Primjena steganografije na audio datotekama

Knezović, Krešimir

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU

FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK

Sveučilišni preddiplomski studij računarstva

PRIMJENA STEGANOGRAFIJE NA AUDIO DATOTEKAMA

Završni rad

Krešimir Knezović

Osijek, 2017.

Sadržaj

1. UVOD 1

2. OPĆENITO O STEGANOGRAFIJI 2

2.1. Steganografija kroz povijest 4

2.2. Tipovi steganografije 5

2.3. Općenito o audio steganografiji 6

3. DIGITALNI VODENI ŽIGOVI 8

3.1. Razvoj digitalnih vodenih žigova u audiotehnici 9

3.2. Osobine i vrste vodenih žigova 10

3.3. Osobine ljudskog slušnog sustava 11

3.4. Frekvencijsko maskiranje 12

3.5. Vremensko maskiranje 13

3.6. Izravno korištenje perceptivnog maskiranja 15

4. ALGORITMI OZNAČAVANJA AUDIO DATOTEKA 17

4.1. LSB supstitucijska metoda 17

4.2. Metoda kodiranja pariteta 19

4.3. Fazno kodiranje 20

4.4. Metoda raspršenog spektra 21

4.5. Metoda skrivenog odjeka 23

4.6. Metoda ugradnje audio vodenih žigova pomoću tehnike zakrpa 24

4.7. Primjena vodenih žigova 25

5. ZAKLJUČAK 28

LITERATURA 29

SAŽETAK 30

ABSTRACT 31

ŽIVOTOPIS 32

1. UVOD

Danas veliki broj internet aplikacija zahtijeva prijenos podataka na siguran način. Prijenos podataka u javnom komunikacijskom sustavu nije siguran zbog prisluškivanja i nepravilne manipulacije digitalnim podatcima. Zbog toga je atraktivan način za rješavanje ovog problema steganografija, koja je umjetnost i znanost o pisanju skrivene poruke na takav način da nitko osim pošiljatelja i primatelja ne sumnja u postojanje poruke.

Posljednjih godina primijećen je trend pretvorbe analognih medija u digitalne. Ovo se odnosi na nepokretne slike, video i audio signale. Opće je mišljenje da je kvaliteta digitalnih sustava daleko bolja od njihovih analognih ekvivalenata. Manipuliranje i rad s digitalnim podatcima je fleksibilnije i jednostavnije, umnožavanje i distribucija digitalnih medija je lakša, pri čemu nema gubitaka u informaciji ili kvaliteti u ovim procesima. Zbog povećanja upotrebe digitalnih medija javljaju se novi problemi, kao što su piratstvo i kršenje autorskih prava. Ovi problemi su bili prisutni još u vrijeme analognih medija, prije pojavljivanja interneta, ali sada kada se izrada potpuno identične kopije nekog, autorskim pravom zaštićenog djela i dijeljenje istog svodi na svega nekoliko klikova mišem, ovaj problem je prisutniji više nego ikad. Ovim problemom najviše je pogođena glazbena industrija, jer sadašnje brzine prijenosa podataka, još koliko toliko štite filmsku industriju dok diskografske kuće i glazbeni umjetnici gube milijarde dolara te su im gubici još uvijek u tendenciji rasta.

Na rješavanju ovog problema se dosta radi te je predloženo nekoliko sustava no neko efikasno i učinkovito rješenje nije pronađeno. Bitno je istaknuti da tradicionalna kriptografija ne može ponuditi potpuno rješenje, ona može omogućiti tajan prijenos, ali sadržaj će morati biti dekriptiran i poslan do zvučne kartice računala. U najgorem slučaju potencijalni napadač će moći uhvatiti zvuk na analognom signalu i time je sadržaj razotkriven.

Ovaj rad se prvenstveno bavi primjenom steganografije na audio datotekama, nekim metodama steganografije te prednostima i nedostacima steganografije. Rad je organiziran u pet poglavlja. Prvo poglavlje je uvodno dok drugo govori općenito o steganografiji. U trećem poglavlju napravljen pregled tipova i metoda audio steganografije, a u četvrtom su navedeni i objašnjeni najpoznatiji algoritmi označavanja audio datoteka. U posljednjem petom poglavlju navedeni su zaključci rada.

2. OPĆENITO O STEGANOGRAFIJI

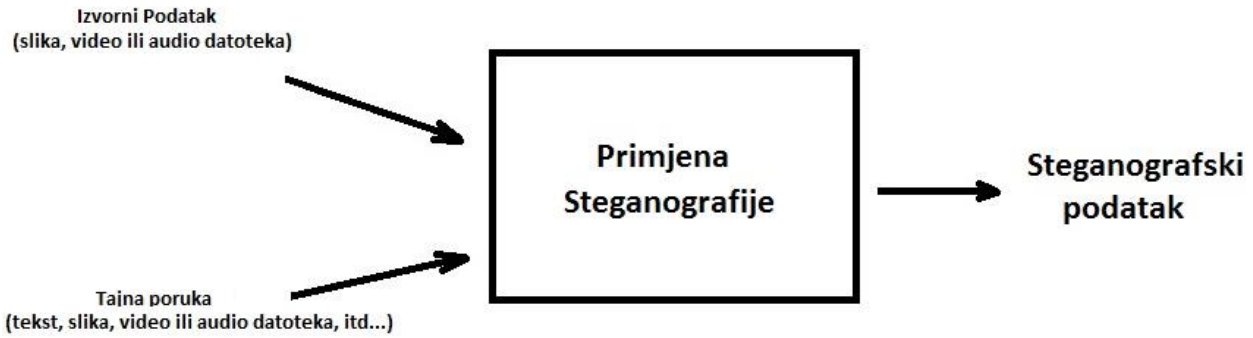
Steganografija (engl. *steganography*) je znanost i vještina zapisivanja poruke na takav način da nitko, osim pošiljatelja i primatelja poruke, ne posumnja u njezino postojanje [4]. Riječ steganografija je proizašla iz grčkih riječi *steganos* i *graphein*, što u prijevodu znači *skriveno pisanje* [1]. Steganografija spada u područje skrivanja informacija (engl. i*nformation hiding*).

Steganografija se legalno koristi kada kriptografija nije dopuštena ili češće kao dodatak kriptografiji. Kriminalci koriste steganografiju za skrivanje informacija ili materijala u svrhu trgovine dječje pornografije, počinjenja prijevare te izbjegavanje vladine cenzure u inozemstvu.

Upotreba steganografije se najčešće odvija u dva smjera:

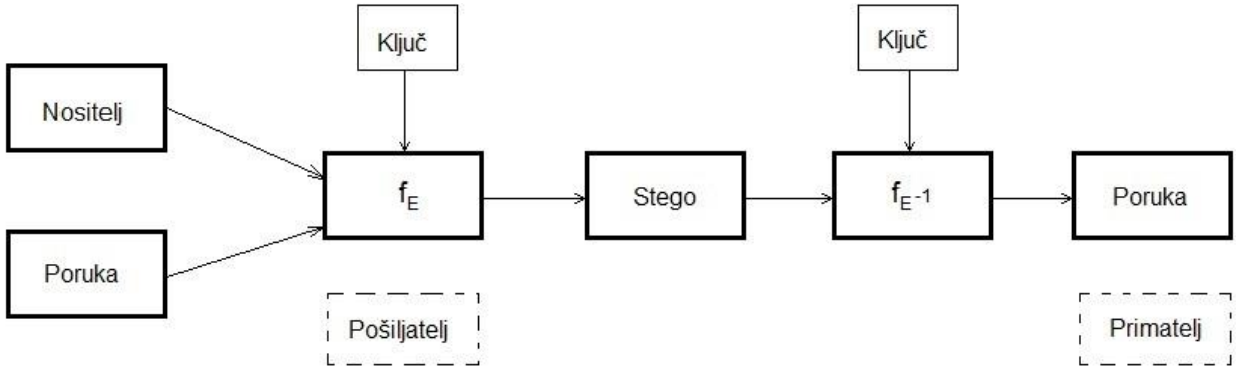
1. zaštita protiv otkrivanja (skrivanje informacija)
2. zaštita protiv uklanjanja:
   a) vodeni žig (svi objekti se obilježavaju na isti način)
   b) otisak prsta (svaki objekt je obilježen jedinstveno) [7].

Slika 2.1. prikazuje primjenu steganografske aplikacije koja skriva različite vrste podataka unutar početne datoteke.



Slika 2.1. Sustav primjene steganografije

Rezultat također sadrži skrivene informacije, iako je virtualno identičan početnom podatku. Steganografija zapravo iskorištava slabost ljudske percepcije jer ljudska osjetila nisu obučena za traženje podataka koji u sebi imaju skrivene informacije, iako postoje programi koji mogu provesti radnju koju nazivamo stegoanaliza (engl. *steganalysis*) odnosno detekcija upotrebe steganografije. Slika 2.2. prikazuje blok dijagram sigurnog steganografskog sustava.



Slika 2.2. Steganografski sustav

Ulazne poruke mogu biti tekst, audio i video zapisi, itd. Komponente steganografskog sustava su:

Nositelj – medij unutar kojeg se skriva tajna poruka

Poruka – tajna poruka koja treba biti skrivena

f_E – steganografska funkcija za ugrađivanje koja sadrži nositelja, poruku i ključ kao parametre i koja proizvodi stego kao izlazni rezultat

f_E^{-1} – steganografska funkcija za izdvajanje koja sadrži stego i ključ kao parametre, a kao izlazni rezultat daje skrivenu poruku. f_E^{-1} je inverzna funkcija od f_E

Ključ – steganografski ključ (parametar funkcije f_E)

Stego – steganografski podatak

Steganografska funkcija ugradnje f_E, skriva tajnu poruku u nositelja. Točna pozicija gdje će se skriti tajna poruka ovisi o ključu. Kao rezultat skrivanja, početna funkcija se vrlo malo mijenja i naziva se stego podatak. Nakon što primatelj primi stego podatak on počinje proces izdvajanja inverznom funkcijom f_E^{-1} sa stego podatkom i ključem kao parametrima. Ukoliko je ključ koji ima primatelj isti kao onaj koji je koristio pošiljatelj za ugradnju tajne poruke i ukoliko je stego podatak koji ima primatelj isti kao onaj koji ima pošiljatelj bez da je promijenjen od strane treće osobe, onda će funkcija izdvajanja kao rezultat imati točnu tajnu poruku.

U kriptografiji, struktura poruke je razbacana da bi ju se prikazalo kao nerazumljivu i beznačajnu, osim ako ključ za dešifriranje nije dostupan, te se zbog toga ne pokušava zamaskirati ili sakriti šifriranu poruku. Odnosno, kriptografija nudi mogućnost prijenosa podataka između dvije osobe na taj način da sprječava čitanje istih od strane treće osobe. Kriptografija također može ponuditi provjeru autentičnosti identiteta nekoga ili nečega. [4]

U steganografiji, šifrirana poruka se ne mijenja nego se skriva unutar medija za prijenos podataka tako da se ne može vidjeti. Poruka u brojčanom tekstu, na primjer, može izazvati sumnju na dijelu kod primatelja poruke dok nevidljiva poruka napravljena steganografskim metodama neće. Drugim riječima, steganografija sprječava sumnju nenamjernog primatelja u postojanje poruke. Zaštita klasične steganografije se zasniva na tajnosti sustava za kodiranje podataka, a onda kada je sustav za kodiranje podataka otkriven, moguće je otkriti i tajnu poruku.[5,6]

Steganografija bi doživjela preporod ukoliko bi se usvojile sljedeće mjere:

- kada bi zakoni zabranili digitalnu kriptografiju. Pojedinci i tvrtke koje traže povjerljivost podataka okrenuli bi se steganografiji kao važnom dodatku budući da spajanje kriptografije i steganografije može pomoći u zaštiti podataka te smanjenju sumnje u postojanje neke tajne informacije ili poruke;
- povećani zahtjevi za zaštitu prava intelektualnog vlasništva putem učinkovitog vodenog žiga od strane vlasnika digitalnih sadržaja;
- trenutno postoji trend elektroničkih komunikacija i ljudska želja da sakriju poruku od znatiželjnih pogleda, te zbog povećanog rasta u tehnologiji, steganografski programi, postaju vrlo uspješni u sakrivanju informacija u slici, video zapisu, audio datoteci, tekstu i slično;

2.1. Steganografija kroz povijest

Kronološki pregled steganografije kroz povijest je vrlo zanimljiv i dan u [2]. U nastavku su navedene neke zanimljivosti preuzete iz [1],[2] i [3].

U drevnoj Grčkoj su se za pisanje upotrebljavale drvene ploče prelivene voskom. Tajna poruka se mogla napisati na drvenu ploču prije nego se ploča prelila voskom. Nakon što se ploča prelila voskom, tajna poruka je ostala skrivena. Osim voštane ploče, tajna informacija se skrivala i na tijelima glasnika. Glava glasnika bi se obrijala i na njoj bi se tetovirala tajna poruka. Nakon što bi kosa narasla, tajna poruka bi ostala skrivena, a čitanje poruke bi se vršilo brijanjem glasnikove glave. Ovakve tehnike su korištene u Grčko-Perzijskim ratovima.

Drevni Kinezi su na tanki komad svile zapisivali poruku, zatim su taj komad stavljali u voštanu kuglicu koju bi glasnik progutao. Redovnik Johannes Trithemius je oko 1500. godine napisao knjigu Steganographia u kojoj je opisao kako sakriti poruku unutar bezazlenog teksta. Knjiga je izdana 1606. Talijanski znanstvenik Giovanni Porta, rođen 1535. godine, je otkrio kako sakriti poruku unutar skuhanog jaja. Kao tintu je koristio mješavinu octa i alauna. Poruku bi nanio na skuhano jaje, a tinta od alauna i octa bi prodrla kroz ljusku jaja. Skrivena poruka bi se očitala s

bjelanjka nakon što bi se jaje ogulilo. Tijekom Drugog svjetskog rata se nevidljiva tinta koristila za prijenos tajne poruke. Dobivanje skrivene poruke se zasnivalo na svojstvu da tinta postaje vidljiva prilikom zagrijavanja, odnosno kontakta s određenom kemijskom supstancom. Također, poruke su se znale prenositi u predivu korištenjem znakova Morseove abecede ili na poleđini poštanskih markica. Tijekom i nakon Drugog svjetskog rata bila je česta uporaba mikrofotografija (engl. *microdots*). Mikrofotografije su bile veličine točke pa su se lako mogle smjestiti, tj. nalijepiti, u tekst. Ipak, tako nalijepljene mikrofotografije bi reflektirale svjetlost kada bi se papir okrenuo pod određenim kutom pa su bile primjetne. Potrebno je spomenuti i korištenje nulte šifre u špijunaži. Tako je Valvalee Dickinson, japanska špijunka i preprodavačica lutaka, slala pisma narudžbe u Južnu Ameriku u kojima su se nalazile skrivene informacije o kretanjima brodova.

2.2. Tipovi steganografije

Dva su osnovna tipa steganografije: tehnička steganografija (engl. *tehnical steganography*) i lingvistička steganografija (engl. *linguistic steganography*).Tehnička steganografija se ogleda u korištenju posebnih tehničkih sprava, uređaja, instrumenata i metoda u skrivanju poruke. U tehničku steganografiju spada

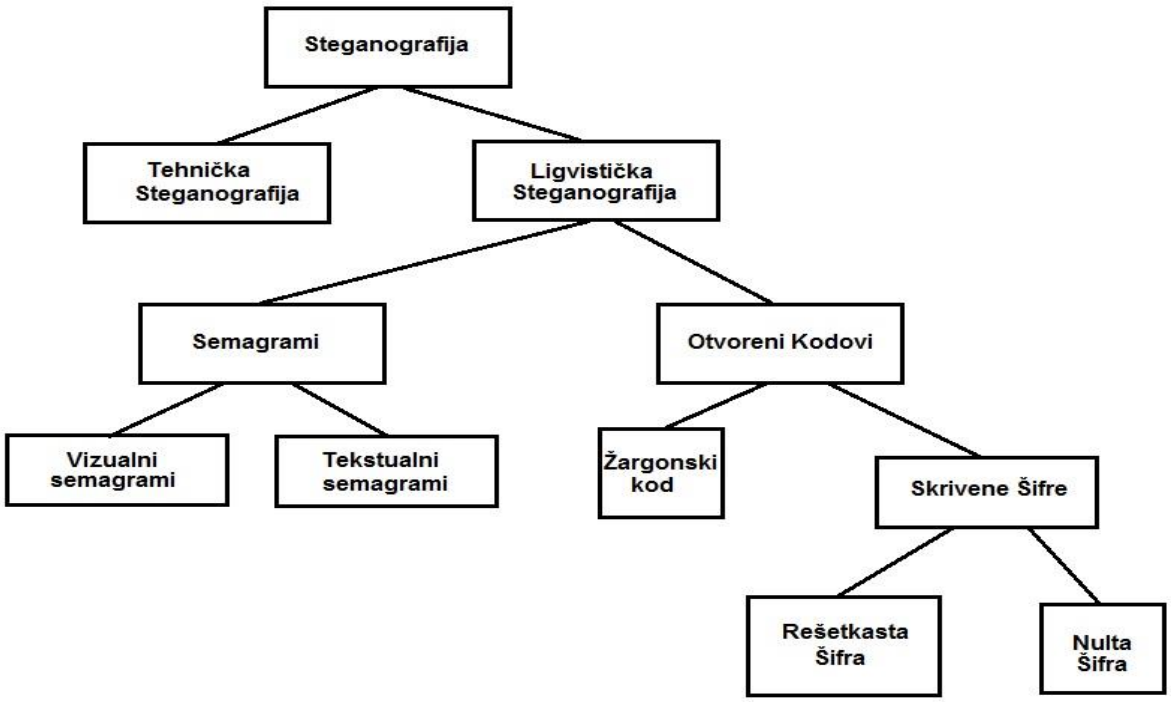
- nevidljiva tinta: tinta koja nema boje dok se ne dovede u kontakt s toplinom ili nekom kemijskom supstancom,
- korištenje skrovitih mjesta: primjerice, skrivanje na dnu pivske bačve ili tetovaža ispod kose,
- mikrofotografije (microdots): fotografije veličine manje od pola milimetra,
- računalom zasnovane metode: mnogobrojne metode proizašle upotrebom računala.

Lingvistička steganografija obuhvaća steganografske metode koje skrivaju tajnu poruku u objekt nositelj jezičnog sadržaja. Lingvistička steganografija dijeli se na [1]:

- Semagrami (semagrams): razmještaju se simboli, znakovi ili objekti, ali tako da promjene koje nose informacije ne budu vidljive. Dvije su vrste:
    - Vizualni semagrami (visual semagrams): fizički objekti i njihov razmještaj upućuju na sadržaj skrivene informacije.
    - Tekstualni semgrami (engl. *tekstual semagrams*): preinakom teksta se postiže skrivanje informacije (primjerice veličina slova, fonta i dr.).
- Otvoreni kodovi (engl. *open codes*): poruka s javnom informacijom se koristi kako bi se skrila tajna poruka. Otvorene kodove dijelimo na:

- Žargonski kod (engl. *jargon code*): koristi se jezik koji razumije samo određena skupina ljudi.
- Skrivene šifre (engl. *covered ciphers*): Poruka se može izvaditi iz stego podatka samo ako je poznat algoritam skrivanja tajne poruke. Tako u skrivene šifre spadaju:
    - Rešetkasta šifra (engl. *grille ciphers*): koriste se maske s otvorima, tj. rupicama, i slova koja se pojavljuju u rupicama upućuju na skrivenu poruku.
    - Nulta šifra (engl. *null ciphers*): skrivena poruka se čita na temelju prethodno definiranih jednostavnih pravila npr. jednostavno pravilo može biti: čita se svako deseto slovo.

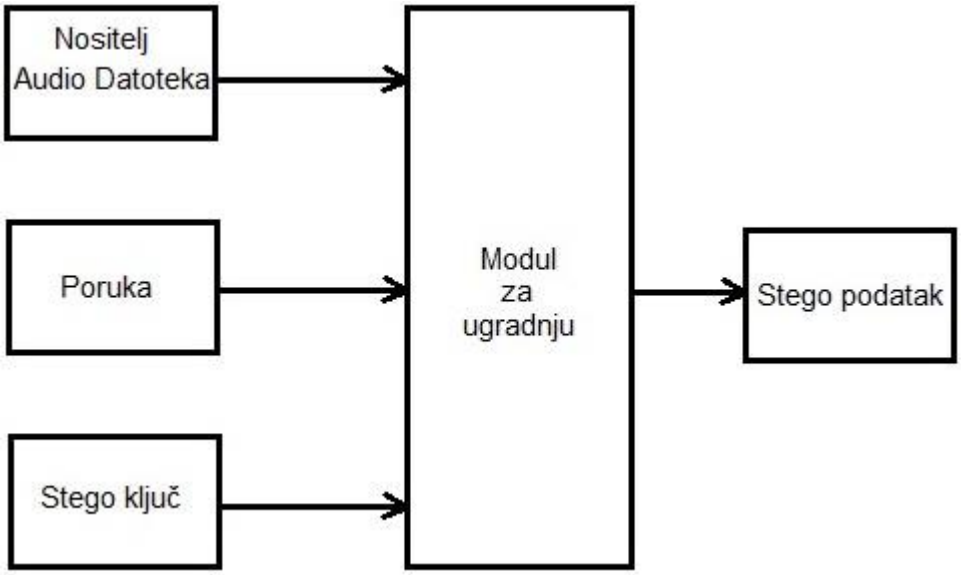
Podjela steganografije je prikazana na slici 2.3.



Slika 2.3. Podjela steganografije

2.3. Općenito o audio steganografiji

Osnovni model audio steganografije se sastoji od nositelja (audio datoteka), poruke i lozinke. Nositelj je također poznat i kao medij u koji se prikriva tajna poruka.



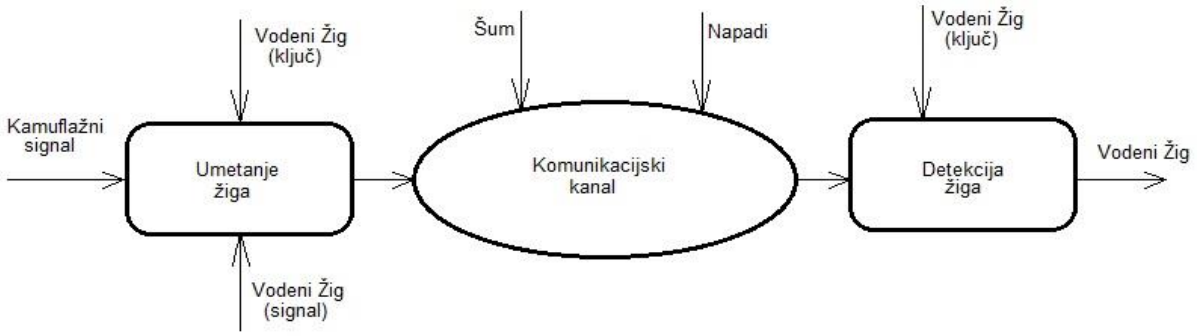
Slika 2.4. Osnovni audio steganografski model

Na slici 2.4. je prikazan osnovni model audio steganografskog sustava, poruka je podatak koji pošiljatelj želi da ostane tajan. Poruka može biti obični tekst, slika, audio ili neki drugi tip podatka. Lozinka je poznata kao stego ključ, koji osigurava da jedino primatelj koji zna odgovarajući ključ može izvući tajnu poruku iz nositelja. Modul za ugradnju je blok u kojem se poruka ugrađuje u nositelja koristeći stego ključ kao parametar za ugradnju, te uz pomoć kojeg primatelj može izvući tajnu informaciju. Nositelj koji sadrži tajnu informaciju je poznat kao stego podatak.

3. DIGITALNI VODENI ŽIGOVI

Vodeni žigovi ne predstavljaju novu tehniku. Oni su zapravo preteča steganografije. Vodeni žigovi se mogu smatrati posebnom tehnikom steganografije, gdje se jedna poruka ubacuje unutar druge te kao takve tvore jednu cjelinu odnosno one su na neki način povezane jedna s drugom. Ime je dobila prema označavanju papira vodenim žigovima. Vodeni žig zapravo je informacija koja se umeće u originalan sadržaj (slika, audio, video, tekst...) tako da korisnik ne vidi (ili ne čuje) razliku između originalnog i označenog sadržaja. Najjednostavniji primjer vodenih žigova su karakteristični oblici na novčanicama koji se mogu vidjeti samo kada je novčanica okrenuta prema svjetlosti ili logo u pozadini tiskanih tekstualnih dokumenata. Tehnike vodenih žigova služe za sprječavanje krivotvorenja i neovlaštenog kopiranja fizičkih objekata. Tehnike označavanja digitalnih vodenih žigova su iste kao tehnike označavanja fizičkih objekata, s tom razlikom da se tehnika označavanja digitalnim vodenim žigovima koristi za digitalne sadržaje, a ne fizičke objekte. Kod tehnike označavanja digitalnim vodenim žigovima, signal male energije se neprimjetno ubacuje u drugi signal. Taj signal se naziva vodeni žig (engl. *watermark*) i on opisuje neke detalje kao što su sigurnosne i tajne informacije o glavnom signalu. Glavni signal (nositelj), u koji se dodaje vodeni žig, se označava kao kamuflažni signal (engl. *cover signal*), jer on skriva vodeni žig. Kamuflažni signal je obično nepokretna slika, audio ili video zapis ili tekst dokument u digitalnom formatu.

Postoje različite definicije termina vodenog žiga koji je u vezi sa digitalnim sadržajem. Jednu od najjednostavnijih je dao Cox: „Mi definiramo proces umetanja vodenih žigova kao obavljanje neprimjetnog mijenjanja jednog djela informacije kako bi ubacili tajnu informaciju baš o tom djelu“. U ovoj definiciji, taj jedan dio informacije se odnosi na pjesmu, video ili sliku. Ključna stvar koja se može izvući iz ove definicije je da informacija koja je skrivena u tome djelu informacije, odnosno vodeni žig, sadrži informaciju o djelu informacije u koji je ubačen. Ova karakteristika predstavlja osnovni uvjet po kojem se proces umetanja vodenih žigova razlikuje od osnovnih principa steganografije. Još jedna razlika između vodenih žigova i steganografije je da kod vodenih žigova postoji dodatna ideja o zaštiti protiv napada. Dakle ako se Cox-ova definicija vodenih žigova svede na domenu obrade audio signala, može se dobiti preciznija definicija o digitalnim vodenim žigovima u audio tehnici. Digitalni vodeni žigovi u audio tehnici se definiraju kao proces „ubacivanja niza bitova specifičnog od strane proizvođača u digitalni audio signal, tako da je dodavanje niza bitova (vodenog žiga) osjetilima beznačajno, odnosno korisnik ne čuje razliku između originalnog i označenog sadržaja“.



Slika 3.1. Osnovna shema sustava digitalnog vodenog žiga

Na slici 3.1. je prikazana osnovna shema jednog sustava digitalnog vodenog žiga. Kao što se može vidjeti sa slike, sustav digitalnog vodenog žiga se sastoji od bloka za umetanje žiga (engl. *watermark embedder*) i bloka za detekciju (engl. *watermark detector*). Blok za umetanje vodenog žiga ubacuje vodeni žig u kamuflažni signal, dok blok za detekciju otkiva prisustvo signala vodenog žiga. Značajno je primijetiti postojanje ključa vodenog žiga (engl. *watermark key*) koji se koristi i tokom procesa umetanja i tokom procesa detekcije digitalnog vodenog žiga. Ključ vodenog žiga ima jedinstvenu povezanost sa signalom vodenog žiga, odnosno za svaki signal vodenog žiga postoji jedinstveni ključ vodenog žiga. Ključ vodenog žiga je tajan i poznat samo ovlaštenim stranama i on osigurava da samo ovlaštene strane mogu detektirati vodeni žig. Na kraju možemo primijetiti da komunikacijski kanal može biti izložen šumu i različitim namjernim i nenamjernim napadima koji mogu dovesti do oštećenja ili potpunog uklanjanja žiga. Nenamjerni napadi na vodene žigove mogu biti kompresije s gubitkom, promjena frekvencije odabiranja, mijenjanje broja kanala u zvuku, itd., i većina žigova ih može preživjeti. U namjerne napade, koje bi zlonamjerni napadači mogli iskoristiti sa svrhom uklanjanja žiga podrazumijevaju se napadi različitim frekvencijskim filterima, napadi desinkronizacijom i slične tehnike.

3.1. Razvoj digitalnih vodenih žigova u audiotehnici

Početak upotrebe digitalnih vodenih žigova u audio signalima se može vezati za 1954. godinu kada je Emil Hembrooke patentirao ideju „identifikacija zvuka i sličnih signala“. On opisuje metodu za umetanje nečujnog identifikacijskog koda u glazbeni zapis u svrhu dokazivanja intelektualnog vlasništva. U tekstu patenta je navedeno da ovaj izum omogućava sigurnu identifikaciju originala nekog glazbenog uratka i na taj način predstavlja efikasnu metodu za sprječavanja piratstva.

Od tada, pojavile su se i razvile brojne tehnologije vodenih žigova za različite aplikacije, razvijeni su sustavi za dokazivanje pravovaljanosti reklama i kontrolu uređaja. 1962. godine tvrtka Lynch

Carrier Systems Inc. patentirala je „međupojasni sustav signalizacije“ napravljen za kontrolu telefonske opreme. Interes za istraživanje digitalnih vodenih žigova nije bio u fokusu sve do 1990-ih godina. U prvoj polovici desetljeća interes je vrlo brzo rastao te danas postoje mnogi znanstveni radovi i konferencije koje za temu imaju digitalne vodene žigove. S napretkom računalne tehnologije i razvojem interneta gorući problem je postala potražnja za zaštitom autorskih prava. Kako bi se pružila što bolja zaštita, osnovane su brojene industrijsko tehnološke grupacije, među najpoznatijima su Copy Protection Tehnical Working Group i Strategic Digital Music Initiative. One su prepoznale da kriptografija može pružiti zaštitu samo prilikom distribucije sadržaja, ali kada ju korisnik jednom dešifrira, sva zaštita je izgubljena. Vodeni žigovi, za razliku od kriptografije, pružaju zaštitu i poslije dešifriranja, čak i kada sadržaj uđe u analogni svijet. Unatoč tome, prvobitna očekivanja od digitalnih vodenih žigova su vjerojatno bila previsoka, posebno s obzirom na konstantne namjerne pokušaje da se digitalni žig odstrani iz sadržaja. Razlog ovome je što još uvijek nije pronađen vodeni žig kojeg nikako nije moguće ukloniti.

3.2. Osobine i vrste vodenih žigova

Osobine vodenih žigova najviše ovise o tome za što će se primjenjivati. Najčešći zahtjevi koje vodeni žigovi moraju ispuniti su slijedeći:

- Umetanjem odnosno ugradnjom žiga, originalni sadržaj treba biti što je moguće manje oštećen, odnosno, razlika između originala i označenog sadržaja ne bi trebala biti čujna;
- Žig mora biti ugrađen direktno u sam sadržaj (zvuk, sliku...), a ne u zaglavlje sadržaja, kako bi ostao netaknut u pretvorbama između različitih formata zapisa, i kako bi bio otporniji na napade;
- Žig bi trebao biti otporan na namjerne i nenamjerne pokušaje njegova uklanjanja kao što su dodavanje šuma, filtriranje, odsijecanje, kompresije s gubitkom, digitalno-analogne (D/A) pretvorbe ili analogno-digitalna (A/D) pretvorbe;
- S obzirom da će označeni signal vjerojatno doživjeti degradaciju, poželjno je da žig sadrži nekakav kod detekcije i ispravljanja grešaka;
- Žig bi trebao biti umetnut preko cijelog originalnog sadržaja, tako da se i u malom odsječenom dijelu sadržaja može otkriti prisustvo žiga;
- Poželjno je da se umetanje i detekcija žiga izvršava direktno u kompresiranoj domeni signala, što donosi uštedu vremena;
- Također je poželjno da sustav omogućava umetanje više od jednog vodenog žiga u sadržaj, na primjer može se umetnuti identifikacijski kod kupca neke pjesme i kod autora pjesme.

Navedene osobine se odnose na vrstu žigova koji su najčešći i najzanimljiviji za primjenu, a zovu se otporni, čvrsti ili nelomljivi žigovi. Osim njih postoje i lomljivi vodeni žigovi (engl. *fragile watermarks*). Razlika je u tome što se otporni žigovi rade tako da ih je nemoguće ukloniti bez značajnijeg oštećenja sadržaja, dok su lomljivi žigovi takvi da ukoliko otkriju bilo kakvu promjenu na sadržaju i ako se ona dogodi, oni se unište (slome se). Oni se koriste za čuvanje integriteta podataka i ukazuju nam ukoliko je sadržaj na bilo kakav način mijenjan. Poželjna osobina koju bi ovi žigovi trebali imati je mogućnost otkrivanja vrste promjene koju je sadržaj pretrpio. Posebna podskupina lomljivih žigova su polu-lomljivi žigovi (engl. *semi-fragile watermarks*). Polu-lomljivi žigovi rade isto što i lomljivi, s razlikom što se ne bi trebali slomiti kod nekih manipulacija koje ne uništavaju signal značajno, kao što je kompresija s gubitkom.

Još jedna podjela digitalnih vodenih žigova je podjela na javne i tajne žigove. Većina današnjih žigova spada u kategoriju tajnih, a karakteristika tajnih žigova je ta da je kod otkrivanja potrebno poznavanje žiga koji je korišten kod označavanja, a taj žig je tajan i nije dostupan javnosti. Karakteristika javnih žigova je ta da kod otkrivanja nije potrebno poznavanje vrijednosti žiga. Takvi žigovi su obično slabije otporni na napade, a mogu omogućavati puno širu primjenu vodenih žigova.

Sami žigovi su u većini primjena predstavljeni kao nizovi realnih ili binarnih brojeva. Čuvanje takvog zapisa žiga u datoteci bi zauzimalo dosta prostora, pa se u većini sustava vodenih žigova koristi neki predefinirani generator pseudoslučajnih brojeva. Time je onemogućeno da se sam žig može sačuvati kao tajni ključ koji se koristi kao slučajno odabran generatora pseudoslučajnih brojeva, a vrijednosti žiga se mogu otkriti kada je to potrebno.

3.3. Osobine ljudskog slušnog sustava

Znanost o psihoakustici opisuje akustiku iz perspektive ljudskog slušnog sustava. Sposobnost slušnog sustava ne samo da se istražuje kao kvalitativni odnos između zvuka i odgovarajućeg dojma nego kao i kvantitativni odnos između predstavljenih poticaja i dojma sluha. Digitalne audio tehnologije poput razvoja MPEG standarda se temelje na detaljnom poznavanju ljudskog čula sluha. Relevantni podaci nisu samo da uho može čuti frekvencije u rasponu od 20 Hz do 20 kHz i dinamičkog raspona preko 96 dB, nego i interakcija različitih frekvencija i odgovarajuće obrade ljudskog slušnog sustava. Također, za dublje razmišljanje važno uzeti u obzir korelacije između akustičnih poticaja i dojma sluha.

Razvoj točnog modela sluha je složen i u određenoj mjeri subjektivan zadatak. Fizički, zvuk je jednostavno opisan kao vremenski promjenjivi zvučni tlak p(t). Osnovna ideja kod digitalnih

vodenih žigova je da ugrađeni žig bude nečujan, što je moguće zahvaljujući nesavršenosti ljudskog slušnog sustava, odnosno ranjivosti na maskiranje u vremenskoj i frekvencijskoj domeni. Međutim treba napomenuti da je ugrađivanje digitalnog vodenog žiga u audio datoteke znatno teži zadatak od ugrađivanja žigova u slike ili video zapise zbog značajno šireg dinamičkog opsega čula sluha u odnosu na čulo vida.

Ljudski slušni sustav ima veliku osjetljivost na aditivni bijeli Gaussov šum. S druge strane, za razliku od velikog dinamičkog opsega, ljudski slušni sustav obuhvaća mali diferencijalni opseg, što znači da jači zvukovi mogu prikriti slabije.

Maskiranje, visina, kritični opseg, pobuda i samo vidljive promjene opisuju aktivne obrade uha. Od ovih učinaka najvažniju ulogu igra maskiranje uz kompresiju s gubitkom digitalnih audio podataka. Za primjenu i učinkovitu kompresiju audio podatka razvijeni su i usavršeni modeli maskiranja u frekvencijskoj i vremenskoj domeni. Maskiranje je pojava koja se pojavljuje svakodnevno u životu zbog nemogućnosti sluha da prepozna neki zvučni signal samo zbog toga što istovremeno stiže neki drugi zvuk koji ga na neki način maskira. Dakle svaki zvuk koji dospije u uho svojom pobudom izaziva efekte zbog kojih nije moguće istovremeno registrirati neke druge zvukove koji su mu u frekvencijskoj ili vremenskoj domeni suviše blizu, ali pri tome ne dovoljno jaki. Do maskiranja može doći zbog bliskosti maskirajućeg i maskiranog zvuka na skali frekvencija (frekvencijsko maskiranje) ili zbog međusobne blizine na vremenskoj osi (vremensko maskiranje).

3.4. Frekvencijsko maskiranje

Frekvencijsko maskiranje je pojava u frekvencijskoj domeni gdje signal malog intenziteta može biti nečujan (maskirani signal), odnosno maskiran od strane signala jačeg intenziteta (maskirajući signal), ako su ova dva signala bliska na frekvencijskoj ljestvici.

Kritični opsezi predstavljaju važan koncept u opisu slušnog dojma. Odgovarajući konstrukt, tzv. stopa razmjera kritičnih opsega, definiran je činjenicom koja se temelji na tome da ljudski slušni sustav analizira široki spektar u različitim dijelovima. Ovi dijelovi su tzv. kritični opsezi. Tablica 3.1. je izrađena dodavanjem jednog kritičnog opsega na sljedeći kritični opseg i to na takav način da gornja granica nižeg kritičnog opsega odgovara donjoj granici sljedećeg višeg kritičnog opsega.

Tablica 3.1. Bark ljestvica kritičnih opsega

z/bark	f_u/Hz	f_0/Hz	f_G/Hz	*z/bark*	f_u/Hz	f_0/Hz	f_G/Hz
0	0	100	100	13	2000	2320	320
1	100	200	100	14	2320	2700	380
2	200	300	100	15	2700	3150	450
3	300	400	100	16	3150	3700	550
4	400	510	110	17	3700	4400	700
5	510	630	120	18	4400	5300	900
6	630	770	140	19	5300	6400	1100
7	770	920	150	20	6400	7700	1300
8	920	1080	160	21	7700	9500	1800
9	1080	1270	190	22	9500	12000	2500
10	1270	1480	210	23	12000	15500	3500
11	1480	1720	240	24	15500		
12	1720	2000	280				

Kritična propusnost ima konstantnu vrijednost od 100 Hz do sredine frekvencije od oko 500 Hz. Iznad 500 Hz, dovoljno dobra aproksimacija za propusnost f_G/Hz iznosi 20% od stvarne frekvencije. Sljedeća dva analitička izraza se koriste za opisivanje ovisnosti kritičnog pojasa:

$$z = 13 \arctan\left(0.76 \frac{f}{kHz}\right) + 3.5 \arctan\left(\frac{f}{7.5\ kHz}\right)^2 \quad \text{[Bark]}$$

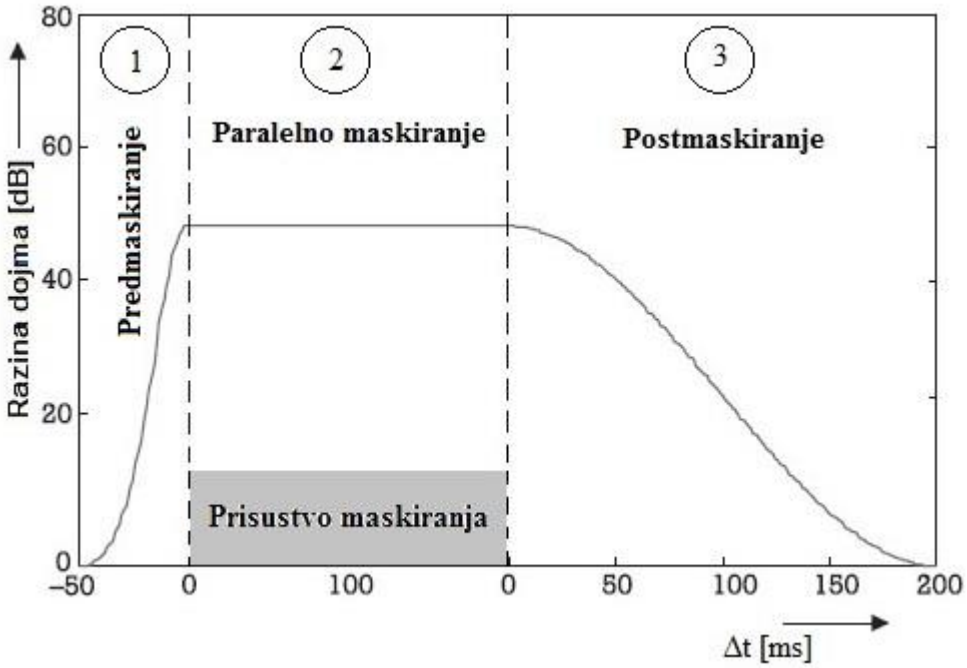
$$\Delta f_G = 25 + 75[1 + 1.4(\frac{f}{kHz})^2]^{0.69} \quad \text{[Hz]}$$

Kritična propusnost kao funkcija frekvencije prikazuje nelinearno ponašanje ljudskog slušnog sustava. Brzina razmjera kritičnog opsega raste od 0 do 24 i ima jedinicu Bark. Brzina kritičnog opsega je povezana s nekoliko drugih ljestvica koje opisuju karakteristike slušnog sustava.

3.5. Vremensko maskiranje

Pri pobudi slušnog sustava nekim zvučnim signalom postoji izvjesna zona na vremenskoj osi prije i poslije njegovog djelovanja u kojoj drugi zvukovi, ako nemaju dovoljan intenzitet, ne mogu biti primijećeni. Skoro svaki tip glazbe ima snažnu privremenu strukturu. Test i maskiranje zvuka imaju vremenski karakteristične proizvode tzv. vremenski maskirane učinke. Zbog zahtjeva za mjerenje vremenskih odnosa između tona i maskirnog signala, test zvuk je pomaknut u odnosu na

maskirni signal. U odnosu na vremenski pomak Δt u odnosu na masker, razlikuju se tri područja: predmaskiranje, paralelno maskiranje i postmaskiranje.



Slika 3.2. Vremensko maskiranje kod slušnog sustava sa tri područja

Predmaskiranje se događa prije nego što je maskirni signal uključen u području 1. Predmaskiranje traje oko 20 ms u svim uvjetima. Dakle, prag ostaje nepromijenjen dok Δt ne dosegne negativnu vrijednost 20 ms prema slici 3.2. Nakon 20 ms ≤ t, prag se povećava i doseže razinu paralelnu maskiranju neposredno prije nego se maskirni signal uključi. Učinak predmaskiranja na prvi pogled izgleda kao slušanje u budućnost. Zbog toga se zaključuje da obrada informacija u ljudskom slušnom sustavu ne radi trenutno. Vrijeme potrebno da se osjeti zvuk ovisi o glasnoći izvedenog zvuka. Dakle, glasniji maskirni zvuk ima kraće vrijeme pripreme od slabašnog ispitnog zvuka i ranije će biti zapažen.

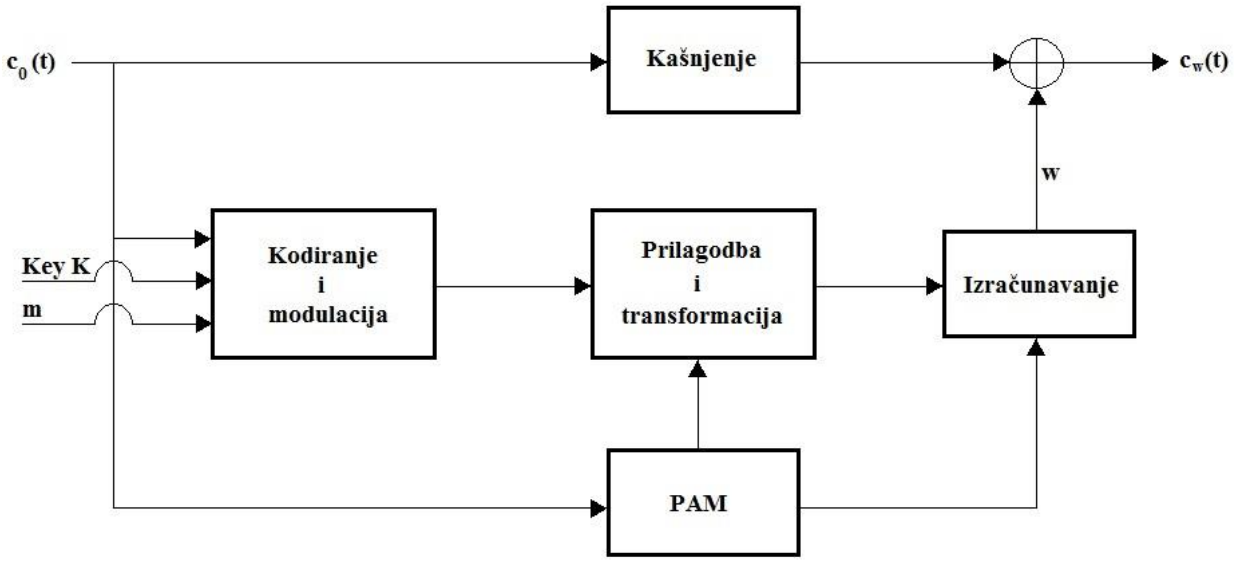
Drugo područje je područje paralelnog maskiranja. Prag u tišini i prag u maskiranoj tišini ovise o duljini trajanja testnog zvuka. Ovo se može objasniti ako se uzme u obzir da slušni sustav integrira jakost zvuka u trajanju od 200 ms. Stoga, za trajanje testnog zvuka kraćeg od 200 ms, prag u tišini i prag maskiranja se povećavaju zbog slabijeg intenziteta te zbog sposobnosti integracije u slušni sustav.

Treće područje opisuje postmaskiranje koje odgovara opadanju učinka maskiranja nakon što je maskirni signal isključen. Nakon 5 ms kašnjenja prag maskiranja dosegne prag tišine.

Postmaskiranje uvelike ovisi o trajanju maskirnog signala. Krivulja opadanja praga maskiranja je puno strmija za kraće maskirne signale.

3.6. Izravno korištenje perceptivnog maskiranja

Zadatak kodera vodenog žiga je prilagoditi signal vodenog žiga kako bi se osigurala nečujnost i istovremeno ugradnja vodenog žiga s maksimalnom snagom prema signalu nositelja da bi se osigurala maksimalna robusnost. Šifriranje perceptivnog audio vodenog žiga obično se sastoji od nekoliko komponenti. Blok kodiranje i modulacija kodira informaciju „m“ pomoću tajnog ključa „K“ i prilagođava izabranom nosaču komponente audio signala kao što su amplituda, faza i magnituda frekvencije u skladu s osnovnim algoritmom. Psihoakustički model (PAM) analizira izvorni signal $c_0(t)$ kako bi se izračunali perceptivni pragovi kao što je minimalni maskirajući prag LT_{min}. Također može predstavljati psihoakustičke kontrolne parametre kao što su maksimalno dopuštene fazne razlike ili vremensko maskiranje pragova. Model koji se koristi pokreće se specifičnim algoritmom. Budući da većina algoritama perceptivnih audio vodenih žigova ugrađuje vodeni žig u Fourrierovoj domeni, pažljivo se proučava spektralno oblikovanje šuma vodenog žiga.



Slika 3.3. Blok shema kodiranja vodenog žiga i njegovih komponenti

U ovom slučaju, blok prilagodbe na slici 3.3. predstavlja spektralnu težinu bloka umnožavanjem frekvencijskih komponenti buke vodenog žiga s koeficijentom težine kojeg izračunava PAM blok. Spektralna težina se često primjenjuje kao filter po dijelovima linearne aproksimacije maskirajućeg praga koji predstavlja frekvencijski odziv, što znači da se izvorni signal mora odgoditi prije nego se doda šum vodenog žiga. Filter korišten u aproksimaciji minimalnog

maskirajućeg praga može biti konačni impulsni odziv (FIR) te može biti kreiran metodom prozora. Gubitci signala zbog prozorskih rubova mogu se smanjiti preklapanjem uzastopnih blokova za 50%. Ovi izračuni moraju biti izvedeni za svaki blok duljine t = $\frac{512\ uzoraka}{\text{fs}\ uzoraka/s}$ s frekvencijom uzorkovanja f_s. Razina tlaka zvuka se mora podesiti nakon filtriranja šuma vodenog žiga. Za izračun točnog prigušenja šuma vodenog žiga procjenjuje se snaga spektra. Maskirni prag je rezultat psihoakustičke analize. Ona se temelji na usporednom izvornom signalu s maksimalnim pomakom od 96 dB. Ova usporedba se mora uzeti u obzir prilikom izračuna bloka, ako se računa snaga šuma vodenog žiga u odnosu na originalni signal. Takozvani omjer maskiranja šuma (engl. *noise masking ratio*) NMR=W-LT_{min} [dB] služi kao dodatni faktor prigušenja koji podešava razinu kvalitete u odnosu na robusnost. Rezultat je stvarni signal vodenog žiga dodan izvornom signalu da bi proizveo stazu vodenog žiga c_w (t). Nakon predstavljanja temeljnih psihoakustičkih metoda i načela koje ih integriraju u algoritme audio vodenih žigova, u sljedećim poglavljima su opisani razni algoritmi razvijeni u posljednjih nekoliko godina.

4. ALGORITMI OZNAČAVANJA AUDIO DATOTEKA

Postoje mnoge tehnike skrivanja informacija ili poruka unutar audio datoteka gdje se alternativno rješenje zasniva na način da su promjene nakon primjene steganografije potpuno neprimjetne. Uobičajeni pristupi audio steganografiji uključuju tehnike u rasponu od jednostavnih LSB metoda do metode raspršenog spektra. Značajke koje se koriste za ugrađivanje vodenog znaka jednog bita audio signala su amplituda u vremenskoj domeni, frekvencija i faza unutar Fourrierove domene i obilježja kompresiranog audio slijeda. Ove tehnike koriste vremensko i frekvencijsko maskiranje da bi ugradili vodeni žig unutar signala nositelja tako da vodeni žig bude neprimjetan. Drugim riječima ove tehnike koriste nedostatke ljudskog slušnog sustava, čula sluha.

4.1. LSB supstitucijska metoda

Jedna od prvih tehnika istraženih na području vodenih žigova je vrlo popularna metoda LSB supstitucie (eng. *last significant bit algorithm*), koja mijenja bitove najmanje važnosti tako da ih uskladi s tajnom porukom. Ona ne koristi psihoakustični model da bi oblikovala žig.

Proces skrivanja informacija se sastoji od dva koraka [8,9].

a) Otkrivanje suvišnog bita unutar nositelja. Suvišni bitovi su oni bitovi koji se mogu promijeniti bez oštećenja kvalitete ili uništavanja izvornog podataka unutar nositelja.
b) Ugradnja tajne informacije unutar nositelja, suvišni bit unutar nositelja se mijenja s bitom koji sadrži tajnu informaciju.

Ovo je obično učinkovita tehnika u slučajevima kada LSB supstitucija ne uzrokuje značajne gubitke kvalitete, kao što je u 24-bitnim bitmapama.

U računarstvu, najmanje značajni bit (LSB) je bit pozicioniran u najdesnijoj binarnoj jedinici dajući jedinici vrijednost, koja je dređuje bez obzira je li broj paran ili neparan. LSB se ponekad naziva i „najdesniji bit“, zbog matematičkog običaja pisanja najmanje značajne znamenke desno. To je analogno najmanje značajnoj znamenki decimalnog broja, koji se piše na najdesnijoj strani.

1	0	0	1	0	1	0	1

Slika 4.1. Binarni oblik decimalnog broja 149

Slika 4.1. prikazuje decimalni broj 149 u binarnom obliku, gdje je najmanje značajni bit označen sivom bojom. Najznačajniji bit (MSB) u 8-binarnom broju predstavlja vrijednost 128. decimale, a LSB predstavlja vrijednost 1. decimale. Npr. da bi sakrili slovo „a“ (ASCII kod 97, koji pretvoren

u binarni oblik izgleda 01100001) unutar 8 bajtova nositelja, LSB svakog bajta podešavamo ovako:

10010010

01010011

10011011

11010010

10001010

00000010

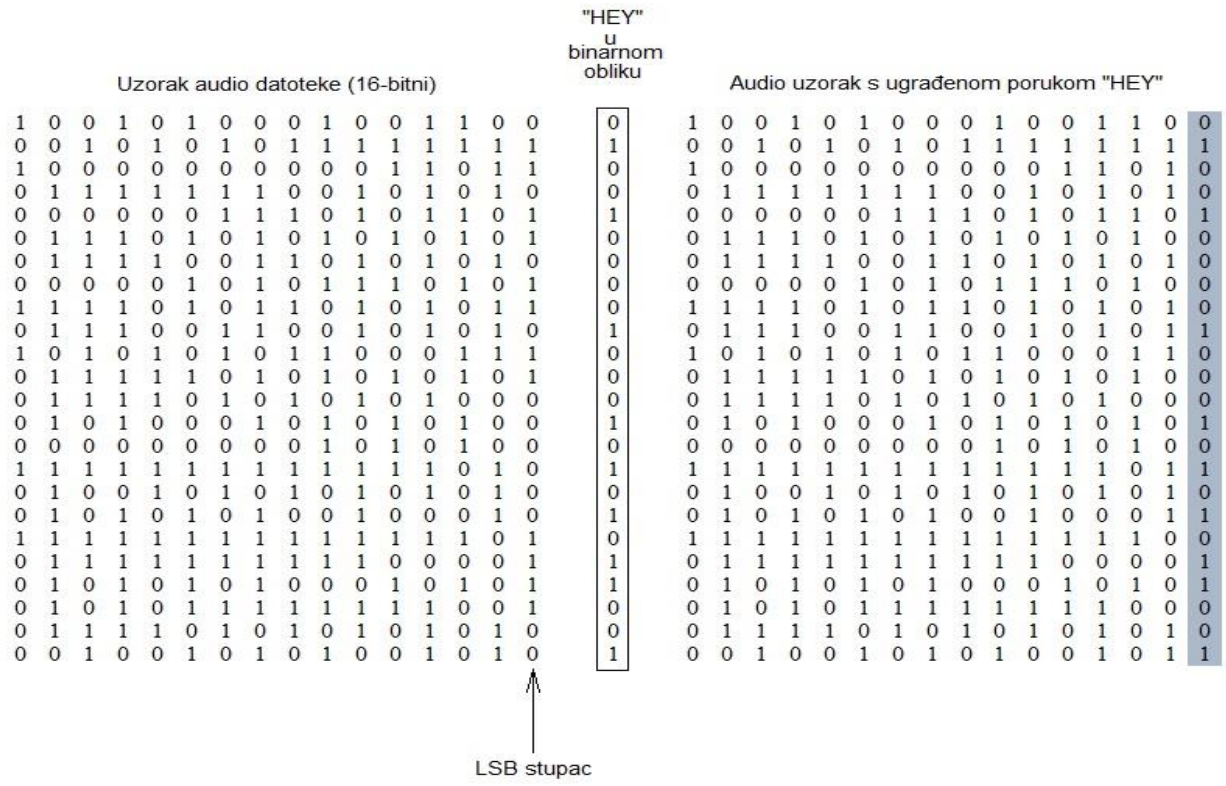
01110010

00101011

Sustav dekodiranja nositelja očitava 8 najmanje značajnih bitova potrebnih za izdvajanje skrivenog bajta koji je 01100001, slovo „a“, Kao što se može vidjeti, korištenjem ove tehnike može se sakriti jedan bit u svakih osam bitova nositelja. Također može se primijetiti da postoje 50% šanse da je bit koji se mijenja isti kao i njegova zamjena, drugim riječima u 50% slučajeva bit se uopće ne mijenja, što pomaže umanjiti degradaciju kvalitete.

Primjer rada LSB supstitucije je dan na slici 4.2. Kod audio podataka prirodan pristup LSB kodiranja je mijenjanje pojedinačnih uzoraka digitaliziranog audio slijeda amplitudne rezolucije npr. 16 bita (uobičajena amplitudna rezolucija za audio datoteke u cd formatu).

Na slici 4.2. je prikazano kako se poruka „HEY“ ugrađuje u 16-bitni audio uzorak CD kvalitete koristeći LSB metodu. Ovdje je tajna poruka „HEY“ i nositelj je audio datoteka. „HEY“ se treba ugraditi unutar audio datoteke. Prvo se tajna poruka „HEY“ i audio datoteka pretvaraju u niz bitova. Stupac najmanje značajnog bita se mijenja s nizom bitova tajne poruke „HEY“, te kao rezultat se dobije stego datoteka. Osim što ima veliku nosivost njegova mala otpornost na napade je glavni nedostatak ove metode, od kojih je najjednostavniji brisanje svakog LSB bita iz svakog uzorka zvuka. Također, LSB će prvi *nastradati* kod kompresije s gubitkom, što je za većinu primjena neprihvatljivo. Ova metoda zahtjeva točnu sinkronizaciju označenog audio signala prilikom procedure otkrivanja. Jedan od mogućih poboljšanja ove tehnike je smanjenje brzine prijenosa podataka. Druga mogućnost je upotreba generatora pseudo-slučajnih brojeva kako bi se poruka prenijela pomoću signala nositelja u slučajnom poretku.

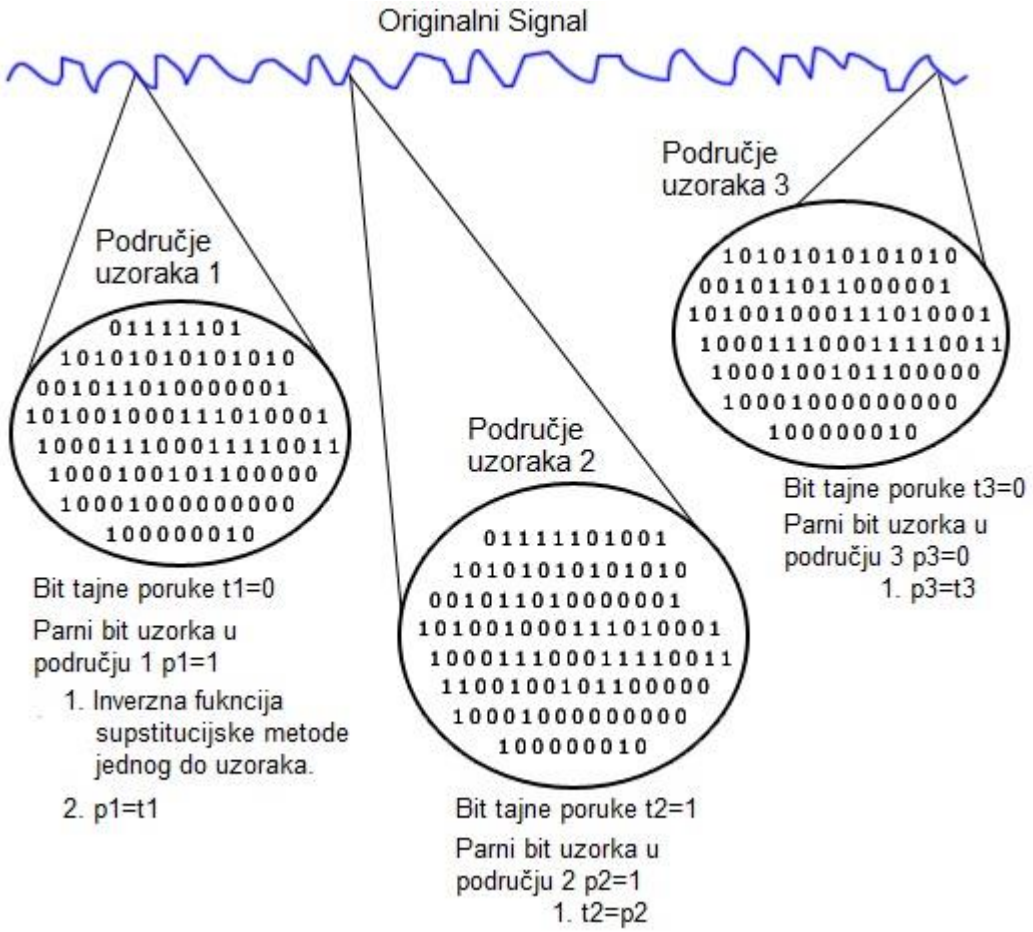


Slika 4.2. Skrivanje poruke LSB metodom

Niz pseudoslučajnih brojeva bi predstavljao redne brojeve uzoraka koji se mijenjaju. Nova, predložena poboljšanja ove tehnike podrazumijevaju transformaciju signala, a zatim promjene najmanje značajnih koeficijenata koji predstavljaju audio signal u transformacijskoj domeni, kako bi se umetnuo vodeni žig. Inverznom transformacijom dobije se audio signal označen vodenim žigom. Neke od transformacija koje se mogu koristiti su diskretna Fourrierova transformacija (DFT) i diskretna kosinusna transformacija (DCT).

4.2. Metoda kodiranja pariteta

Metoda kodiranja pariteta je jedna od robusnijih audio steganografskih metoda. Umjesto dijeljenja signala u pojedinačne uzorke, ova metoda dijeli signal na odvojene uzorke i ugrađuje svaki bit tajne poruke u parni bit odvojenog uzorka signala. Ukoliko se parni bit ne podudara odnosno nije isti kao i bit tajne poruke unutar područja odvojenih uzoraka tada sustav radi inverziju supstitucijske metode jednog od uzoraka. Prema tome pošiljatelj ima više izbora pri ugradnji bita tajne poruke. Metoda kodiranja pariteta je prikazana na slici 4.3.



Slika 4.3. Metoda kodiranja pariteta

4.3. Fazno kodiranje

Tehnika faznog kodiranja radi tako da zamjenjuje fazu inicijalnog audio segmenta s referentnom bazom koja predstavlja tajnu informaciju. Preostali segmenti faze se podešavaju tako da predstavljaju relativnu bazu između susjednih segmenata. Kada se može koristiti i ako se uzme u obzir omjer signala i šuma, fazno kodiranje je jedna od najefikasnijih metoda za kodiranje. Ukoliko postoji drastična promjena u odnosu faza između svake frekvencijske komponente, pojavit će se primjetna disperzija faze. Međutim, sve dok su promjene u fazi dovoljno male, može se postići nečujno kodiranje. Pristupi koji ugrađuju vodeni žig u fazu izvornog signala ne koriste vremenske ili spektralne maskirne učinke. Ova metoda se temelji na činjenici da faza komponente zvuka nije opipljiva ljudskom uhu. To znači da ljudski slušni sustav ima nisku osjetljivost na relativne promjene faze koje se definiraju kao šum.

Koraci faznog kodiranja su sljedeći:

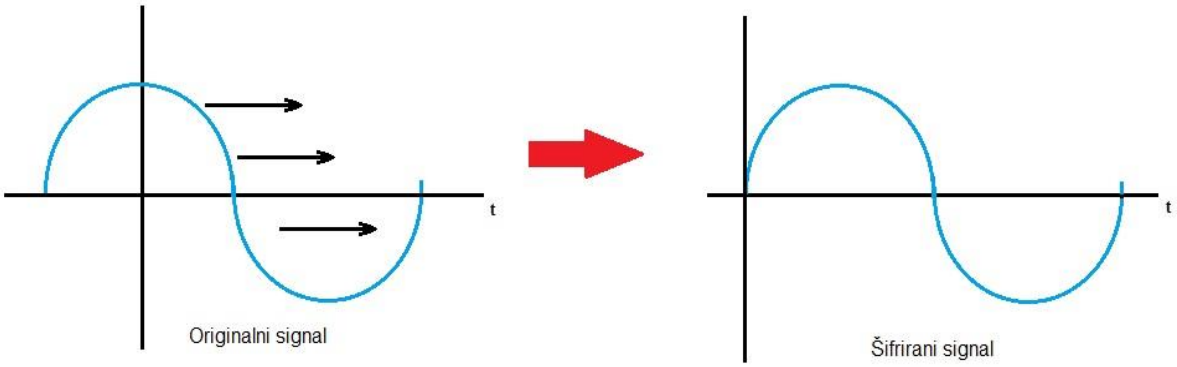
a) Originalni signal se dijeli u manje segmente tolike duljine da su iste veličine kao veličina poruke za ugradnju.

b) Matrica faza je stvorena primjenom diskretne Fourrierove transformacije (DFT)
c) Izračunavaju se fazne razlike između susjednih segmenata
d) Fazni pomaci između susjednih segmenata se mogu lako otkriti. To znači, apsolutne faze segmenata se mogu mijenjati, ali relativne faze između susjednih segmenata moraju biti očuvane. Tako je tajna informacija ubačena samo u faznom vektoru prvog segmenta signala:

$$\text{nova\_faza}=\begin{pmatrix} \pi/2 & if & bit\ poruke = 0 \\ -\pi/2 & if & bit\ poruke = 1 \end{pmatrix}$$

e) Koristeći novu fazu prvog segmenta kreira se nova matrica sa fazama koja ima originalne fazne razlike.
f) Zvučni signal se rekonstruira primjenom inverzne funkcije diskretne Fourrierove transformacije koristeći novu matricu faza i originalne veličine matrice, a zatim nadovezivanjem i spajanjem zvučnih segmenata zajedno.

Primatelj mora znati duljinu izdvojene tajne informacije iz zvučne datoteke. Tada može koristiti DFT da bi dobio fazu te izdvojio tajnu informaciju. Fazno kodiranje je prikazano na slici 4.4.



Slika 4.4. Fazno kodiranje

4.4. Metoda raspršenog spektra

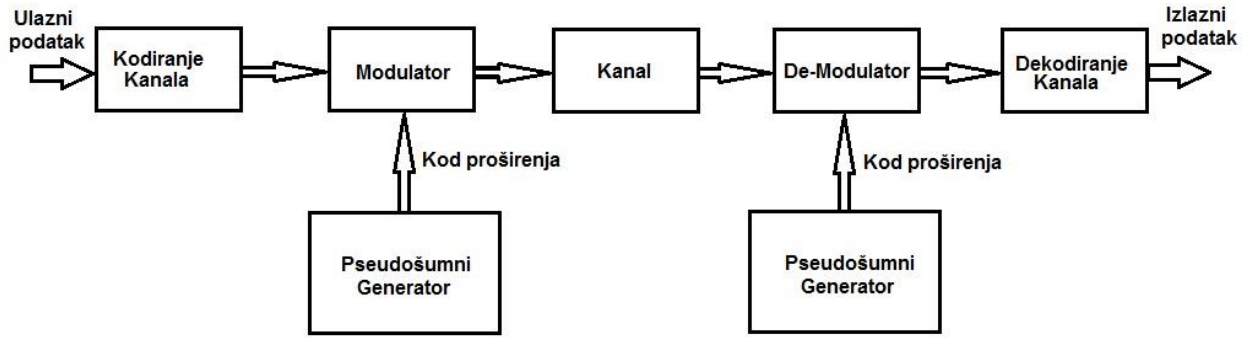
Metoda raspršenog spektra, izvorno zamišljena za prikrivanje porijekla radio prijenosa i jačanja otpornosti protiv ometanja, se često koriste u prijenosu digitalnih podataka. Budući da su zahtjevi smanjenja ometanja tijekom prijenosa (skrivanje signala od neželjenog slušatelja i osiguravanje privatnosti informacije vrlo slični onima u primjeni metode vodenih žigova) ove tehnike su najčešće korištene u razvoju algoritama vodenih žigova. S gledišta metode raspršenog spektra

izvorni audio signal se može smatrati kao ometanje isprepleteno sa signalom koji nosi informaciju o vodenom žigu. Modulacija raspršenog spektra je posebni oblik modulacije vodenih žigova.

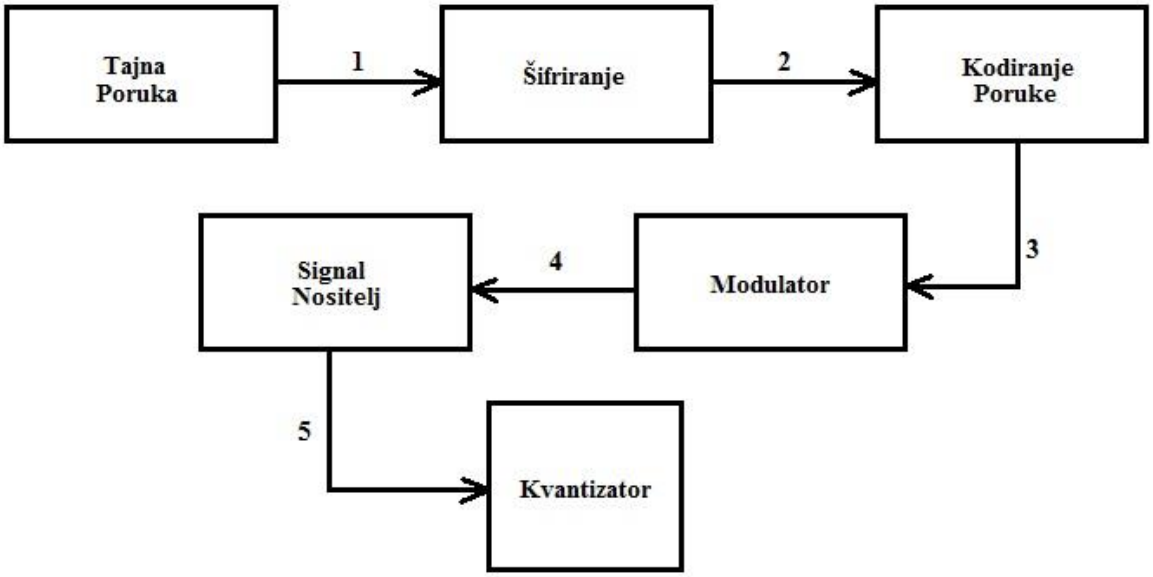
U normalnom komunikacijskom kanalu poželjno je koncentriranje informacije u što je moguće užem području frekvencijskog spektra kako bi se održao raspoloživi propusni opseg i smanjila snaga.

U audio steganografiji, osnova metode proširenog ili raspršenog spektra (SS – eng. *Spread Spectrum*) je da pokuša raspršiti tajne informacije preko što većeg područja frekvencijskog spektra audio signala. Na taj način omogućen je prijem signala čak i ako je na nekim frekvencijama prisutna interferencija. Sličan sustav je sustav koji koristi provedbu LSB supstitucijske metode koji raspršuje bitove poruke nasumično preko cijele audio datoteke, ali za razliku od LSB kodiranja, metoda proširenog ili raspršenog spektra raspršuje tajnu informaciju preko frekvencijskog spektra zvučnog signala koristeći šifru koja je potpuno nezavisna od stvarnog signala.

Kao rezultat, konačni signal zauzima propusnost više nego potrebnu za prijenos. Kod tehnike ugrađivanja vodenog žiga metodom raspršenog spektra osnovna ideja je umetanje uskopojasnog signala (vodeni žig) u širokopojasni kanal (audio signal). Metoda raspršenog spektra može pridonijeti bolje performanse u nekim dijelovima u usporedbi s LSB kodiranjem, faznim kodiranjem i metodom kodiranja pariteta, jer nudi umjerene brzine prijenosa podataka i visok stupanj otpornosti protiv tehnika uklanjanja. Glavni nedostatak ove metode je moguće uvođenje buke u zvučne datoteke. Na slici 4.5. je prikazan općeniti model raspršenog spektra digitalnog komunikacijskog kanala.



Slika 4.5. Općeniti model raspršenog spektra digitalnog komunikacijskog kanala



Slika 4.6. Metoda raspršenog spektra

Slika 4.6. prikazuje postupak metode raspršenog spektra koja je opisana sljedećim koracima:

1. tajna poruka se šifrira koristeći simetrični ključ,
2. šifrirana poruka se ugrađuje koristeći kod za ispravljanje s niskom stopom pogreške, ovaj korak povećava robusnost ove metode,
3. ugrađena poruka se modulira s pseudo-slučajnim signalom koji je generiran s drugim simetričnim ključem,
4. rezultirajući slučajni signal koji sadrži poruku je isprepleten sa signalom nositeljem,
5. završni signal je kvantiziran da bi stvorio novu audio datoteku koja sadrži poruku,
6. proces se radi obratno da bi se izdvojila tajna poruka.

4.5. Metoda skrivenog odjeka

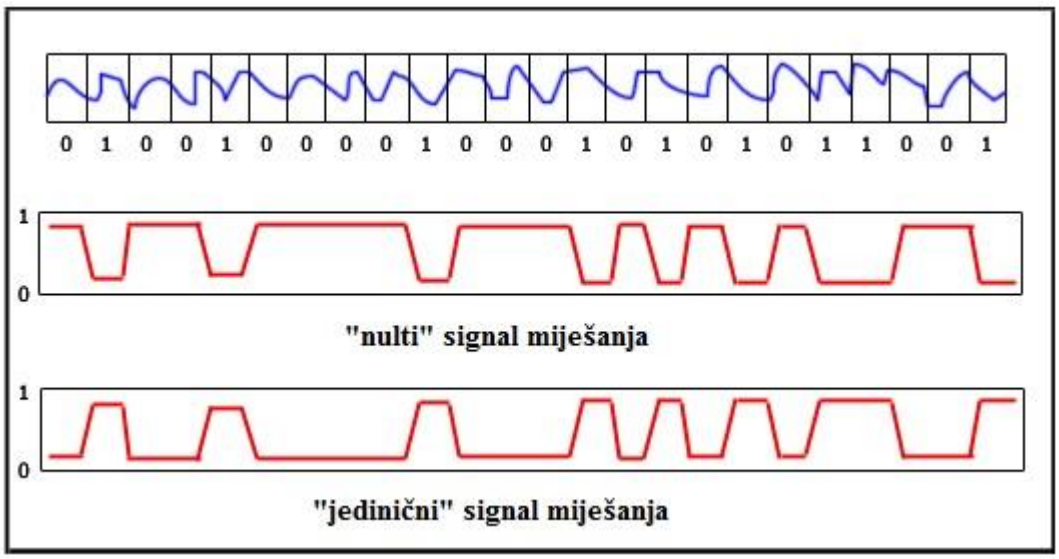
Razne vrste algoritama vodenih žigova se zasnivaju na tzv. metodi skrivenog odjeka. Algoritmi skrivenog odjeka se zasnivaju na ugradnji vodenog žiga u signal $c_0(t)$ s dodavanjem odjeka (jeke) $c_0(t-\Delta t)$ kako bi se proizveo označeni signal $c_w(t)$:

$$c_w(t) = c0(t) + \alpha c_0(t - \Delta t) \qquad (4\text{-}1)$$

Jednadžba 4-1 sadrži dva parametra koji se mogu mijenjati kako bi se osigurala nečujnost vodenog žiga te ugradnja bitova u audio signal. Promjena vremenskog kašnjenja Δt i oba parametra α i t se moraju prilagoditi kako bi se osigurala nečujnost ugrađenog odjeka. Odjek je zakašnjela verzija istog zvuka nešto manje amplitude. Metoda označavanja zvuka koja se naziva metoda skrivenog odjeka ili skrivene jeke (engl. *echo hiding*) se zasniva na svojstvu da ljudsko uho ne primjećuje

jeku malog kašnjenja, jer su takve vrste jeke česta pojava u našoj okolini koja se događa zbog odbijanja zvuka od zid i sl. Ova metoda ugradnju tajne informacije obavlja dodavanjem jeke malog kašnjenja u diskretni signal. Podaci se skrivaju u originalni audio signal mijenjanjem tri parametra: početne amplitude, brzine opadanja (eng. *decay rate*), i brzine kašnjenja (engl. *offset*). Porastom kašnjenja između originalnog signala i jeke dolazi do miješanja dva signala. U određenom trenutku, ljudsko uho neće moći razlikovati ova dva signala, a taj trenutak je teško precizno odrediti. On ovisi o kvaliteti originalne snimke, vrsti zvuka koji proizvodi jeku, te naravno i o slušatelju. Primijer metode skrivenog odjeka je prikazan na slici 4.6.

Prednosti ove metode su visokopodatkovna prijenosna stopa te visoka robusnost u odnosu na ostale metode. Samo jedan mali dio tajne informacije može biti kodiran ako je samo jedna jeka proizvedena iz izvornog signala. Stoga, prije nego kodiranje počne izvorni signal se razbija u blokove. Nakon kodiranja, blokovi se spajaju natrag kako bi se stvorio konačni signal.



Slika 4.6. Primjer metode skrivanja odjeka

4.6. Metoda ugradnje audio vodenih žigova pomoću tehnike zakrpa

Tehniku zakrpa (eng. *patchwork tehnique*) prvi je predstavio Bender za ugradnju vodenih žigova u slike. Tehnika je statistička metoda temeljena na testiranju hipoteze. Te metode koriste slučajne modele oslanjajući se na velike skupove, što ih čini primjenjivima na audio podatke CD-kvalitete s obzirom na količinu uzoraka. Postupak kodiranja vodenim žigovima koristi pseudoslučajni proces za ugradnju određenih statistika u skup podataka koji je otkriven u procesu čitanja s pomoću numeričkih pokazatelja (kao što su srednje vrijednosti) koji opisuju specifičnu distribuciju. Ova metoda je primijenjena na magnitude u Furierovoj domeni kako bi širenje vodenog žiga u vremenskoj domeni bilo robusnije na operacije slučajnog izrezivanja uzorka.

4.7. Primjena vodenih žigova

Raspravljati o tome da li je tehnika vodenih žigova primjenjiva u praksi ili nije nema smisla s obzirom da već godinama postoje kompanije koje se bave isključivo prodajom svojih rješenja za zaštitu autorskih prava kao Digimarc Corporation, te velike kompanije koje nude rješenja za vodene žigove poput Philips-a koji nudi svoju aplikaciju CompoTrack WAV koja umeće vodene žigove u zvučne zapise u WAV i AAC formatu. Također postoje kompanije koje se bave prodajom raznih multimedijalnih sadržaja na internetu, koje vjerojatno označavaju sadržaje ali razumljivo je da nikakve podatke o tome ne objavljuju javno.

Digitalni vodeni žigovi se smatraju neprimjetnim, čvrstim i sigurnim načinom razmjene podataka pridruženih osnovnom signalu, koja uključuje umetanje u signal i izdvajanje iz izvornog signala. Osnovni cilj je da umetnuta informacija, koja predstavlja vodeni žig prati označeni multimedijalni sadržaj i da izdrži nenamjerne i namjerne pokušaja uklanjanja. Jedan od glavnih izazova je umetnuti vodeni žig tako da se može pouzdano otkriti na prijemu. Relativna važnost spomenutih osobina značajno ovisi o primjeni za koju je algoritam umetanja žigova napravljen. Za primjenu zaštite od kopiranja, vodeni žig mora imati mogućnost da se povrati čak i kada signal označen žigom trpi značajnu razinu izobličenja. Kod primjene kažnjavanja neovlaštenog mijenjanja, vodeni žig mora prepoznati promjene koje su izvršene. Najvažnije primjene digitalnih vodenih žigova su:

- Zaštita vlasnišvta (engl. *ownership protection*). Vodeni žig, koji sadrži informacije o vlasništvu, te je poznat samo vlasniku autorskih prava, je umetnut u multimedijalni signal, te kao takav treba biti vrlo otporan i postojan, odnosno treba preživjeti uobičajene promjene pri obradi signala i namjerne napade, kako bi omogućio vlasniku da dokaže prisustvo vodenog žiga u slučaju nekog spora, radi dokazivanja vlasništva. Samo otkrivanje vodenog žiga mora imati malu vjerojatnost lažnog alarma. S druge strane, zaštita vlasništva zahtjeva mali kapacitet utiskivanja sustava, budući da broj bita koji može biti umetnut i potom izdvojen s malom vjerojatnošću greške ne mora biti velik.
- Dokazivanje vlasništva (engl. *proof of ownership*). Još zahtjevnija je upotreba vodenih žigova ne samo u identifikaciji vlasništva autorskih prava, nego kao konkretan dokaz o vlasništvu. Problem raste kada suprotna strana koristi softver za korekciju kako bi zamijenila originalni žig o vlasništvu sa svojim i zatim tvrdila da posjeduje autorska prava. U slučaju ranih sustava vodenih žigova, problem je bio što je detektor vodenih žigova brzo bio dostupan svima. Tako je svatko tko bi detektirao žig bio u mogućnosti i da ga ukloni. Dakle, zbog toga što suprotna strana može lako nabaviti detektor, ona može i odstraniti originalan žig te ga zamijeniti svojim. Kako bi se dostigla razina sigurnosti koja je

neophodna za dokazivanje vlasništva, neophodno je ograničiti dostupnost detektora. Kada suprotna strana nema detektor, odstranjivanje vodenog žiga može biti izuzetno teško.

- Autorizacija i detekcija krivotvorenja (engl. *authentication and tampering detection*). U slučaju autorizacije sadržaja, niz sekundarnih podataka se umeće u originalni signal i kasnije se koristi kako bi se ustanovilo je li signal neovlašteno mijenjan. Otpornost na uklanjanje vodenog žiga ili izrada neprimjetnog žiga ovdje nije od velikog značaja, jer ne postoji motivacija za tako nešto od strane napadača. Međutim, krivotvorenje ispravnog autoriziranog vodenog žiga u neovlašteni ili krivotvoreni signal mora biti spriječeno. U praktičnim primjenama poželjno je locirati u vremenu i prostoru i razlikovati nenamjerne promjene od krivotvorenja sadržaja. Kapacitet umetanja vodenih žigova mora biti visok kako bi zadovoljio potrebu za više dodatnih podataka nego kao kod dokazivanja vlasništva. Detekcija žiga mora biti moguća i bez originalnog signala zato što original ne mora uvijek biti na raspolaganju ili njegova valjanost tek treba biti utvrđena. Ova vrsta detekcije se naziva slijepa detekcija.
- Fingerprinting. Dodatni podaci koji su umetnuti vodenim žigom kod ove aplikacije se koriste kako bi bilo moguće ući u trag tvorcu ili korisniku pojedinačne kopije multimedijalnog podatka. Na primjer, vodeni žigovi koji nose različite serijske ili identifikacijske (ID) brojeve se umeću u različite kopije glazbenih CD-ova ili DVD-ova prije nego se distribuiraju velikom broju korisnika. Algoritmi koji su ovdje ostvareni moraju pokazati visoku otpornost na namjerne napade i promjene koje nastaju prijenosom signala, kao što su kompresije s gubitkom i filtriranje. Također, mora se onemogućiti umetanje više od jednog ID broja u originalni multimedijalni podatak, inače detektor neće moći razlikovati koja kopija je u pitanju. Kapacitet umetanja koji se ovdje zahtjeva je u rangu kapaciteta potrebnog za zaštitu autorskih prava, s nekoliko bita po sekundi.
- Kontrola radio emitiranja (engl. *broadcast monitoring*). Veliki broj primjena vodenih žigova se odnosi na pojam radio emitiranja. Vodeni žigovi predstavljaju očiglednu alternativnu metodu kodiranja identifikacijskih informacija za aktivnu kontrolu emitiranja. Oni imaju prednost u odnosu na druge metode jer su umetnuti u sam multimedijalni signal, a ne koriste se pojedinačni segmenti siganala koji se emitiraju. Zbog toga, vodeni žigovi su kompatibilni s već instaliranom osnovnom opremom za emitiranje, uključujući digitalne i analogne kanale za komunikaciju. Osnovna mana je što je postupak umetanja znatno složeniji od jednostavnog smještanja podatka u zaglavlje datoteke. Također postoji zabrinutost da bi vodeni žig mogao unijeti izobličenja i na taj način mogao umanjiti vizualnu ili audio kvalitetu multimedijalnog sadržaja. Kod kontrole radio emitiranja postoji

veći broj primjera upotrebe vodenih žigova kao što su, identifikacija tipa programa, reklamno istraživanje, istraživanje pokrivenosti emitiranja, itd.

- Kontrola kopiranja (engl. *copy control*). Ova tehnika sprječava ilegalno kopiranje djela zaštićenog autorskim pravima. Ona podrazumijeva da sav software i hardvare koji omogućava kopiranje sadržaja može detektirati vodeni žig i spriječiti kopiranje sadržaja koji nije dopušteno kopirati. Jedan od problema kod kontrole kopiranja je nešto što se naziva *trusted client* problem. To znači da će napadači uvijek naći način da razbiju zaštitu na ovakvim uređajima ili programskim playerima (kao što je razbijena CSS zaštita na DVD-ima), ali ipak ovo može spriječiti dosta ilegalnog kopiranja i ima smisla. Drugi problem je ekonomske prirode i predstavlja otpor proizvođača softwareske ili hardwareske opreme uvođenju ovakve zaštite. Njima je to dodatan trošak kod implementacije, a predstavlja im problem jer će korisnici uvijek radije kupiti uređaj koji im omogućuje ilegalno kopiranje nego uređaj koji to ne dopušta.
- Nositelj informacija (engl. *information carrier*). Ovdje se očekuje da umetnuti žig ima veliki kapacitet i može biti detektiran i dekodiran pomoću algoritma slijepe detekcije. Otpornost na namjerne napade nije neophodna, ali je poželjan određen stupanj otpornosti na uobičajenu obradu, kao što je na primjer MPEG kompresija. Javni vodeni žig koji je umetnut u multimedijalni signal može se koristiti kao link s vanjskim bazama podataka koje sadrže određene dodatne informacije o samom multimedijalnom podatku, kao što su informacije o autorskim pravima i uvjetima korištenja. Moguće je da podaci koji su umetnuti u neki audio signal, nose informaciju o kompozitoru, izvođaču, glazbenom žanru, itd.

5. ZAKLJUČAK

Sustavi vodenih žigova za digitalni zvuk pojavili su se naknadno, nakon što su predstavljeni sustavi za digitalne slike, a predloženi su kao alternativna metoda koja pruža zaštitu od piratstva i kršenja autorskih prava kod digitalnih medija. Oni su definirani kao neprimjetan, robustan i siguran oblik razmjene podataka koji su povezani sa signalom nositeljem. Kao takva vrsta zaštite pokazuje se sve veća potreba za ovakvim sustavima s obzirom na porast trgovine digitalnom glazbom na internetu. Nezaštićenu glazbu je danas lako kopirati i zatim ilegalno distribuirati, čime umjetnici i izdavačke kuće gube sve veća i veća novčana sredstva. S obzirom na to, logično je očekivati potrebu za sustavima zaštite intelektualnih vlasništva nad glazbom i zvukom općenito. Tehnika vodenih žigova će sigurno pronaći svoje mjesto u takvim sustavima. Do sada je predstavljeno puno dobrih sustava za digitalni zvuk, a interes za ovim područjem je velik i to rezultira da se, prema nekim procjenama, broj novih predstavljenih tehnika vodenih žigova udvostručuje svake godine. Iako mogu poslužiti kao jedna od tehnika zaštite intelektualnog sadržaja, sami ne mogu pružiti dovoljnu sigurnost.

Kao dokaz da ne mogu biti jedina mjera protiv ilegalnog kopiranja može poslužiti SDMI challenge natječaj, 2001. godine. SDMI (engl. *Secure Digital Music Initiative*) je organizacija koju je osnovala udruga izdavačkih kuća RIAA (engl. *Recording Industry Association of America*), kako bi pronašla siguran standard za distribuciju glazbe preko interneta. U tom natječaju iz 2001. godine, javnosti je objavljeno 6 označenih zvučnih datoteka, dok algoritmi koji su korišteni kod označavanja nisu objavljeni. Natječaj je bio takav da je javnosti dano dva tjedna vremena za pokušaje uklanjanja žigova iz 6 označenih zvučnih uzoraka. Rezultat je bio takav da su svih 6 žigova uspješno uklonjeni, a osoba koja je to napravila je bio profesor Felton sa sveučilišta Princeton. On je javno objavio rad s detaljnim opisom postupaka koje je koristio kod uklanjanja žigova, što je rezultiralo tužbom protiv njega od strane udruge RIAA.

Iz ovoga možemo zaključiti da do danas nije izmišljen digitalni vodeni žig kojeg iskusni napadač ne bi mogao ukloniti. Međutim, većina korisnika nema ni znanja ni volje za uklanjanjem žigova tako da i primjena najjednostavnijih shema vodenih žigova može biti opravdana.

Još jedna stvar koja pokazuje kako je ovo područje relativno novo i neistraženo je i nedostatak bilo kakvog standarda, bilo službenog bilo neslužbenog. U svijetu simetričnog kriptiranja postoji AES (engl. *Advanced Encryption Standard*) naziv za sadašnji američki državni standard za šifriranje, u svijetu asimetričnog postoji RSA (ime za algoritam šifre javnog ključa), ali kod vodenih žigova je puno algoritama, a nepostojanje standarda također onemogućava širu primjenu.

LITERATURA

[1] CARnet CERT, Steganografija, CCERT-PUBDOC-2006-04-154, Revizija v1.0, 2006.,

Dostupno na:

http://sigurnost.lss.hr/documents/LinkedDocuments/CCERT-PUBDOC-2006-04-154.pdf

[2] Kipper G., Investigator's Guide to Steganography, Auerbach Publications, London, 2004.

[3] Wikipedia: Steganography, Steganalysis, Digital watermarking, RC4, JPEG, Dostupno na: http://wikipedia.org/, Pristupano siječanj 2017.

[4] Robert Krenn, „Steganography and steganalysis“, članak Siječanj 2004.

[5] Nedeljko Cvejić, Tapio Seppben „Increasing te capacity of LSB-based audio steganography“ FIN-90014 University of Oulu Finland, 2002.

[6] W.Bender, W. Buttera, D.Gruhl, R. Hwang, F. J. Paiz, S. Pogreb, „Techniques for data hidding“, IBM Systems Journal, Svezak 39, izdanje 3-4. str. 547-568, srpanj 2000.

[7] R.Popa, „An Analysis of Steganographics Tehnique“, The Politehnica University of Timisoare, Faculty of Automatics and Computers, Department of Computer Science and SE, 1998

[8] N.Taraghi-Delgarm, „Speech Watermarking“, M.Sc.Thesis, Computer Engineering Department, Sharif University of Tehnology, Teheran,Iran, Svibanj 2006.

[9] W.Bender, D.Gruhl, A.Morimoto, Techniques for data hiding, IBM systems journal, svezak 35, 1996

[10] The International Journal of Multimedia & Its Applications (IJMA) Svezak 3, Broj 3, Kolovoz 2011

[11] The first 50 years of electronic watermarking, Ingemar J. Cox, Matt L. Miller, travanj 2002.

[12] Robust audio watermarking using perceptual masking, Mitchell D. Swanson, Bin Zhu, Ahmed H. Tewfik, Laurence Boney, svibanj 1998.

[13] Audio watermarking and applications, Eric Metois, rujan 1999.

[14] Katzenbeisser S., Petitcolas F.: Information Hiding Techniques for Steganography and Digital Watermarking, Artech house, Boston, 2000.

SAŽETAK

Glavni zadatak ovog rada je analizirati primjenu steganografije na audio datotekama. U radu je objašnjen pojam steganografije, navedene su vrste steganografije te su opisane prednosti i nedostaci odabranih metoda steganografije. Posebna pozornost posvećena je digitalnim vodenim žigovima koji su preteča steganografije. Analizirane su najčešće korištene metode kodiranja audio datoteka. Zadatak audio steganografije je zaštita autorskih prava, što je još uvijek jedan od najvećih problema u glazbenoj industriji koji uzrokuje novčane gubitke koji konstantno rastu. Trenutno ne postoji digitalni vodeni žig kojeg iskusniji napadač ne bi mogao ukloniti. Kao znanost, steganografija je i dalje neistražena te postoje brojne mogućnosti za poboljšanja.

Ključne riječi: audio datoteka, autorska prava, digitalni vodeni žig, kodiranje, steganografija

ABSTRACT

The main task of this paper is to analyze the application of steganography on audio files. The paper describes the terminology of steganography, the types of steganography are described, and the advantages and disadvantages of the selected methods of steganography are described. Special attention is dedicated to digital watermarks that are the forerunner of steganography. The most commonly used audio file encoding methods are analyzed. The task of audio steganography is copyright protection, which is still one of the biggest problems in the music industry that causes cash losses that are constantly growing. There is currently no digital watermark that a more experienced attacker could not remove. As a science, steganography is still unexplored and there are numerous opportunities for improvement.

Keywords: audio file, copyright, digital watermark, coding, steganography

ŽIVOTOPIS

Krešimir Knezović rođen je 17. rujna 1986. godine u Brčkom. Osnovnu školu Antun i Stjepan Radić je završio u Gunji 2001. godine a srednju školu Elektrotehničku školu u Županji 2005. godine. Iste godine upisuje se na prvu godinu Elektrotehničkog fakultetu u Osijeku, sveučilišni preddiplomski studij računarstva. Za vrijeme redovnog studiranja radio je na raznim studentskim poslovima od kojih se najviše ističu rad u tiskari Glas Slavonije te rad u HT hrvatskom telekomu (T-com) na tehničkoj podršci za širokopojasne i fiksne telefonske usluge. U slobodno vrijeme se bavi košarkom, nogometom, vožnjom bicikla. Trenutno živi u Zagrebu i radi u Atlantic Trade-u kao trgovački predstavnik.

_____

Krešimir Knezović