|  |
| --- |
|  |
| Steganografija |
|  |
|  |
|  |
|  |

|  |
| --- |
| Jelena Lukić 1219 |

Sadržaj

[Uvod 3](#_Toc99667621)

[Šta je steganografija? 3](#_Toc99667622)

[Steganografija kroz istoriju 5](#_Toc99667623)

[Moderna steganografija 6](#_Toc99667624)

[Tehnike steganografije 6](#_Toc99667625)

[UBACIVANJE 7](#_Toc99667626)

[ZAMENA 7](#_Toc99667627)

[GENERISANJE 7](#_Toc99667628)

[Metode steganografije 7](#_Toc99667629)

[HTML STEGO METODA 8](#_Toc99667630)

[LSB METODA 9](#_Toc99667631)

[SPREAD SPECTRUM METODA 10](#_Toc99667632)

[WHITE SPACE METODA 11](#_Toc99667633)

[DIGITALNI VODENI PEČAT (WATERMARK) 11](#_Toc99667634)

[Stegoanaliza 12](#_Toc99667635)

[Zaključak 13](#_Toc99667636)

[Literatura 14](#_Toc99667637)

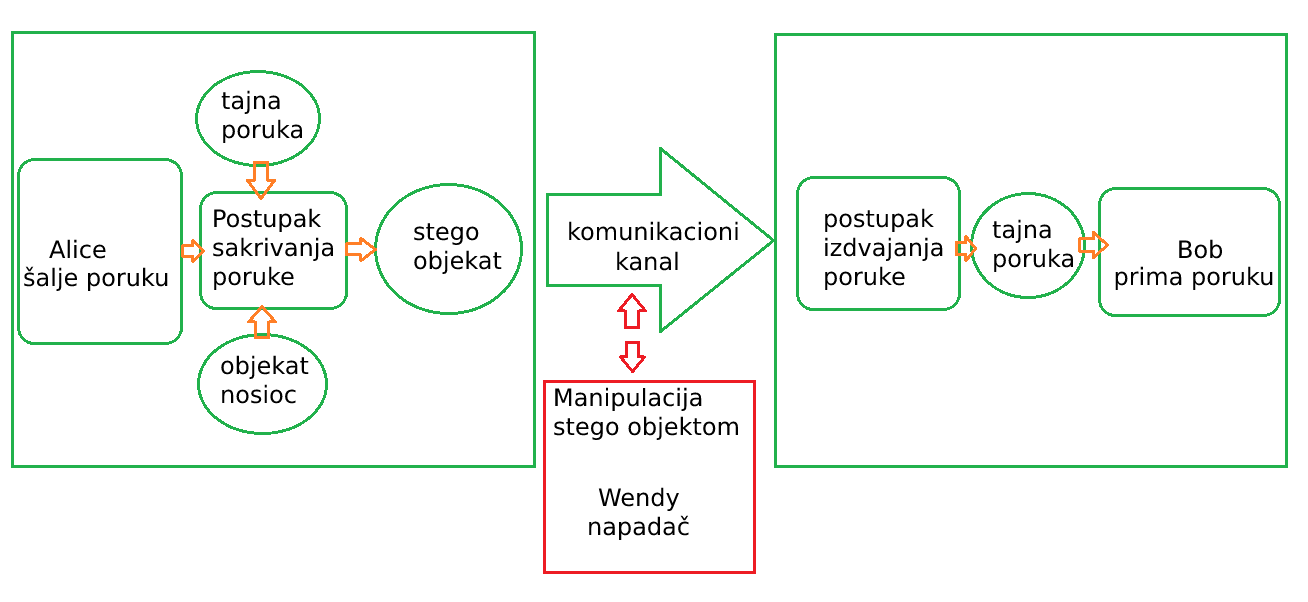
# Uvod

Steganografija datira još iz vremena pre nove ere. U ovom radu biće pomenuti najzanimljiviji primeri njenog razvijanja kroz istoriju. Pojavom masovne upotrebe kompijutera i interneta steganografija doživljava ekspanziju. Usko je povezana sa kriptografijom i najbolje je kada se koriste u kombinaciji. Cilj steganografije je uspešno prenošenje tajne poruke do krajnjeg cilja pomoću nekog drugog sadržaja, tako da niko ne primeti da se komunikacija uopšte desila. U ovom radu biće obrađene najpoznatije tehnike i metode prenošenja tajne poruke pomoću bezazlenog medija. Takođe biće prikazan osnovni princip steganografije kao i stegoanalize koja se bavi otkivanjem tajnih poruka u odredjenoj datoteci. Web aplikacija koja je priložena uz ovaj rad detaljnije obrađuje temu sakrivanja teksta u slici LSB metodom.

# Šta je steganografija?

Steganografija je naučna disciplina koja proučava metode skrivanja poruke unutar nekog medija bezazlenog sadržaja. Takođe, steganografija predstavlja veštinu zapisivanja poruke na takav način da niko osim onoga ko je poslao poruku i onoga kome je poruka namenjena ne primeti da se komunikacija desila. Naziv ove veštine potiče iz grčkih reči *seganos* i *graphein*, koje u prevodu znače skriveno pisanje. Steganografija je jako slična kriptografiji, obe nauke se koriste kao sredstva za prikrivanje informacija. Za razliku od kriptografije, steganografija ne menja samu informaciju već je kamuflira i samim tim ne privlači pažnju na nju.

Osnovni principi steganografije se mogu predstaviti kroz jednostavni primer pod nazivom *problem zatvorenika*. Alice i Bob su zatvorenici koji planiraju bekstvo iz zatvora. Wendy je upravnik zatvora. Alice i Bob se nalaze u različitim delovima zatvora i mogu da komuniciraju samo pisanim putem. Sve poruke koje međusobno razmenjuju kontroliše upravnik. Zatvorenici moraju da razmenjuju poruke koje nisu sumnjivog sadržaja kako bi plan bekstva ostao u tajnosti. Wendy, koji kontroliše komunikaciju, može pokušati da otkrije da li postoji skriveni sadržaj poruka i može da promeni sadržaj istih. Sam pokušaj otkrivanja skrivenog sadržaja predstavlja pasivan napad. Menjanje sadržaja poruke predstavlja aktivan napad. Ako Wendy namerno izmeni poruku i prosledi je zatvorenicima to se smatra zlonamernim napadom.



Slika 1: Šematski prikaz steganografskog sistema.

Na slici 1 predstavljen je šematski prikaz steganografskog sistema. Alice šalje tajnu poruku Bobu. Ona je sakrila tajnu poruku tako što je umetnula u objekat nosioc i time dobija stego objekat. Stego objekat se prenosi komunikacionim kanalom do Boba koji zna kako da izdvoji sadržaj tajne poruke. Na slici vidimo i treću osobu, Wendy, koja može da manipuliše stego objektom. Wendy može da prisluškuje komunikacioni kanal ili da modifikuje sadržaj stego objekta. Cilj napadača je da otkrije da li objekat koji se prenosi komunikacionim kanalom sadrži tajne poruke. Ako otkrije da tajna poruka postoji, on može da je izdvoji ili može da utiče na stego objekat tako da se tajna poruka izgubi.

Postupak skrivanja, odnosno izdvajanja poruke može biti tajni ili javni. Ukoliko je postupak javni, često se koristi dodatni ključ koji određuje tačan redosled umetanja poruke. Ključ se razmenjuje sigurnim komunikacionim kanalom. Na taj način se izbegava da napadač dođe do tajne poruke. Osim toga preporučuje se da poruka bude kriptovana nekim algoritmom kako bi imala dodatnu zaštitu. Bitno je naglasiti da je osnovni cilj napadača detektovanje poruke, a ne nužno i dešifrovanje. Pretpostavlja se da napadač može da manipuliše stego objektom i tako naruši tajnu komunikaciju.

Koliko je neki steganografski sistem siguran zavisi od toga koliko je otporan na pasivne, aktivne i zlonamerne napade. Siguran sistem ispunjava sledeće uslove:

- Algoritam za sakrivanje poruke je javan, ali se korisi tajni ključ

- Samo onaj ko poseduje tajni ključ može da detektuje i pročita poruku

- Ako napadač zna sadržaj jedne poslate poruke, mala je verovatnoća da će otkriti sadržaj preostalih poruka

- Detekcija tajne poruke je hardverski prezahtevna

Ponekad i sistem koji ima javni algoritam sakrivanja, a ne koristi tajni ključ može da se koristi za komunikaciju i smatraće se relativno bezbednim. To se odnosi na sisteme koji koriste velike količine podataka jer se tada ne mogu analizirati svi objekti nosioci informacija. Nepostojanje ključa je u tim situacijama olakšavajuća okolnost jer nije potrebno na siguran način prenositi tajni ključ.

# Steganografija kroz istoriju

Prvi zapisani slučaj steganografije datira 440 godina pre nove ere. Herodot je naveo dva primera steganografije u svome delu *Herodotova istorija*. U delu je navedeno kako je Demaratus poslao upozorenje o predstojećem napadu na Grčku zapisivanjem poruke na drveni kalup voštane ploče za pisanje, pre izlivanja voska. Voštane ploče su se koristile kao papir, jer su mogle ponovo da se upotrebe. Drugi drevni primer je priča o Histaeusu i njegovom vernom robu na čiju je glavu Histiaeus ispisao poruku i sačekao da mu kosa poraste. Kasnije je rob tu poruku neprimećeno preneo kako bi pokrenuo ustanak protiv Persijanaca.

Prošlo je puno vremena pre nego što su zabeleženi složeni oblici steganografije. U 4. veku pre nove ere Aneas Tacticus spomenuo je tehniku bušenja rupa. Filo iz Vizantije bio je prvi koji je raspravljao o nevidljivim bojama kojima je pisao u 3. veku pre n. e. On je koristio orahe za pisanje nevidljivog teksta i bakar sulfat kako bi ga otkrio.

Izraz steganografija prvi put se koristi u knjizi *Stefanografija* čiji je autor Johannes Trithemius. Ovo je bila knjiga koja se navodno bavila magijom, ali je koristila kriptografiju i steganografiju da sakrije svoj stvarni sadržaj. Nakon Trithemiusove smrti 1518. godine izdata je knjiga *Polygraphia* koja je detaljnije objasnjavala steganografiju u praksi.

Godine 1605. Frabcus Bacon osmislio je Baconovu šifru i to se smatra ključnim u razvoju ove nauke. Ova šifra koristila je dva različita slova za kodiranje tajne poruke.

Mikrodoti su prvi put razvijeni na kraju 19. veka, ali nisu se intenzivno koristili za steganografiju do Prvog svetskog rata. Oni podrazumevaju smanjivanje poruke ili slike do veličine tačke.

Tokom godina razvio se širok spektar tehnika. Steganografija je nastavila svoj razvoj i u digitalnoj eri.

# Moderna steganografija

Moderna steganografija podrazumeva skrivanje tajnih poruka unutar digitalnih fajlova. Digitalna tehnologija daje puno mogćnosti da se steganografija primeni. Najzastupljeniji oblik je skrivanje informacija u digitalnoj slici. Sve digitalne datoteke se čuvaju kao nizovi bitova. Redundantni bitovi ne nose informacije koje su važne za datoteku, tako da mogu biti neprimetno zamenjeni bitovima koji nose informaciju koju želimo da sakrijemo. Nisu sve digitalne datoteke pogodne za sakrivanje informacija. Nekada su svi bitovi datoteke važni, kao što je slučaj sa izvršnim verzijama programa, pa bi i najmanja promena makar jednog bita mogla da onesposobi program.

# Tehnike steganografije

Sa gledišta nauke, steganografija se može podeliti na tehničku i lingvističku. Tehnička se bavi metodama za otkrivanje steganografskog uzorka u pisanom tekstu ili mikrofilmovima, dok lingvistička steganografija obuhvata tehnike skrivanja podatka u datoteci na način da originalna datoteka bude verodostojna stego-datoteci. Lingvistička steganografija se može podeliti na semagrame i otvorene kodove.

Semagrami se baziraju se na upotrebi simbola i znakova za skrivanje poruka, a mogu biti vizuelni i tekstualni. Vizuelni semagrami za generisanje skrivene poruke koriste svakodnevni raspored predmeta i objekata u prostoru, dok tekstualni za skrivanje koriste različite modifikacije teksta na nosiocu podataka. To može biti suvišan razmak između reči, promena veličine i boje fonta i sl. Otvoreni kodovi koriste razne načine prenosa skrivene poruke. Dele se na žargonski kod i skrivene šifre. Žargonski kod koristi predefinisane fraze pri komunikaciji koje su poznate samo osobama koje komuniciraju. To mogu biti unaprijed dogovoreni pojmovi i sl. Skrivene šifre predstavljaju steganografsku tehniku kod koje se skrivena poruka može izdvojiti iz stego-datoteke samo u slučaju ako je poznata metoda kojom je skrivena informacija utisnuta u datoteku. Skrivene šifre se dele na rešetkaste i na nulte kodove. Princip rada rešetkastih šifara bazira se na šablonima koji se koriste za skrivanje poruke u nosiocu, dok se metoda nultog koda bazira na usvajanju određenog pravila za umetanje podataka u nosiocu podataka. To može biti izuzimanje svakog neparnog reda ili svake parne reči u redu i sl. U steganografiji postoji nekoliko različitih tehnika koje se mogu koristiti za skrivanje informacija u datotekama. To su:

 Zamjena (Substitucija) i

 Generisanje (Generation)

- Ubacivanje (Injection ili Insertion)

- Zamena (Substitucija) i

- Generisanje (Generation)

## UBACIVANJE

Ova tehnika omogućava skrivanje postojanja podataka u delovima datoteka koji su od manjeg značaja za zlonamernog korisnika. Tehnika se temelj na dodavanju bitova u datoteke tako da površinski deo datoteke ostane savršeno čist. Dodavanjem određenog broja dodatnih bezopasnih bitova u izvršnu datoteku neće bitno uticati na proces koji se izvršava, a prisustvo metode neće se odraziti na konačan ishod metode, tako da krajnji korisnik ne može osetiti prisustvo skrivenog podatka u datoteci. Međutim, upotreba tehnike umetanja menja veličinu datoteke u zavisnosti od ukupnog broja ubačenih bitova, što može dovesti da neuobičejeno velika datoteka izazove određenu pažnju kod zlonamernog korisnika.

## ZAMENA

ZAMJENA

Pristup zamene zasniva se na zameni najmanje značajnih bitova datoteke, i to na takav način da primena ove metode ima što manji efekat na originalnu datoteku. Glavna prednost ove tehnike je u tome što se veličina datoteke ne menja prilikom primene algoritma. S druge strane, ova metoda ima i dva nedostatka. Prvi je degradacija steganografski obrađene datoteke i ograničenje broja manje značajnih bitova koji se mogu upotrijebiti za primenu ove metode.

GENERISANJE

## GENERISANJE

Nedostatak kod prethodno pomenutih tehnika je taj što se originalna slika može porediti sa stego slikom i tom prilikom moguće je otkriti razlike. Tehnika generisanja ne zahteva originalnog nosioca podataka, već sama generiše datoteku u kojoj će biti sadržana poruka. Kada se koristi tehnika generisanja konačan rezultat je originalna datoteka koja je imuna na komparaciju sa drugim datotekama.

# Metode steganografije

U suštini, steganografija koristi ograničene sposobnosti našeg vizuelnog sistema. Bilo koji otvoreni ili šifrovani tekst, slika i slično korišćenjem određenih metoda može biti utisnut u određenu sliku nosioca podataka, a da to ne bude vidljivo golom okom. Postoji više metoda koje se koriste za skrivanje informacija unutar teksta, slike, audio ili video datoteke. Neke od metoda koje se koriste u steganografiji su:

 HTMLstego

 LSB(leastsignificantbit)

 SS(SpreadSpectrum)

 DCT(DiskretnaKosinusnaTransformacija)i

 WS(WhiteSpace)metoda

- HTML stego

-LSB (least significant bit)

-SS (Spread Spectrum)

-DCT (Diskretna Kosinusna Transformacija)

-WS (White Space) metoda

3.1. HTML STEGO METODA

## HTML STEGO METODA

Ova metoda koristi tehniku zamene. Bazira se na skrivanju informacija u izvornom HTML kodu tako da podaci koji se prezentuju korisniku ostaju nepromenjeni. Tehnika se zasniva na zameni bitova manje važnih identifikatora decimalnog oblika koji se odnosi na boju teksta sa njihovim ekvivalentima u tekstualnom obliku. Sledeći primjer pokazuje kako se steganografija koristi prilikom pisanja HTML koda.

Dat je izvorni tekst:

“Your quest objective is Erratic Sentries, which roam the northeast section of the Isle. After you have killed them, use the provided Attuned Crystal Cores. This will reactive the Arcane Sentries to turn them into friendly units.”

Your quest objective is Erratic Sentries,

which roam the northeast section of the Isle. font>

After you have killed them,

use the provided Attuned Crystal Cores.

This will reactive the Arcane Sentries

to turn them into friendly units.

Your quest objective is Erratic Sentries,

which roam the northeast section of the Isle. font>

After you have killed them,

use the provided Attuned Crystal Cores.

This will reactive the Arcane Sentries

to turn them into friendly units.

Your quest objective is Erratic Sentries,

which roam the northeast section of the Isle. font>

After you have killed them,

use the provided Attuned Crystal Cores.

This will reactive the Arcane Sentries

to turn them into friendly units.

Your quest objective is Erratic Sentries,

which roam the northeast section of the Isle. font>

After you have killed them,

use the provided Attuned Crystal Cores.

This will reactive the Arcane Sentries

to turn them into friendly units.

Izvorni kod u HTML-u:

<font color="#01001100"> Your quest objective is Erratic Sentries,</font><br/>

<font color="#01000000"> which roam the northeast section of the Isle. font><br/>

<font color="#01010010"> After you have killed them,</font><br/>

<font color="#01000001"> use the provided Attuned Crystal Cores.</font><br/>

<font color="#01000110"> This will reactive the Arcane Sentries</font><br/>

<font color="#01000000">which roam the northeast section of the Isle. font><br>

<font color="#01010010">After you have killed them,</font><br>

<font color="#01000001">use the provided Attuned Crystal Cores.</font><br>

<font color="#01000110">This will reactive the Arcane Sentries</font><br

Steganografski obrađen kod bi bio ovakav:

<font color="#01001110">Your quest objective is Erratic Sentries,</font><br/>

<font color="#01000001">which roam the northeast section of the Isle. font><br/>

<font color="#01010000">After you have killed them,</font><br/>

<font color="#01000001">use the provided Attuned Crystal Cores.</font><br/>

<font color="#01000100">This will reactive the Arcane Sentries</font><br/>

<font color="#01001110">Your quest objective is Erratic Sentries,</font><br>

<font color="#01000001">which roam the northeast section of the Isle. font><br>

<font color="#01010000">After you have killed them,</font><br>

<font color="#01000001">use the provided Attuned Crystal Cores.</font><br>

<font color="#01000100">This will reactive the Arcane Sentries</font><br>

Skrivena poruka glasi: 01001110 01000001 01010000 01000001 01000100, što u prevodu

znači: NAPAD.

HTML metoda se najviše koristi za obmanu računara koji u potrazi za informacijama pretražuju Internet.

## LSB METODA

LSB (Least Significant Byte), ili bit najmanje težine, je metoda koja koristi tehniku zamene vrednosti najmanje značajnih piksela u binarnom obliku. U datoteci se obično nalazi nekoliko bitova koji nisu stvarno potrebni, ili na određeni način nisu toliko važni. Ti bitovi u datotekama mogu poslužiti za prenos skrivenih informacija na taj način da neće bitno promeniti datoteku ili je oštetiti. LSB metoda najbolju primenu je našla u slikovnim datotekama koje imaju visoku rezoluciju uz upotrebu različitih boja, i u audio datotekama koje reprodukuju različite zvukove na velikim brzinama. LSB metoda obično ne povećava veličinu datoteke, ali zavisno od veličine informacije koja se skriva, može primetno deformisati datoteku. Za skrivanje informacija u slikama upotrebom LSB metode najčešće se koriste 24-bitne BMP slike. Slika treba da bude različitih boja i inteziteta svetlosti na različitim delovima. Razlog tome je što je u sliku visokog kvaliteta i rezolucije mnogo lakše sakriti informcije nego u sliku niskog kvaliteta. Iako je 24 bitna slika najbolja za skrivanje informacija, zbog svoje veličine i česte primene može se upotrebiti 8-bitna BMP slika ili eventualno drugi format slike, kao što je GIF. Razlog tome je što postavljanje slika velikih formata na Internetu može probuditi sumnju potencijalnih napadača i samim tim ugroziti komunikaciju. Važno je napomenuti, da će skrivena informacija unutar slike biti izgubljena ako se izvrši konverzija slike iz jednog formata u drugi. Ako je slika veličine 3264 x 1840 = 6.005.760 piksela, i ako se uzme u obzir da se za svaki kanal uzima po jedan bajt, a u ovom slučaju se koriste R, G i B kanali, onda je za skladištenje 6.005.760 piksela potrebno 18017280 bajtova, odnosno 144138240 bitova. Upotrebom svakog osmog bajta za skrivanje sadržaja dokumenta koji se utiskuje u nosioca podataka dobija se rezultat do 2252160 bajtova, odnosno 2,14 MB prostora za skrivanje podataka. Ako se pomoću ove računice uzme slika 2 čija stvarna veličina iznosi 5.454.969 bitova, odnosno, 5.20 MB, dolazimo do zaključka da je koeficijent iskorišćenja slike 41 %, tj., 2.252.160 / 5.454.969 = 0.412863.



Slika 2: Originalna slika i slika nakon obrade

## SPREAD SPECTRUM METODA

Ova metoda koristi tehniku ubacivanja a zasniva se na širenju frekvencijskog spektra signala u određenom domenu. Koristi slabosti koje imaju ljudski organi čula. Takođe, koristi se i za kontrolu bezbednosti komunikacionog kanala, povećanje otpornosti na prirodne smetnje, sprečavanje otkrivanja i za ograničenje snage određenih prenosnih linkova. U audio steganografiji implementacija je moguća pažljivim biranjem audio sadržaja u koji se utiskuju podaci. Trenutne steganografske aplikacije koje koriste ovu metodu su pre svega ograničene na potvrdu dokaza o autorskim pravima, kao i garancijama integriteta sadržaja. Ova metoda se koristi i u audio steganografiji i to za WAV i AIFF formate koji koriste 16-bitnu linearnu kvantizaciju primenjenu za distorziju prenosnog signala. Pošto se koristi tehnika zamene niskih talasa, slično kao kod LSB metode, problem kod ove metode je što su niski talasi uočljivi za ljudsko uho tako da je ovo praktično prilično ranjiva metoda. Ova metoda radi na dodavanju šumovi u slučajne odabrane signale. Informacije se kriju unutar nosača i širi se preko frekvencijskog spektra. Slična ovoj metodi je i ECHO metoda koja takođe koristi tehniku ubacivanja podataka. Ova metoda za skrivanje informacija koristi odjeke u audio datotekama. Princip rada se zasniva na jednostavnim ubacivanjem dodatnog zvuka buke unutar audio datoteka u kom je sadržana informacija. Ono što ovu metodu izdvaja od ostalih audio-steganografskih metoda je to da se zapravo audio zvuk unutar datoteke može dodatno poboljšati.

## WHITE SPACE METODA

White Space metoda je još jedna steganografska metoda koja se bazira na tehnici

White Space metoda je još jedna steganografska metoda koja se bazira na tehnici

Ova metoda je još jedna steganografska metoda koja se bazira na tehnici ubacivanja. Dodatnim dodavanjem belog prostora unutar pisanog teksta na listovima papira jednostavnim pritiskom tastera “space” na tastaturi, običnom korisniku verovatno neće izazvati pažnju. Prazni prostori su uobičajena pojava u svim dokumentima koji se svakodnevno koriste, pa je primena ove metode veoma efikasna za većinu tekstualnih datoteka. Ova metoda se može primenjivati u skoro svim datotekama u kojima je smešten tekst za čitanje: doc, pdf, rtf. Za detekciju white space metode koristi se program koji se zove SNOW.

## DIGITALNI VODENI PEČAT (WATERMARK)

Digitalni vodeni pečat (wathermark) predstavlja digitalni identifikator ili digitalni pečat na podatku, koji se koristi zbog autorizacije izvora nosioca podataka. Najčešće se koristi radi odbrane od softverske i muzičke piraterije. Postoji više vrsta wathermark-a:

-nevidljivi

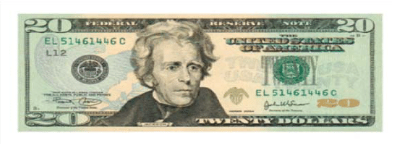
-vidljivi

-robusni

-osetljivi

Nevidljivi wathermark se utiskuje u nosioca podataka tako da on za korisnika nije vidljiv golim okom. Vidljivi wathermark je vidljiv golim okom i on može da nosi neku konkretnu oznaku kao što je TOP SECRET ili sl. Robustni wathermark je čitljiv za korisnika i u slučaju napada ne menja svoju strukturu. Osetljivi wathermark je sličan robustnom, samo što kod njega u slučaju napada dolazi do samouništenja samog pečata.

Wathermark se može ugrađivati i u digitalnu sliku. Nevidljivi wathermark veličine jednog kvadratnog inča je dovoljan da cela fotografija dimenzija 1024x768 stane u njega. Prilikom oštećenja, iz neoštećenog dela fotografije može se izvaditi nevidljivi wathermark i na osnovu njega rekonstruisati cela slika. Naša moneta sadrži zaštitnu nit kao zaštitno sredstvo protiv kopiranja, ali samo U.S. moneta sadrži wathermark u obliku slike koji se vidi pod odgovarajućim svetlom. Prikazano na slici 3.



Slika 3. Moneta sa vidljivim robusnim wathermarkom

Na domaćem tržištu još uvijek je u određenoj meri prisutna softverska i muzička piraterija. Internet nudi neiscrpnu bazu nelegalnog digitalnog materijala. Uvođenjem digitalnih vodenih pečata u izvorne nosioce podataka sigurno će se redukovati broj piratskog materijala koji se može naći na crnom tržištu. Utiskivanjem robustnog nevidljivog pečata u digitalnu muziku može se ući u trag originalnom izvoru ako se piratska muzika pojavi na Internetu. Ako je u audio fajl dodat osjetljivi nevidljivi pečat on se neće kopirati. Kopiranjem se narušava integritet podatka zbog toga što osjetljivi nevidljivi pečat nije kopiran i fajl neće biti čitljiv. Često se primjenjuje kombinacija više pečata, npr. nevidljivi i vidljivi robustni.

# Stegoanaliza

Umetnost ili veština otkrivanja steganografski obrađenih datoteka naziva se stegoanaliza. Cilj svake stegoanalize je da otkrije mogući umetnuti podatak koji je pomoću određene steganografske tehnike i metode ubačen u nosioca podatka. Postoji više metoda koje se koriste pri stegoanalizi datoteka. Najčešće korišćene su:

-metoda vizuelnog pregleda

-Audio-reproduktivna i

-Softverska metoda

Metoda vizuelnog pregleda se odnosi na slikovne i tekstualne datoteke. Zasniva na pronalaženju istih detalja iz različitih izvora podataka, njihovom poređenju sa potencijalnom stego-datotekom i sumiranjem razlika. Audio-reproduktivna metoda sa zasniva na uzastopnom preslušavanju istih audio datoteka na različitim brzinama. Pri izboru audio datoteka mora se voditi računa o stepenu kompresije koji je upotrebljen pri kompresiji u potencijalnoj steganografski obrađenoj audio datoteci (MP3). Ako se dođe do zaključka da se prostim okom ne mogu utvrditi bitne razlike između potencijalne steganografske i originalne datoteke, u tu svrhu se može primeniti softverska metoda, koja podrazumeva upotrebu određenog steganografskog alata. Neki od njih su: Xsteg, Jsteg, Stegoanalisys, Camouflage, Stegalyzer, ImageHide, TiPi, Steganography i sl.

# Zaključak

Voštane pločice i nevidljiva tinta samo su neke od steganografskih tehnika koje su se koristile još od grčkog doba kao način skrivenog prenosa informacija. Dolaskom modernog doba i digitalne tehnologije, steganografija dobija sasvim novu dimenziju upotrebe. Razvijaju se efikasne tehnike i metode koje omogućuju pouzdan i siguran prenos skrivenih informacija.

Svaka od navedenih metoda ima svoje prednosti i nedostatke. Tako je LSB metoda najčešće korišćena metoda koja pruža prenos velikog kapaciteta skrivenog sadržaja, ali bilo kakva konverzija formata multimedijskog nosioca znači gubitak skrivene informacije.

Bolje rezultate na konverziju multimedijskog nosioca daju metode koje nisu zavisne od toga koji je format slike tako da skrivena informacija ostaje sačuvana i nakon izvršene konverzije. Steganografija predstavlja alternativu kriptografiji. Kriptovana informacija, koliko god dobro zaštićena bila, skreće pažnju napadača i uvek postoji verovatnoća njenog otkrivanja. S obzirom na veliku količinu multimedijskog sadržaja na mrežama, nemoguće je analizirati i detektovati svaki steganografski sadržaj.

Međutim, treba voditi računa da slika bude visoke rezolucije i kontrasta te da skrivena poruka ne bude prevelika kako nebi došlo do deformacije nosioca. Ako se uzme u obzir da većina steganografskih programskih alata ima mogućnost kriptovanja sadržaja tako da tajna poruka nije vidljiva napadaču, informacija je dobro zaštićena, čak ako napadač i izdvoji skriveni sadržaj on je i dalje kriptovan i nerazumljiv. Pored navedenih prednosti, steganografija ima i svoje nedostatke.

Za prenos skrivene poruke kanalom uvek je potrebno koristiti nosioc koji sam po sebi nosi puno veću količinu podataka nego što nosi sama poruka. Takođe, pojavljuju se problemi kao što su osetljivost pri manipulaciji s podacima, kompresiji ili rotaciji slike i sl.. S obzirom da se jako teško detektuje, vrlo brzo je postala zanimljiva osobama koje se bave raznim ilegalnim i kriminalnim aktivnostima. Bez obzira na brojne prednosti i mogućnosti primene, ova tehnika zaštite podataka još uvek nije u potpunosti iskorišćena. U budućnosti se očekuje njen ubrzani razvoj. Uz male modifikacije ima perspektivu da postane jedna od najboljih sigurnosnih tehnika.

# Literatura

Cole, E., Hiding in Plain Sight, Steganography and the Art of Covert

Communication, Wiley, 2003

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

Peter Wayner, Disappearing cryptography Information hiding: Steganography & watermarking, Morgan Kaufmann, 2008.

Abid Yahya, Steganography Techniques for Digital Images, Springer, 2019.

Kharrazi, M.; Sencar, H.T.; Memon, N.: Image steganography: Concepts and practice, WSPC / Lecture Notes, Polytechnic University, Brooklyn, New York, 2004.

Katzenbeisser, S., Information Hiding Techniques for Steganography and Digital

Milosavljević, M. i Grubor, G., Osnovi bezbednosti i zaštite informacionih sistema

Univerzitet Singidunum, 2006.

Mirolsav Ćajić, Bogdan Brkić, Mladen Đuro Veinović, Analiza steganografskih tehnika i metoda, Jul , 2010

Watermarking, Artech House, 1999.