- tehnike stvaranja nositelja objekta (engl. *cover generation methods*)

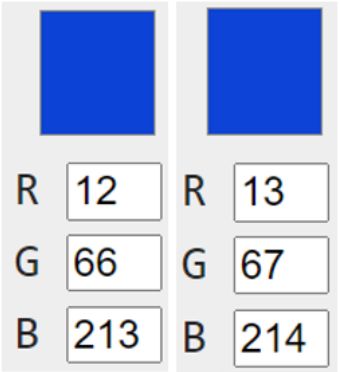
3.1. Tehnike supstitucije

Tehnike supstitucije rade na principu da se suvišni dijelovi objekta nositelja koriste za ugradnju tajnih informacija. Primatelj može izvući tajne informacije ukoliko mu je poznato na kojim dijelovima su informacije skrivene. S obzirom na to da se prilikom ugradnje koriste neke manje modifikacije objekta nositelja, pretpostavlja se da ih pasivni napadač ne bi primijetio. Postoji više različitih tehnika koje su zasnovane na supstituciji, a neke od najpoznatijih su supstitucija bita najmanje važnosti (engl. *least significant bit supstitution, LSB supstitution*), sortiranje paleta, degradacija slike i kvantizacija. Prilikom korištenja tehnika supstitucije, kao objekt nositelj najčešće se koriste slikovne datoteke stoga je potrebno poznavati strukturu RGB (engl. *Red-Green-Blue*) aditivnog modela boja. U RGB modelu boja, svaka je boja prikazana pomoću crvene, zelene i plave komponente. Za svaki od ovih primara koristi se 8 bita, tj. jedan oktet, a vrijednost intenziteta može varirati od 0 do 255. S obzirom na to da ovaj model koristi 3 primara, radi se od 24-bitnoj shemi (svaki piksel predstavljen je s 24 bita) sa ukupno 256^3=16 777 216 mogućih kombinacija boja. Osim 24-bitne sheme, često se koristi i 8-bitna shema zbog uštede na veličini slike, tj. manje zauzeća memorije. Kod 8 bitne sheme svaki je piksel predstavljen s 8 bita i 256 kombinacija boja. Stvaraju se palete s 256 boja koje su specifične za određenu sliku i svakoj od tih boja dodijeljen je indeks zapisa boje u specificiranoj paleti.

3.1.1. Supstitucija bita najmanje važnosti

Supstitucija bita najmanje važnosti najraširenija je tehnika i jedna od temeljnih koja se koristi za prikrivanje tajnih informacija. Tehnika funkcionira na principu zamjene bitova najmanje važnosti s bitovima tajne informacije i lako se implementira. Moguće je sakriti veliku količinu informacija s iznimno malim utjecajem na datoteku koja predstavlja objekta nositelja. U obzir se uzima činjenica da je ljudski vizualni sustav nedovoljno osjetljiv na takve male promjene te ih neće uočiti. Na slici 3.1. prikazane su dvije različite boje čije vrijednosti RGB komponenta

odstupaju za po jednu jedinicu vrijednosti za svaku komponentu. Može se primijetiti da su te promjene ljudskom oku teško primjetne i da bi ljudsko oko teško raspoznalo da se radi o različitim bojama, pogotovo kada su te boje tek dio skupa svih boja koje čine određenu sliku. Kada bi se za objekt nositelj koristila 24- bitna slikovna datoteka, u svaki piksel moglo bi se ugraditi tri bita tajne informacije jer bi se iskoristio bit najmanje važnosti svake od tri komponente RGB modela boja.



Slika 3.1. Prikaz RGB vrijednosti za dvije različite boje [10]

Bit najmanje važnosti predstavlja onaj bit koji ima najmanju aritmetičku vrijednost u oktetu, a bit najveće važnosti je onaj koji ima najveću aritmetičku vrijednost. Kako bi bilo jasnije, na slici 3.2. prikazan je binarni zapis decimalnog broja 101 i označeni su bitovi koji imaju najmanju, odnosno, najveću važnost.

$$101_{(10)} = 01100101_{(2)}$$

Slika 3.2. Binarni zapis broja s označenim bitovima

Ukoliko bi se napravila promjena na bitu najmanje važnosti, to bi imalo najmanji učinak na cijeli oktet, a isto tako bi se promjena bita najveće važnosti odrazila s najvećom promjenom vrijednosti okteta. Ideja same tehnike je da se tajna informacija rastavi na bitove i odabere se datoteka koja će predstavljati objekt nositelj. Nakon toga se odabere podskup bitova najmanje važnosti određenih okteta objekta nositelja u koje će se ugraditi bitovi tajne informacije. Zatim se nekim redoslijedom na mjesta bitova najmanje važnosti odabranih okteta ugrađuju bitovi

tajne informacije, sve dok se cijela tajna informacija ne ugradi. Broj bitova odabranog podskupa odgovara broju bitova tajne informacije.

Implementacija tehnike je jednostavna, no postoje i neki nedostaci. S obzirom na to da ova tehnika koristi bitove najmanje važnosti, osjetljiva je i na najmanje transformacije i tehnike obrade provedene na slici te bi korištenjem bilo koje kompresije s gubitcima došlo do gubitka bitova tajne informacije. Također, važan je i odabir redoslijeda kojim će se bitovi tajne informacije ugrađivati u objekt nositelj. Ukoliko se podskup bitova za ugradnju odabere na jednostavan način (npr. bitovi okteta na početku datoteke), može doći do sigurnosnih problema jer će taj dio datoteke imati drugačija statistička svojstva od ostatka datoteke i time će biti više primjetan. Kako bi se prevenirao ovaj sigurnosni problem, često se koriste generatori pseudoslučajnih brojeva za određivanje podskupa bitova za ugradnju. Time je udaljenosti između odabranih bitova određena na potpuno slučajan način i potencijalnom napadaču je teže detektirati bitove tajne informacije. Da bi primatelj mogao detektirati odabrani podskup, mora poznavati stego ključ koji predstavlja početnu vrijednost (engl. *seed*), tj. ulaz u sam generator, pomoću koje su generirani bitovi podskupa, [8].

Iako 24-bitne slike pružaju veću količinu suvišnih bitova za skrivanje tajnih informacija, moguće je koristi i 8-bitne slike kao objekt nositelj. Zbog manje suvišnih bitova i različitih svojstava, 8-bitne slika zahtijevaju pažljiviji pristup pri procesu steganografije, tj. potrebno je pažljivije odabrati sliku koja će biti objekt nositelj, [9].

3.1.2. Degradacija slike

Degradacija slike (engl. *image downgrading*) tehnika je koja omogućava skrivanje slike u slici, a temelji se na prethodno opisanoj tehnici supstitucije bitova najmanje važnosti. Ova tehnika poseban je slučaj supstitucijskih tehnika jer slikovna datoteka je ujedno i objekt nositelj i tajna poruka. Da bi ova tehnika funkcionirala, potrebno je odabrati sliku objekta nositelja i sliku tajne poruke na način da budu jednakih dimenzija. Kada se odaberu odgovarajuće slike, četiri bita najmanje važnosti RGB modela boja svakog piksela objekta nositelja zamjenjuje se s četiri bita najveće važnosti RGB modela boja odgovarajućeg piksela tajne poruke. Kako bi primatelj mogao izdvojiti tajnu sliku iz stego objekta, mora izdvojiti četiri bita najmanje važnosti svake vrijednosti boje u svakom pikselu i tako će dobiti pristup četiri najznačajnija bita tajne slike. Nakon izvlačenja tih bitova, potrebno ih je nadopuniti s još četiri proizvoljna bita, npr. nulama. Time je na prijemnoj strani izvučena aproksimacija tajne slike. U većini slučajeva, degradacija

slike objekta nositelja nije znatno uočljiva, a tajna se slika uspije prenijeti sa zadovoljavajućom kvalitetom, [8].

3.1.3. Sortiranje paleta

Neki formati slika koriste palete boja za prikaz boja korištenih na slici, a najčešće korišteni formati su GIF (engl. *Graphic Interchange Format*) i BMP. Na takvim formatima može se primijeniti tehnika sortiranja paleta. Formati slika koji koriste tu tehniku sastoje se od same palete boja i o podatcima o slici. Paleta boja specificira podskup od *N* boja kao listu uređenih parova (i, c_i), pri čemu je c_i vektor boje koji se dodjeljuje pripadnom indeksu *i*. Podatci o slici sadrže informacije o tome koji je indeks palete pridružen kojem pikselu. Ukoliko je na slici korišten manji podskup boja, ukupna se veličina datoteke značajno smanjuje, [8].

Dva su moguća pristupa za skrivanje tajnih informacija u slike koje koriste palete boje – može se manipulirati ili paletom boja ili podatcima o slici. Kada je riječ o manipulaciji palete boja, za prijenos tajnih informacija koriste se bitovi najmanje važnosti vektora boja. Redoslijed sortiranja palete boja može biti bilo koji što omogućava da se informacije ugrade na način na koji su boje pohranjene u samoj paleti. S obzirom na to da postoji N! različitih načina koji određuju redoslijed sortiranja palete, stvara se kapacitet koji omogućava ugradnju tajnih informacija manjih veličina. Iako primjena zvuči jednostavno, ovaj princip u praksi nije pouzdan. Potencijalni napadač može jednostavno odabrati sortiranje nekim drugim redoslijedom, što ne bi uzrokovalo nikakve vidljive promjene na slici, ali bi došlo do uništavanja tajnih informacija, [8].

Drugi pristup odnosi se na manipulaciju podatcima o slici kako bi se ugradile tajne informacije. Susjedne vrijednosti boja palete ne moraju biti perceptivno slične i zbog toga se na njima ne može primijeniti tehnika zamjene bitova najmanje važnosti. Kako bi se to omogućilo, prije procesa ugradnje paleta se može sortirati na način da perceptivno slične vrijednosti budu i susjedne vrijednosti. Također, poznato je da je ljudski vizualni sustav osjetljiv na promjene u svjetlini boje pa bi drugi način sortiranja vrijednosti boja palete bio prema njihovoj luminantnoj komponenti. U oba slučaja, nakon što se paleta sortira, moguće je primijeniti tehniku bita najmanje važnosti, [8].

3.2. Tehnike transformacije domene

Tehnike transformacije domene za skrivanje tajnih informacija koriste metode manipuliranja matematičkih funkcija i algoritama, tj. sve modifikacije rade se u transformiranoj domeni. Tajne se informacije skrivaju na značajnim mjestima objekta nositelja (slikovne datoteke) i

tako postaju otpornije na eventualne izmjene poput kompresije, obrade slike i sl. Tehnike transformacije koje se najčešće koriste su diskretna kosinusna transformacija (engl. *DCT - Discrete Cosine Transform*) i diskretna valna transformacija (engl. *DWT - Discrete Wavelet Transform*). Ove tehnike temelje se na činjenici da je ljudski vizualni sustav najmanje osjetljiv na visoke frekvencije. Čovjek će teško raspoznati promjene na tim frekvencijama te ih je zbog toga moguće smanjiti bez vidljivog utjecaja na samu slikovnu datoteku. S druge strane, ljudski je vizualni sustav najviše osjetljiv na srednje vrijednosti frekvencija, a nešto manje osjetljiv na niske frekvencije. Također, ljudsko će oko prije uočiti promjene u svjetlini slike nego u promjene u prijelazima boja piksela. Zbog svega navedenog, tajne je informacije moguće ovih tehnikama smjestiti na mjesta značajnih frekvencija koje se kompresijom neće izgubiti ili uništiti, a isto tako proces ugradnje ne bi trebao previše utjecati na sam izgled objekta nositelja.

3.2.1. DCT – diskretna kosinusna transformacija

DCT je temelj JPEG kompresije i formata prikaza slika, a s obzirom na to da je slika dvodimenzionalni signal, koristi se dvodimenzionalna DCT. Kako se sadržaj slike mijenja po njezinim dijelovima, tako se i frekvencijski sadržaj mijenja. Zbog toga se kod JPEG formata prvo radi podjela slike na blokove veličine 8x8 piksela kako bi se najbolje prikazale njezine značajke. Na tih blokovima radi se DCT, a blokovi se šalju slijedno – s lijeva na desno i odozgo prema dolje. Svakom se bloku oduzima 128 od njegove vrijednosti, a svaki blok ima po 64 vrijednosti amplitude. Nakon što se primijeni DCT na blok, dobiju se po 64 koeficijenta u svakom bloku koji predstavljaju amplitude dvodimenzionalnih prostornih frekvencija *u* i *v*. Koeficijenti f(u,v) za svaki blok piksela veličine 8x8 određuju se prema sljedećoj formuli (3-1), [12]:

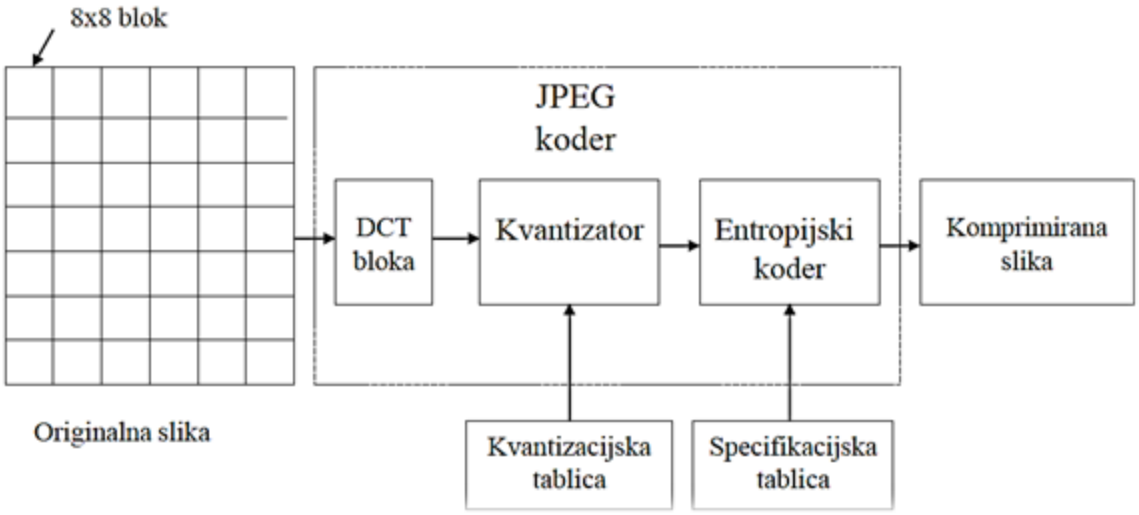
$$F(u,v) = \frac{1}{4}\, c(u)c(v) \sum_{x=0}^{7} \sum_{y=0}^{7} \cos\left(\frac{(2x+1)\,u\pi}{2\times 8}\right) cos\left(\frac{(2y+1)\,v\pi}{2\times 8}\right) f(x,y) \qquad (3\text{-}1)$$

Pri čemu vrijedi sljedeće [12]:

$$c(u) = c(v) = \begin{Bmatrix} \frac{1}{\sqrt{2}},\ za\ u = v = 0 \\ 1,\ za\ u = v \neq 0 \end{Bmatrix} \qquad (3\text{-}2)$$

Dakle, uz pomoć te transformacije, sadržaj slike prebacuje se u frekvencijsko područje. Zatim se na svakom DCT koeficijentu primjenjuje kvantizacija uz pomoć kvantizacijske tablice – svaki se od koeficijenta dijeli s odgovarajućom veličinom. Primjenom kvantizacije koeficijenti

se zaokružuju na najbliže cjelobrojne vrijednosti čime smanjuje se broj bitova i količina podataka, ali isto tako se unosi određena greška, tj. gubitak informacija slikovne datoteke. Kvantizacijska se tablica može formirati na način da prati glavne značajke ljudskog vizualnog sustava, čime bi se za više frekvencije koristio veći kvantizacijski korak. Nakon kvantizacije vrši se još i Huffmanovo kodiranje DCT koeficijenata koje omogućuje dodatan stupanj kompresije, a kao krajnji rezultat se dobije komprimirana slika, [12]. Na slici 3.3. prikazan je cijeli objašnjeni proces JPEG kompresije.



Slika 3.3. Proces JPEG kompresije [12]

S obzirom na to da tajnih podatci moraju biti očuvani, a kompresijom se oni uništavaju, važno je znati u kojeg trenutku procesa je moguće sigurno ugraditi bitove tajne informacije. Steganografija se kod JPEG formata može odviti između faze kvantizacije i Huffmanovog kodiranja. Umetanje bitova prije kvantizacije bilo bi beskorisno jer ona donosi gubitak bitova, a Huffmanovo kodiranje ne unosi dodatne gubitke te je moguće prije samog kodiranja sigurno umetnuti tajne informacije. Za ugradnju bitova koristi se prethodno objašnjena LSB tehnika – tajni se bitovi se ugrađuju na mjesta bitova najnižih vrijednosti svih frekvencijskih koeficijenata većih od nule, [12].

3.2.2. DWT – diskretna valna transformacija

Valne funkcije (engl. *wavelet*) su lokalizirane oscilirajuće i vremenski ograničene funkcije. Svaka valna funkcije generira se pomoću skaliranja i translacije iz osnovne „*mother wavelet*“ funkcije Ψ(t) prikazane sljedećom formulom (3-3), [12]:

$$\Psi_{j,k}(t) = 2^{\frac{j}{2}} \Psi(2^j t - k) \qquad (3\text{-}3)$$

Za razliku od ostalih transformacija, ove funkcije mogu biti proizvoljnog oblika i prilagoditi se ovisno o upotrebi. Diskretna valna transformacija odvija se korištenjem piramidalnog algoritma gdje se niskopropusni i visokopropusni valni filtri primjenjuju u horizontalnom, a onda u vertikalnom smjeru (redci i stupci). Time se slika dijeli na četiri frekvencijska podpojasa, tj. razine, a postupak filtriranja ponavlja se samo na koeficijentima koji se nalaze u niskofrekvencijskom podpojasu, [12].

3.3. Tehnike proširenog spektra

Komunikacijske tehnologije proširenog spektra (engl. *spread spectrum*) razvijaju se još od 1950-ih s ciljem stvaranja komunikacije koju će se teško omesti i koja će imati nisku vjerojatnost presretanja, [8]. Ove tehnologije mogu se definirati kao sredstvo prijenosa signala u kojem dolazi do procesa širenja propusnosti uskopojasnog signala preko širokog frekvencijskog pojasa. Signal zauzima veću širinu pojasa nego što mu je minimalno potrebna za prijenos informacija, [12]. Signale proširenog spektra teško je ukloniti i zbog toga su tehnike koje se temelje na takvim signalima pogodne za steganografiju. Za tajnu informaciju koristi se signal uskog spektra i on se umeće u objekt nositelj. Prije umetanja u objekt nositelj, uskopojasni valni oblik tajne poruke modulira se sa širokopojasnim valnim oblikom – signalom šuma. Proširenjem spektra, energija uskopojasnog signala tajne poruke bit će niska u bilo kojem frekvencijskom pojasu, održavat će se ista snaga signala i time će biti teže razlikovati signal od šuma i otkriti ga, [11]. Također, tajne se informacije umeću u dijelove objekta nositelja koji imaju najveću važnost što otežava ometanje. Ove se tehnike temelje na činjenici da se male modifikacije napravljene na slikovnoj ili zvučnoj datoteci u dijelovima objekta nositelja najviše energije najteže otkrivaju.

Koriste se dvije tehnike proširenog spektra – direktni slijed (engl. *direct-sequence*) i frekvencijski skok (engl. *frequency-hopping*). U tehnikama direktnog slijeda, tajni se signal širi konstantom, modulira se korištenjem pseudoslučajnog signala i umeće se u objekt nositelj. Kod tehnika frekvencijskog skoka, frekvencija signala nositelja mijenja se na način da brzo skače s jedne frekvencije na drugu, [8].

3.4. Statističke tehnike

Statističke tehnike temelje se na korištenju bita 1. Na početku se objekt nositelj podijeli na blokove na način da je broj blokova jednak veličini poruke. Svaki se nastali blok zatim koristi za skrivanje jednog bita tajne informacije. Ukoliko je bit tajne informacije koji se prenosi jednak 1, tada dolazi do modificiranja objekta nositelja na način da mu se statističke karakteristike značajno promjene. Ukoliko se prenosi bit tajne informacije koji je jednak 0, tada se statističke karakteristike bloka objekta nositelja ne mijenjaju. Na prijemnoj strani, korištenjem testnih funkcija može se otkriti koji je blok promijenjen i tako razlikovati modificirane i nemodificirane objekte nositelje. Koriste se funkcije za testiranje hipoteze – testira se hipoteza da određeni blok nije modificiran protiv hipoteze da je modificiran. Za tu upotrebu koriste se teorije testiranja hipoteza iz matematičke statistike. Ove su tehnike u praksi teško primjenjive u većini slučajeva. Teško je pronaći dobru testnu statistiku koja bi omogućila razlikovanje modificiranih i nemodificiranih blokova objekta nositelja, [8].

3.5. Tehnike izobličenja

Tehnike izobličenja zahtijevaju poznavanje originalnog objekta nositelja u procesu otkrivanja tajne poruke. Pošiljatelj tajne informacije primjenjuje niz modifikacija na objekt nositelj kako bi kreirao stego objekt. Niz modifikacija koji se izvršava odabran je na način da odgovara specifičnoj tajnoj informaciji koja se prenosi sustavom. Primatelj mjeri razlike između originalnog objekta nositelja i stego objekta kojeg je primio kako bi mogao rekonstruirati slijed primijenjenih modifikacija i otkriti tajnu informaciju. Ovakvi sustavi nisu korisni za mnoge primjene zbog toga što prijemna strana mora imati pristup originalnom objektu nositelju. Ukoliko neka treća strana također ima pristup tom objektu nositelju, lako može otkriti postojanje modifikacija učinjenih na objektu nositelju i time dokazati tajnu komunikaciju. Također, bitno je koristiti stego ključ kako treća strana ne bi mogla rekonstruirati poruku ukoliko dođe do otkrivanja postojanja tajne komunikacije. Objekt nositelj potrebno je distribuirati sigurnim kanalom, [8].

3.6. Tehnike stvaranja objekta nositelja

Tehnike stvaranja objekta nositelja jedinstvene su u usporedbi s prethodno navedenim tehnikama. Kod ovih se tehnika koristi obrnuti proces nego u ostalima – tajna informacija ne skriva se u objektu nositelju, nego se odgovarajući objekt nositelj stvara na temelju odabrane tajne

informacije. Steganografske aplikacije stvaraju jedinstveni objekt nositelj samo u svrhu skrivanja tajne informacije, [8].

4. STEGANALIZA

Glavni je cilj steganografije izbjeći privlačenje pozornosti i sumnje na postojanje prijenosa tajne poruke. Ukoliko dođe do sumnje da postoji tajna komunikacija, taj cilj nije ispunjen. Steganaliza (engl. *steganalysis*) je znanost otkrivanja postojanja tajnih poruka skrivenih steganografskim metodama. Osim otkrivanja tajne poruke, steganalizom se procjenjuje veličine tajne poruke, tajne se poruke izdvajaju iz stego objekta, dešifriraju, izmjenjuju ili uništavaju. Stoga se steganalizu može smatrati napadom na steganografske tehnike i testom njihove sigurnosti.

Osnovna pretpostavka je da se sve steganografske tehnike mogu svesti na sljedeću jednostavnu formulu (4-1), [8]:

$$C = t + p \tag{4-1}$$

Pri čemu su:

- t – količina informacija objekta nositelja kojom se može manipulirati na način da ne dođe do primjetnog izobličenja u ljudskoj percepciji
- p – količina informacije objekta nositelja koja će, ukoliko se njome manipulira, uzrokovati izobličenja primjetna ljudskoj percepciji
- C – potencijalni objekt nositelj

Veličina t dostupna je i korisniku steganografskih tehnika i potencijalnom napadaču koji želi razotkriti i onemogućiti prijenos tajne informacije. Dokle god je veličina t u području koji nije perceptivan, postoji veličina t' koju koristi napadač i postoji C' koji je zbroj p i t' te ne postoji razlika između C i C' koja bi bila primjetna ljudskoj percepciji. Ova činjenica može se iskoristiti za napad na način da se područje veličine t ili ukloni ili zamijeni. Bilo kojim stego objektom može se manipulirati s namjerom da se tajni podatci unište ili promjene bez obzira postoji li tajna poruka ili ne. No otkrivanje postojanja tajne poruke skraćuje postupak tako što se obrađuju samo oni objekti koji uistinu sadrže tajne informacije, [8].

4.1. Oblici napada steganalize

S obzirom na informacije koje su dostupne steganaliticaru, postoje sljedeći oblici napada: [13]

- samo steganografska datoteka (engl. *stego-only attack*) - dostupna je samo steganografska datoteka nad kojom se mogu vršiti analize
- poznati objekt nositelj (engl. *known cover attack*) – za analizu su dostupni originalni objekt nositelj u kojeg je ugrađena tajna informacija i steganografska datoteka, tj. stego objekt
- poznata poruka (engl. *known message attack*) – napadaču je dostupna tajna poruka; analizom stego objekta i traženjem uzoraka u stego objektu koji odgovaraju tajnoj poruci može se doći do rezultata koji bi bili od pomoći u daljnjim fazama napada
- odabrana steganografska tehnika (engl. *chosen stego attack*) – za analizu su poznati korišteni steganografski alat, tj. tehnika kojom je tajna poruka ugrađena u objekt nositelj i stego objekt
- odabrana poruka (engl. *chosen message attack*) – za analizu je poznat steganografski alat i odabrana poznata poruka iz kojih steganaliticar generira stego objekt; u ovom je napadu cilj odrediti postojeće odgovarajuće uzorke u stego objektu koji bi mogli ukazivati na upotrebu specifičnih steganografskih tehnika
- poznati objekt nositelj i odabrana steganografska tehnika (engl. *known stego attack*) – za analizu su dostupni objekt nositelj, stego objekt i korištena steganografska tehnika

Ugrađenu tajnu poruku u objekt nositelj i dalje može biti vrlo teško izdvojiti bez obzira na informacije dostupne za napad. Ponekad se za napade koristi drugačiji pristup, a to je napad na stego ključ kojim se tajna poruka štiti. Taj je pristup učinkovit protiv nekih steganografskih alata, ali svejedno je potrebno uložiti značajnu količinu vremena za obradu kako bi se postigli rezultati.

4.2. Tehnike steganalize

Postoje dva ključna pristupa rješavanju problema steganalize pri čemu svaki ima svojih prednosti i nedostataka. Prvi je razvijanje tehnike specifične za točno određeni steganografski algoritam. Ovaj bi pristup dao vrlo dobre rezultate kada bi se primjenjivao za specifični steganografski algoritam, ali bi vjerojatno podbacio s ostalim algoritmima. Drugi je pristup razvijanje

univerzalnih tehnika koje bi radile neovisno o tome koji je steganografski algoritam korišten. Ovaj bi pristup dao generalno nešto lošije rezultate, ali bi oni i dalje bili zadovoljavajući za većinu algoritama, [6].

Smatra se da je steganalitička tehnika uspješna ukoliko može detektirati postojanje tajne poruke bez njenog dešifriranja, a neke novije tehnike osim otkrivanja tajne poruke mogu i dosta precizno procijeniti njenu veličinu. Najpoznatije tehnike steganalize su tehnika neobičnih uzoraka i tehnika vizualne detekcije, a njihove karakteristike opisane su u nastavku.

4.2.1 Tehnika neobičnih uzoraka

Postojanje neobičnih uzoraka u stego objektima predstavlja mogućnost postojanje skrivene tajne poruke u istima. Takve je uzorke moguće identificirati ukoliko se koriste odgovarajući alati i tehnike. Jedan od primjera neobičnih uzoraka je postojanje dodanih razmaka i tabulatora u tekstualnoj datoteci koji prikazom teksta na zaslonu nisu očiti, no upotrebom odgovarajućeg programa za obradu teksta moguće ih je lako otkriti. Nadalje, za skrivanje tajnih informacija mogu se koristiti i neiskorištena područja na disku. Korištenjem alata za analizu diska, filtriranjem se otkrivaju tajne informacije. Filteri se mogu koristiti i za pronalazak TCP/IP paketa koji u svojim zaglavljima imaju ugrađene tajne informacije. Traženje neobičnih uzoraka primjenjivo je i na multimediju koja je česti objekt nositelj zbog svojih svojstava. Uzorci na koje je potrebno obratiti pažnju su npr. neuobičajeno sortiranje paleta, pretjerana količina šuma, [5, 9].

4.2.2 Tehnika vizualne detekcije

Tehnika vizualne detekcije jedna je od starijih i poznatijih tehnika. Vizualnim metodama analizira se stego objekt, najčešće slikovna datoteka, kako bi se uočile bilo kakve degradacije. Uspoređuju se dostupni podatci, analiziraju se promjene u nijansama boja i različita svojstva slike. Ukoliko je poznat objekt nositelj, tada je jednostavnije uočiti nepravilnosti. Uspoređivanjem originalnog objekta nositelja i stego objekta mogu se detektirati promjene i nepravilnosti u samoj kvaliteti slike i u bojama. Također, uz određeno iskustvo, steganalitičari mogu doći do spoznaje kojim je steganografskim alatom tajna informacija skrivena. Problem je što nije uvijek dostupna originalna slika, tj. objekt nositelj s kojim se stego objekt može usporediti pa potencijalna izobličenja i šumovi mogu proći neopaženo čineći se kao sastavni dio slike. U takvim se situacijama najčešće provjerava veličina slike. Analizom se obraća pozornost na to

je li slika izrezana, nadopunjena i sl. Analizira se i paleta boja koja se koristila na slici. Vizualnom detekcijom utvrđuje se sadrži li paleta mnoštvo boja koje joj ne odgovaraju ili postoji li previše jednoličnih tonova, što su znakovi mogućeg skrivanja tajnih informacija, [5,9].

4.3. Uništavanje ugrađenih tajnih informacija

Otkrivanje postojanja tajnih informacija već je poraz za steganografiju, ali osim otkrivanja, ugrađene tajne informacije mogu se zatim izdvojiti i uništiti, tj. onemogućiti.

Kada su tekstualne datoteke u pitanju, ugrađene tajne informacije u obliku dodatnih razmaka i „nevidljivih" znakova lako se mogu otkriti pomoću programa za obradu teksta. Nakon otkrivanja, isto tako ih je lako i jednostavno ukloniti, tj. obrisati iz tekstualne datoteke čime je tajna poruka uništena.

Treba biti oprezan i prilikom ugrađivanja informacija unutar nekorištenog prostora datoteka i sustava jer su to mjesta koja se često pretražuju u potrazi za tajnim informacijama. Ukoliko steganografski ugrađene informacije nisu zaštićene, operacijski sustav bi mogao iskoristiti taj prostor za neku drugu namjenu (npr. predmemoriranje, stvaranje privremenih datoteka) i pisati preko tih ugrađenih informacija. Opasnost dolazi i od raznih uslužnih programa za optimizaciju koji brišu predmemoriju i neiskorišteni prostor za pohranu čime se također uništavaju ugrađene tajne informacije.

Ugrađivanje informacija u zaglavlja TCP/IP paketa također ima svojih opasnosti od uništavanja informacija. Filtriranjem paketa uz odgovarajuću konfiguraciju mogu se pronaći oni paketi koji sadrže informacije u dijelovima koji bi trebali biti neiskorišteni ili rezervirani. Rizik je i što se zaglavlja paketa i rezervirani bitovi mogu prebrisati i uništiti informacije bez utjecaja na usmjeravanje paketa. Također, riskantno je i skrivanje informacija manipulacijom vremenskih oznaka unutar paketa jer se i one filtriranjem mogu obrisati i onemogućiti skrivene informacije.

Kada se radi o slikama, neke metode onemogućavanja skrivenih informacija zahtijevaju značajne izmjene stego objekta, tj. stego slike. Uništavanje skrivenih informacija na slikama najčešće se svodi na korištenje različitih tehnika za obradu slike. Kada je u pitanju LSB, i samo korištenje kompresije s gubitkom dovoljno je da se tajne informacije unište, pri čemu će slika i dalje izgledati normalno ljudskom oku. Ukoliko se koriste tehnike transformacije domene, potrebna je značajnija obrada slike kako ugrađene informacije više ne bi bile čitljive. Pri tome se koriste višestruke tehnike obrade slike, npr. obrezivanje, zamućivanje, rotiranje, kako bi slika bila dovoljno izobličena da se uništi tajna informacija. Kombinacije različitih tehnika za

obradu slike često se koriste i za testiranje robusnosti i sigurnosti steganografskih tehnika. Testiranjem se stego objekt mijenja do te mjere da se ugrađene tajne informacije više ne mogu dohvatiti. Jedan od ciljeva ovakvih testiranja je otkrivanje kakve napade steganografske tehnike mogu podnijeti i razotkrivanje glavnih nedostataka. Testovi uključuju pretvaranje između formata bez gubitaka i formata s gubitkom, pretvaranje iz 24 bitnih u 8 bitne formate i obrnuto, zamućivanje, dodavanje i uklanjanje šuma, izoštravanje, zrcaljenje, rotiranje, pretvaranje iz digitalnog u analogno i natrag i dr. Također, postoje i testovi koji utvrđuju koja je najmanja veličina slike koja se može koristiti da bi ugrađivanje informacija bilo uspješno.

5. PRIMJENA I PRAKTIČNI PRIMJERI

U ovom će poglavlju biti opisane različite primjene za koje se koristi steganografija. Također, bit će prikazani različiti praktični primjeri koji se temelje na nekoj od prethodno opisanih steganografskih tehnika. Svi korišteni programi za realizaciju primjera besplatni su i dostupni za preuzimanje.

5.1. Primjena steganografije

Steganografske tehnike mogu se koristiti u bilo kojem slučaju kada je potrebno skrivanje informacija, za različita područja i potrebe. Postoje mnogi razlozi zbog kojih bi postojala potreba za skrivanjem informacija, ali svi se oni uglavnom svode na sprječavanje neovlaštenih osoba da saznaju za postojanje tajnih informacija. Primjena steganografije danas može se podijeliti na onu koja se u koristi u legalne svrhe i na onu koja se koristi u ilegalne svrhe.

Korištenje steganografije u legalne svrhe:

- vojska, obavještajne službe, državne agencije - koriste steganografske tehnike za skrivanje i prijenos osjetljivih informacija međusobno ili usmjereno prema određenom pojedincu.

- medicinske svrhe – uz postojanje Interneta, udaljenost između pacijenta i liječnika više nije bitna jer se medicinski podatci lako mogu razmjenjivati između različitih medicinskih ustanova i pacijenta. Steganografija se koristi za sigurno i neprimjetno ugrađivanje osobnih podataka pacijenata u njihove medicinske slike kako bi se povećala povjerljivost u slučaju dijagnoze na daljinu i osigurala tajnost pacijentovih podataka [14]. Na primjer, unutar rendgenske snimke mogu se ugraditi podatci o pacijentu i njegovoj povijesti bolesti bez narušavanja snimke, a uz dodatno korištenje enkripcije, pristup tim tajnim informacijama može imati samo liječnik s odgovarajućim ključem.

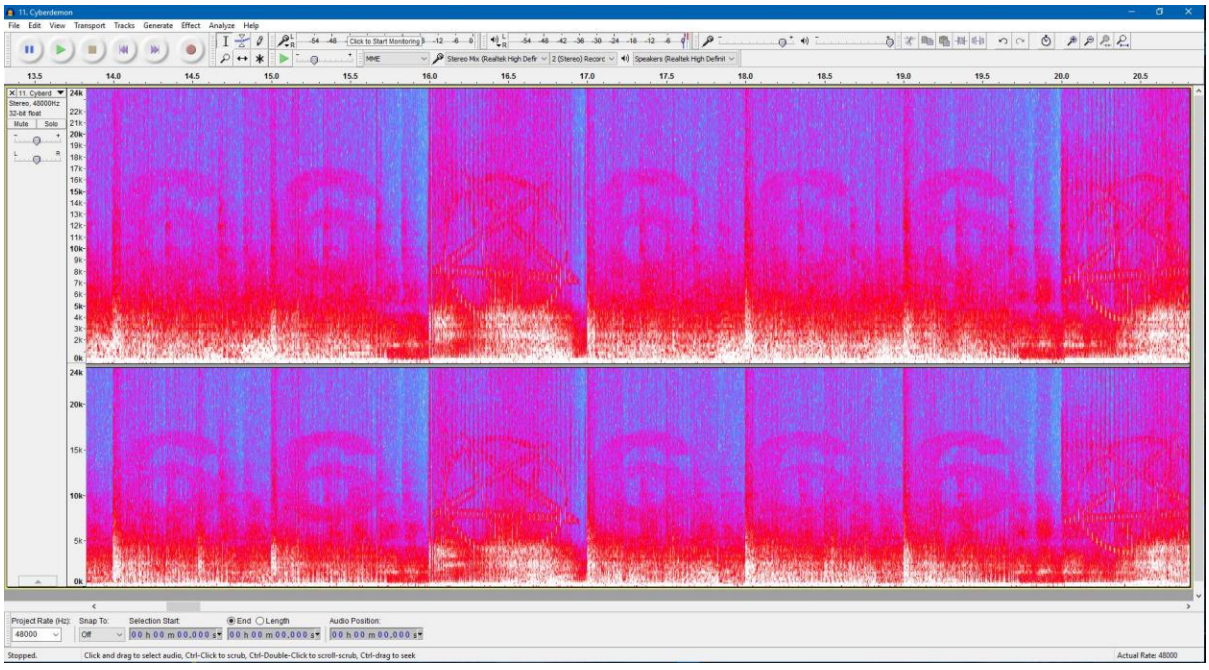
- digitalni vodeni pečat – sam koncept digitalnog vodenog žiga nije nužno steganografija, ali koriste se određeni steganografski pristupi za implementaciju vodenog žiga kako bi se osigurala zaštita autorskih prava i vlasništvo nad multimedijskim datotekama. Glavna razlika je u tome da je cilj steganografije skrivanje podataka, dok vodeni pečat predstavlja samo proširenje objekta nositelja dodatnim informacijama. Budući da bi

sam vodeni pečat unio vidljive promjene u slikovne, zvukovne i video datoteke, koriste se metode steganografije kako bi se informacije prikrile, [15].

- *hash* vrijednosti – korištenje steganografije kao supstitut prilikom generiranja jednosmjernih *hash* vrijednosti. Obradom ulaznog skupa podataka varijabilne duljine dobiva se izlazni skup podataka fiksne duljine kojim je moguće utvrditi je li došlo do kakvih promjena na izvornom ulaznom skupu podataka, [1].

- ostalo – korištenje steganografije za povjerljivu komunikaciju i tajno čuvanje podataka, za zaštitu izmjene podataka, za sustave medijskih baza podataka, u pravne svrhe, u svrhu zaštite kupaca u e-trgovini, u svrhu skrivanja tajnih poslovnih informacija i planova i dr.

Steganografske postupke koriste i aktivisti i umjetnici za iskazivanje svojih kontroverznih mišljenja i stavova. Jedan od takvih primjera je pretvaranje slikovne datoteke u zvučnu datoteku kako bi se prikrila poruka, što su koristili razni izvođači. Na primjer, 2016. godine objavljena je nova verzija DOOM igre za PlayStation4 koja se uglavnom bazirala na borbi protiv demonskih sila i drugih neprijatelja. Ubrzo nakon toga, ljubitelji ove igre otkrili su da se unutar zvučne podloge igre, koju je skladao Mick Gordon, krije slikovna datoteka. Analizom zvučnog zapisa pomoću spektrograma, otkrivene su slike koje prikazuju pentagrame i niz brojeva „666“, što je vidljivo na slici 5.1, [16].



Slika 5.1.: Otkrivena slika pomoću spektrograma iz zvučne podloge DOOM igre [16]

Unatoč raznim prednostima steganografije koje osiguravaju zaštitu i povjerljivost informacija, steganografija se, nažalost, danas koristi u razne ilegalne svrhe. Pogodna je za korištenje u ilegalnim aktivnostima zbog toga što omogućuje prikrivanje postojanje dokaza o istima. Neki od primjera korištenja steganografije u ilegalne svrhe su sljedeći:

- zlonamjerni stego softver (engl. *stegomalware*) – vrsta zlonamjernog softvera koja koristi steganografske tehnike kako bi se spriječilo otkrivanje. Koristi se u svrhe skrivanja zlonamjernog koda unutar podataka koji izgledaju bezazleno. Primjenjuje se i implementacija tajnih kanala za izvlačenje tajnih informacija
- terorizam – korištenje steganografije u svrhu očuvanja tajne komunikacije i koordiniranja napada
- krađa tajnih podataka – u industriji, u poslovnom sektoru; koristi se i za prikrivanje ukradenih podataka u izlaznom toku podataka
- malvertizacija (engl. *malvertising*) – upotreba steganografskih tehnika na mrežama za oglašavanje na način da se umeću lažni oglasi koji u sebi skrivaju tajne zlonamjerne softvere i koji navedu korisnike na preuzimanje tih softvera [17]
- pornografija – korištenje steganografskih tehnika za tajno razmjenjivanje dječje pornografije

Općenito govoreći, steganografskim tehnikama najčešće se koriste hakeri koji mijenjajući određene bitove datoteka, umeću svoj zlonamjerni kod. Nakon toga korisnik nenamjerno preuzme taj kod otvaranjem određene datoteke ili slike, zlonamjerni softver se aktivira i čini štetu korisniku. Steganografska datoteka toliko se suptilno razlikuje od izvorne da ju je teško odmah detektirati. Programeri zlonamjernih softvera najčešće koriste LSB metodu za skrivanje koda, [18].

Sljedeći primjeri opisuju neke od situacija ugrađivanja zlonamjernih softvera korištenjem steganografije u bližoj povijesti: [19]

- ugrađivanje unutar digitalnih medijskih datoteka – krajem 2016. godine događali su se napadi velikih razmjera vezani uz e-trgovinu *Magento*. Koristile su se metode slikovne steganografije za prikrivanje podataka o platnim karticama. Nakon što je platforma za e-trgovinu zaražena zlonamjernim softverom, on je prikupljao podatke o plaćanjima i skrivao ih unutar slika stvarnih proizvoda dostupnih na e-trgovini.

- oponašanje legitimnih programa – primjer je varijanta Android/Twitoor.A trojanskog konja koji se širi putem SMS-a ili zlonamjernih URL-a. Zlonamjerni softver oponaša pornografski reproduktor medijskih sadržaja ili aplikaciju za slanje multimedijskih poruka, ali bez ispravne funkcionalnosti, jedina svrha je prevariti korisnika da instalira aplikaciju i širi zarazu zlonamjernim softverom.

- ucjenjivački softver (engl. *ransomware*) – sredinom 2016. godine identificiran je *Cerber* zlonamjerni ucjenjivački softver koji se širio putem aplikacija za dijeljenje datoteka u oblaku. Za širenje softvera, *Cerber* je koristio dokument kao mamac koji, kada se otvori, učitava zlonamjerni kod koji preuzima JPEG datoteku na ciljano računalo. JPEG datoteka u sebi ima steganografski ugrađenu zlonamjernu izvršnu datoteku. Još jedan primjer takvog softvera je *SyncCript* koji je koristio slikovnu steganografiju za ugrađivanje osnovnih komponenata ucjenjivačkog softvera.

- komplet za iskorištavanje (engl. *exploit kit*) – primjer je Stegano/Astrum komplet za iskorištavanje koji je korišten 2016. godine kao dio velike zlonamjerne kampanje. Zlonamjerni kod ugrađivao se u reklamne oglase mijenjanjem prostora boja PNG slikovne datoteke. Žrtvin preglednik zatim analizira umetnuti JavaScript kod, izdvajajući zlonamjerni kod i preusmjerava korisnika na odredišnu stranicu kompleta za iskorištavanje. Zaraza softverom zatim se izvršava na odredišnoj stranici, uglavnom uz korištenje slabih točaka Adobe Flash softvera.

- zlonamjerni program za preuzimanje – primjer je *Lurk,* zlonamjerni softver koji koristi LSB metodu za modifikaciju bitova BMP i PNG datoteka. Na taj način ugrađuje šifrirane URL-ove u slikovnu datoteku kako bi se omogućilo preuzimanje dodatnih komponenti zlonamjernog softvera, a rezultirajuća datoteka ima dodatne bitove koji su neprimjetni korisniku. Svrha je preuzimanje i izvršavanje sadržaja zlonamjernog softvera.

Kibernetički kriminal samo će nastaviti rasti jer je vrlo unosan, a steganografske će tehnike, zbog svojih karakteristika, u tome još više pomoći. Stručnjaci vjeruju da će kibernetički kriminalci staviti sve veći naglasak na otežavanje otkrivanja i ulaženja u trag porijeklu zlonamjernog softvera, što će povećati upotrebu skrivanja informacija, tj. steganografskih tehnika.

5.2. Praktični primjeri

5.2.1 Primjer temeljen na LSB supstituciji

Kako bi se što bolje prikazao način rada tehnika temeljenih na LSB supstituciji, prvi će primjer biti jednostavan primjer prikazan pomoću binarnog zapisa. Neka je tajna poruka koja se želi sakriti u objekt nositelj slovo B. Prema Američkom standardnom znakovniku za razmjenu informacija (engl. *American Standard Code for Information Interchange, ASCII*), ekvivalent slovu B je $66_{(10)}$, a u binarnom zapisu to je $01000010_{(2)}$. Za skrivanje odabranog slova dovoljna su tri piksela i neka su to sljedeći pikseli:

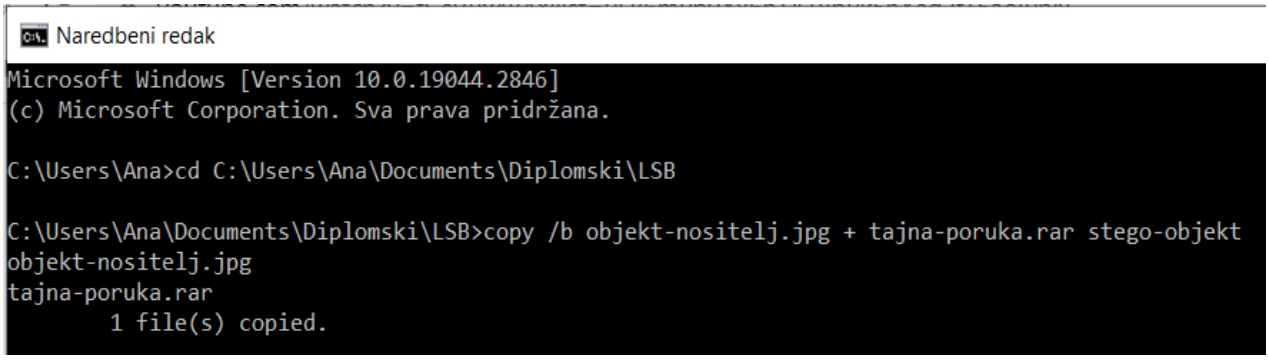
(11001000, 00100111, 11101001), (00100111, 11101001, 11001000), (00100111, 11001000, 11101001).

Podebljani bitovi su bitovi najmanje važnosti odabranih piksela. Na njihovo se mjesto upisuju bitovi binarnog zapisa tajne poruke. Nakon ugrađivanja bitova, pikseli su sljedećeg oblika:

(11001000, 00100111, 11101000), (00100110, 11101000, 11001000), (00100111, 11001000, 11101001).

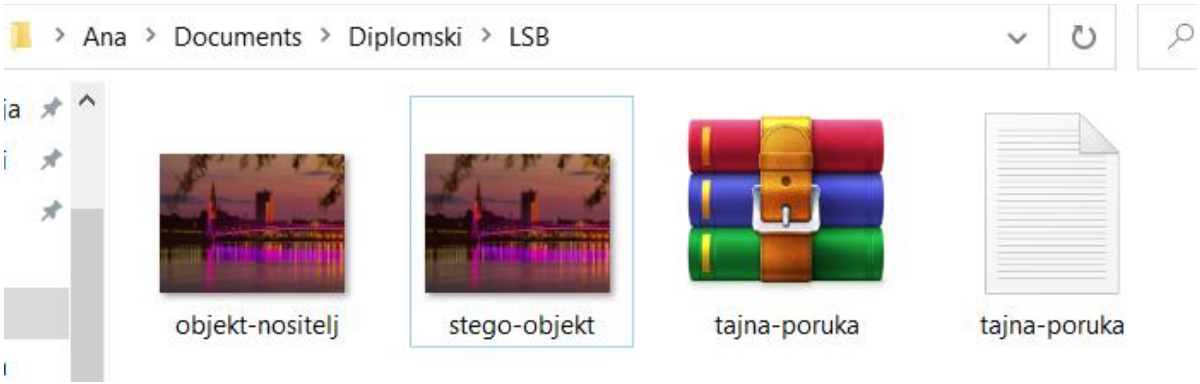
Bitovi koji su promijenili vrijednost u odnosu na početne piksele podcrtani su. Prema podcrtanim bitovima, vidljivo je da je za ugrađivanje tajne poruke bilo potrebno izmijeniti vrijednost samo 3 od 8 korištenih bitova najmanje važnosti. Općenito govoreći, u prosjeku je najčešće potrebno promijeniti vrijednost samo polovici korištenih bitova kako bi se ugradila tajna informacija, a takva promjena neće biti percipirana ljudskim okom.

Sljedeći primjer je umetanje tekstualne datoteke u sliku. Najprije je kreirana tekstualna datoteka naziva „tajna-poruka“ sa tajnom porukom „Ana je diplomirala!“ u mapi naziva „LSB“. U istu mapu dodana je slika koja će se koristiti za objekt nositelj pod nazivom „objekt-nositelj“. Nakon toga, potrebno je tekstualnu datoteku spremiti u RAR obliku odabirom opcije desnog klika na datoteku „Dodaj u tajna-poruka.rar“. Sada su datoteke spremne za ugrađivanje i potrebno je otvoriti naredbeni redak (engl. *Command Prompt, cmd*) u sustavu Windows. Prvo se pristupa mapi u kojoj se nalaze datoteke kojima će se manipulirati koristeći naredbu cd (engl. *change directory,* cd) za promjenu direktorija. Nakon toga koristi se naredba „*copy /b*“ kojom se kopiraju datoteke tretirajući ih kao binarne zapise. Potrebno je upisati naredbu u obliku „*copy /b imeslike.jpg + imetekstualnedatoteke.rar imenovedatoteke*“. Na slici 5.2. prikazan je opisani postupak u naredbenom retku s odgovarajućim nazivima datoteka.



Slika 5.2.: Kopiranje datoteka u naredbenom retku

Nakon izvršenja naredbe, u mapi „LSB“ stvorena je nova datoteka pod nazivom „stego-objekt“ kako je i naznačeno u naredbenom retku. Novonastalu datoteku potrebno je preimenovati u „stego-objekt.jpg“ kako bi se prikazala u JPG obliku. Izgled datoteka u mapi „LSB“ nakon izvršavanja ovih naredbi prikazan je na slici 5.3.



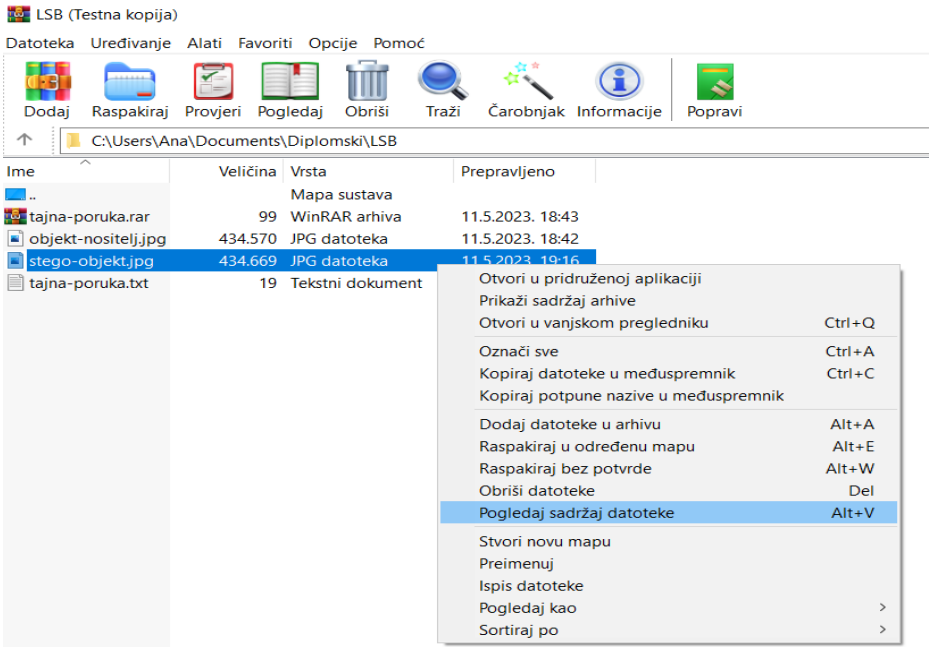
Slika 5.3.: Prikaz mape „LSB“ nakon izvršavanja naredbi

Otvaranjem slika „objekt-nositelj“ i „stego-objekt“ vidljivo je da se one ne razlikuju, barem ne primjetno ljudskom oku čime je tajna poruka uspješno ugrađena. Na slici 5.4. prikazan je objekt nositelj, a na slici 5.5. stego objekt.

Slika 5.4.: Prikaz objekta nositelja

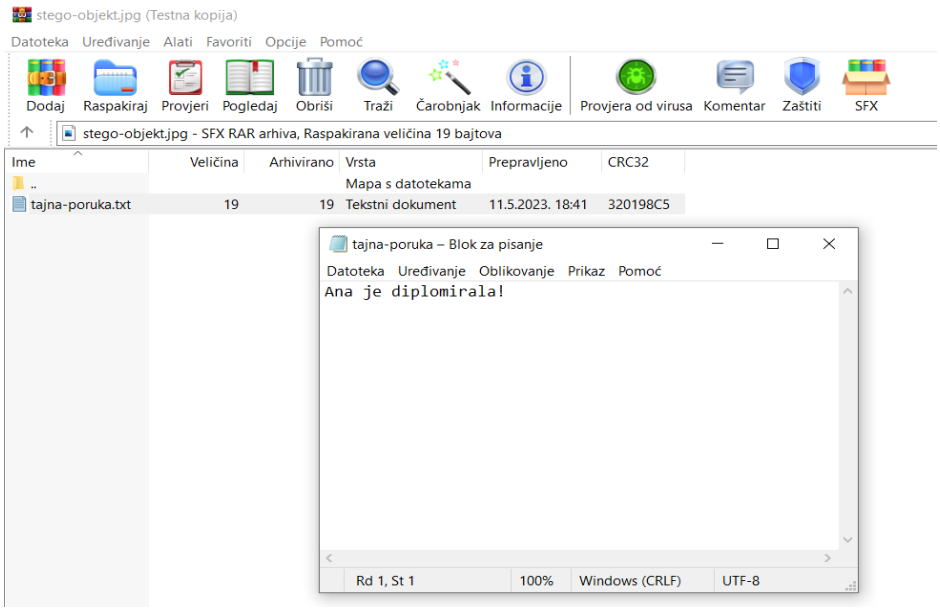
Slika 5.5.: Prikaz stego objekta

Da bi se otkrila tajna poruka iz stego objekta, potrebno je pronaći datoteku „stego-objekt“ u mapi „LSB“ korištenjem WinRAR programa. Desnim klikom na datoteku „stego-objekt“ odabire se opcija „Pogledaj sadržaj datoteke“ kao što je prikazano na slici 5.6.



Slika 5.6.: Otvaranje datoteke „stego-objekt“ u WinRAR programu

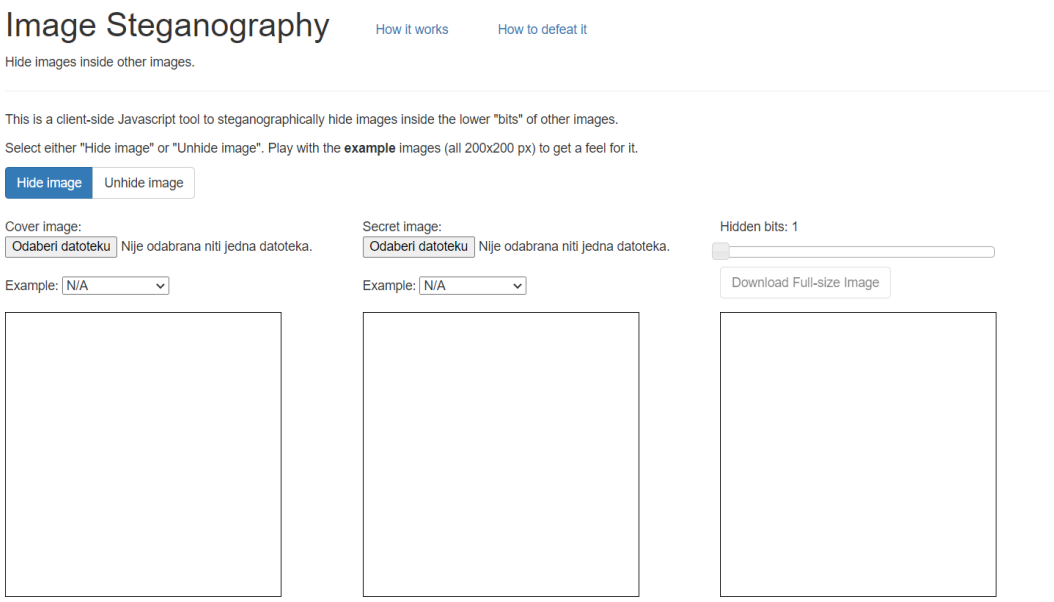
Nakon toga, vidljivo je da se unutar datoteke „stego-objekt“ nalazi i tekstualna datoteka „tajna-poruka“ te klikom na tu datoteku otvara se tajni sadržaj, kao što je prikazano na slici 5.7.



Slika 5.7.: Prikaz sadržaja tajne poruke

5.2.2 Primjer temeljen na degradaciji slike

Za prikaz primjera skrivanja slike u slici metodom degradacije slike korištene su datoteke PNG formata veličine 200x200 piksela. Korišten je javno dostupan alat *Image Steganography* [20] za skrivanje slike u slici koji je napravio programer James Stanley u JavaScript skriptnom programskom jeziku. Kako bi se tajna slika sakrila u sliku koja je objekt nositelj, program zamjenjuje n najmanje značajnih bitova piksela vrijednosti objekta nositelja s istim brojem najvažnijih bitova piksela vrijednosti tajne slike. Korisnik sam odabire veličinu n, tj. broj korištenih bitova. Na slici 5.8. prikazan je izgled sučelja ovog alata, a na slikama 5.9. i 5.10. prikazane su originalne slike objekta nositelja i tajne slike.



Slika 5.8.: Izgled alata za ugrađivanje slike u sliku od James Stanley-a, [20]

Slika 5.9.: Objekt nositelj

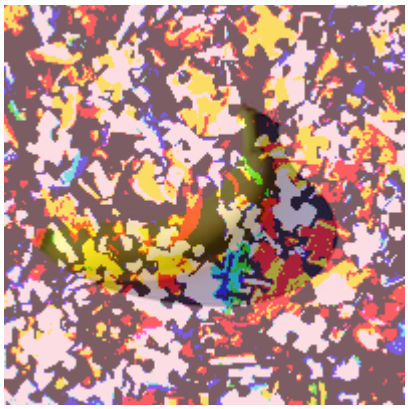
Slika 5.10.: Tajna slika

Na sljedećim slikama 5.11., 5.12., 5.13., 5.14. prikazana je stego slika u ovisnosti korištene veličine n, tj. korištenih bitova za skrivanje tajne slike. Za veličinu n odabrane su vrijednosti 1, 3, 5 i 7 kako bi se bolje prikazao utjecaj ugrađivanja informacija na originalni objekt nositelj i vidjelo koja stego slika najbolje odgovara originalu.

Slika 5.11.: Stego slika, n=1

Slika 5.12.: Stego slika, n=3

Slika 5.13.: Stego slika, n=5



Slika 5.14.: Stego slika, n=7

Iz priloženih fotografija može se primijetiti da je tajna slika dobro prikrivena i da stego slika liči originalu pri korištenju n=1 i n=3. Manja odstupanja primjetna su kada je n=5, dok se pri n=7 tajna slika već nazire u pozadini i jasno je vidljivo da je u stego objekt izmijenjen te da sadrži ugrađene informacije. Korištenje većeg broja bitova, tj. veličine n, kvaliteta skrivene tajne slike biti će veća, ali će ju biti lakše otkriti iz stego objekta. Na slikama 5.15., 5.16., 5.17., 5.18. prikazane su tajne slike izvučene iz stego objekta u ovisnosti o broju korištenih bitova n.

Slika 5.15.: Tajna slika iz stego objekta, n=1

Slika 5.16.: Tajna slika iz stego objekta, n=3

Slika 5.17.: Tajna slika iz stego objekta, n=5

Slika 5.18.: Tajna slika iz stego objekta, n=7

Iz priloženih slika može se zaključiti da je najbolja kvaliteta izvučene tajne slike kada je n=7, no tada je iz stego objekta jasno vidljivo da postoji skrivena informacija. S druge strane, kada je n=1, tajna se slika u većoj mjeri razlikuje od originalne tajne slike. To prikazuje koliko je važan odabir veličine n kako bi se postigao kompromis gdje stego objekt neće biti sumnjiv, a da istovremeno tajna poruka bude vjerodostojno prikazana.

Na sljedećim slikama bit će prikazano koliko je važan odabir slike koja će biti objekt nositelj kako bi rezultat bio zadovoljavajući i kako ne bi privlačio pažnju i sumnju na skrivanje informacije. Neka je sada slika 5.19. objekt nositelj, a slika 5.20. tajna slika koju je potrebno sakriti.

Slika 5.19.: Objekt nositelj

Slika 5.20.: Tajna slika

Ponavljajući isti postupak kao i u prošlom primjeru, na slikama 5.21.,5.22.,5.23. i 5.24. vidljivi su rezultati ugrađivanja tajne slike u odabrani objekt nositelj, tj. stego slika u ovisnosti korištene veličine n, pri čemu je n=1, 3, 5 i 7.

Slika 5.21.: Stego slika, n=1

Slika 5.22.: Stego slika, n=3

Slika 5.23.: Stego slika, n=5

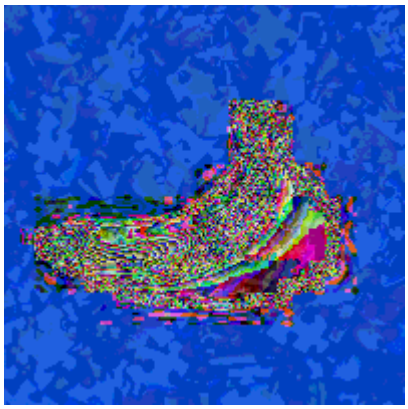
Slika 5.24.: Stego slika, n=7

Promatrajući dobivene stego slike i uspoređujući ih sa prošlim primjerom, vidljivo je da je odabir slike za objekt nositelj puno lošiji, a time je i puno lošiji rezultat dobivene stego slike. Kada je n=1, stego slika liči na original, nema značajnih odstupanja koja bi ju odala da se u

njoj skrivaju neke dodatne informacije. Pri n=3 već su vidljive naznake tajne slike koja je skrivena, ne može se jasno otkriti o čemu se radi, no dovoljna je i sama činjenica što se vidi da postoji nešto skriveno. Kada je n=5 tajna slika dolazi još više do izražaja, sada je već jasno o kakvoj slici se radi, dok kod n=7 tajna slika većinski preuzima izgled stego slike, originalni objekt nositelj nije u prvom planu.

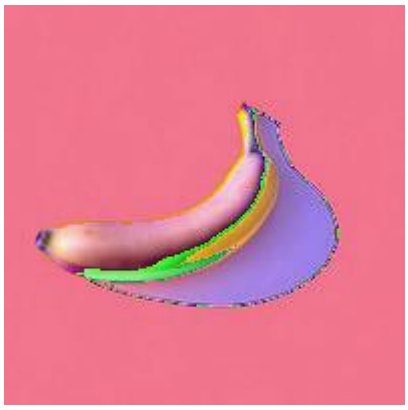
Na slikama 5.25., 5.26., 5.27., 5.28. prikazane su tajne slike izvučene iz stego objekta u ovisnosti o broju korištenih bitova n.

Slika 5.25.: Tajna slika iz stego objekta, n=1



Slika 5.26.: Tajna slika iz stego objekta, n=3

Slika 5.27.: Tajna slika iz stego objekta, n=5



Slika 5.28.: Tajna slika iz stego objekta, n=7

Iz priloženih slika izvučenih tajnih informacija iz stego objekta, jasno je vidljivo da je odabir objekta nositelja bio potpuno pogrešan. Kada je n=1, djelomično je vidljiva tajna slika koja je ugrađena, nije potpuno čista, ali jasno se može zaključiti o čemu se radi. Pri n=3, naziru se samo obrisi tajne slike, ali nije jasno vidljivo o kakvoj tajnoj informaciji je riječ. Kada je n=5, obrisi tajne slike još su manje vidljivi, dok kod n=7 nisu uopće vidljivi i može se reći da ugrađivanje tajne informacije nije uspjelo. Iz ovog primjera vidljivo je da odabiru odgovarajućeg objekta nositelja treba postupiti s puno pozornosti kako bi rezultati bili zadovoljavajući. U ovom je slučaju objekt nositelj bio s premalo detalja i jednoličan, a svaka

izmjena na takvom objektu rezultira vidljivim izobličenjem i neuspjehom steganografskog postupka.

5.2.3 Steganografija pomoću MP3Stego alata

Audio formati koriste se u steganografiji zbog postojanja redundantnih informacija, a MP3 format kao tehnika kompresije s gubitkom izrazito je pogodan. Ideja je da se tijekom kompresije umjesto eliminiranja svih redundantnih informacija, one zamjene s drugim podatcima. Skrivanje tajnih informacija u audio format može se postići metodom najmanje značajnog bita, faznim kodiranjem, raspršenim spektrom. Sve se te metode oslanjaju na slabost percepcije ljudskog sluha u određenim područjima. Za primjer skrivanja tajnih poruka u audio format, specifično MP3 format, korišten je alat MP3Stego koji je kreirao Fabien Petitcolas, steganografski stručnjak, [21]. Alat izvršava proces skrivanja informacija tijekom procesa kompresije MP3 formata. Podatci se prvo sažimaju, šifriraju i zatim ugrađuju u tok bitova MP3 formata. Proces ugrađivanja podataka odvija se tijekom procesa kodiranja sloja 3 u unutarnjoj petlji koja kvantizira ulazne podatke i povećava korak kvantizacije dok god se kvantizirani podatci ne mogu kodirati s dostupnim brojem bitova. Pri tome se veće amplitude kodiraju s većim korakom kvantizacije. Postoji i druga petlja koja provjerava jesu li izobličenja uzrokovana kvantizacijom unutar praga koji je definiran psihoakustičnim modelom. U alatu postoji varijabla naziva „part2_3_length“ koja sadržava broj bitova podataka koji su korišteni kao faktori skaliranja. Bitovi se kodiranju prema paritetu, a samo nasumične vrijednosti varijable „part2_3_length“ se modificiraju. MP3Stego koristi 3DES enkripciju i SHA-1 za zaštitu tajnih podataka. Izbor varijabli vrši se korištenjem pseudoslučajnih generatora temeljenih na SHA-1, [21]. Za prikaz primjera potrebno je preuzeti MP3Stego alat dostupan na [21].

Za rad MP3Stego alata koriste se linije u naredbenom retku koje korisniku omogućavaju kodiranje i dekodiranje datoteka. Prije primjene ovih linija, potrebno je kreirati tekstualnu datoteku u kojoj će biti skrivena poruka i audio datoteku u koju će se ta poruka sakriti.

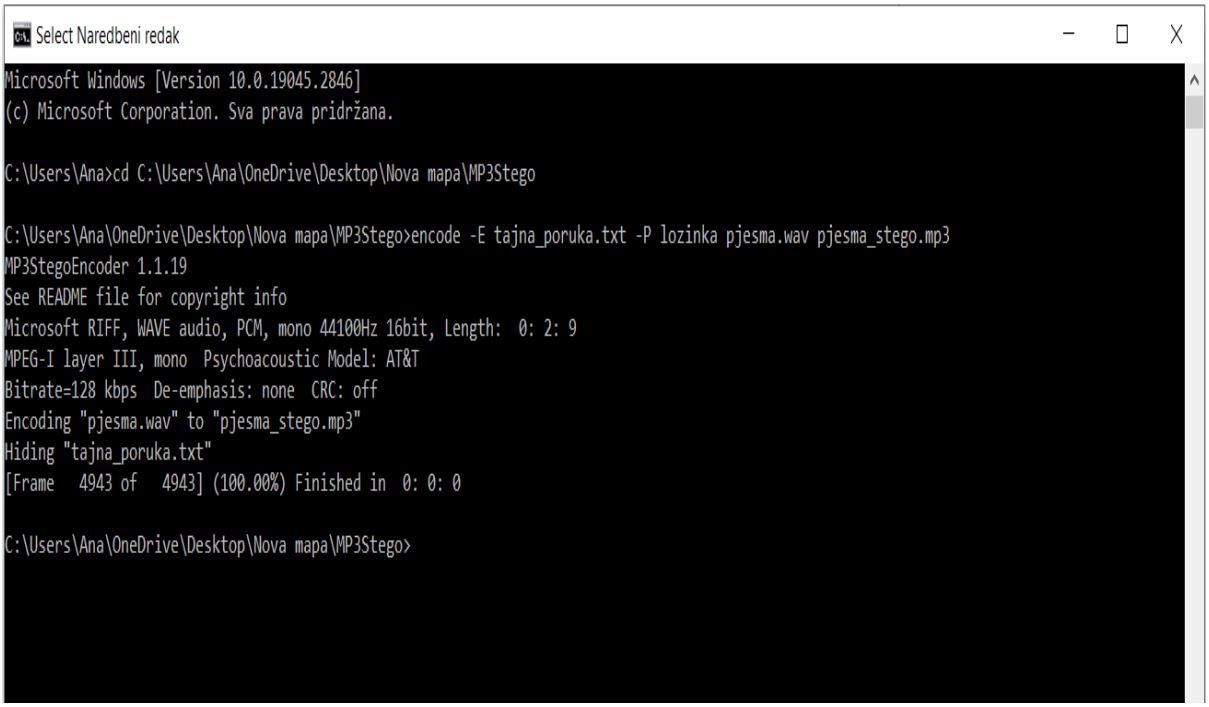
Linija za kodiranje upisuje se u sljedećom obliku:

encode –E tajna_poruka.txt –P lozinka audio_datoteka.wav stego_datoteka.mp3

Linija za dekodiranje upisuje se u sljedećem obliku:

decode –X –P lozinka stego_datoteka.mp3

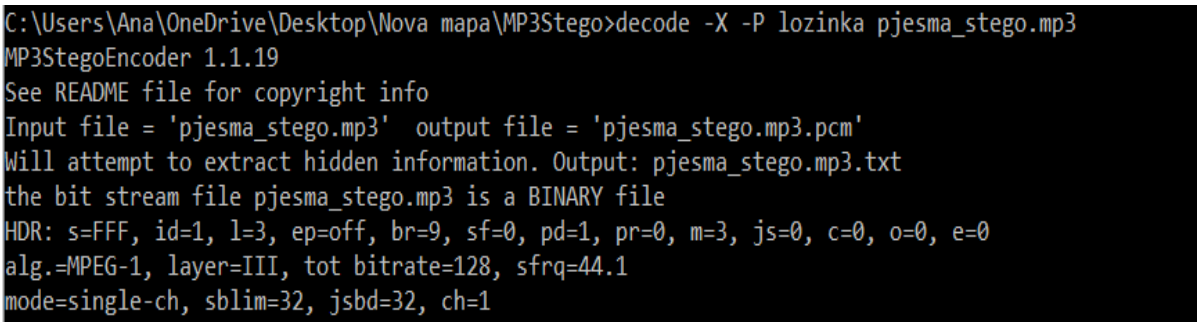
Na slici 5.29. prikazan je postupak kodiranja gdje je tajna poruka naziva tajna_poruka.txt, audio datoteka naziva pjesma.wav, a stego datoteka naziva pjesma_stego.mp3.



Slika 5.29.: Postupak skrivanja tekstualne datoteke u audio format

Ova linija sažima audio datoteku pjesma.wav (mono, 44,1kHz, 16-bitno kodirano) i skriva tajnu poruku koja se nalazi u datoteci tajna_poruka.txt. Tajna poruka šifrirana je korištenjem lozinke naziva „lozinka“. Kao izlazni rezultat nastala je datoteka pod nazivom pjesma_stego.mp3. Reproduciranjem datoteka pjesma.wav i pjesma_stego.mp3 ne može se čuti neko odstupanje da bi se primijetilo ugrađivanje tajne poruke, datoteke zvuče jednako.

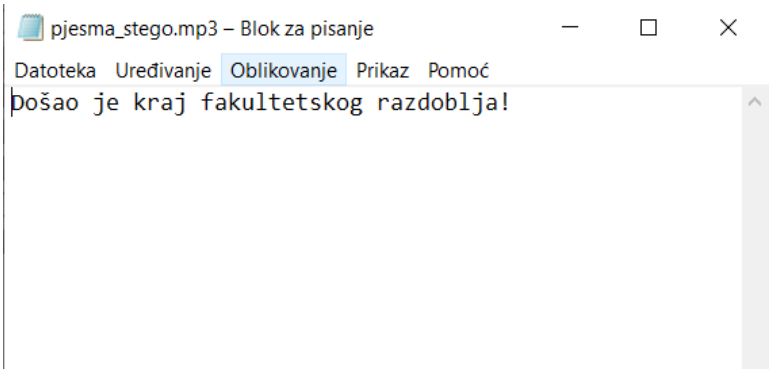
Na slici 5.30. prikazan je postupak dekodiranja, tj. izdvajanja tajne poruke iz stego datoteke.



Slika 5.30.: Postupak izdvajanja tajne poruke iz stego datoteke

Ovom se linijom dekomprimira stego datoteka pjesma_stego.mp3 u datoteku pjesma_stego.mp3.pcm i izdvajaju se tajne informacije. Skrivena se poruka tada dekriptira,

dekomprimira i sprema u pjesma_stego.mp3.txt datoteku. Otvaranjem tekstualne datoteke može se iščitati skrivena poruka, što je vidljivo na slici 5.31.



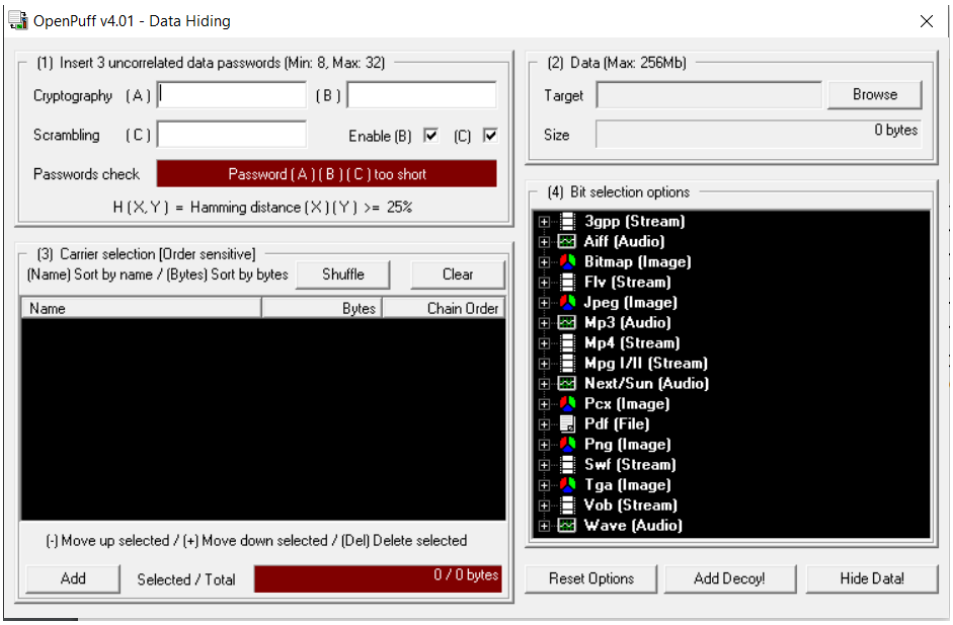
Slika 5.31.: Prikaz izdvojenog tajnog teksta

Ovaj alat podržava samo jednostavne poruke u txt formatu, a audio objekt nositelj mora biti u WAV formatu. Dakle, MP3Stego tekstualnu datoteku ugrađuje u WAV datoteku i pretvara u mp3.

5.2.4 Steganografija pomoću OpenPuff alata

OpenPuff besplatni je steganografski alat koji podržava razne formate objekta nositelja – slikovne datoteke (npr. BMP, JPG, PNG), audio datoteke (npr. WAV, MP3), video datoteke (npr. MP4, MPG), PDF i dr. Zbog svojih značajki, pogodan je za tajni prijenos osjetljivih podataka, tj. podataka visoke važnosti. Alat funkcionira na način da stvara slijed objekata nositelja gdje se tajni podatci dijele među njima. Ukoliko je dovoljno objekta nositelja na raspolaganju, moguće je tajno sakriti do 256 MB podataka. Koristi tehniku supstitucije bita najmanje važnosti. Samo poznavanje ispravnog slijeda objekata nositelja omogućava otkrivanje podataka. Posljednji objekt nositelj u slijedu nadograđuje se nasumičnim bitovima kako bi izgledao neprimjetno u odnosu na ostale. Prije ugrađivanja podataka, vrše se visoke mjere sigurnosti na tri razine – enkripcijom i kodiranjem pomoću tri ključa (A,B i C) i „izbjeljivanjem“, tj. miješanjem podataka s velikom količinom nasumičnog šuma. „Izbijeljeni“ podatci uvijek su kodirani korištenjem nelinearne funkcije koja kao ulaz koristi izvorne bitove objekta nositelja. Tako će modificirani objekti nositelji trebati manje promjena i zavarat će mnoge steganalitičke testove, [22].

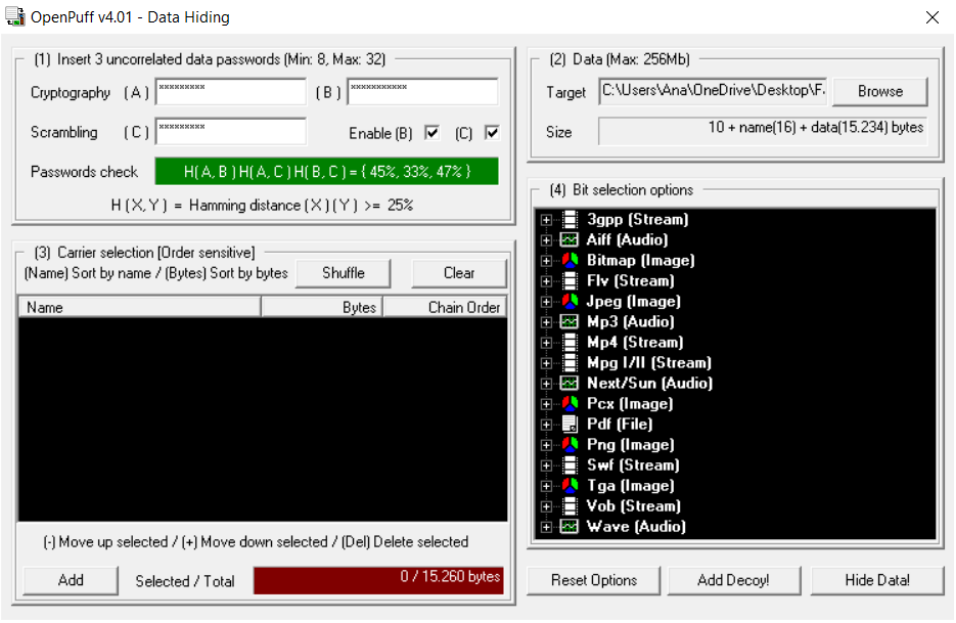
Kada se aplikacija pokrene i odabere se opcija skrivanja podataka, otvara se sučelje prikazano na slici 5.32.



Slika 5.32.: Sučelje OpenPuff alata prilikom skrivanja podataka [22]

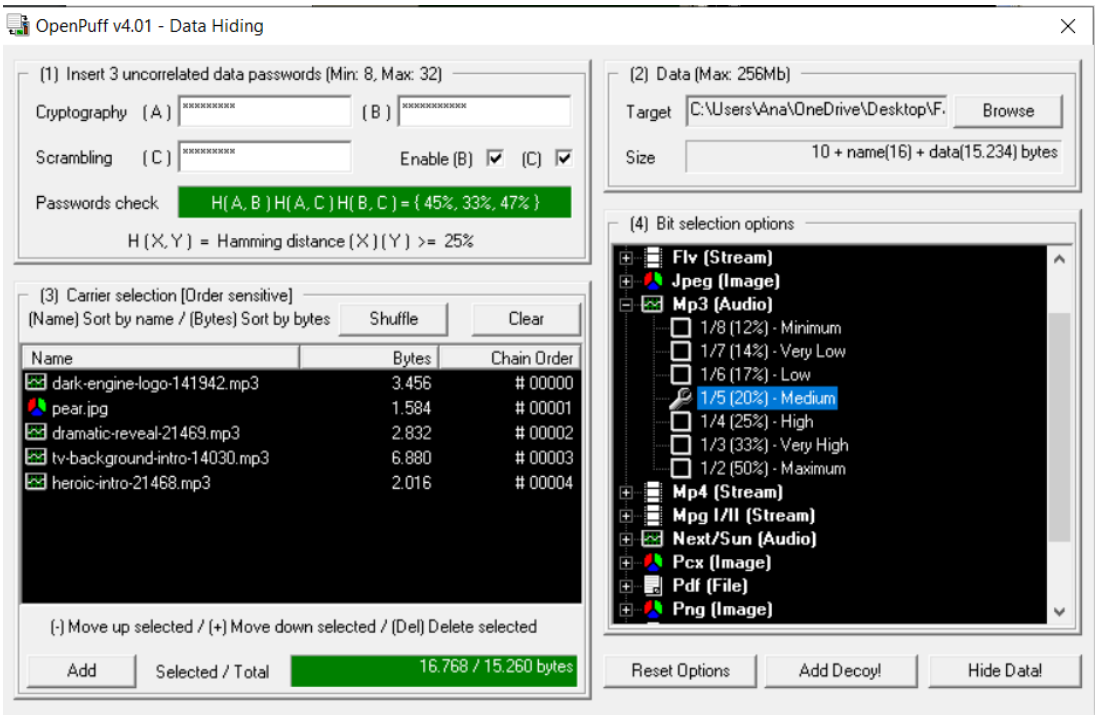
Kao prvi korak potrebno je odabrati tri lozinke kojima će se osigurati tajni podatci. Svaka lozinka mora biti drugačija (na bitnoj razini) i dugačka najmanje 8 znakova, a najviše 32 znaka. Ukoliko se bilo koja od lozinki približno podudara nekoj drugoj, neće biti moguće daljnje korištenje programa. Moguće je odabrati i korištenje samo jedne ili dvije lozinke, no treba uzeti u obzir da će se tada i razina sigurnosti tajnih podataka smanjiti. Odabrane su sljedeće lozinke: lozinka A „!1StegA5:“, lozinka B „di.PLO.ma23“, lozinka C „/seCurE!7“.

Drugi korak je odabir datoteke koja će biti tajna poruka maksimalne veličine 256Mb. U ovom primjeru odabrana je PDF datoteka naziva „LV4_-_Zadaci“. Na slici 5.33. prikazan je odabir lozinka i tajne poruke s izračunatom veličinom.



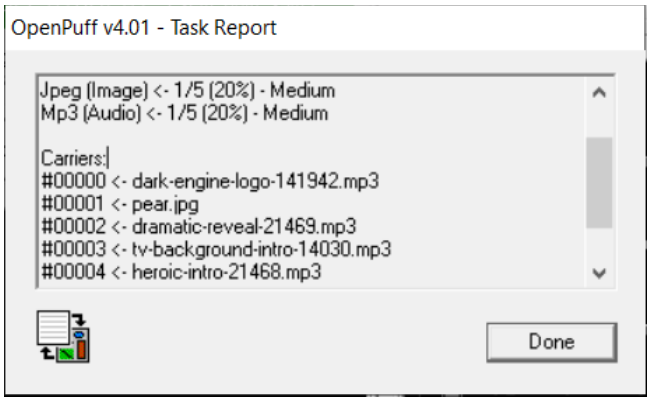
Slika 5.33.: Odabir lozinka i datoteka s tajnim podatcima

Treći je korak odabir slijeda objekta nositelja u koji će se ugrađivati tajni podatci. Nakon dodavanja dovoljnog broja objekta nositelja u slijed, moguće je odabrati opciju „nasumičan redoslijed“ (engl. *shuffle*) koja nasumičnim redoslijedom razmješta objekte nositelje u slijed. Odabrane su tri datoteke MP3 formata i jedna datoteka JPG formata čime je zadovoljena količina potrebnih podataka objekta nositelja. Četvrti je korak odabir razine odabira bitova koja bi trebala biti drugačija za svaki proces skrivanja. Odabrana razina je srednja (engl. *medium*), što znači da se koristi 20% bitova podataka, a ostalih 80% se „izbjeljuje“. Na slici 5.34. prikazan je izgled sučelja nakon izvršenih koraka tri i četiri.



Slika 5.34.: Odabrani koraci (3) i (4)

Nakon sva 4 izvršena koraka, odabire se opcije „Sakrij podatke!“ (engl. *hide data*) i direktorij u kojem će izlazne datoteke biti spremljene. Tada se izvršava cijeli proces ugrađivanja tajnih podataka i na kraju se prikaže izvještaj koji prikazuje odabrane razine i slijed objekta nositelja, kao što je vidljivo na slici 5.35.

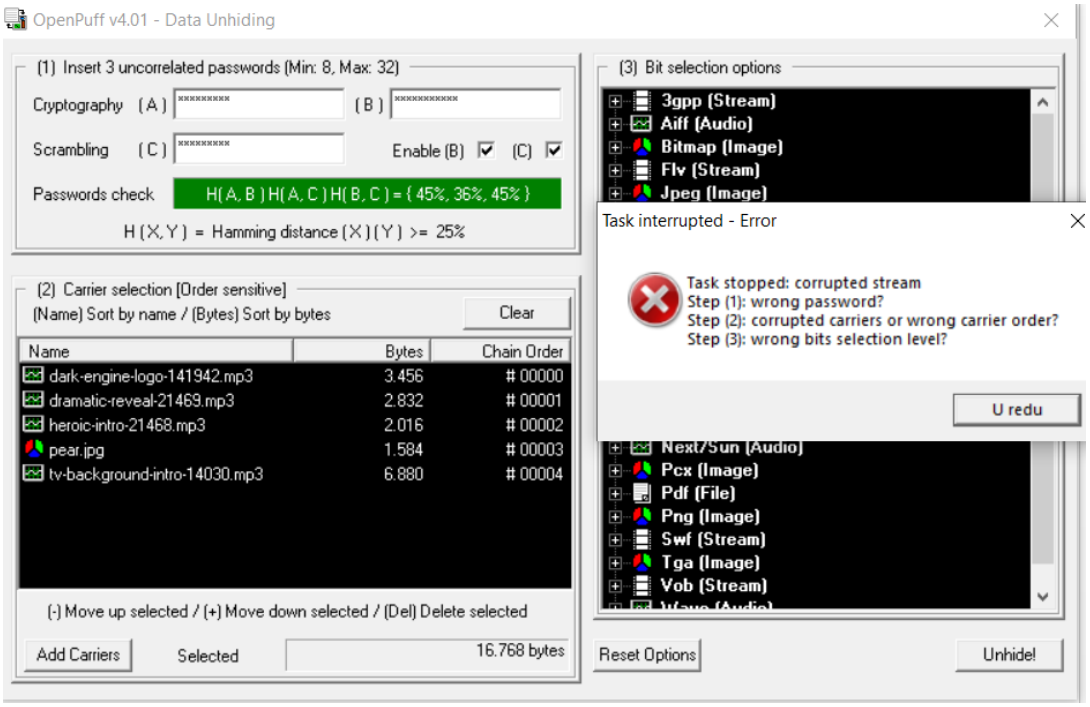


Slika 5.35.: Izvještaj o izvršenju zadataka

Datoteke s ugrađenim tajnim podatcima, tj. stego objekti, spremljene su u odabrani direktorij i njihovim pregledom ne može se uočiti neka primjetna razlika u odnosu na originalne objekte nositelje.

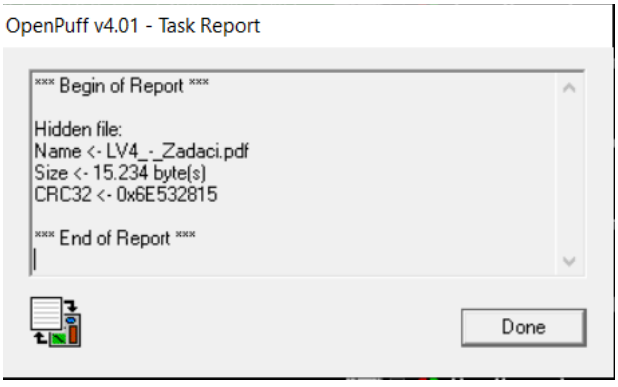
Kako bi se iz stego objekata izvukle ugrađene tajne informacije, potrebno je ponoviti prvi, drugi i treći korak. Dakle, unijeti odgovarajuće lozinke A, B i C, odabrati ispravan slijed

objekta nositelja i razinu. Ukoliko se bilo koji od tih koraka ne podudara s podatcima iz procesa skrivanja, tajne informacije neće se moći otkriti. To je vidljivo na slici 5.36. kada je odabran drugačiji redoslijed slijeda objekta nositelja nego prilikom skrivanja podataka. Prikazuje se upozorenje da nije moguće otkriti tajne podatke jer je jedan od koraka krivo odabran.



Slika 5.36.: Nemogućnost otkrivanja tajnih podataka zbog krivo odabranih koraka

Ukoliko su svi koraci ispravno odabrani, otkrivanje tajnih podataka bit će uspješno i na kraju izvršenja zadataka bit će prikazan izvještaj o uspješnosti kao što je prikazano na slici 5.37. Iz slike 5.37. može se iščitati da je otkrivena tajna datoteka pod nazivom „LV4_-_Zadaci.pdf“ što odgovara odabranoj datoteci prilikom skrivanja podataka. Otkrivena tajna datoteka spremljena je u odabrani direktorij i njenim pregledavanjem nisu uočena nikakva izobličenja, datoteka je jednaka izvornoj datoteci.

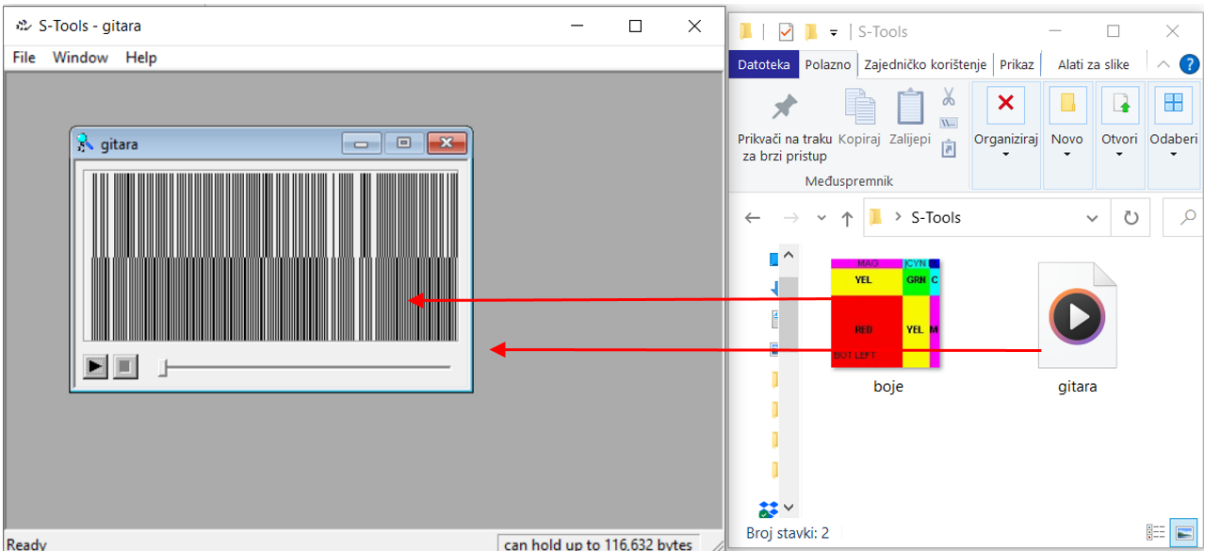


Slika 5.37.: Izvještaj o uspješnosti izvršenja otkrivanja tajnih podataka

5.2.5 Steganografija pomoću S-Tools alata

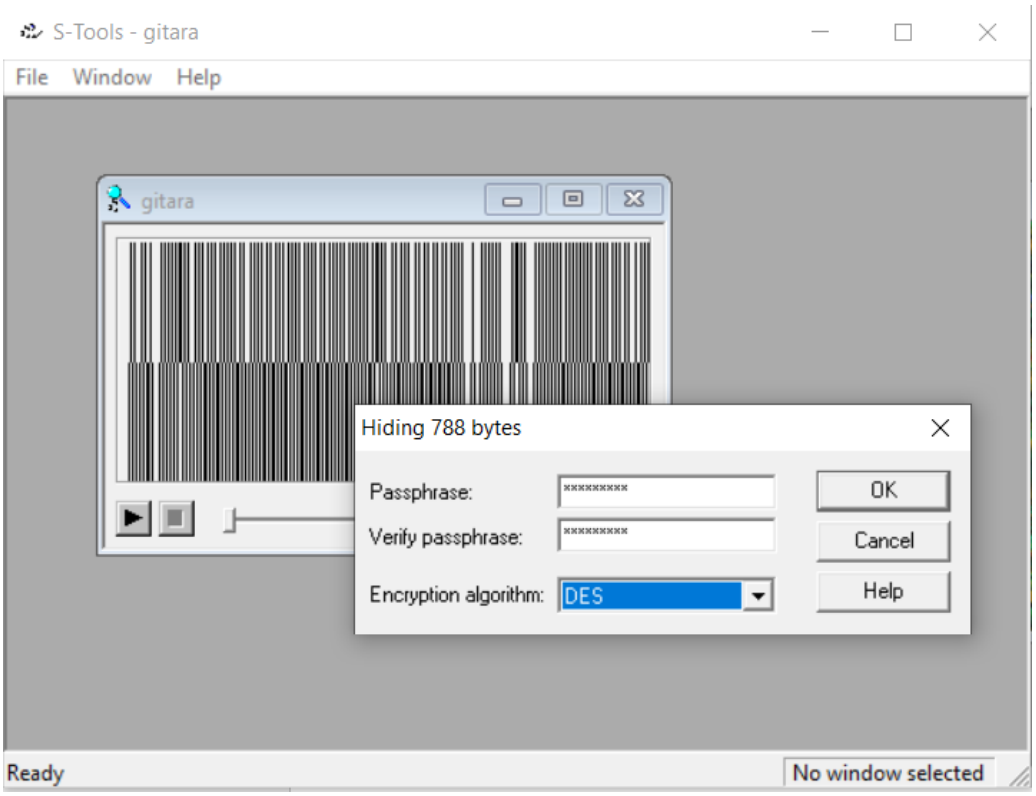
S-Tools steganografski je alat koji je kreirao Andy Brown. Pri korištenju ovog alata, objekt nositelj može biti GIF, BMP i WAV formata. Skrivanje tajnih informacija odvija se korištenjem tehnike supstitucije bita najmanje važnosti. Bitovi se odabiru nasumično korištenjem pseudo slučajnog generatora. S-Tools pruža izbor između različitih algoritama šifriranja tajnih podataka – DES (engl. *Data Encryption Standard*), IDEA (engl. *International Data Encryption Algorithm*), MDC (engl. *Message Digest Cipher*) i Triple-DES. Korištenje alata vrlo je jednostavno, temelji se na „povuci i ispusti“ tehnici (engl. „Drag and Drop“). [23]

Kada se otvori S-Tools alat, najprije se spomenutom tehnikom odabere objekt nositelj, u ovom primjeru to je zvukovna datoteka WAV formata naziva „gitara“. Nakon toga, na isti način odabire se tajna poruka koja će se ugraditi u objekt nositelj. U ovom primjeru to je slikovna datoteka BMP formata naziva „boje“. Opisani postupak prikazan je na slici 5.38.



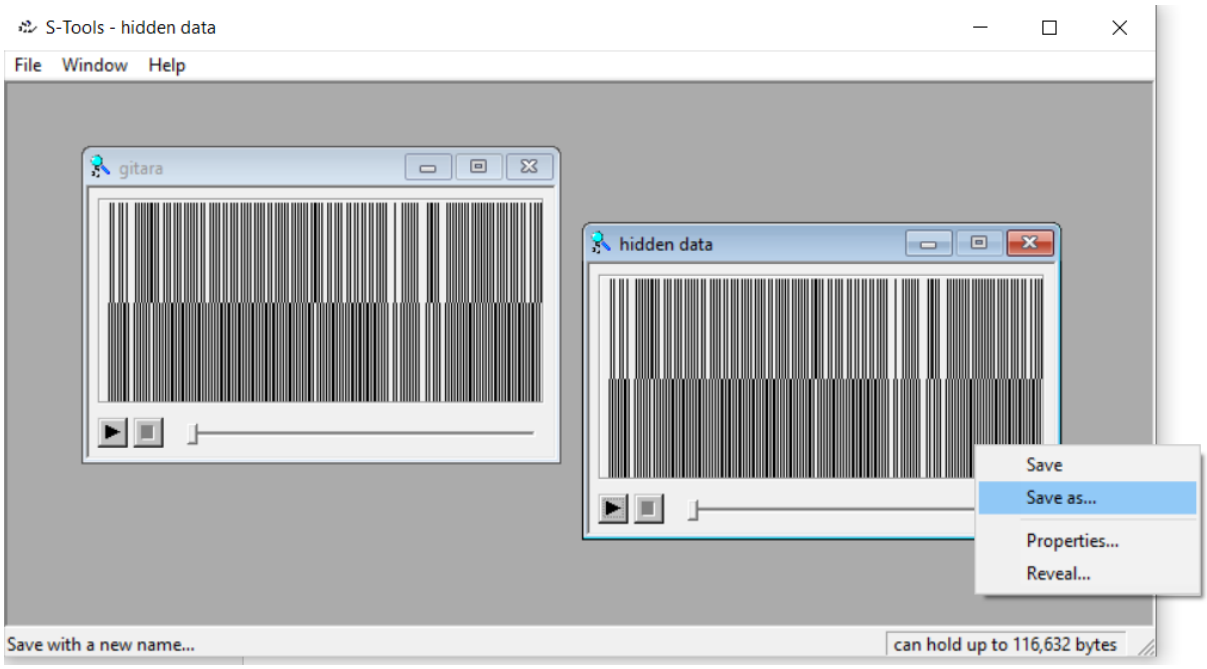
Slika 5.38.: Odabir objekta nositelja i tajne poruke u S-Tools alatu

Kada se odabere tajna datoteka, u sučelju se pojavi dijaloški okvir koji zahtijeva unos lozinke, koja se koristi za generiranje bitova pseudo slučajnim generatorom, i odabir algoritma za šifriranje. U ovom primjeru odabrana lozinka je „LozinkA13“, a odabrani algoritam DES, kao što je prikazano na slici 5.39. Također, vidljivo je da je se skriva 788 bajtova. Nakon toga, klikom na „OK“ pokreće se postupak ugradnje tajnih informacija.

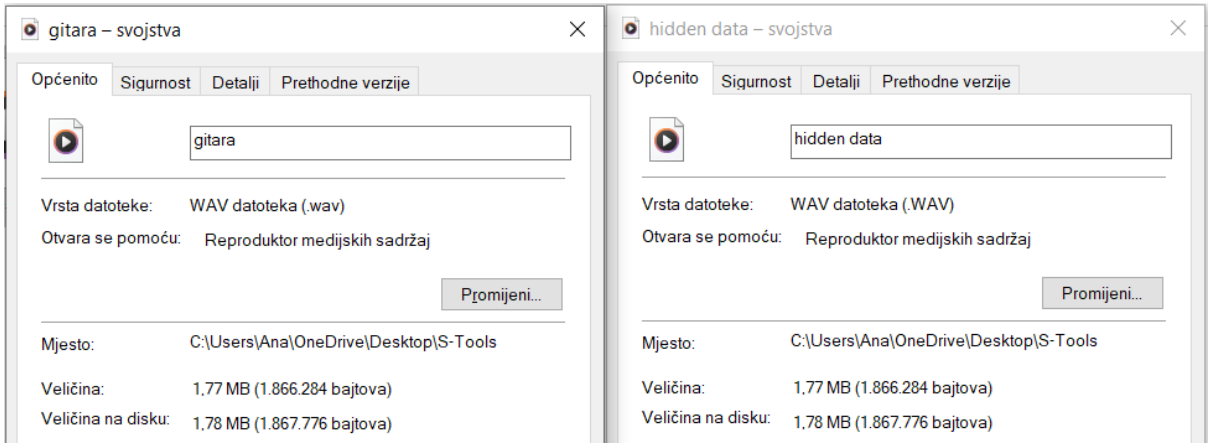


Slika 5.39.: Odabir lozinke i algoritma šifriranja tajnih podataka

Kada je proces ugradnje tajnih podataka izvršen, u sučelju alata pojavljuje se nova datoteka naziva „hidden data“, tj. stego objekt istog formata kao i objekt nositelj. Kako bi spremili nastali stego objekt u odabrani direktorij, potrebno je desnim klikom odabrati opciju „Spremi kao…“ (engl. „Save as…“), što je vidljivo na slici 5.40. Stego objekt izgledom i reproduciranjem ne odaje nikakve razlike u odnosu na original i ne privlači pažnju s potencijalnom sumnjom na skrivanje informacija. Također, na slici 5.41. prikazana su svojstva originalnog objekta nositelja i nastalog stego objekta ih koje je vidljivo da i veličina datoteke odgovara te da ni na taj način nastala stego datoteka neće biti sumnjiva potencijalnom napadaču.

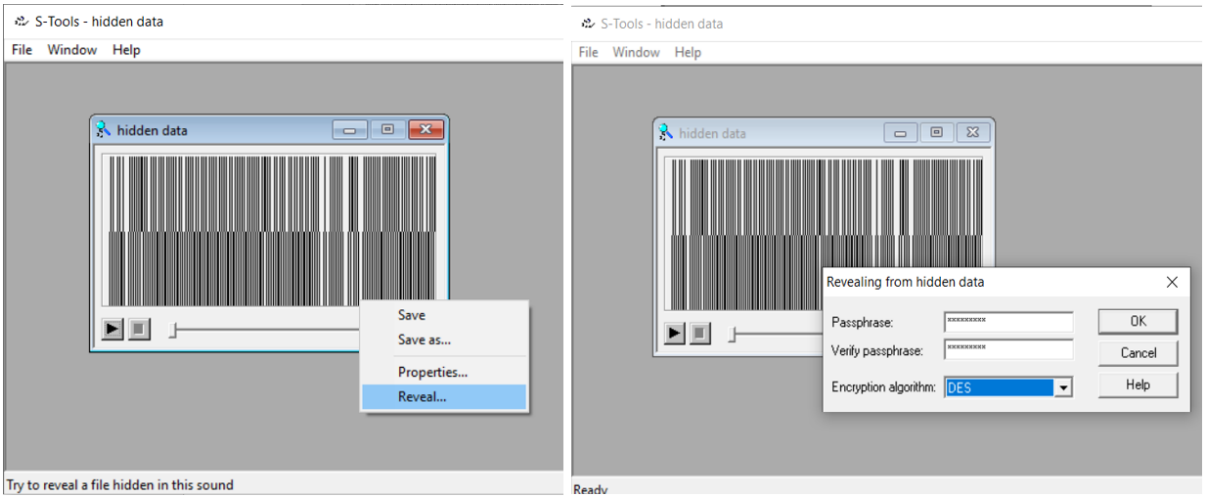


Slika 5.40.: Spremanje nastalog stego objekta



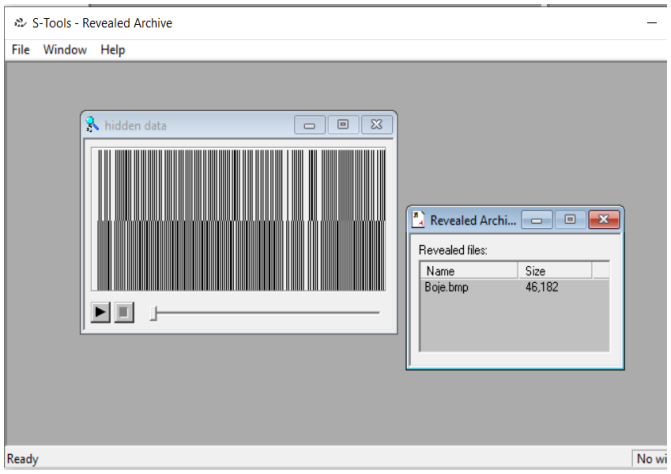
Slika 5.41.: Svojstva objekta nositelja i stego objekta

U obrnutom postupku, kako bi izdvojili tajne informacije iz stego objekta, potrebno je u sučelju učitati odabrani stego objekt, u ovom slučaju datoteku WAV formata naziva „hidden data“. Nakon toga, desnim klikom miša na učitanu datoteku odabire se opcija „Otkrij…“ (engl. „Reveal…“) pri čemu se pojavljuje dijaloški okvir koji zahtijeva unos lozinke i odabir algoritma šifriranja, što je vidljivo na slici 5.42. U ovom je koraku važno upisati jednaku lozinku kao i kod ugradnje tajnih informacija i odabrati jednaki algoritam šifriranja, u suprotnom će otkrivanje informacija biti neuspješno.



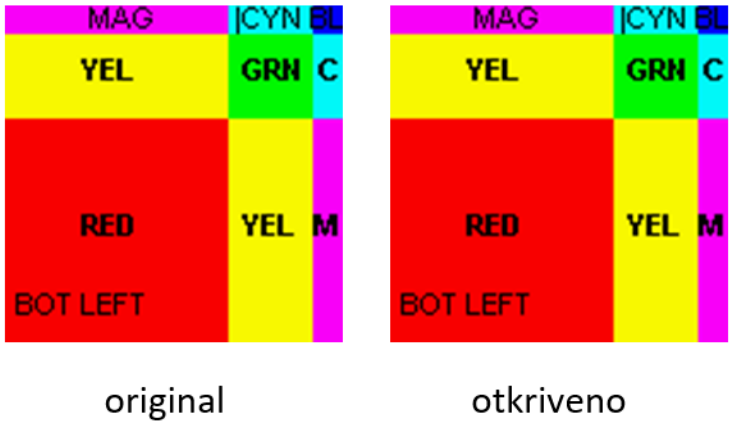
Slika 5.42.: Proces otkrivanja tajnih informacija iz stego objekta

Nakon uspješno unesenih podataka, u sučelju alata pojavljuje se novi dijaloški okvir s popisom i nazivom otkrivenih datoteka u stego objektu, slika 5.43. U ovom slučaju to je datoteka naziva „Boje.bmp“ što odgovara tajnoj datoteci koja je ugrađena u objekt nositelj.



Slika 5.43.: Otkrivene datoteke iz stego objekta

Spremanjem otkrivene datoteke u odabrani direktorij može se pregledati datoteka i provjeriti odgovara li originalnoj tajnoj datoteci koja je ugrađena. Slika 5.44. prikazuje usporedbu originalne datoteka koja se ugrađivala u objekt nositelj i datoteke koje je otkrivena iz stego objekta. Slike su identične, nema nikakvih izobličenja prouzrokovanih skrivanjem podataka i tajna informacija jasno se može iščitati.



Slika 5.44.: Tajna informacija prije i nakon ugradnje podataka

5.2.6. Steganografija pomoću SNOW alata

SNOW je steganografski alat koji koristi znak za razmak za skrivanje tajnih poruka u ASCII formatu u tekstualnim datotekama. Ugradnjom tajne poruke, dodaju se razmaci na kraj redaka. Program omogućava i korištenje lozinke za šifriranje kojom se osigurava tajna poruka od čitanja neovlaštene treće strane ukoliko se detektira njeno postojanje, [24].

Princip rada SNOW alata temelji se na činjenici da su razmaci i tabulatori, kada se pojavljuju na kraju redaka, nevidljivi prilikom pregledavanja teksta u većini programa za pregledavanje teksta. To omogućava skrivanje tajnih poruka bez utjecaja na vizualni izgled tekstualne datoteke.

Alat omogućava rad u 2 načina – ugrađivanje tajnih poruka i izdvajanje tajnih poruka. U procesu ugrađivanja tajnih poruka odvijaju se sljedeći koraci: izbor poruke, opcionalna kompresija, opcionalno šifriranje, ugrađivanje u tekst. U procesu izdvajanja tajne poruke koraci se odvijaju obrnuto: izdvajanje tajne poruke iz teksta, opcionalno dešifriranje, opcionalna dekompresija, prikaz poruke, [24].

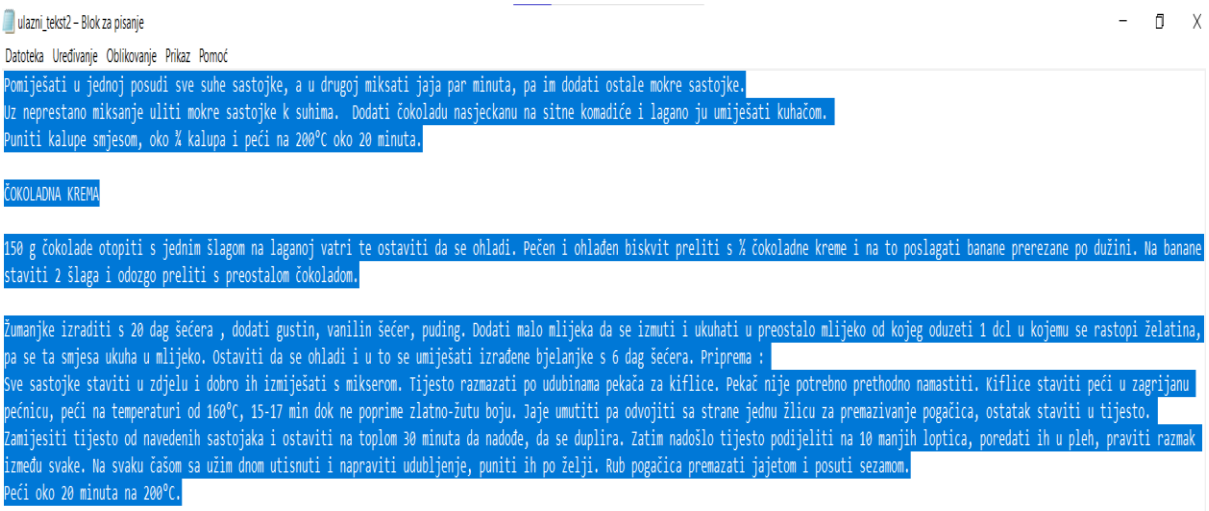
Podatci se zapisuju po 3 bita odjednom, dodavajući sekvence sa od 0 do 7 razmaka, ispresječene tabulatorima. Svaka poruka koja nije višekratnik 3 bita nadopunjava se nulama. Prilikom izdvajanja poruke, zadnji bit ili dva na kraju zanemaruju se. Tabulatori se koriste za odvajanje blokova razmaka te se 3 bita obično kodiraju u 8 stupaca teksta. Zadana duljina retka je 80 znakova, što omogućava pohranjivanje 30 bita u praznim redovima. Ako poruka ne stane u zadani tekst, dodat će se prazni redovi, [24].

Alat podržava kompresiju korištenjem Huffmanove tablice i šifriranje korištenjem ICE (engl. *Information Concealment Engine*) algoritama šifriranja.

Sljedeće opcije dostupne su u navedenom alatu: [24]

- -C – komprimira podatke prilikom ugrađivanja, dekomprimira prilikom izdvajanja
- -Q – tihi način rada; ukoliko nije postavljen, aplikacija će prikazati statistiku o postotku kompresije i dr.
- -S – izvješće o približnoj količini prostora dostupnog za skrivanje tajne poruke u tekstualnoj datoteci, pri čemu se uzima u obzir duljina linije
- -p – opcija za postavljanje lozinke za šifriranje podataka prilikom skrivanja ili dešifriranje prilikom izdvajanja poruke
- -f – sadržaj datoteke ugradit će se u ulaznu datoteku
- -m – sadržaj upisan pod ovom opcijom ugradit će se u ulaznu datoteku

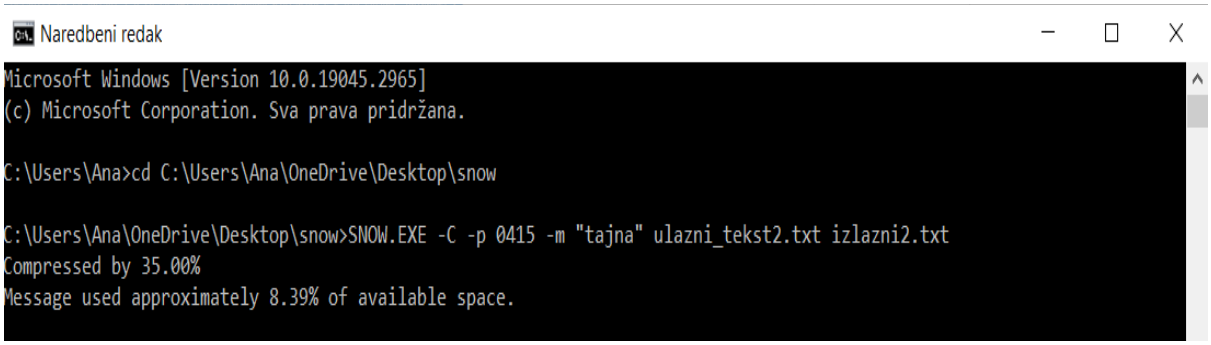
Primjer koji slijedi prikazat će opisani način rada ovog alata. Za početak je potrebno odabrati tekstualnu datoteku u koju će se ugraditi tajna poruka, tj. objekt nositelj. Odabrana je tekstualna datoteka naziva „ulazni_tekst2“, a njezin sadržaj prikazan je na slici 5.45.



Slika 5.45.: Sadržaj tajne poruke

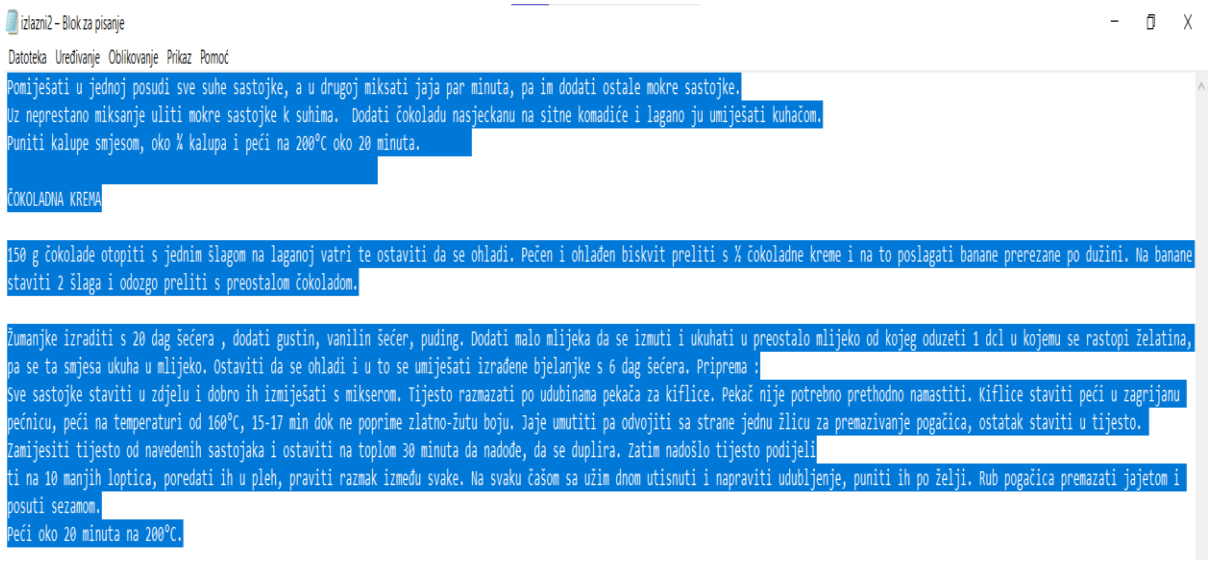
Nakon toga, potrebno je otvoriti Naredbeni redak u Windows operacijskom sustavu i pristupiti mapi u kojoj je preuzeta izvršna datoteka SNOW alata. Zatim se upisuje sljedeća naredba: „SNOW.EXE –C –p 0415 –m „tajna“ ulazni_tekst2.txt izlazni2.txt“. Redom kako je naredba pisana, njeno značenje je sljedeće: naredbenom retku se ukazuje na korištenje SNOW steganografskog alata, koristi se komprimiranje, koristi se lozinka za šifriranje koja glasi „0415“, ugrađuje se tajna poruka „tajna“ u tekstualnu datoteku „ulazni_tekst2.txt“, a izlazna

datoteka je naziva „izlazni2.txt“. Na slici 5.46. prikazano je izvršavanje navedene naredbe u Naredbenom retku.



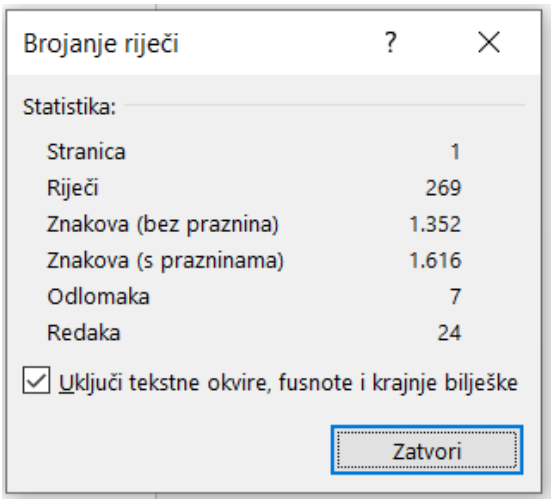
Slika 5.46.: Izvršavanje naredbe SNOW alata u Naredbenom retku

Nakon izvršavanja naredbe, aplikacija vraća povratne informacije. Prilikom ugrađivanja tajne poruke, izvršena je kompresija s postotkom od 35%, a tajna je poruka zauzela 8.39% od ukupnog raspoloživog prostora objekta nositelja. Otvaranjem nastalog stego objekta, i označavanjem teksta, vidljivi su dodatni razmaci koji su na prvu neprimjetni sve dok se sav sadržaj ne označi, slika 5.47.

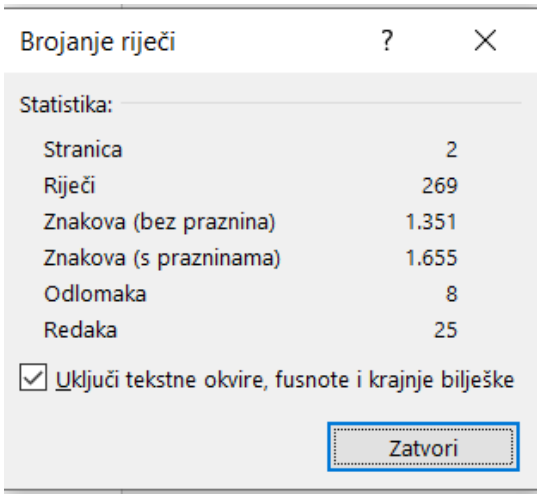


Slika 5.47.: Prikaz sadržaja stego objekta

Sadržaj tekstualnih datoteka objekta nositelja i stego objekta kopiran je u MS Word program za obradu teksta i otvoren je dijaloški okvir „Brojanje riječi“ za svaki od sadržaja. Na slici 5.48. prikazani su podatci za objekt nositelj, a na slici 5.49. podatci za nastali stego objekt. Iz podataka je vidljivo da je broj riječi ostao isti, ali broj znakova s prazninama veći je kod nastalog stego objekta, kao što je i očekivano. Također, broj odlomaka i broj redaka veći su za po 1 kod stego objekta.



Slika 5.48.: Statistika sadržaja objekta nositelja



Slika 5.49.: Statistika sadržaja stego objekta

Kako bi se iz nastalog stego objekta izdvojila ugrađena tajna poruka, u Naredbeni redak potrebno je upisati sljedeću naredbu: „SNOW.EXE –C –p 0415 izlazni2.txt“. Naredba označava sljedeće: Naredbenom retku ukazuje se na korištenje SNOW steganografskog alata, izvršava se dekompresija i izvršava se dešifriranje pomoću lozinke „0415“ na tekstualnoj datoteci naziva „izlazni2.txt“. Kao rezultat dobije se izdvojena tajna poruka „tajna“, što odgovara unesenoj poruci pri procesu ugrađivanja. Izvršavanje naredbe izdvajanja tajne poruke u Naredbenom retku prikazano je na slici 5.50.

```
C:\Users\Ana\OneDrive\Desktop\snow>SNOW.EXE -C -p 0415 izlazni2.txt
tajna
```

Slika 5.50.: Izvršavanje naredbe izdvajanja tajne poruke u Naredbenom retku

6. ZAKLJUČAK

Steganografija zbog svojih karakteristika i digitalizacije ima široko područje primjene, a dokazi o njenoj primjeni sežu daleko u prošlost. Zbog sigurnosti koju pruža, predstavlja alternativu kriptografiji. Ukoliko se uz steganografiju koristi i kriptografija, sigurnost cijelog sustava dodatno se povećava. Kada bi došlo do izdvajanja poruke iz stego objekta, potencijalnom napadaču ona bi bila nerazumljiva zbog kriptiranja. Kako bi sustav bio što efikasniji, potrebno je posvetiti pažnju pri odabiru objekta nositelja, koji se uglavnom sastoji od veće količine podataka nego tajna poruka koja se prenosi.

Postoje razne steganografske tehnike od kojih se neke temelje na odabiru objekta nositelja, a druge na odabiru modifikacije koja će biti učinjena na objektu nositelju prilikom ugradnje tajne poruke. U radu su detaljno analizirane tehnike s obzirom na učinjene modifikacije na objektu nositelju. Proučavanjem različitih tehnika, može se zaključiti da je najjednostavnija, a i najraširenija, tehnika koja se temelji se na supstituciji bita najmanje važnosti.

U radu su opisana i zapažanja o steganalizi, znanosti koja se bavi otkrivanjem i izdvajanjem tajnih poruka iz potencijalnih stego objekata, tj. naizgled bezazlenih informacija. Može se zaključiti da steganaliza služi i kao test sigurnosti steganografskog sustava jer ukazuje na njegove slabe točke. Steganalizom mogu se provesti i statistički testovi pomoću kojih se može odrediti približna veličina tajne poruke.

Istraživanjem o primjeni steganografije, zaključeno je da se ove tehnike sve više primjenjuju u ilegalne svrhe, a najviše u obliku različitih zlonamjernim softvera. Steganografske tehnike omogućavaju skrivanje postojanja dokaza, što kibernetičkim kriminalcima olakšava izvršavanje cilja. Steganografija se, naravno, primjenjuje i u korisne svrhe, poput očuvanja tajnosti podataka, medicine, digitalnih vodenih pečata i dr.

Prikazani su različiti praktični primjeri pomoću besplatno dostupnih steganografskih alata. Svaki od tih alata temelji se na nekoj od steganografskih tehnika, bilo da je riječ o modifikaciji objekta nositelja ili vrsti objekta nositelja. Rezultati su iskazani slikama. Većina primjera dala je zadovoljavajuće rezultate, naizgled identične stego objekte u usporedbi s originalnim objektom nositeljem. Kroz primjere je prikazana i važnost odabira odgovarajućeg objekta nositelja, tj. kako steganografska tehnike neće biti uspješna ukoliko se ne odaberu odgovarajući parametri.

LITERATURA

[1] CARNet CERT, LS&S, „*Steganografija*“, 2006., dostupno na: https://www.cert.hr/wp-content/uploads/2006/06/CCERT-PUBDOC-2006-04-154.pdf

[2] A. Choudary, „*Steganography Tutorial – A Complete Guide For Beginners*“, Edureka, 2023., dostupno na: https://www.edureka.co/blog/steganography-tutorial

[3] D. Kahn, „*The Codebreakers - The Story of Secret Writing*“, The New American Library, Inc., New York, 1973.

[4] K. Kristijan, „*Steganografija i steganaliza*“, završni rad, Sveučilište Jurja Dobrile u Puli, Fakultet informatike u Puli, Pula, 2019., dostupno na: https://repozitorij.unipu.hr/islandora/object/unipu%3A3533/datastream/PDF/view

[5] Z. Kh. AL-Ani, A. A. Zaidan, B. B. Zaidan, H. O. Alanazi, „Overview: Main Fundamentals for Steganography“, Journal of computing, br.3, sv.2, Ožujak, 2010., dostupno na: https://arxiv.org/ftp/arxiv/papers/1003/1003.4086.pdf

[6] M. Kharrazi, H. T. Sencar, N. Memon, „*Image Steganography: Concepts and Practice*“, Department of Electrical and Computer Engineering, Department of Computer and Information Science Polytechnic University, New York, USA, 2004., dostupno na: https://sharif.edu/~kharrazi/pubs/ims04.pdf

[7] S. Channalli, A. Jadhav, „*Steganography - An Art of Hiding Dana*“, Sinhgad College of Engineering, Pune, 2004., dostupno na: https://arxiv.org/ftp/arxiv/papers/0912/0912.2319.pdf

[8] S. Katzenbeisser, F.A. P. Petitcolas, „*Information Hiding Techniques for Steganography and Digital Watermarking“,* Artech house, USA, 2000.

[9] J.R. Krenn, „*Steganography and Steganalysis*“, 2004., dostupno na: https://www.krenn.nl/univ/cry/steg/article.pdf

[10] RapidTables, „*RGB Color Codes Chart*“, dostupno na:

https://www.rapidtables.com/web/color/RGB_Color.html

[11] T. Morkel, J.H.P. Eloff, M.S. Olivier, „*An overview of image steganography*“, Information and Computer Security Architecture (ICSA) Research Group, University of Pretoria, Pretoria, South Africa, 2005., dostupno na: http://martinolivier.com/open/stegoverview.pdf

[12] S. Rimac-Drlje, M. Vranješ, „*DCT i DWT transformacija*“, Multimedijski sustavi, FERIT, Osijek, 2021.
[13] A. Yahya, „*Steganography Techniques for Digital Images*“, Springer, Švicarska, 2019.

[14] Hussah N. AlEisa, "*Data Confidentiality in Healthcare Monitoring Systems Based on Image Steganography to Improve the Exchange of Patient Information Using the Internet of Things*", Journal of Healthcare Engineering, sv. 2022, 2022., dostupno na: https://doi.org/10.1155/2022/7528583
[15] Tutorials Point, „*What is the uses of Steganography?“,* 2022., dostupno na: https://www.tutorialspoint.com/what-is-the-uses-of-steganography

[16] U. Jawad, „*Pentagrams and "666" appear in DOOM's soundtrack in a spectrogram*“, Neowin, 2016., dostupno na: https://www.neowin.net/news/pentagrams-and-666-appear-in-dooms-soundtrack-in-a-spectrogram/

[17] T. Hunter, „*Steganography: The Undetectable Cybersecurity Threat*“, Built In, 2022. dostupno na: https://builtin.com/cybersecurity/steganography

[18] Intellipaat Software Solutions Pvt. Ltd.“*What is Steganography? A Complete Tutorial*“, 2023., dostupno na**:** https://intellipaat.com/blog/what-is-steganography/?US#no1

[19] L. Cameron, „*How steganography works*“, Computer Society Digital Library, dostupno na: https://www.computer.org/publications/tech-news/research/how-steganography-works

[20] J. Stanley, „*Image Steganography*“, Tech Makers, dostupno na:

https://incoherency.co.uk/image-steganography/
[21] F. Petitcolas, „*The information hiding homepage*“, 2018., dostupno na:

https://www.petitcolas.net/steganography/mp3stego/

[22] Embbeded SW, „*OpenPuff –Steganography*“, dostupno na:

https://embeddedsw.net/OpenPuff_Steganography_Home.html

[23] Flylib, „*S-Tools Tutorial*“, dostupno na: https://flylib.com/books/en/1.496.1.144/1/

[24] M. Kwan, „*The SNOW*“, Darkside Technologies, 2013., dostupno na: https://darkside.com.au/snow/

SAŽETAK

U ovom su diplomskom radu navedene i opisane različite tehnike steganografije te su prikazani različiti praktični primjeri. Opisana su osnovna načela steganografije, povijest steganografije, podjela steganografije i detaljno je objašnjen princip rada steganografskih tehnika. Navedene su i opisane tehnike steganalize. Nadalje, navedeni su mogući načini primjene steganografskih tehnika, kao i neki od primjera tih primjena iz stvarnog života. Za prikaz praktičnih primjera korišteni su različiti besplatni steganografski alati koji se temelje na nekoj od steganografskih tehnika. Za svaki od primjera opisan je postupak i način korištenja alata, a dobiveni rezultati prikazani su slikama.

KLJUČNE RIJEČI: steganografske tehnike, steganaliza, primjena steganografije, steganografski alati

ABSTRACT

Steganography – practical examples

In this master thesis, various steganography techniques are listed and described along with a few practical examples. The basic principles of steganography, the history of steganography, the division of steganography and the working principle of steganographic techniques are explained in detail. Steganalysis techniques are listed and described. Furthermore, possible ways of applying steganographic techniques are listed, as well as some examples of these applications from real life. Various free steganographic tools based on some of the steganographic techniques were used to show practical examples. For each of the examples, the procedure and method of using the tool is described, and the obtained results are shown in pictures. Conclusion is given on various techniques and their application in real life.

KEYWORDS: steganographic techniques, steganalysis, steganography applications, steganography tools