|  | **Univerzitet u Nišu, Elektronski fakultet**  **Katedra za računarstvo** |  |
| --- | --- | --- |

**Anđela Kričak**

**Steganografija slike**

**Seminarski rad**

**Niš, 2024. godina**

**Sadržaj**

[Uvod 3](#_Toc159181502)

[Steganografija kao pojam 4](#_Toc159181503)

[Steganografija kroz istoriju 4](#_Toc159181504)

[Komponente steganografske poruke 5](#_Toc159181505)

[Steganografski pristupi 6](#_Toc159181506)

[Pure Steganography 6](#_Toc159181507)

[Private key steganography 6](#_Toc159181508)

[Public key steganography 6](#_Toc159181509)

[Tehnike steganografije 7](#_Toc159181510)

[Ubacivanje 7](#_Toc159181511)

[Zamena 8](#_Toc159181512)

[Generisanje 8](#_Toc159181513)

[Steganografija slike 8](#_Toc159181514)

[Metode steganografije slike 9](#_Toc159181515)

[Steganografija slike pomoću diskretne kosinusne transformacije 10](#_Toc159181516)

[Poznati alati za steganografiju pomoću slike 11](#_Toc159181517)

[Primer korišćenja alata OpenStego 12](#_Toc159181518)

[Zaključak 15](#_Toc159181519)

[Literatura 16](#_Toc159181520)

# Uvod

Potreba za skrivanjem sadržaja poruke koja se prenosi putem posrednika postojala je od davnina, a poseban značaj imala je u ratovima. U doba kada je komunikacija bila ograničena na primitivne načine komuniciranja, putem goluba ili glasnika, bilo je neophodno biti izuzetno dovitljiv, kako poruka od značaja, u slučaju presretanja ne bi bila pročitana i zloupotrebljena.

Danas postoje izuzetno napredni vidovi komunikacije, ali je takođe i presretanje, kao i dešifrovanje samih poruka unapređeno. Sa napretkom tehnologije, razvili su se različiti načini skrivanja značajnih poruka od “čoveka u sredini”, odnosno lica kome nije namenjena.

Steganografija podataka predstavlja jedan od savremenih načina skrivanja poruke unutar neke druge, beznačajne poruke. Pomoću različitih metoda, omogućava se bezbedan prenos podataka od značaja, od pošiljaoca do primaoca, ali tako da se i njihov identitet skriva. Ona predstvalja nauku, ali i umetnost skrivene komunikacije između dve strane.

Kroz ovaj rad, biće ukratko objašnjen sam pojam steganografije, steganografski pristupi, tehnike steganografije, pojam steganografije slike i neke od najznačajnijih metoda steganografije slike. Takođe, upotrebom jednog od poznatijih alata, biće praktično objašnjena steganografija pomoću slike.

# Steganografija kao pojam

Steganografija je nauka koja se bavi skrivanjem informacija u drugim podacima, tako da je i samo postojanje šifrata sakriveno u nosiocu podatka. Reč steganografija je kovanica od dve reči grčkog porekla, στεγανοσ (steganos) i γραφο (grafo), što u prevodu znači pisati skriveno. Cilj steganografije je da prenese informacije od pošiljaoca do primaoca, tako što se podatak utisne u nosioca podatka, koji mora da bude čitljiv i razumljiv za odredište.

Za razliku od kriptografije, gde je neprijatelju omogućeno da presretne poruku i pokuša da je promeni, odnosno, naruši njen integritet, steganografija je nauka i umetnost razmene osetljivih ili privatnih podataka, koja skriva postojanje tajne komunikacije, tako da neprijatelj ili “čovek u sredini” neće posumnjati da postoji skrivena poruka.

Pored kriptografije, postoje još dve metode, koje se često dovode u vezu sa steganografijom, a to su *watermark* i *fingerprint.* “Vodeni žig” je obično potpis za identifikaciju porekla i sve kopije su označene na isti način, dok *fingerprint* svaku kopiju čini jedinstvenom za primaoca, jer se dodaje na sam sadržaj radi obeležavanja i zaštite autorskih prava ili autentičnosti.

# 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. 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.

Još jedna klasična primena drevne steganografije je metoda zamotavanja traka oko drvenog štapa od vrha do dna. Ključ ove metode jeste odgovarajuća debljina štapa, jer će samo pomoću nje biti moguće dešifrovati poruku. Takođe, važno je napomenuti da postojanje same poruke nije definitivno, jer se od pošiljaoca do primaova prenosi samo traka.

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 objašnjavala 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 predstavljaju jednu od prvih modernih metoda steganografije i prvi put su razvijeni na kraju 19. veka, ali nisu se intenzivno koristili do Drugog svetskog rata. Oni podrazumevaju smanjivanje poruke ili slike do veličine tačke, pri čemu se ta poruka sakriva u naizgled bezazlen tekst.

Nagli razvoj steganografije dogodio se ranih devedesetih kada su industrije, građani, pa čak i neke od ekstremističkih organizacija počele da koriste softverske aplikacije za ugrađivanje poruka i fotografija u različite vrste medija kao što su digitalne fotografije, digitalni video zapisi, audio datoteke i tekstualne datoteke.

# Komponente steganografske poruke

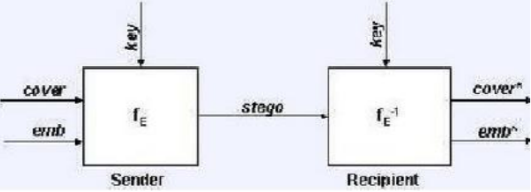
Postoje tri komponente koje svaka steganografska poruka poseduje i to su:

1. *Secret message*
2. *Cover data*
3. *Stego message*

“Tajna poruka” se odnosi na deo poruke koji treba da bude sakriven. Ovo poruka će kasnije biti šifrovana, kako bi bilo još komplikovanije doći do otvorene poruke.

Sledeći deo je komponenta *cover data*. Ovo komponenta se odnosi na “kontejner” tj. omot u kome je skrivena tajna poruka i to mogu biti bilo koji podaci, poput digitalnih fotografija, digitalnih video zapisa, audio datoteka i tekstualnih datoteka.

Poslednja komponenta je *stego* poruka koja je ključna kao i tajna poruka i ona se odnosi na finalni proizvod, koji se prenosi komunikacionim putem.



Slika 1. Prikaz steganografskog Sistema

# Steganografski pristupi

Postoje različite vrste steganografskih pristupa i neke od njih su:

* *Top-down* pristup
* *Bottom-up* pristup.

Ovi pristupi su ponovo podeljeni na podslojeve, pa je *top-down* pristup podeljen na:

* Pure steganography
* Private key steganography
* Public key steganography

Ove kategorije saopštavaju nivo sigurnosti sa kojim je stego poruka ugrađena, preneta i pročitana.

## Pure Steganography

Definiše se kao steganografski sistem koji ne zahteva razmenu šifre kao što je stego-ključ. Ovaj metod steganografije je najmanje bezbedno sredstvo za tajnu komunikaciju, jer pošiljalac i primalac mogu biti bezbedni samo pod pretpostavkom da treća strana nije upoznata sa ovom tajnom porukom.

U ovom pristupu *stegobject* sadrži samo omot i skrivenu poruku.

## Private key steganography

Ova tehnika koristi tip skrivenog ključa, koji se naziva tajni ključ. Stegoobjekat sadrži omot, skrivenu poruku i tajni ključ. Samo strane koje znaju tajni ključ mogu da preokrenu proces i pročitaju tajnu poruku. Za razliku od čiste steganografije gde je prisutan nevidljivi komunikacioni kanal, steganografija tajnog ključa razmenjuje stego-ključ, što ga čini podložnijim presretanju. Prednost steganografije tajnog ključa je čak i ako je presretnuta, samo strane koje znaju tajni ključ mogu izdvojiti tajnu poruku

## Public key steganography

Ova tehnika koristi dve vrste ključeva za ugradnju tajne poruke u omot. Prvi ključ se naziva privatni ključ, a drugi ključ se naziva javni ključ. Stego objekat sadrži omot, skrivenu poruku, privatni ključ i javni ključ. Pošiljalac će koristiti javni ključ tokom procesa kodiranja i samo privatni ključ, koji ima direktnu matematičku vezu sa javnim ključem, može da dešifruje tajnu poruku. Steganografija javnog ključa pruža robusniji način implementacije steganografskog sistema jer može da koristi mnogo robusniju i istraženiju tehnologiju u kriptografiji javnog ključa.

# 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 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, na primer, mogu biti unapred dogovoreni pojmovi. 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.

U steganografiji postoji nekoliko različitih tehnika koje se mogu koristiti za skrivanje informacija u datotekama i to su:

 Zamjena (Substitucija) i

 Generisanje (Generation)

- Ubacivanje (eng. *Injection* ili *Insertion*)

- Zamena (eng. *Substitution*) i

- Generisanje (eng. *Generation*)

## Ubacivanje

Ova tehnika omogućava skrivanje postojanja podataka u delovima datoteka koji su od manjeg značaja za zlonamernog korisnika. Tehnika se temelji 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 upotrebiti 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.

# Steganografija slike

Steganografija slike je proces skrivanja tajnih ili dodatnih informacija unutar digitalnih slika na način koji je neprimetan golim okom. Ova tehnika se koristi u različite svrhe, uključujući sakrivanje poruka, proveru autentičnosti slika, formiranje vodenih digitalnih žigova, kao i zaštitu privatnosti. Proces steganografije slika je sledeci:

1. **Priprema slike**: Prvi korak u steganografiji slika je odabir slike koja će biti korišćena kao osnovna slika. Ovo je slika u koju će se sakriti dodatne informacije. Takođe, potrebno je odabrati informacije koje će biti sakrivene ili dodate, kao što su tekstualne poruke, dodatne slike ili druge vrste podataka.
2. **Transformacija slike (opciono)**: U nekim slučajevima, slika može biti transformisana pre procesa steganografije kako bi se povećala efikasnost ili sigurnost skrivanja informacija. Ovo može uključivati primenu diskretne kosinusne transformacije (DCT), diskretne talasne transformacije (DWT) ili neke druge vrste transformacija.
3. **Odabir metode steganografije**: Postoji nekoliko različitih metoda steganografije koje se mogu koristiti za skrivanje informacija u digitalnim slikama. Neke od njih bice detaljnije opisane u narednim pogravljima.
4. **Skrivanje informacija**: Nakon odabira metode, informacije se sakrivaju unutar slike korišćenjem odabrane tehnike steganografije. Ovaj korak uključuje manipulaciju slikom ili njenim komponentama kako bi se dodale ili promenile informacije na način koji neće biti primetan golim okom.
5. **Čuvanje rezultujuće slike**: Kada su informacije uspešno sakrivene u slici, rezultujuća slika se može sačuvati na odgovarajući način, često pod novim imenom ili formatom.

Važno je napomenuti da proces steganografije slika zahteva pažljivo planiranje i implementaciju kako bi se postiglo uspešno sakrivanje informacija. Takođe, ovaj proces može biti podložan različitim tehnikama detekcije, stoga je potrebno razmotriti i odgovarajuće mere zaštite informacija.

# Metode steganografije slike

Neke od najznačajnijih i najčešće korišćenih metoda su:

1. **Least Significant Bit (LSB) steganografija**: Ova tehnika uključuje skrivanje podataka u najmanje značajnim bitovima (LSB) piksela slike. Male promene u LSB-ovima obično su neprimetne golim okom, što omogućava skrivanje informacija bez primetnog uticaja na vizuelni izgled slike.
2. **DCT (Discrete Cosine Transform) skrivanje:** Ova metoda koristi diskretnu kosinusnu transformaciju za transformisanje blokova piksela u frekvencijski domen. Zatim se informacije skrivaju modifikacijom određenih koeficijenata transformacije.
3. **DWT (Discrete Wavelet Transform) skrivanje:** Ova metoda koristi diskretnu talasnu transformaciju za transformisanje slike u talasni domen. Informacije se zatim skrivaju modifikacijom koeficijenata transformacije.
4. **Metode zasnovane na boji:** Ove metode koriste specifične karakteristike boje kako bi sakrile informacije. Na primer, može se koristiti metoda zasnovana na zasićenju ili nijansama boje.
5. **Metode zasnovane na teksturi:** Ove metode koriste karakteristike teksture slike za skrivanje informacija. Na primer, moguće je koristiti teksturne karakteristike kao što su gradijenti ili statistički podaci.

## Steganografija slike pomoću diskretne kosinusne transformacije

Steganografija slike pomoću DCT (Diskretne kosinusne transformacije) metode uključuje transformaciju blokova piksela slike u frekvencijski domen pomoću DCT-a, a zatim modifikaciju određenih koeficijenata transformacije kako bi se sakrile informacije. Osnovni koraci za obavljanje steganografije slike pomoću DCT metode su:

1. **Podela slike na blokove**: Prvo se slika deli na predefinisane blokove piksela. Ovi blokovi obično imaju dimenzije poput 8x8 piksela.
2. **Primena DCT transformacije**: Svaki blok piksela transformiše se pomoću DCT-a, što rezultira setom koeficijenata transformacije.
3. **Kvantizacija**: Nakon DCT transformacije, primenjuje se kvantizacija na dobijene koeficijente. Ovo uključuje deljenje koeficijenata odgovarajućim kvantizacionim matricama. Kvantizovani koeficijenti su obično zaokruženi na najbližu celobrojnu vrednost.
4. **Sakrivanje informacija**: Informacije se zatim sakrivaju modifikacijom određenih koeficijenata transformacije. Na primer, možete zameniti najmanje značajne koeficijente ili ih modifikovati na osnovu tajne poruke koja se skriva.
5. **Rekonstrukcija slike**: Nakon sakrivanja informacija, kvantizovani koeficijenti transformacije se koriste za rekonstrukciju slike. To uključuje primenu inverzne kvantizacije i inverzne DCT transformacije na blokove piksela.

Steganografija slika pomoću DCT predstavlja koristan i efikasan način za skrivanje informacija unutar digitalnih slika, sa različitim prednostima i ograničenjima koje treba uzeti u obzir prilikom njenog korišćenja.

Važno je napomenuti da se proces steganografije može kombinovati sa enkripcijom kako bi se dodatno osigurala tajnost skrivenih informacija. Takođe je važno pravilno upravljati kapacitetom skrivanja, kako bi se izbegla degradacija kvaliteta slike ili otkrivanje skrivenih podataka.

# Poznati alati za steganografiju pomoću slike

Postoji nekoliko popularnih alata za steganografiju pomoću slike koji se često koriste za skrivanje informacija u digitalnim slikama. Ovi alati obično pružaju različite funkcionalnosti i mogućnosti prilagođavanja u zavisnosti od potreba korisnika. Evo nekoliko najpoznatijih alata za steganografiju slika i kako se koriste:

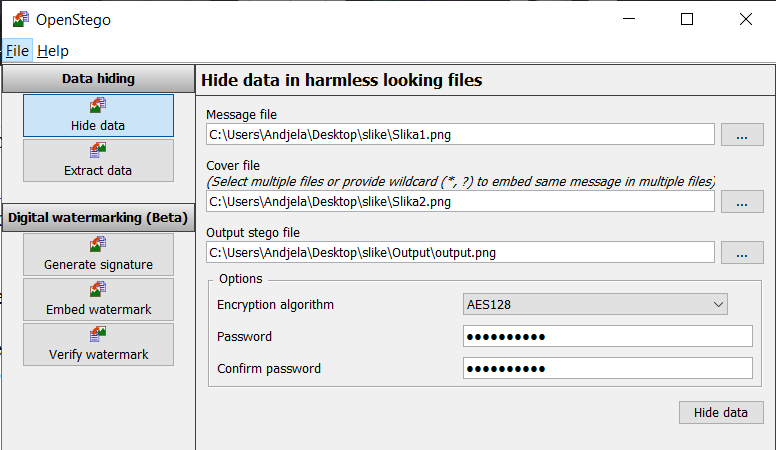
1. **Steghide**:
   * Steghide je jedan od popularnih alata za steganografiju slika dostupnih za Unix-bazirane operativne sisteme.
   * Ovaj alat omogućava korisnicima da sakriju tajne poruke unutar digitalnih slika koristeći različite metode, uključujući Least Significant Bit (LSB) i DCT steganografiju.
   * Za korišćenje Steghide-a, korisnici moraju prvo instalirati softver, a zatim koristiti komandnu liniju za sakrivanje i izvlačenje tajnih poruka iz slika.
   * Primer korišćenja: **steghide embed -cf cover\_image.jpg -ef secret\_message.txt**.
2. **OpenStego**:
   * OpenStego je besplatan alat za steganografiju slika dostupan za Windows, Linux i Mac operativne sisteme.
   * Ovaj alat omogućava korisnicima da sakriju tajne podatke unutar digitalnih slika koristeći različite metode, uključujući LSB i DCT.
   * OpenStego ima korisnički interfejs sa intuitivnim opcijama koje omogućavaju korisnicima da lako sakriju i izvuku tajne podatke iz slika.
   * Primer korišćenja: korisnici mogu jednostavno prevlačiti slike u prozor OpenStego-a radi sakrivanja ili izvlačenja tajnih podataka.
3. **OutGuess**:
   * OutGuess je još jedan alat za steganografiju slika koji je dostupan za različite platforme, uključujući Windows, Linux i Mac.
   * Ovaj alat se obično koristi za skrivanje informacija unutar digitalnih slika koristeći metod Least Significant Bit (LSB).
   * OutGuess podržava različite formate slika, uključujući JPEG, BMP i PNG.
   * Primer korišćenja: **outguess -d hidden\_message.txt cover\_image.jpg stego\_image.jpg**.
4. **SteganoGFX**:
   * SteganoGFX je jednostavan i lagan alat za steganografiju slika koji je dostupan za Windows platformu.
   * Ovaj alat omogućava korisnicima da sakriju tajne podatke unutar digitalnih slika koristeći metodu Least Significant Bit (LSB).
   * SteganoGFX ima jednostavan korisnički interfejs koji omogućava korisnicima da lako sakriju i izvuku tajne podatke iz slika.
   * Primer korišćenja: korisnici jednostavno odaberu sliku i tajnu datoteku, a zatim kliknu na odgovarajuće dugme za sakrivanje ili izvlačenje tajnih podataka.

## Primer korišćenja alata OpenStego

Na slici 2 prikazan je proces skrivanja jedne slike, unutar druge korišćenjem LSB metode steganografije. Ova verzija omogućava i šifrovanje tajnih podataka AES128 i AES256 algoritmomima, kojima se prvo šifriraju podaci slike koja se skriva (tajna slika). Zatim se šifrirana tajna slika ugrađuje u „nosač“ sliku.

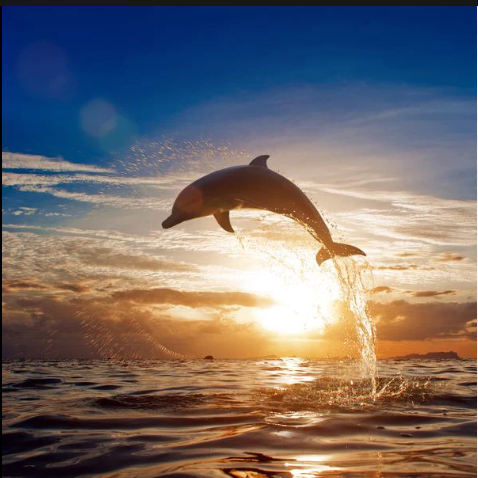
Prilikom ugrađivanja šifrirane tajne slike u nosač sliku, ključ za dešifrovanje (tj. ključ koji se koristi za AES128 šifriranje) mora biti poznat onima koji žele da pristupe tajnim podacima nakon što su izvađeni iz nosača. Bez pravilnog ključa, šifrirani podaci unutar nosača slike neće biti čitljivi.

Ovo omogućava dodatni nivo sigurnosti prilikom korišćenja steganografije za skrivanje slike unutar druge slike, jer osim što se slika skriva, podaci su i šifrirani kako bi se otežalo otkrivanje i pristupanje tajnim podacima od strane neovlašćenih osoba.



Slika 2. Proces sakrivanja podataka

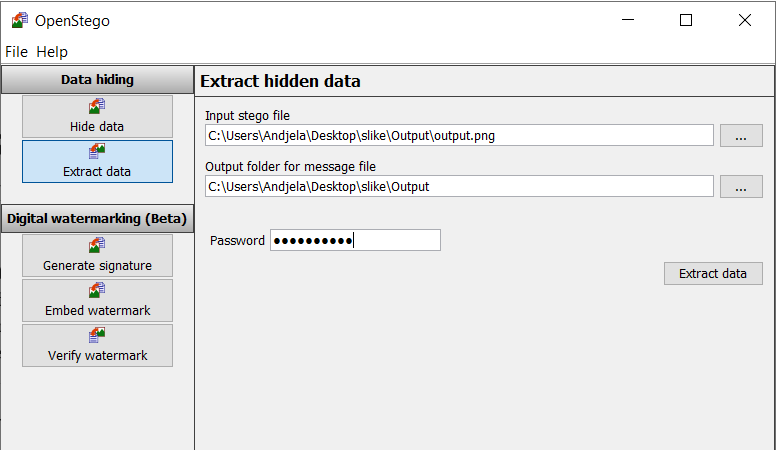
Kao tajna slika koririćena je slika 3, a kao „nosač“ slika 4. Slika 5 predstavlja retultat steganografije.

  A dolphin jumping out of water

Description automatically generated Slika 3. Tajna slika Slika 4. Slika „nosač“ Slika 5. Rezultat steganografije

Ono što je primetno, posmatrano očima nasumičnog posmatrača slika 4 i 5, jeste da je nemoguće uočiti razliku, a samim tim i posumnjati da se iza slike 5 krije neka informacija od značaja.

Na slici 6 prikazan je inverzan proces steganografije, kojim se kao rezultat dobija slika 3.



Slika 6. Inverzni proces steganografije

# Zaključak

Steganografija slika predstavlja moćan alat za skrivanje informacija unutar digitalnih slika na način koji je neprimetan golim okom. Kroz analizu različitih metoda steganografije, uključujući upotrebu najmanje značajnih bitova (LSB), diskretnu kosinusnu transformaciju (DCT), frekvencijsku domensku steganografiju, otkrili smo raznolike pristupe i tehnike koje se koriste za sakrivanje informacija u slikama.

Steganografija slika ima brojne praktične primene, uključujući označavanje autentičnosti i vlasništva nad digitalnim sadržajem, skrivanje tajnih poruka ili podataka, zaštitu privatnosti, digitalno potpisivanje dokumenata, kao i digitalno vodeno žigovanje radi zaštite autorskih prava. Ovi primeni se mogu naći u različitim oblastima, uključujući sigurnost informacija, forenziku, digitalni marketing, umetnost, arhiviranje podataka i mnoge druge.

Međutim, i pored svojih koristi, steganografija slika nosi sa sobom i određene izazove i pretnje. Postoji mogućnost zloupotrebe ovih tehnika za skrivanje zlonamernog sadržaja, kao što su štetni programi, ilegalni materijali ili terorističke poruke. Zbog toga je važno pridržavati se etičkih standarda i zakonskih propisa prilikom korišćenja steganografije slika, kako bi se sprečila zloupotreba i očuvala sigurnost i privatnost korisnika.

U budućnosti, možemo očekivati dalji razvoj tehnika steganografije slika, uz nastavak istraživanja u oblastima kao što su mašinsko učenje i veštačka inteligencija. Ovo će omogućiti razvoj naprednijih metoda koje će pružiti veću sigurnost, efikasnost i otpornost na detekciju, istovremeno čuvajući sve prednosti koje steganografija slika nudi u savremenom digitalnom svetu.

# Literatura

1. <https://www.researchgate.net/publication/265003223_ANALIZA_STEGANOGRAFSKIH_TEHNIKA_I_METODA>
2. <https://www.rcciit.org/students_projects/projects/it/2018/GR11.pdf>
3. <https://www.researchgate.net/publication/337399092_Image_in_Image_Steganography_Based_on_DCT>
4. <https://www.researchgate.net/publication/330565811_Hiding_data_in_images_using_DCT_steganography_techniques_with_compression_algorithms>
5. <https://resources.infosecinstitute.com/topics/cryptography/steganography-and-tools-to-perform-steganography/>
6. <https://www.openstego.com/>