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

**Mihajlo Veljković**

**Steganografija u zvučnim zapisima**

**Seminarski rad**

**Niš, 2023**

**Sadržaj**

[Uvod 3](#_Toc127887391)

[Steganografija u audio zapisima 4](#_Toc127887392)

[Tehnike steganografije 5](#_Toc127887393)

[Least Siginificant Bit Encoding 5](#_Toc127887394)

[Skrivanje ehoa 6](#_Toc127887395)

[Skrivanje u intervalima tišine 7](#_Toc127887396)

[Ubacivanje tonova 7](#_Toc127887397)

[Kodiranje faza 8](#_Toc127887398)

[Skrivanje u raširenom spektru 9](#_Toc127887399)

[Skrivanje pomoću logaritamskog spektruma 9](#_Toc127887400)

[Kodiranje amplitude 9](#_Toc127887401)

[Skrivanje pomoću diskretnih wavelet transformacija 10](#_Toc127887402)

[Ostale tehnike skrivanja 10](#_Toc127887403)

[Alati za audio steganografiju 13](#_Toc127887404)

[Hide4PGP 13](#_Toc127887405)

[S-Tools 14](#_Toc127887406)

[MP3Stego 17](#_Toc127887407)

[Invisible Secrets 17](#_Toc127887408)

[Rezultati skrivanja fajlova 18](#_Toc127887409)

[Audio steganografija danas 19](#_Toc127887410)

[Zaključak 20](#_Toc127887411)

[Prilog A 21](#_Toc127887412)

[Literatura 22](#_Toc127887413)

# Uvod

Steganografija je tehnika skrivanja tajnih poruka gde samo prijemnik i predajnik imaju znanje o postojanju poruke. Ova tehnika je postojala još pre nove ere, kada je Histiaeus napisao poruku na glavi svog vernog roba i čekao da mu izraste kosa. Kasnije je taj rob uspeo da prenese poruku neprimećeno i pokrene pobunu protiv Persijanaca.

Steganografija se najviše razvijala nastankom kompjutera i digitalnih podataka, jer takvi podaci po svojoj prirodi omogućavaju lakše skrivanje poruka. Srž digitalnih podataka i deo koji se konvertuje u “analogne” odnosno ono što ljudi mogu da pročitaju ostaje nepromenjen, dok se poruke mogu skrivati u ostatku podataka. Neki od primera ovakve steganografije su skrivanje poruka u najmanje značajnim bitovima slika, namerno usporavanje računarske mreže ili promena redosleda paketa unutar računarske mreže ili preslikavanje metapodataka datoteke kako bi je prerušili u neku drugu datoteku. Stegangorafija u zvučnim zapisima može da ima različite primene. Najčešća primena je praćenje korisnika sa pametnim uređajima puštanjem neprimetnih tonova u okviru nekih multimedijalnih zapisa (npr. reklama na televiziji ili internetu).

U ovom radu biće opisane tehnike skrivanja poruka u audio zapisima, zbog čega su takvi zapisi pogodni za skrivanje poruka i koji algoritmi se mogu koristiti za steganografiju. Na kraju ovog rada biće opisana i tehnička implementacija jednog načina skrivanja poruka, a kao prilog radu dolaze datoteke sa primerom skrivene poruke u njima.

# Steganografija u audio zapisima

Jedan od glavnih razloga za korišćenje audio zapisa u steganografiji je njihova široka zastupljenost i popularnost. Za razliku od steganografije u slikama, skrivanje informacija u zvučnim zapisima je slabije zastupljeni postupak. Skrivanje poruka u slici ne mora biti savršeno, dok isti postupak u zvučnom zapisu može relativno lako da se primeti. Ljudsko čulo zvuka u idealnim situacijama pokriva opseg od 20 do 20 000 Hz, pa bilo kakvi dodatni zvučni signali u tom opsegu mogu lako da se primete. Takođe, ako je izvor zvuka bez šumova i kvalitetan, onda se još lakše primećuju bilo kakve skrivene poruke.

Postoje kriterijumi koji se uzimaju u obzir prilikom steganografije i to su [1]:

* količina sakrivenih podataka – Mereno u bps, označava koliko podataka je skriveno i uspešno izvučeno iz fajla
* neprimiteljivost – Ovaj krrterijum je zasnovan na ljudskom sluhu i označava da li čovek moze da razlikuje skrivenu poruku od osnovnog audio signala. Takođe je poznat i kao PESQ test. Vrednuje se od 4.5 do 1. Vrednost od 4.5 označava da je rezultat identičan kao original sa stanovišta ljudskog sluha, dok vrednost od 1 označava da je došlo do ozbiljne degradacije zvučnog zapisa. Moguće je korisiti i SegSNR (Signal to Noise Ratio) vrednost.
* pojačavanje signala – Koliko je tehnika skrivanja otporna na povećavanja inteziteta audio signala
* filterovanje signala – Koliko je tehnika otporna na napad odsecanjem frekvencija signala
* ponovna kvantizacija – Koliko je tehnika otporna na ponovnu kvantizaciju (npr. konvertovanje 16-bitnog audio zapisa u 8-bitni pa nazad u 16-bitni)
* ponovno uzorkovanje – Otpornost na promenu frekvencije uzorkavanja (npr. uzorkovanje zapisa iz 16 KHz u 8 KHz pa nazad u 16 KHz)
* otpornost na šum
* otpornost na enkodiranje/dekodiranje – Koliko je tehnika otporna na te procese ili na proces konvertovanja u druge formate (npr. konvertovanje wave datoteke u MP3)
* transkodiranje – Otpornost na dekodiranje od strane drugih algoritama

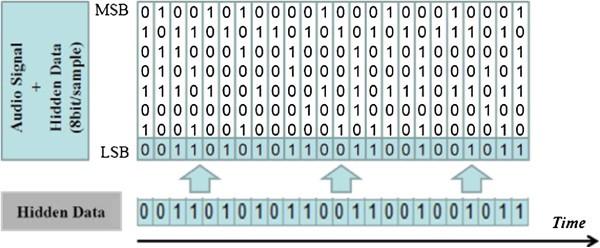
Različite tehnike steganografije će dati različite rezultate, pa treba uzeti u obzir kakvu poruku i koju količinu podataka želimo da sakrijemo, kao i kakav je tip zvučnog zapisa sa kojim radimo.

# Tehnike steganografije

U okviru ovog rada biće opisane različite tehnike steganografije, uključujući:

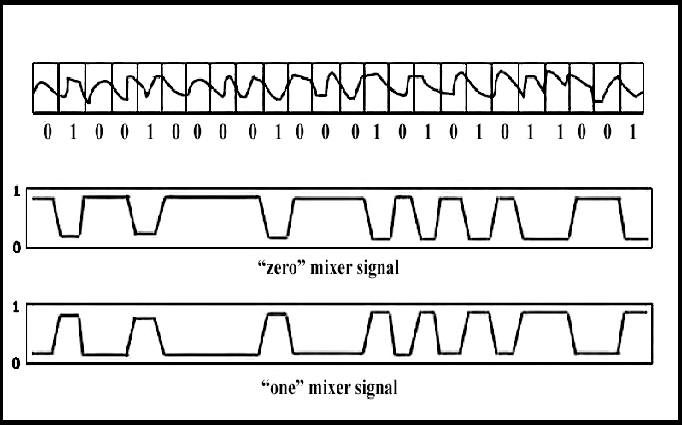
* LSB – Least Significant Bit Encoding
* Skrivanje ehoa
* Skrivanje u intervalima tišine
* Ubacivanje tonova
* Kodiranje faza
* Skrivanje u raširenom spektru
* Skrivanje pomoću logaritamskog spektruma
* Kodiranje amplitude
* Skrivanje pomoću diskretnih wavelet transformacija

## Least Siginificant Bit Encoding

Ova tehnika je poznata i kao Low-bit encoding i nastala je kao jedna od prvih metoda sakrivanja informacija u digitalnim podacima. Poruka se kodira u binarni zapis, i svaki bit poruke se smešta u najmanji bit zvučnog zapisa. Za zvuk sa frekvencijom uzorkovanja od 16 KHz, 16 kbps podataka može da bude prikriveno. Ova metoda ima veliki potencijal za skrivanje podataka i vrlo je jednostavna za implementaciju. Mane su to što je vrlo jednostavno pronaći skrivenu poruku i uz to nije otporna na bilo kakve izmene originalnog podataka (filterovanje zvuka, pojačavanje, dodavanje šuma, transkodiranje). 

Slika 1.1 Primer LSB algoritma

## Skrivanje ehoa

Skrivanje ehoa je metoda u kojoj se uvodi kratak eho u izvornom signalu. Dodavanje eha sa kašnjenjem do jedne milisekunde znači da ljudski sluh ne može da primeti razliku između originala i signala sa porukom. Takođe, amplitudu i stopu opadanja možemo podešavati tako da eho signal ne može da bude detektovan od strane ljudskog čula sluha. Ulazni signal se deli na blokove, pa se zatim uvode slojevi eho signala dok se ne enkodira cela poruka. Prijemnik kasnije mora da signal „razbije“ na blokove i pomoću FFT[[1]](#footnote-2)-ova dobija specifične talasne oblike koji otkrivaju poruku.

Slika 1.2 Primer dekodirane poruke

Mane ove metode je što je propusni opseg vrlo mali, a i vrlo je lako otkriti dodat eho u originalnom signalu, pa samim tim i izvući poruku, pa u slučaju da poruka nije i enkriptovana, ova metoda uopšte nije bezbedna za skrivanje.

## Skrivanje u intervalima tišine

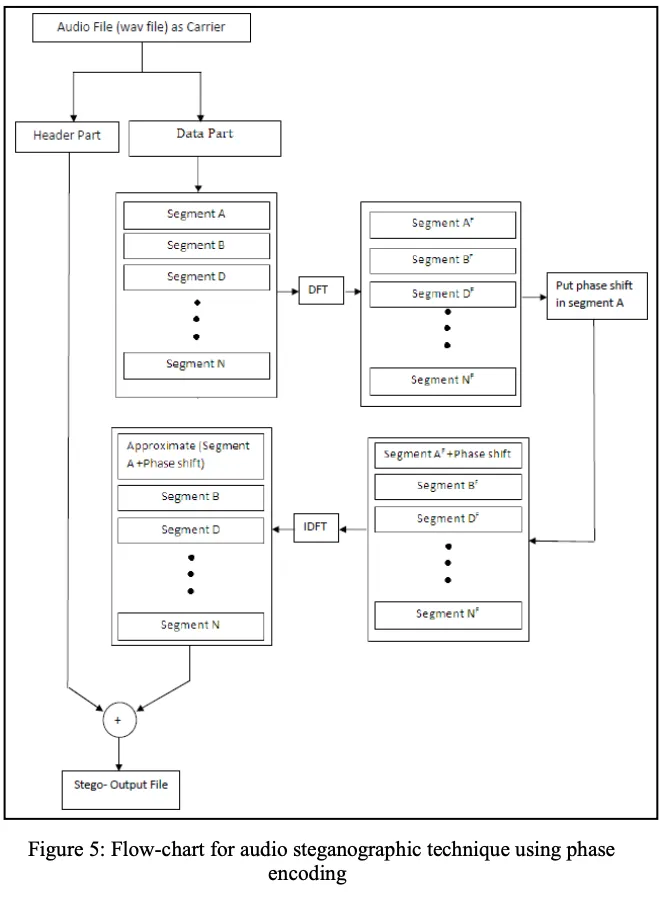
Ova metoda je jedna od jednostavnijih i efektivnijih i koristi se kod zvučnih zapisa koji imaju intervale tišine (kao npr. kod govora). Prvi korak je merenje količine i intervala tišine. Nakon toga se bira vrednost izmedju 0<x<2n, gde je n broj bitova potreban za reprezentaciju podatka. Na originalnom signalu, skraćujemo interval tišine za x. Pri vađenju podataka, x se računa kao mod(Interval,2n). Ako želimo da sačuvamo vrednost 6, potrebno je 3 bitova, pa uzimamo da je x=7. Ako nam je interval dužine 109, novi interval će biti dužine 102. Pri vađenju podataka računamo mod(102,8)=6 i dobijamo originalnu vrednost. Za kompresiju u MP3 format, ova metoda ignoriše prvi i zadnji interval tišine. Mana ove metode je slaba količina podataka (~64bps).

## Ubacivanje tonova

Ova tehnika je zasnovana na neprimetljivosti tonova slabijeg inteziteta u prisustvu tonova sa jačim intezitetom. Da bi se sačuvao jedan bit podataka, biraju se tonovi generisani na 2 frekvencije, f0 i f1. Intezitet tonova maskiranih frekvencija pf0 i pf1 se postavljaju na specifičan odnos generalnog pojedinačnog zvučnog segmenta (frame) pi, gde je i=1,..n, a n je broj segmenta. Tonovi se ubacuju sa poznatim frekvencijama i niskim intezitetima. Pri vađenju podataka, računa se pi kao intezitet svakog segmenta, kao i pf0 i pf1 sa odabrane frekvencije skrivanja. Ako je > , onda je sakriveni podatak “0”, a u suprotnom “1”. Mane ove metode su mali propusni opseg, i laka detekcija postojanja skrivenih podataka.

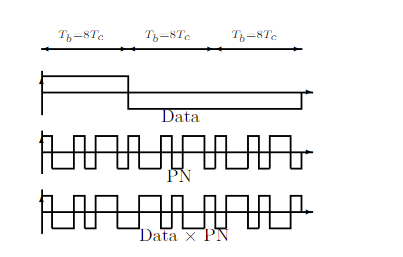
Slika 1.3 Dijagram ubacivanja tonova

## Kodiranje faza

Ova tehnika iskorišćava ljudski sluh i činjenicu da ne možemo primetiti male razlike u fazama zvučnog signala. Nad originalnim signalnom se vrši FFT. Ako čuvamo bit “1” onda oduzimamo fazu signala za , u suprotnom dodajemo . Nakon prolaska kroz ceo signal, vršimo obrunutu Furijeovu transformaciju signala i dobijamo zapis sa skrivenom porukom. Jedina mana ove tehnike je relativno mala količina podataka koji budu skriveni u zapisu (~333bps).

Slika 1.4 Algoritam kodiranja faza

## Skrivanje u raširenom spektru

Rašireni spektar (spread spectrum) je tehnika razvijena u telekomunikacionim tehnologijama radi očuvanja originalnog signala poslatog preko kanala sa mnogo šumova. Funkcioniše tako što duplira originalni signal, raširen na veći spektar frekvencija. Prijemnik i predajnik znaju kod prostiranja, a skrivena poruka se krije u zvučnom signalu. Ova metoda nije otporna na promenu brzine reprodukcije signala, i podaci mogu biti izgubljeni pri takvoj modifikaciji.

## Skrivanje pomoću logaritamskog spektruma

Slika 1.5 Promena signala nakon skrivanja

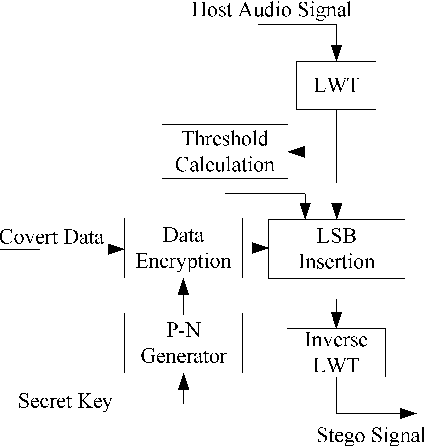
Nakon izvršavanja obrnute Furijeove transformacije nad logaritmom spektra signala, dobijamo rasprostranjenost frekvencija po učestalosti. Biraju se frekvencije koje se najotpornije na sve promene signala f1 i f2 i neznatno se menjaju kako bi se sačuvali bitovi “1” i “0”. Mana ove metode je laka detekcija distorcije nad signalom i mala količina podataka koji mogu da se sačuvaju.

## Kodiranje amplitude

Skrivanje poruke se vrši odabirom frekvencije tako da se originalni signal ne menja pri slušanju. Pronalazak frekvencije se vrši tako što se bira maska na 13dB ispod originalnog spektruma signala. Analizom spektruma se mogu naći frekvencije za kodiranje podataka koje ne prave distorziju originalnog signala. Za ljudski govor, opseg frekvencija za kodiranje signala je 7-8 KHz. Moguće je potpuno zameniti ovaj opseg frekvencija porukom sa manjom amplitudom i ljudsko uho ne bi moglo da primeti razliku. Mana ove metode je vrlo specifična primena, nije pogodna za sve vrste signala.

## Skrivanje pomoću diskretnih wavelet transformacija

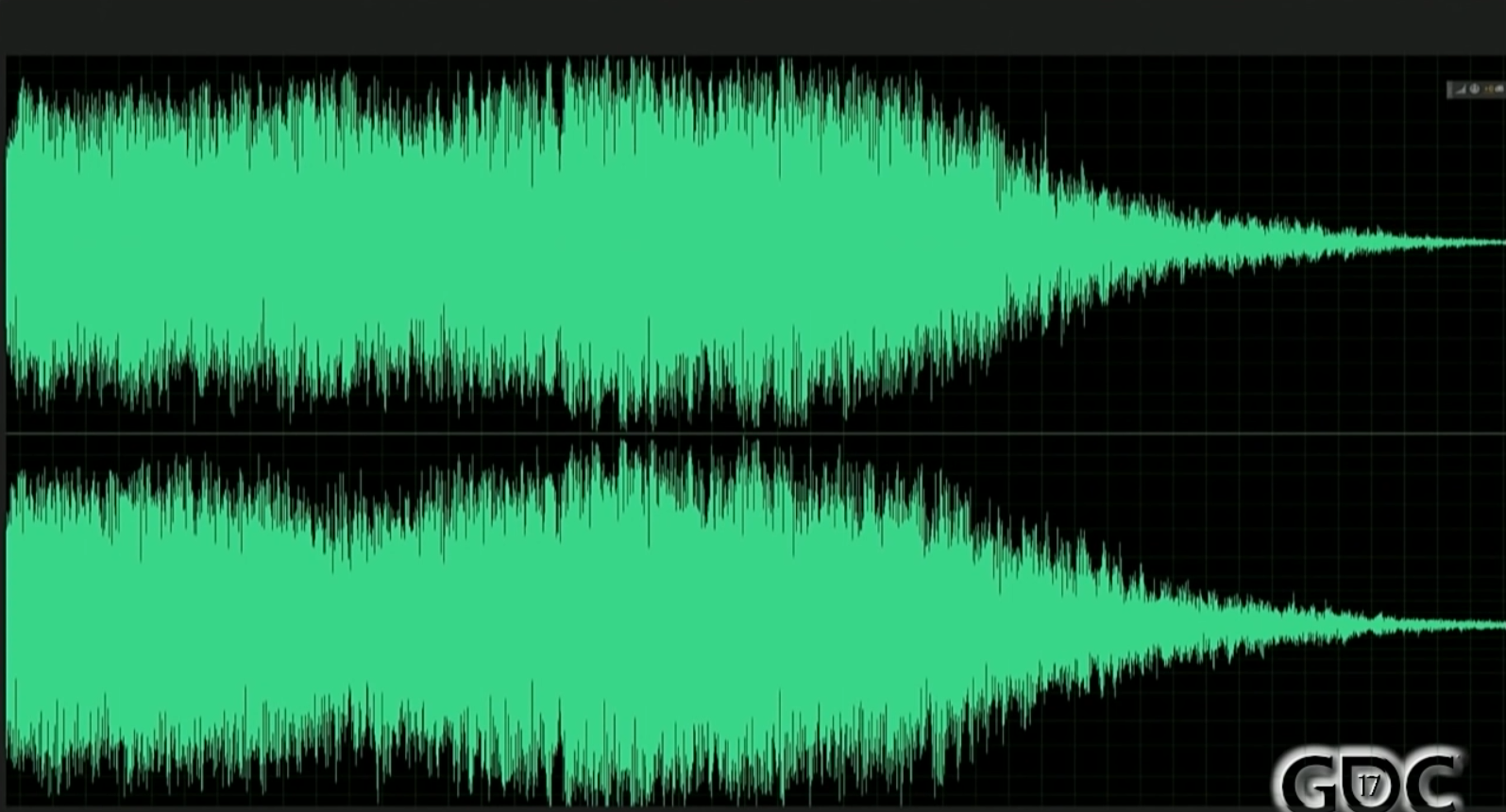
Nad originalnim zvučnim signalom se vrši diskretna wavelet transformacija. Podaci se skrivaju u LSB-ovima u wavelet koeficijentima signala. Izbegava se skrivanje podataka u delovima signala gde je tišina ili jačina signala niska. Ova tehnika nudi najveći propusni opseg podataka, ali izvlačenje sakrivenih podataka nije uvek uspešno.



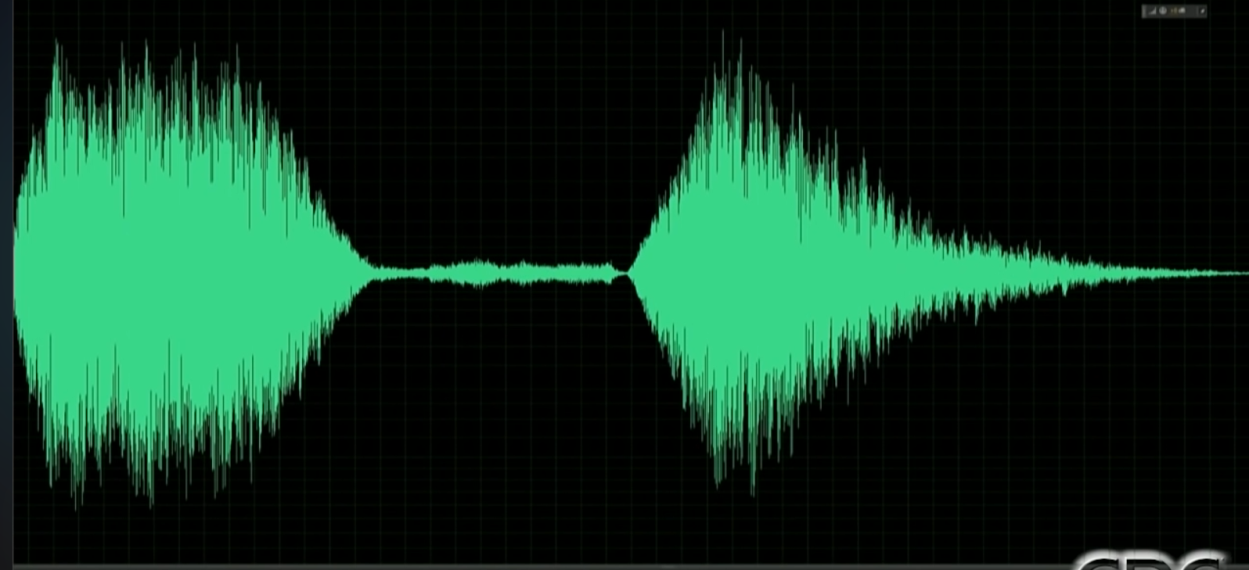
Slika 1.6 Dijagram skrivanja pomoću wavelet transformacija

## Ostale tehnike skrivanja

Steganografija nema uvek unapred definisana pravila i algoritme, pa je moguće sakriti podatke i na druge načine. Jedan od ranih primera steganografije u zvučnim zapisima je snimanje poruke unazad. Puštanje zvuka u normalnom pravcu, slušalac će verovatno čuti samo neke čudne reči ili zvukove, a puštanje unazad će otkriti pravu poruku. Iako ova tehnika nije bezbedna za sakrivanje podataka, služi kao primer rane steganografije. Kao unapređenje ove tehnike, u popularnoj video igri DOOM (2016), kompozitor Mick Gordon je sakrio poruku u dva odvojena kanala (levi i desni). Reprodukcijom zvuka u stereo formatu, slušalac ne primećuje ništa, ali prilikom reprodukcije u mono formatu, zbog interferencije levog i desnog kanala, slušalac može da čuje jasnu poruku koja je opet snimljena unazad.

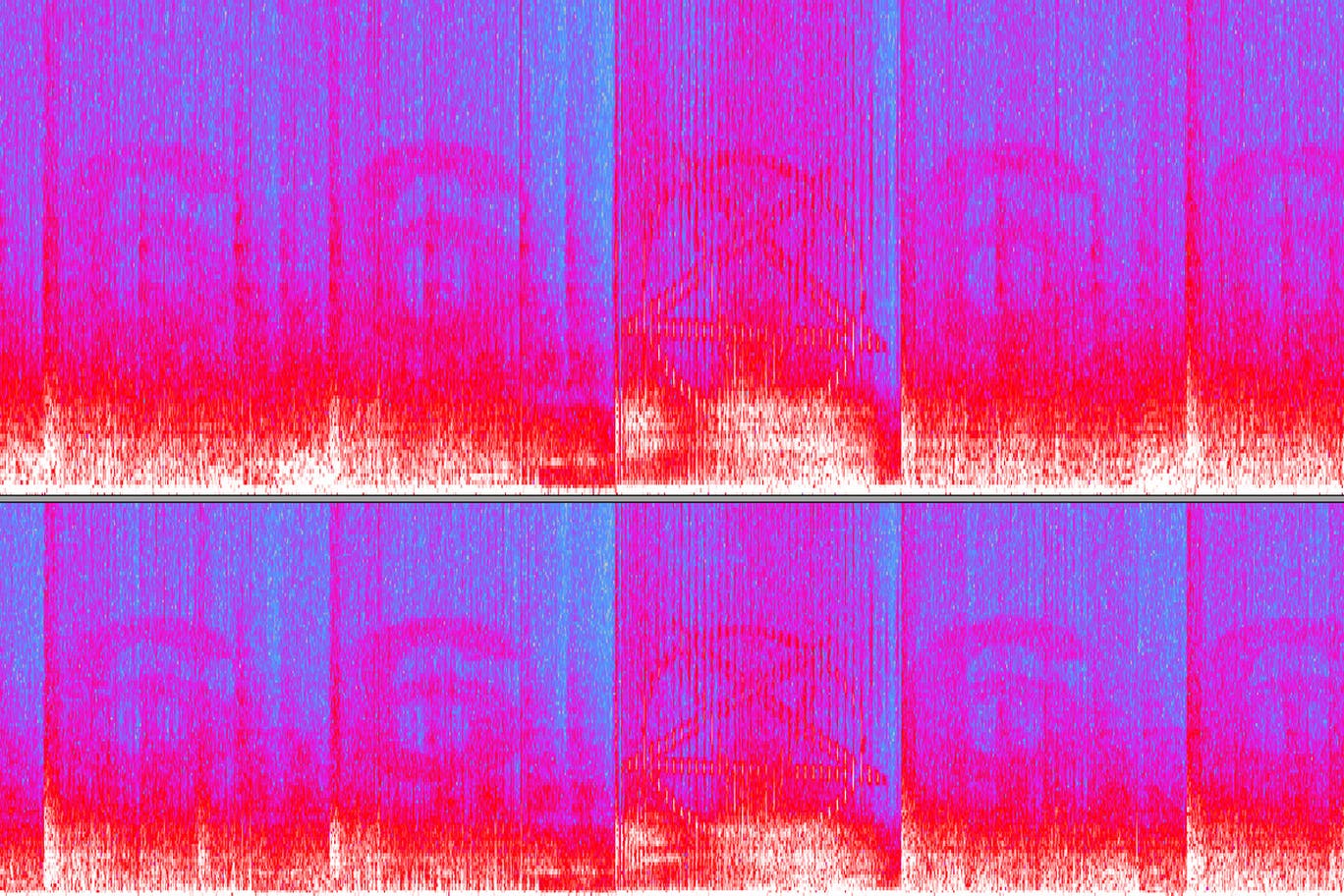


Slika 1.7 Izgled levog i desnog kanala



Slika 1.8 Izgled zvučnog zapisa u mono obliku

Još jedna tehnika koja je takođe korišćenja u toj video igri je skrivanje slike unutar zvučnog zapisa. Slika se može videti samo u spektogramu zapisa, dok je prisustvo sakrivenog podatka neprimetno.



Slika 1.9 Spektogram sa skrivenom slikom

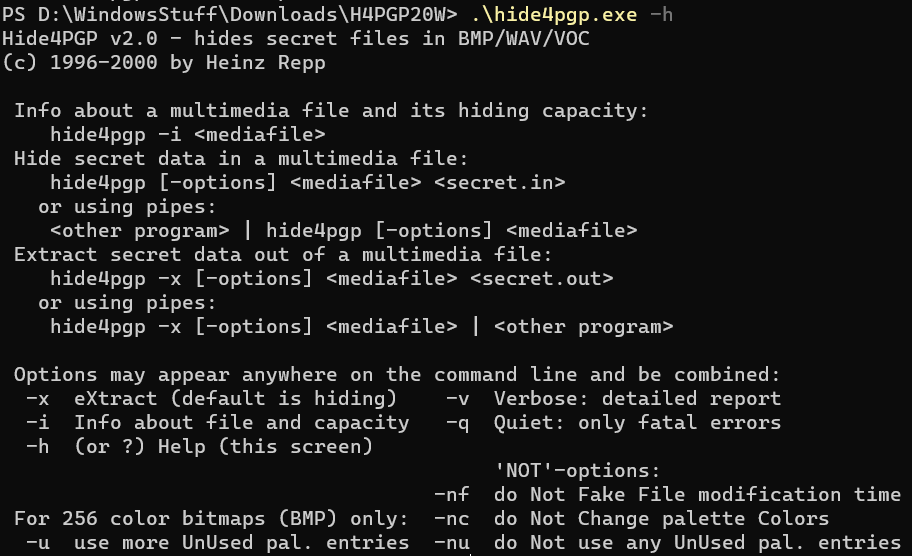
Kompozitor je u ovom slučaju iskoristio frekvencije zvuka koje ne mogu da se čuju uz kombinaciju korišćena tonova koji su prekriveni pomoću drugih, jačih tonova u okviru kompozicije. Uz to, kompzicija je glasna, i priroda dela je da ima grub zvuk sa povremenim “grebanjem”, pa nije previše teško sakriti dodatne tonove kao slike. Ova tehnika skrivanja nije idealna za sve slučajeve korišćena, a i može biti lako primećena ukoliko neko otvori spektogramski prikaz fajla.

# Alati za audio steganografiju

Iako audio steganografija nije standardizovana, postoje alati koji mogu da olakšaju proces skrivanja podataka. Neki od alata koji će biti opisani u ovom radu su:

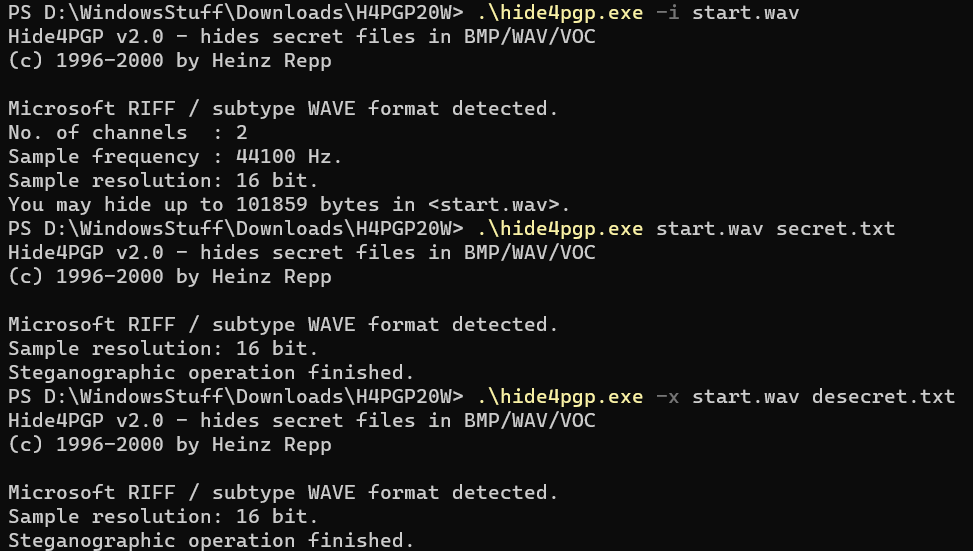
* Hide4PGP
* S-Tools
* MP3Stego
* Invisible Secrets

## Hide4PGP

Jedan od prvobitnih programa za steganografiju, napravljen kao projekat otvorenog koda. Ovaj alat može da sakrije poruke u slikama u .BMP formatu i u audio fajlovima u .WAV i .VOC formatu. Napravljen je kao prateći alat za tadašnji standard Pretty Good Privacy, koji je danas slabo korišćen. Alat je jednostavan za korišćenje, nema korisnički interfejs i radi na Windows i Linux operativnim sistemima.

Slika 2.1 Hide4PGP u terminalu

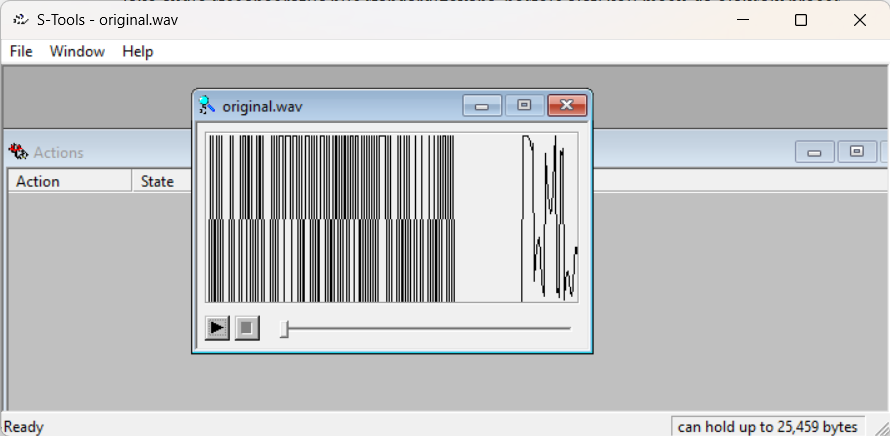
Alat se pokreće iz terminala i može da sakrije podatke ili da izvuče podatke iz prosleđenog fajla. Moguća je i analiza fajla za količinu podataka koju može da sakrije.



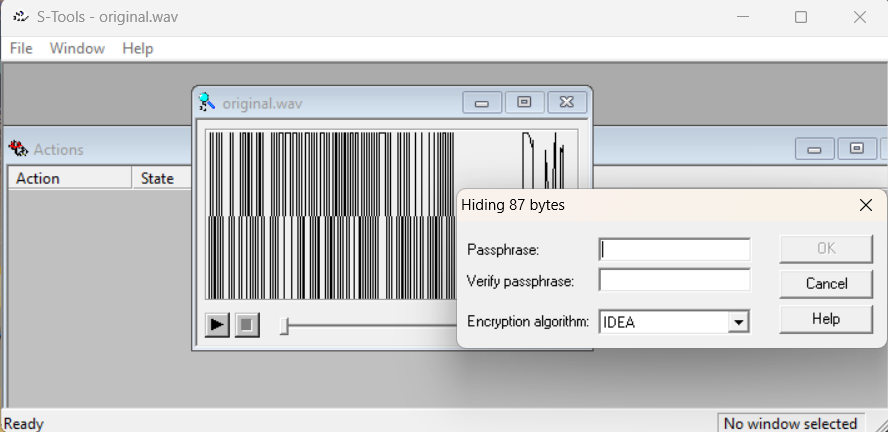
Slika 2.2 Analiza, skrivanje i izvlačenje podataka u Hide4PGP

## S-Tools

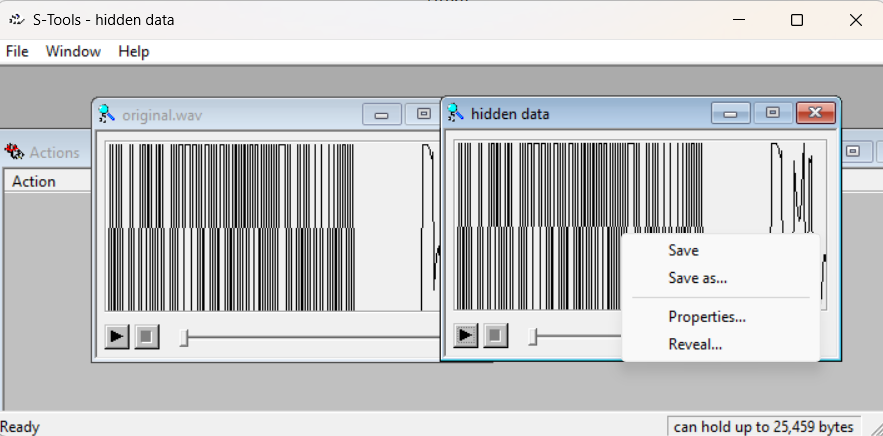
Jedan od alata sa korisničkim interfejsom koji služi za steganografiju u multimedijalnim zapisima. Postupak skrivanja je sledeći:

1. Prevučemo fajl u koji želimo da sakrijemo podatke u aplikaciju

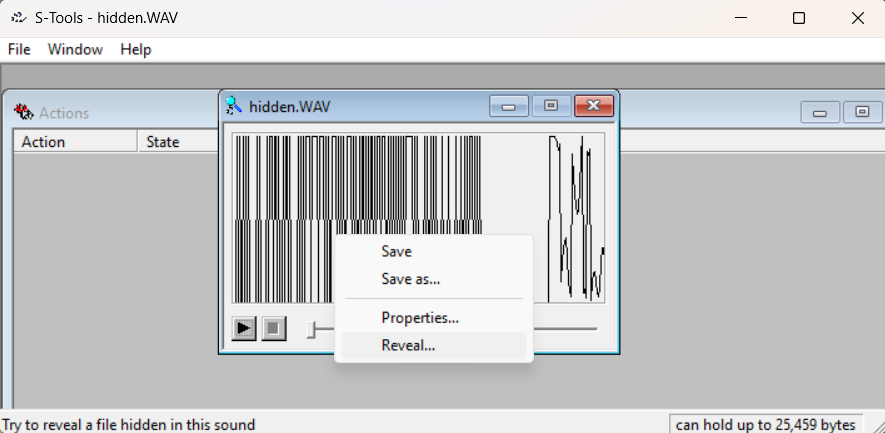
Slika 2.3 Učitavanje fajla u S-Tools

1. Prevučemo podatke koje želimo da sakrijemo unutar našeg fajla u prozor našeg fajla

Slika 2.4 Skrivanje poruke u fajlu

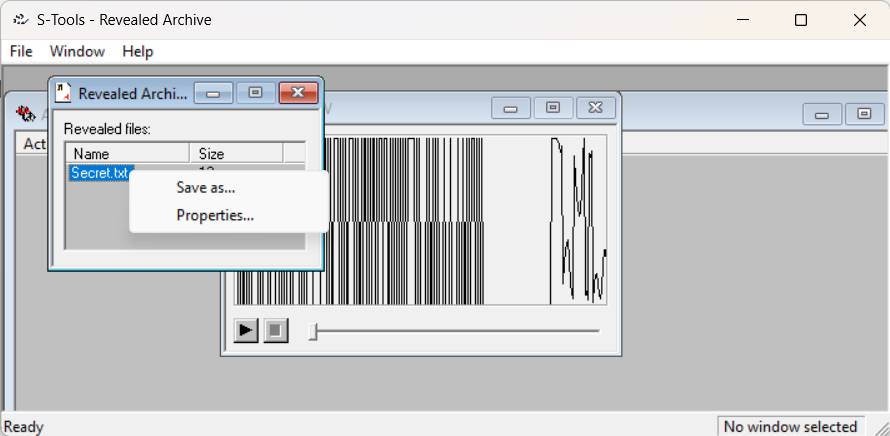
1. Podatke moramo da zaštitimo nekom šifrom, a opcionalno možemo i da promenimo algoritam enkripcije (IDEA, DES, Triple DES, MDC)
2. Pojavljuje se novi prozor sa novim fajlom koji ima skrivene podatke. Klikom na Save As.. čuvamo novi fajl

Slika 2.5 Čuvanje fajla sa skrivenom porukom

1. Za dekripciju podataka, radimo korak 2. i onda desni klik na prozor fajla i biramo opciju Reveal..

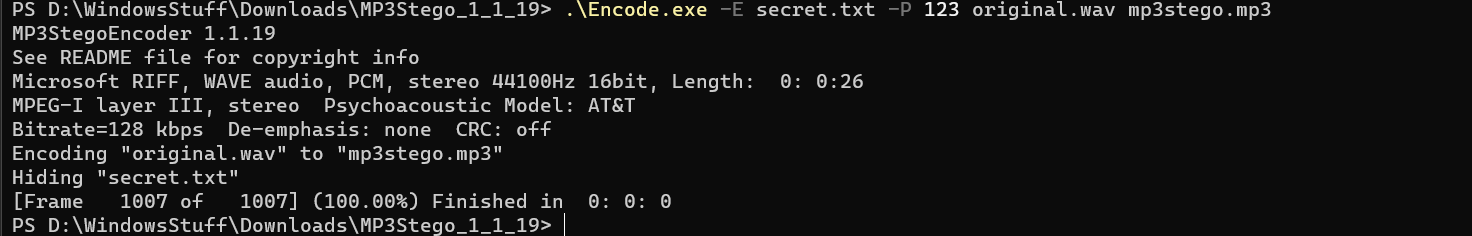
Slika 2.6 Izvlačenje skrivene poruke

1. U slučaju da postoje skriveni podaci, kreira se novi prozor sa pronađenim skrivenim podacima koje možemo da sačuvamo desnim klikom na Save As..

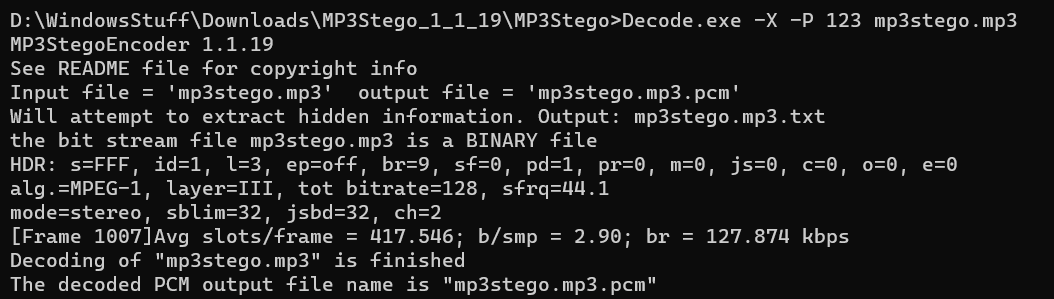


Slika 2.7 Prikaz skrivenih poruka/fajlova

## MP3Stego

Po rečima autora, MP3Stego je nastao kao jedan od prvih alata za skrivanje informacija u MP3 fajlovima. Alat funkcioniše tako što krije informacije u fajlu tokom kompresije zvuka u MP3 format. Ulazni fajl treba da bude nekompresovan zvučni fajl .WAV formata, a kao rezultat se dobija MP3 fajl. Izvlačenje informacija se vrši tako što alat kreira .PCM fajl zvučnog zapisa i tekstualni fajl skrivenih podataka, ukoliko postoje. Ovaj alat ne može da se koristi za male fajlove i može da ima problema sa nekim ulaznim fajlovima. Za skrivanje podataka pozivamo program Encode.exe sa argumentima.

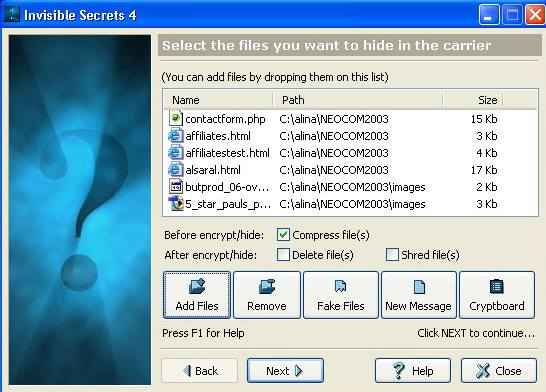
Slika 2.8 Skrivanje fajla pomoću MP3Stego

Za izvlačenje podataka pozivamo program Decode.exe sa argumentima.

Slika 2.9 Izvlačenje skrivenog fajla pomoću MP3Stego

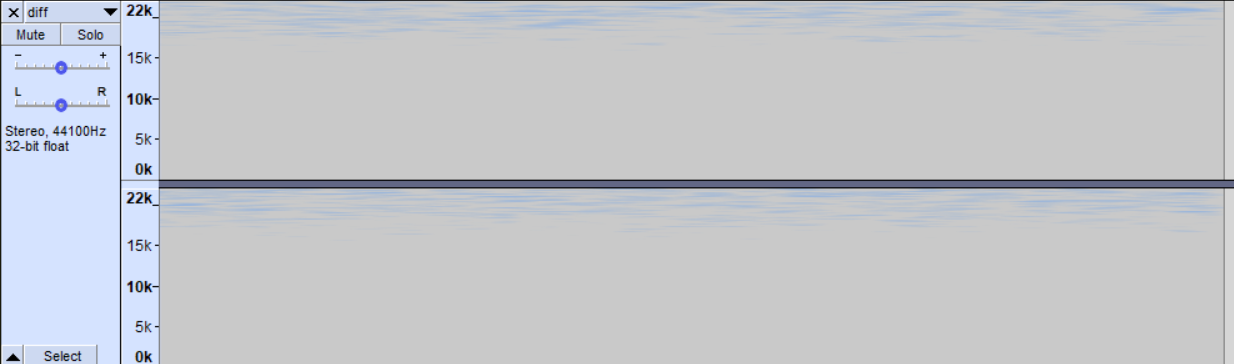
## Invisible Secrets

Invisible Secrets je jedan od mnogih generičnih alata za skrivanje podataka unutar fajlova. Ovakvi tipovi alata nisu otvorenog koda i vrlo često imaju skupe licence za korišćenje. Imaju korisnički interfejs sa mnogo opcija, uključujući i enkripciju fajlova i celih diskova, a najčešće rade samo na Windows operativnim sistemima. Alat funkcioniše tako što se odabere “carrier” i nakon toga izaberu fajlovi koje želimo da sakrijemo unutar našeg “carrier” fajla. Moguće je enkriptovati fajlove, kompresovati ih i uništiti originalne fajlove nakon sakrivanja.



Slika 2.10 Skrivanje fajlova pomoću Invisible Secrets

## Rezultati skrivanja fajlova

Nakon izvršavanja procesa skrivanja fajlova sa navedenim programima, ne možemo primetiti razlike između originala i fajlova sa podacima. Pomoću programa Audacity, moguće je videti razlike u vizuelnom obliku i možemo primetiti da su naši podaci skriveni u frekvencijskom opsegu van onoga što ljudsko čulo sluha može da čuje.

Slika 2.11 Skrivene poruke vidljive u spektogramu

# Audio steganografija danas

Uz ogromnu rasprostanjenost IoT uređaja i mobilnih telefona danas, povećava se i korišćenje skrivenih poruka unutar zvučnih zapisa. Najčešća primena audio steganografije danas je skriveno praćenje korisnika preko reklama. Kompanija SilverPush stavlja skrivene signale u svojim reklamama, i na osnovu toga pametni uređaji mogu da prepoznaju koju reklamu je korisnik odgledao do kraja i na osnovu toga preporuče slične proizvode. Amazonov Echo uređaj takođe može da prepozna kada se njemu obraća čovek, a kada je u pitanju prenos sa neke reklame pomoću različitih skrivenih frekvencija u zvučnim zapisima.

Osim korišćenja u svrhe marketinga, mnogi umetnici i kompozitori koriste audio steganografiju za skrivanje poruka u svojim delima. Vrlo popularna tehnika ranih 60ih godina je bila snimanje skrivenih poruka tako da slušalac može da ih čuje samo ako pusti ploču u suprotnom smeru. Postoji preko 100 kompozicija koje imaju ovakvu skrivenu poruku, a još uvek je popularna metoda za skrivanje. Osim toga, neki umetnici skrivaju i slike unutar svojih dela, kao već pomenuti Mick Gordon. Pored njega je bend Nine Inch Nails u svojoj pesmi My Violent Heart imao skrivenu sliku, a postoje i još drugih, možda još uvek skrivenih poruka koristeći ovu metodu.

Na Github-u postoje 18 aktivnih projekata koji su tagovani samo za audio steganografiju, a postoje i mnogo komercijalnih alata koji funkcionišu, pa je očigledno da ovaj vid skrivanja poruka još uvek popularan i aktivan.

# Zaključak

Iako se čini da je razviće audio steganografije stagniralo ranih 2000-ih godina, videli smo da je ova tema još uvek popularna i još uvek se koristi u današnjim tehnologijama. Originalni koncept iza tehnologije je još uvek validan, i u najvećem broju slučajeva, vrlo efektivan ako zvučni zapis sa porukom analizira čovek samo pomoću svog čula sluha. Videli smo i da popularnost ove tehnologije raste zbog sve većeg broja pametnih uređaja koji u sebi imaju mikrofon, a uz to postoji ogroman potencijal za prenos informacija van opsega ljudskog sluha.

Treba porazmisliti i o budućnosti ove tehnologije. Sa sve većim brojem sistema veštačke inteligencije sa mogućnoti sinteze govora, postoji potencijal da ti sistemi skrivaju poruke u svom govoru koje bi bile relevantne samo drugim računarskim sistemima, a bile bi neprimetne ljudskom sluhu. Kao još jedan slučaj korišćenja možemo uzeti i autonomna vozila, gde vozilo ili semafori mogu da prave zvučne signale koji bi služili za identifikaciju stanja na putevima, lokacije ili bilo kakvih drugih potrebnih informacija za bezbedniju vožnju.

Uz porast korišćenja streaming tehnologija, pitanje je vremena kada će velike produkcijske kuće početi da koriste steganografiju za obeležavanje autorskih prava u nekom medijumu. Ovo je trenutno ogroman problem na internetu, pogotovo na sajtovima kao što su YouTube i Twitch, gde se vrlo često dešavaju ili slučajne identifikacije autorskih medijuma, ili korisnici uspevaju da zamaskiraju reprodukciju zaštićenih medijuma pomoću nekih filtera (ubrzavanje, usporavanje, uvođenje šuma itd). Takođe, uz pojavu NFT tehnologija, korišćenje steganografije za obeležavanje vlasnika može biti vrlo jednostavan i bezbedan način za sve vrste provera potrebnih za verifikaciju.

Potencijal audio steganografije je ogroman u kombinaciji sa novim tehnologijama i problemima koji se pojavljuju sa njima.

# Prilog A

U okviru ovog dokumenta, a i u Github repozitorijumu biće fajlovi bez i sa skrivenim porukama kreirani pomoću alata iz ovog rada.











# Literatura

<https://medium.com/@achyuta.katta/audio-steganography-using-phase-encoding-d13f100380f2>

<https://www.researchgate.net/publication/242743625_Spread_Spectrum_Cryptography_and_Information_Hiding>

<https://aircconline.com/ijma/V3N3/3311ijma08.pdf>

<https://iopscience.iop.org/article/10.1088/1757-899X/226/1/012084/pdf>

<https://youtu.be/U4FNBMZsqrY?t=2566>

<http://www.heinz-repp.onlinehome.de/Hide4PGP.htm>

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

<https://www.insecure.in/steganography.asp>

<https://www.east-tec.com/invisiblesecrets/features/securely-hide-your-sensitive-information/>

<https://techcrunch.com/2014/07/24/silverpush-audio-beacons/>

<https://github.com/topics/audio-steganography>

<https://en.wikipedia.org/wiki/Audio_watermark>

1. Fast Fourier Transform - brza Furijeova transfromacija [↑](#footnote-ref-2)