

SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

DIPLOMSKI RAD br. 618

**Primjena digitalnog vodenog žiga u zaštiti
vlasništva slika u digitalnom zapisu**

Hrvoje Šalković

Zagreb, lipanj 2013.

Sadržaj

1. Uvod	1
2. Digitalni vodeni žig	2
2.1. Osnovni zahtjevi	2
2.2. Važnost vodenog žiga	4
2.3. Ciljevi	6
2.4. Klasifikacija digitalnih vodenih žigova	6
2.4.1. Prema vidljivosti	6
2.4.2. Prema otpornosti (robustnosti)	8
2.4.3. Prema domeni primjene	9
2.5. Primjena digitalnih vodenih žigova	10
2.5.1. Zaštita autorskih prava	10
2.5.2. Autentifikacija i zaštita od neovlaštenog rukovanja	11
2.5.3. Vidljivi reverzibilni vodeni žig za distribuciju	12
2.5.4. Komunikacijski sustavi	13
2.6. Distorzije i napadi na vodeni žig	14
2.6.1. Napadi uklanjanja	14
2.6.2. Geometrijski napadi	17
2.6.3. Kriptografski napadi	17
2.6.4. Protokolarni napadi	18
3. Tehnike implementacije digitalnog vodenog žiga	19
3.1. Prostorna domena	19
3.2. Frekvencijska domena	21
4. Implementacija i analiza u Matlabu	25
4.1. Diskretna Fourierova transformacija	26
4.2. Diskretna kosinusna transformacija	36
4.3. Diskretna wavelet transformacija	46
Zaključak	56
Literatura	57
Sažetak	58
Privitak	60

1. Uvod

U današnje vrijeme kada su računala, printer, prijenosni mediji sve rašireniji u široj populaciji, sve većom dostupnošću te sve nižom cijenom, postaje to veći problem zaštite privatnih podataka. Uz to razvojem internet, te pojavom društvenih mreža, stranica specijaliziranih za razmjenu podataka (slika, fotografija, filmova, video igara, glazbe i sl.), foruma i općenito dostupnosti medija na internetu, sve je lakše doći do tih podataka. Svatko sa imalo znanja i iskustva može doći do privatnih podataka, te ih mijenjati, dijeliti, falsificirati ili zlouporabiti na neki drugi način bez većih problema. To predstavlja rastući problem na tržištu, te se postavlja pitanje rješavanja tog problema. Digitalni vodeni žig predstavlja relativno jednostavno i efikasno rješenje tog problema. Umetanjem određene informacije u glazbeni isječak, video uradak ili digitalnu sliku garantira se autentičnost podatka krajnjem korisniku, ali i omogućava autoru ili vlasniku tog sadržaja praćenje bilo kakvih promjena istog.

Primjena digitalnog vodenog žiga još uvijek je aktivno područje istraživanja, a uz zaštitu podataka od neautorizirane upotrebe koristi se i za autentifikaciju, provjeru integriteta, verifikaciju, upravljanje digitalnim pravima i mnoge druge aplikacije. Uvedeno je mnogo tehnika s različitim obećanjima vezano uz svojstva, uključujući otpornost, transparentnost, kapacitet, kompleksnost i sigurnost. Ovisno o načinu primjene nije jednostavno procijeniti te tvrdnje o učinku.

U ovom radu bit će dan kratak pregled svojstava digitalnog žiga, načina i tehnika implementacije, te mogućih napada na zaštićene podatke. Određene tehnike, koje su češće korištene (DFT, DCT, DWT) u primjeni digitalnog žiga bit će obrađene nešto detaljnije, te će biti dana usporedba njihovih performansi.

2. Digitalni vodeni žig

Kao što je već spomenuto u uvodnom poglavlju, digitalni vodeni žig je rastuće područje istraživanja za označavanje digitalnog vlasništva umetanjem zaštitnih informacija unutar digitalnog sadržaja. Ova tehnika zaštite digitalnog vlasništva omogućava dodatne primjene i korisne dodatke za mnoga područja (upravljanje digitalnim vlasništvom, provjera integriteta, autentifikacija, verifikacija i dr.). Zaštita digitalnim vodenim žigom primanjiva je na sve vrste podataka, uključujući audio, video, slike, pa i multimedijske podatke. U nastavku poglavlja bit će ukratko objašnjena osnovna svojstva, napadi, moguće klasifikacije i primjene digitalnog vodenog žiga.

2.1. Osnovni zahtjevi

Svaki algoritam za implementaciju trebao bi biti konzistentan u sljedećim svojstvima i parametrima:

- *Transparentnost:* Jedan od najosnovnijih zahtjeva na metodu implementacije vodenog žiga jest da je on transparentan krajnjem korisniku. Sadržaj označen vodenim žigom mora biti upotrebljiv na korisniku bez vidljivih, odnosno primjetnih smetnji. Vodeni žig pojavljuje se samo na uređaju za detekciju vodenog žiga.
- *Otpornost:* Vodeni žig mora biti dovoljno otporan da se odupre bilo kakvim operacijama obrade signala, napadima i neautoriziranom pristupu. Svaki pokušaj, namjeren ili slučajan, kojim se pokušava promijeniti sadržaj smatra se napadom. Otpornost na te napade je ključan zahtjev za vodeni žig i uspjeh korištenja ove metode za zaštitu autorskih prava ovisi o njegovoj pravilnoj implementaciji.
- *Kapacitet:* Opisuje količinu podataka koji moraju biti umetnuti u neki sadržaj kao vodeni žig za uspješnu detekciju prilikom izvlačenja vodenog žiga. Vodeni žig mora imati mogućnost prijenosa dovoljnoe

količine informacije za prikazivanje jedinstvenosti sadržaja. Količina potrebnih informacija ovisi o specifičnoj primjeni vodenog žiga.

- *Sigurnost*: Informacijama o vodenom žigu smiju pristupati samo ovlaštene osobe. Također, samo ovlaštene osobe imaju mogućnost promjene sadržaja označenog vodenim žigom. Za sprečavanje neovlaštenog pristupa sadržaju uobičajena je primjena nekog oblika šifriranja vodenog žiga.
- *Jednostavnost umetanja i izvlačenja žiga*: Idealno, korištenje vodenog žiga u digitalnim medijima bi trebalo biti moguće “u letu”. Vrijeme potrebno za izvođenje određenih računskih operacija mora biti minimalno moguće.
- *Utjecaj na širinu pojasa*: Način korištenja vodenog žiga trebao bi biti implementiran na način da ne povećava propusnost (tj. širinu pojasa) potrebnu za prijenos podataka. U slučaju da vodeni žig postane teret za dostupnu propusnost, metoda implementacije se odbacuje.
- *Interoperabilnost*: Sadržaj označen digitalnim vodenim žigom mora biti interoperabilan, na način da se može prikazati ili izvesti u heterogenim mrežama, bez obzira jesu li one svjesne postojanja digitalnog vodenog žiga ili ne.

2.2. Važnost vodenog žiga

Do naglog porasta zanimanja zaštite podataka korištenjem digitalnog vodenog žiga vrlo vjerojatno je došlo zbog porasta brige o zaštiti autorskih prava nad tim podacima. Kako je internet postao pristupačniji korisnicima uvođenjem interaktivnih web pretraživača, postalo je jasno kako ljudi žele preuzimati slike, video i glazbu u digitalnom obliku. Internet je odličan sustav za razmjenu podataka zbog svoje niske cijene, uklanjanja potrebe za skladištenjem medija za pohranu podataka, odnosno njihove količine u zalihama i gotovo trenutne dostave traženih podataka. Međutim, vlasnici autorskih prava nad tim podacima u tome vide veliku mogućnost i rizik od zlouporabe tih podataka, odnosno piratstva. Taj rizik je dodatno povećan razvojem digitalnih sustava za pohranu podataka velikog kapaciteta (pr. DVD, blu-ray, USB itd.).

Prije pojave digitalnih medija, kada je jedini način prosječnog korisnika za snimanje glazbe ili videa bila na analognoj vrpici, piratske kopije su obično bile slabije kvalitete nego originali, dok se svakim ponovnim kopiranjem istih kvaliteta dodatno narušavala. Nažalost, pojavom digitalnih medija za snimanje tih podataka, gotovo da i nema razlike u kvaliteti originala i ilegalne kopije. Korištenjem takvih digitalnih snimača, te korištenjem internet za dijeljenje snimljenih podataka, bilo tko može, bez većih poteškoća snimiti i dijeliti bilo kakvu vrstu sadržaja bez nadoknade za vlasnike autorskih prava na te sadržaje. Zato vlasnici tih sadržaja željno očekuju razvoj tehnologije za zaštitu njihovih prava. Prva tehnologija korištena u tu svrhu bila je kriptografija, vjerojatno i najčešće korištena za tu svrhu, a sigurno jedna od najbolje razvijenih znanosti za tu primjenu. Sadržaj je šifriran prije isporuke, a ključ za dešifriranje dostupan samo onima koji taj sadržaj i plate. Tada se željeni sadržaj može i objaviti na internet, jer je bez ključa za dešifriranje beskoristan nekom tko ga želi zlorabiti. Nažalost, šifriranje ne omogućava vlasniku nadziranje načina na koji će legitiman korisnik koristiti sadržaj koji je kupio. Korisnik može kupiti određeni sadržaj, te nakon kupovine ilegalno distribuirati dešifriranu (nezaštićenu) kopiju. Drugim riječima, šifriranje možda

štiti sadržaj za vrijeme prijenosa do krajnjih korisnika, ali nakon dešifriranja postaje nezaštićen.

Iz tog razloga javlja se potreba za razvojem novog načina zaštite autorskih prava nad sadržajem, tehnologije koja će zaštititi sadržaj nakon što je dešifriran. Digitalni vodeni žig predstavlja moguće rješenje, jer umeće informaciju, koja se ne mijenja tokom normalnog korištenja, unutar samog sadržaja. Digitalni vodeni žig može biti dizajniran da preživi dešifriranje, ponovno šifriranje, kompresiju, digitalno analognu pretvorbu, te promjenu tipa datoteke. Digitalni vodeni žig iskoristiv je u mnogobrojnim primjenama sprečavanja kopiranja sadržaja i zaštite autorskih prava. Kod sprečavanja ilegalnog kopiranja, digitalni vodeni žig može obavijestiti hardver ili softver o zabrani kopiranja, dok kod zaštite autorskih prava može biti iskorišten za detekciju vlasnika sadržaja i osiguranje plaćanja honorara vlasniku. Iako su zabrana kopiranja i zaštita autorskih prava možda i najveća područja primjene digitalnog vodenog žiga, njegova iskoristivost nije ograničena na ta dva područja. Ostala područja između ostalog uključuju: praćenje emitiranja sadržaja, praćenje transakcija, autentifikaciju, kontrolu kopiranja te kontrolu uređaja [1].

2.3. Ciljevi

Efikanas vodeni žig trebao bi imati sljedeća svojstva:

- Mogućnost detekcije promjene zaštićenog sadržaja
- Mogućnost lociranja promjene na slici
- Mogućnost integriranja autentifikacije unutar zaštićenog sadržaja
- Nevidljivost umetnutih podataka za autentifikaciju pod normalnim uvjetima gledanja sadržaja
- Mogućnost spremanja sadržaja u formatu kompresije s gubitcima [2]

2.4. Klasifikacija digitalnih vodenih žigova

Neke od važnijih klasifikacija digitalnih vodenih žigova dane u nastavku poglavlja:

2.4.1. Prema vidljivosti

Vidljivi

Vidljivi vodeni žigovi su svojevrsna ekstenzija na koncept loga. Takvi se žigovi mogu koristiti samo za označavanje slika. Vodeni žig (logo) se umeće u sliku, ali ostaje transparentan. Ne mogu se ukloniti izrezivanjem centralnog dijela slike i otporni su na statističku analizu.

Nedostaci ovakvih žigova su degradacija kvalitete slike, te detekcija samo vizualnim putem, odnosno nije ih moguće detektirati putem određenih programa i uređaja. Koriste se u izradi karti, grafici i softverskih korisničkih sučelja.



Slika 1 - Primjer vidljivog digitalnog vodenog žiga

Nevidljivi

Nevidljivi vodeni žigovi su skriveni unutar sadržaja. Mogu se detektirati samo pomou ovlaštenih programa ili agencija. Koriste se za zaštitu i autentifikaciju autorskih prava, te detekciju neovlaštenog kopiranja.

2.4.2. Prema otpornosti (robustnosti)

Otporni (robustni)

- Umetnuti nevidljivi vodeni žigovi
- Otporni na obradu slike i napade
- Koriste se za zaštitu autorskih prava i potvrdu vlasništva

Ranjivi

Vrsta digitalnog vodenog žiga koji se lako uništi, svakim pokušajem njegove promjene. Ranjivi vodeni žigovi se uništavaju bilo kakvom uporabom manipulacije podacima, pa se zato i koriste u svrhu otkrivanja promjena na digitalnom sadržaju.

Polu-ranjivi

- Osjetljivi na izmjene i promjene signala
- Osobine otpornih i ranjivih žigova
- Pružaju mogućnost autentifikacije podataka [3]

2.4.3. Prema domeni primjene

U ovom poglavlju je dana samo podjela na dvije moguće domene (prostorna i domena transformacije), dok će u narednim poglavljima biti detaljnije objašnjene pojedine metode unutar tih domena.

Prostorna domena

Obično se digitalni vodeni žig umeće na pozicije nižih bitova koji nisu toliko bitni za prikaz slike i ne narušava se kvaliteta prikaza. Tehnike umetanja digitalnog vodemog žiga su prilično jednostavne i predstavljaju relativno efikasan način umetanja nevidljivog vodenog žiga unutar slike. Nažalost, tehnike u prostornoj domeni nisu baš otporne na češće oblike manipulacije slikama, pa neće biti detaljnije obrađivane unutar ovog rada, već će biti dan samo kratak pregled par mogućih tehnika umetanja digitalnog vodenog žiga u ovoj domeni.

Domena transformacije (frekvencijska)

Drugi način umetanja digitalnog vodenog žiga unutar slike (ili bilo kojeg digitalnog sadržaja) je prvotno transformacija originalne slike u frekvencijsku domenu pomoću Fourierove (DFT), diskretne kosinusne (DCT) ili valićne (DWT) transformacije. Ovim tehnikama žigovi se ne dodaju na intenzitete pojedinih dijelova slike već na transformacijske koeficijente, te se zatim inverznom transformacijom dobiva slika označena digitalnim vodenim žigom. Ovakve tehnike su puno efikasnije, jer se uzimaju u obzir karakteristike ljudskog vizualnog sustava kod određivanja intenziteta i pozicije digitalnog vodenog žiga unutar slike. Ove će tehnike biti nešto detaljnije obrađene unutar rada, zbog svojih svojstava.

2.5. Primjena digitalnog vodenog žiga

Unutar ovog poglavlja bit će navedene i objašnjene neke od češćih primjena digitalnog vodenog žiga.

2.5.1. **Zaštita autorskih prava**

Jedna od tradicionalnih upotreba digitalnog vodenog žiga je zaštita autorskih prava. Osnovni razlog korištenja vodenog žiga je mogućnost identifikacije vlasnika određenog sadržaja pomoću oznake (žiga) umetnute unutar tog sadržaja. U većini slučajeva digitalni vodeni žig se koristi uz neku vrstu šifriranja sadržaja, koje osigurava siguran prijenos označenog sadržaja kroz medijske kanale do krajnjih korisnika, dok vodeni žig omogućava vlasnicima praćenje daljnjeg korištenja tog sadržaja, te otkrivanje neautoriziranog korištenja i umnažanja istog. Bez uporabe vodenog žiga vlasnicima je nemoguće pratiti daljnju upotrebu njihovog sadržaja nakon što je isporučen krajnjim korisnicima. Digitalni vodeni žig koristi se za proširenje zaštite i pružanje mogućnosti daljnje zaštite nad elektroničkim sadržajem njihovim vlasnicima. Unutar sadržaja umeće se digitalni potpis vlasnika, identifikacija sadržaja i ograničenje moguće upotrebe tog sadržaja. Ovaj mehanizam pruža mogućnost zaštite vlasništva nakon njegove distribucije krajnjim korisnicima. Glavni tehnički zahtjevi za ovu primjenu su:

- Vodeni žig ne smije uzrokovati vidljive artefakte krajnjim korisnicima
- Vodeni žig je neovisan o krajnjem formatu sadržaja
- Informacija prenesena putem vodenog žiga je otporna na manipulaciju sadržaja, kompresiju s gubicima i sl.
- Vodeni žig je moguće detektirati bez originalnog sadržaja (neoznačenog)
- Vodeni žig je moguće identificirati putem nekog ključa za jedinstvenu identifikaciju velikog broja individualnih podataka

2.5.2. Autentifikacija i zaštita od neovlaštenog rukovanja

Cilj ove primjene nije zaštita sadržaja od kopiranja ili krađe, već pružanje metode za autentifikaciju slike i osiguravanje njenog integriteta. Pojavom relativno jeftinih digitalnih kamera, metoda se razvija i na velik broj industrijskih primjena, jer cijena razvoja digitalnih slika je mnogo jeftinija i vrijeme za obradu i izradu digitalnih slika je mnogo brže od razvoja klasičnih. Međutim, dolazi do kritičnih pitanja u nekim primjenama, gdje se digitalne slike koriste kao dokaz za neku vrstu poslovne prosudbe. Jedan od primjera su tvrtke za automobilsko osiguranje koje koriste slike oštećenja vozila poslana od strane auto mehaničara za procjenu cijene štete na vozilu. Prebacivanje na digitalne fotografije u ovom slučaju uvelike bi smanjilo potrebno vrijeme i novac za ovakve procese. Dakako, takve digitalne fotografije mogu se izmjeniti na način da se šteta uveliča ili u potpunosti izmisli, što postaje sve jednostavnije korištenjem naprednijih programa za obradu slike (npr. Photoshop). Na taj način tvrtke za automobilsko osiguranje mogu biti oštećene za poprilične svote novaca ili im može biti narušen kredibilitet, što je još ozbiljniji problem. U tu svrhu koristi se posebni oblik vodenog žiga za detekciju promjena na slici kojim se osigurava sigurno okruženje za dokazne materijale (u ovom slučaju fotografije). Način realizacije ovakvog oblika zaštite je umetanje dodatnog sloja s autentifikacijskim potpisom unutar fotografije pomoću vodenog žiga. Taj dodatni sloj služi kao senzor za otkrivanje promjena na digitalnoj fotografiji. Tehnički zahtjevi za ovu vrstu primjene su:

- Nevidljivost običnim korisnicima
- Primjenjivost na komprimirani format slike (većina kamera je kompatibilna s JPEG formatom)
- Osjetljivost na manipulaciju sadržajem, dodatnu kompresiju i sl.

2.5.3. Vidljivi reverzibilni vodeni žig za distribuciju

Za razliku od prethodnih primjena ovakav vodeni žig mora biti vidljiv, a zaštićeni sadržaj je dostupan kao komercijalni proizvod. Ova jedinstvena forma upotrebe digitalnog vodenog žiga dopušta vlasniku sadržaja umetanja vidljivog oblika ili vlastitog loga na sliku. Vodeni žig može se ukloniti samo korištenjem pravilnog ključa i softvera za uklanjanje vodenog žiga. Ovakav vodeni žig primjenjuje se modifikacijom DCT koeficijenata slike komprimirane JPEG – om po predefiniranim pravilima i rezultatima vizualnih analiza na način da je polu transparentan, ali ne u potpunosti uništiv. Uz korištenje ključa i softvera za uklanjanje, vidljivi vodeni žig se briše, te često na njegovo mjesto dolazi nevidljivi vodeni žig za potrebe daljnjeg praćenja upotrebe zaštićenog sadržaja. S primjenom ovakvog vidljivog digitalnog vodenog žiga sadržaj štiti sam sebe, te ga vlasnik može bez problema distribuirati preko interneta. Ukoliko korisnik želi ukloniti takav žig, sve što treba je ključ za dešifriranje (i softver, naravno) koji je moguće nabaviti uz određenu nadoplatu. Ovom metodom se uvelike smanjuju sigurnosni rizici objave vlastitog sadržaja [4].



Slika 2 - Primjer reverzibilnog digitalnog vodenog žiga

2.5.4. Komunikacijski sustavi

Sustav za umetanje digitalnog vodenog žiga može se promatrati kao svojevrsni komunikacijski sustav. Poslana poruka P , kodirana kao vodeni žig W , modulira se i šalje preko komunikacijskog kanala do detektora vodenog žiga. U ovom modelu prikrivanje vodenog žiga predstavlja komunikacijski kanal, pa se tretira kao izvor šuma. Ostali izvori šuma uzrokovani su distorzijama korištenjem obrade signala ili napadima. Modeliranje vodenog žiga u obliku komunikacijskog sustava je bitno zbog mogućnosti korištenja raznih tehnika komunikacijskih sustava, poput modulacije, ispravljanja grešaka, kodiranja, proširenog spectra i dr. na vodeni žig. Te tehnike mogu biti ključne u konstrukciji vodenog žiga koji se bave sljedećim:

- Kako umetnuti i detektirati jedan bit informacije
- Koju domenu obrade koristiti
- Kako koristiti informacije za osiguranje neprimjetnosti
- Kako koristiti modulacije i multipleksiranje za umetanje više od jednog bita informacije
- Kako poboljšati otpornost i sigurnost vodenog žiga [5]

2.6. Distorzije i napadi na vodeni žig

Prije svega treba razlikovati dvije vrste ili svrhe napada na vodeni žig:

- *Neprijateljski* ili *zlonamjerni* kojima je cilj oslabiti, izbrisati, uništiti ili promijeniti vodeni žig, te
- *Slučajni*, do kojih može doći prilikom standardne obrade slike i nemaju za cilj promijeniti vodeni žig.

Kompresija s gubicima se smatra jednim od najčešćih napada s kojim se vodeni žig mora oduprijeti. Termin napad (govoreći o kompresiji) može se opravdati činjenicom da je cilj kompresije prigušavanje ili odbacivanje percepcijski nebitne informacije unutar slike (između ostalog, i vodenog žiga). Mogući napadi na vodeni žig mogu se podijeliti u sljedeće 4 veće kategorije:

- Napadi uklanjanja
- Geometrijski napadi
- Kriptografski napadi
- Protokolarni napadi

2.6.1. Napadi uklanjanja

Napadi uklanjanja (jednostavni) pokušavaju odvojiti i ukloniti vodeni žig iz zaštićenog sadržaja. Ako napadač pokušava ukloniti vodeni žig iz zaštićenog sadržaja tada se napad smatra napadom uklanjanja. Najčešći način uklanjanja je upotreba modela filtriranja preuzetih iz statističke teorije signala. Uklanjanje šuma pomoću visokopropusnih (highpass) ili medijan filtara, nelinearna skraćivanja i prostorna predviđanja digitalnog vodenog žiga smatraju se prilično uspješnim metodama uklanjanja žiga. Cilj je dodati distorziju na sliku, na način da vodeni žig postane nemoguće detektirati ili pročitati [3]. Napad se smatra uspješnim ako se vodeni žig više ne može

detektirati, a slika je i dalje iskoristiva za željenu namjenu. Neki od mogućih napada su:

- Kompresija s gubicima (JPEG, JPEG 2000)
- Dodavanje Gauss-ovog šuma
- Uklanjanje šuma
- Filtriranje
- Median filtriranje i zamućivanje
- Promjene signala (izoštavanje, pojačavanje kontrasta)

Kompresija: uglavnom nenamjieran napad, ali se pojavljuje dosta često u multimedijским aplikacijama. Većina slika distribuiranih na internet je podložena nekoj vrsti kompresije. Kako je za vodeni žig potrebno da bude otporan na različite stupnjeve kompresije, poželjno je umetanje vodenog žiga u domeni u kojoj se vrši kompresija. Npr., umetanje vodenog žiga u DCT domeni je otpornije na JPEG kompresiju od umetanja vodenog žiga u prostornoj domeni, dok je umetanje vodenog žiga u DWT domeni otporno na JPEG 2000 kompresiju.

Aditivni šum: nasumični signal s određenom distribucijom (npr. Gauss, Poisson, uniformna) je nenamjerno dodan na sliku. U nekim primjenama do aditivnog šuma može doći prilikom A/D ili D/A pretvorbe ili zbog pojave grešaka tokom prijenosa. Međutim, napadač može umetnuti perceptualno oblikovani šum maksimalne snage koja se neće primjetiti. Time se obično postiže podizanje pragova usporedbe za detekciju prisutnosti vodenog žiga.

Uklanjanje šuma bavi se teorijom da je sam digitalni vodeni žig aditivni šum u odnosu na originalnu sliku. Ovakvi napadi uključuju: lokalni

medijan, usrednjavanje, Wienerov filter, te manipulacija pragovima usporedbe.

Napadi filtriranjem: koriste se linearni fltri – niskopropusni, visokopropusni, Gaussov, filter za izoštravanje itd. Niskopropusno filtriranje, na primjer, ne uzrokuje velike degradacije u označenoj slici, ali može jako utjecati na performanse, jer vodeni žigovi umetnuti tehnikom proširenog spectra imaju vrlo nečitljive spektralne komponente na visokim frekvencijama. Za otpornost na ovakvu vrstu napada tehnika umetanja vodenog žiga mora biti dizajnirana na način da većinu energije vodenog žiga sprema unutar onih frekvencija na koju grupa filtera ima najmanji utjecaj.

Statističko usrednjavanje: cilj ove vrste napada je dohvaćanje originalne slike ili vodenog žiga statističkom analizom većeg broja označenih skupova podataka. Napadač može pokušati procijeniti vodeni žig i nakon toga ga ukloniti jednostavnim oduzimanjem procjene od označene slike. Ovaj način je opasan ako vodeni žig ne ovisi uvelike o podacima. Zato je dobra ideja koristiti percepcijske maske za izradu vodenog žiga. U ovu grupu napada spadaju usrednjavanje i napadi krivotvorenja. Napadi usrednjavanja uzimaju više instance istog sadržaja, označenog drugačijim vodenim žigom. Ovim načinom izračunava se procjena originalne slike i oslabljuje se učinak pojedinog vodenog žiga. Napadima krivotvorenja usrednjava se više različitih sadržaja, ali označenih istim vodenim žigom. Na ovaj način dobiva se dobra procjena vodenog žiga, koja se može iskoristiti za njegovo uklanjanje iz zaštićenog sadržaja.

2.6.2. Geometrijski napadi

Ova vrsta napada nije usmjerena na uklanjanje vodenog žiga, već na njegovo uništavanje ili onemogućivanje njegove detekcije. Pokušavaju uništiti detekciju korelacije originalnog i izvučenog vodenog žiga pomoću translacije, rotacije, te skaliranjem označene slike. To je moguće postići miješanjem piksela u slici. Njihove vrijednosti ostaju iste, međutim mijenja se njihova pozicija unutar same slike. Ovi se napadi mogu dodatno podijeliti na one koji koriste opće affine transformacije i one koje koriste projekcijske transformacije.

2.6.3. Kriptografski napadi

Kriptografski napadi ciljaju na probijanje sigurnosnih metoda korištenih u implementaciji digitalnog vodenog žiga čime traže način uklanjanja vodenog žiga ili umetanja lažnog na njegovo mjesto. Jedna takva tehnika je brute-force pretraživanje za umetnutom tajnom informacijom. U praksi, korištenje ovakvih napada je vrlo ograničeno zbog visoke razine kompleksnosti njihovog izvođenja. Pokrivaju direktne napade na traženje tajnog ključa, te napade krivotvorenja spomenute u prošlim poglavljima.

Kriptografski napadi na digitalni vodeni žig vrlo su slični onima koji se koriste u području kriptografije. To su, na primjer, prethodno spomenuti brute-force napadi s ciljem pronalaska tajnog ključa. Kako mnoge implementacije digitalnog vodenog žiga koriste tajni ključ, poželjno je da on bude zadovoljavajuće duljine za dovoljnu sigurnost. Još jedan od napada u ovoj kategoriji je tzv. Oracle napad koji se može iskoristiti za stvaranje neoznačene slike kada napadač ima pristup uređaju za detekciju digitalnog vodenog žiga.

2.6.4. Protokolarni napadi

Protokolarnim napadima cilj nije uklanjanje utisnute informacije, kao ni njezino uništavanje, niti onemogućavanje detekcije (deaktivacija digitalnog vodenog žiga). Naprotiv, ovi napadi iskorištavaju semantičke nedostatke u implementaciji digitalnog vodenog žiga. Ciljaju na shvaćanje koncepta implementacije digitalnog vodenog žiga.

Prvi protokolarni napad imao je zadatak prikazati da za korištenje digitalnog vodenog žiga za zaštitu autorskih prava, on mora biti neinvertibilan. Ideja inverzije vodenog žiga sastoji se od činjenice da napadač posjeduje zaštićeni materijal i može tvrditi da taj materijal sadrži i njegov digitalni vodeni žig jednostavnim oduzimanjem vlastitog žiga. To može stvoriti nejasnost u otkrivanju pravog vlasnika zaštićenog sadržaja.

Zahtjev neinvertibilnosti tehnologije umetanja digitalnog vodenog žiga implicira da mora biti nemoguće izvući digitalni vodeni žig iz slike ako ona nije označena vodenim žigom. Kao rješenje tog problema uvode se digitalni vodeni žigovi ovisni o samom signal korištenjem jednosmjerne funkcije. Prema tome, vodeni žig ne smije biti invertibilan niti mogućnost da bude kopiran. Napad kopiranjem ciljao bi, na primjer, kopiranje digitalnog vodenog žiga s jedne slike na drugu bez poznavanja tajnog ključa. Takav napad također spada u protokolarnu napade i za cilj nema uništavanje vodenog žiga ili onemogućavanje njegove detekcije, već samo estimaciju tog žiga iz nekog zaštićenog sadržaja, te njegovo kopiranje na neki drugi sadržaj [6].

3. Tehnike implementacije digitalnog vodenog žiga

Osnovna podjela tehnika implementacije digitalnog vodenog žiga je po domeni rada, a može se podijeliti na dvije:

- Prostorna domena
- Frekvencijska domena

Unutar ovog poglavlja bit će dan kratak pregled nekih mogućih tehnika u obje domene, dok će tri tehnike iz frekvencijske domene (DFT, DCT, DWT) biti obrađene detaljnije u sljedećem poglavlju i testirane pomoću programskog okruženja Matlab.

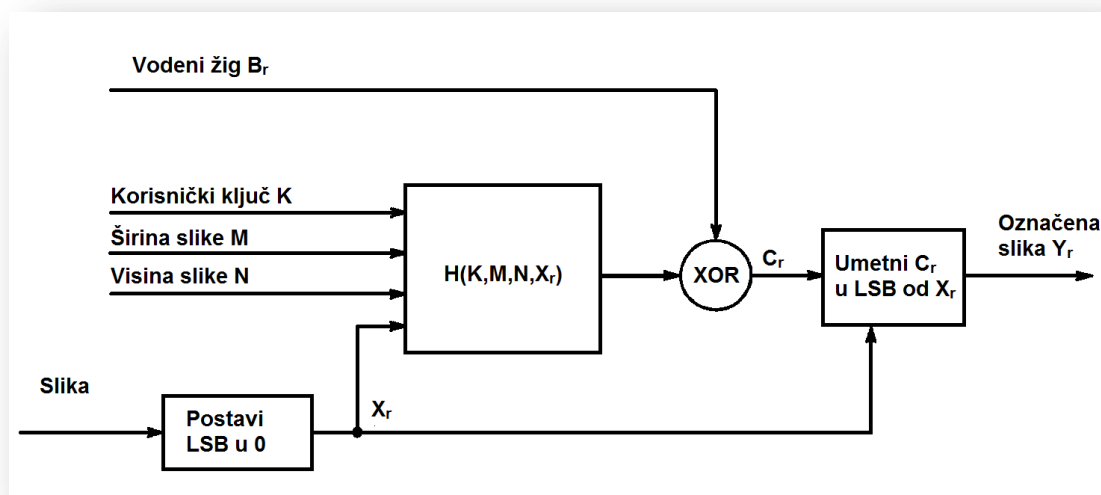
3.1. Prostorna domena

Umetanje vodenog žiga u prostornoj domeni može se izvesti korištenjem razdvajanja krominantnih komponenti slike. Na taj način, digitalni vodeni žig pojavljuje se samo u jednom krominantnom pojasu slike. Digitalni vodeni žig je teško vidljiv pod normalnim uvjetima promatranja korištenjem ovih tehnika. Međutim, vodeni žig postaje vidljiv kod separacije boja za vrijeme ispisivanja slike. Time dokument postaje bekoristan nakon printanja, dok se vodeni žig ne ukloni iz pojasa u kojem se nalazi. Metoda nalazi komercijalnu upotrebu u novinarstvu, gdje novinari mogu pregledavati označene digitalne slike prije kupovine njihovih neoznačenih verzija. U ovoj domeni u nastavku su dane dvije tehnike implementacije.

LSB (Least Significant Bit)

Najranije metode za umetanje digitalnog vodenog žiga bazirane su na umetanju žiga u najniže bitove pojedinih piksela. Bilo koja slika sastoji se od piksela, a kako je svaki piksel reprezentiran sekvencom od 8 bita, vodeni žig se umeće na mjesto zadnjih (najmanje bitnih) bitova, na mjesta odabranih

piksela unutar slike. Ovu metodu lako je implementirati i ne generira vidljive smetnje unutar slike, ali nije otporna na napade. Napadaču je dovoljno da nasumično promijeni sve zadnje bitove, čime se efektivno uništava skrivena informacija, odnosno digitalni vodeni žig [7].



Slika 3 - Primjer sheme za tehniku LSB

Modulacija proširenog spektra (SSM)

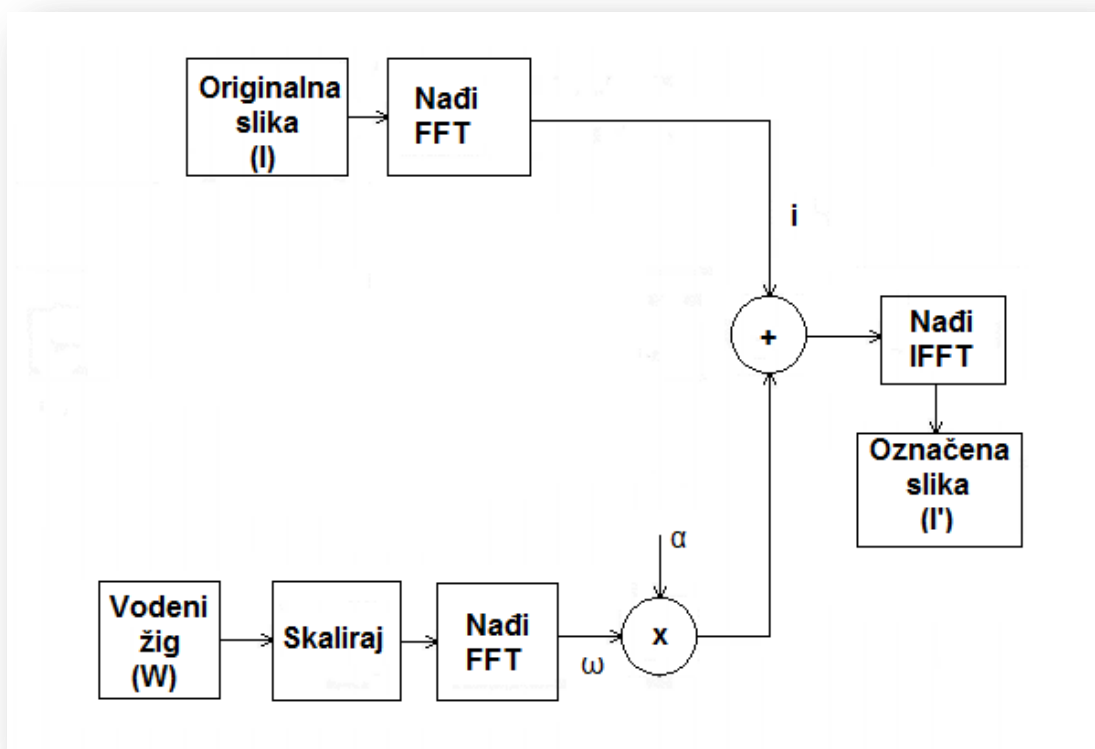
Tehnike proširenog spektra su metode koje energiju lokaliziranu na točno određenim diskretnim frekvencijama namjerno šire, odnosno distribuiraju po vremenu. To se radi zbog mnoštva razloga, uključujući uspostavu sigure komunikacije, povećanje otpornosti na šumove i elektroničko ometanje, te prevenciju detekcije. Primjena u kontekstu digitalnog vodenog žiga obuhvaća linearnu kombinaciju originalne slike s nekim signalom šuma moduliranim utisnutim vodenim žigom [8].

3.2. Frekvencijska domena

U usporedbi s tehnikama koje djeluju u prostornoj domeni, češće su korištene. Cilj je umetanje vodenog žiga unutar spektralnih komponenti slike. Najčešće korištene transformacije su diskretna kosinusna (DCT), diskretna Fourierova (DFT) i diskretna valićna transformacija (DWT). Razlog za korištenje frekvencijske domene pri implementaciji digitalnog vodenog žiga je bolja prilagođenost spektralnih koeficijenata karakteristikama ljudskog vizualnog sustava. Ljudsko oko je osjetljivije na promjene u nižim frekvencijama, nego na promjene viših frekvencija. Drugim riječima, informacije sadržane u nižim frekvencijama su percepcijski bitnije, pa samim time promjene na koeficijentima nižih frekvencijama uzrokuju veće vidljive distorzije na samoj slici. S druge strane visokofrekvencijske komponente smatraju se nebitnima, tako da se sve tehnike obrade slike, kao što je kompresija baziraju na uklanjanju tih komponenti. Za postizanje dobrog balansa između otpornosti i nevidljivosti digitalni vodeni žig se najčešće utiskuje na položaje koeficijenata u području srednjeg frekvencijskog pojasa [9].

Diskretna Fourierova transformacija (DFT)

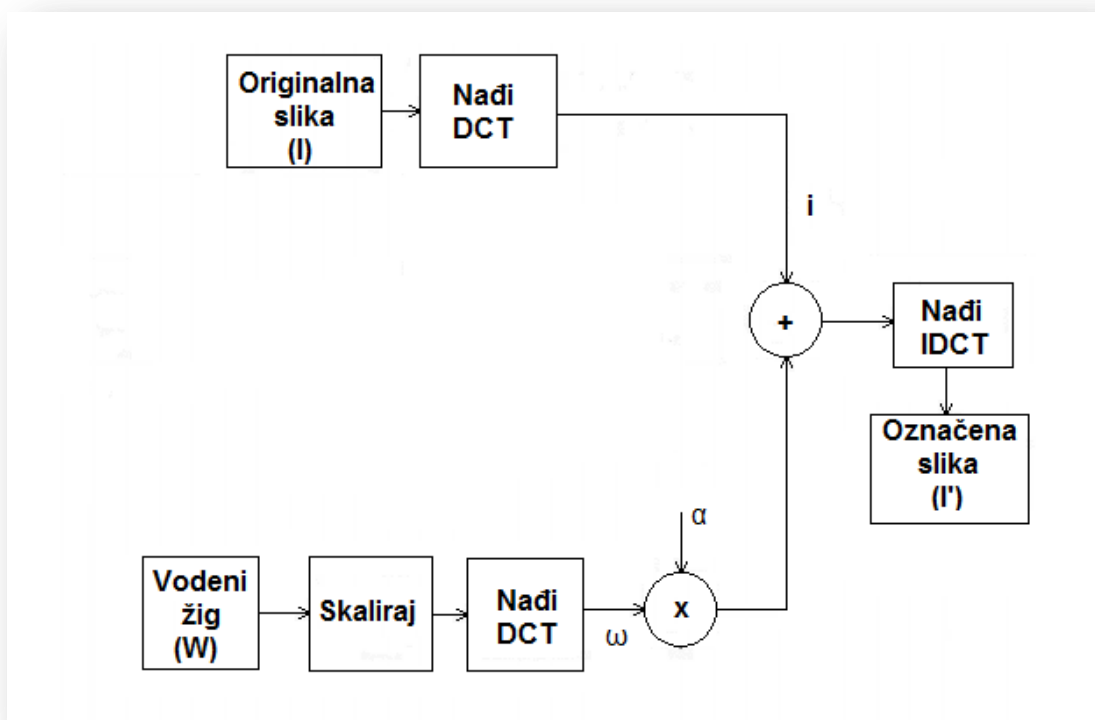
Domena diskretne Fourierove transformacije istraživana je za korištenje kod implementacije digitalnog vodenog žiga zbog svoje otpornosti na geometrijske promjene na slici, poput rotacije, translacije, skaliranja itd. Kao i kod ostalih frekvencijskih tehnika umetanje digitalnog vodenog žiga obavlja se u pojasu srednjih frekvencija, dok svojstva Fourierove transformacije omogućavaju relativno jednostavnu detekciju digitalnog vodenog žiga unutar slike, čak i nakon podvrgavanja slike distorzijama poput kompresije, rotacije, zamučivanja i sl. Iz tog razloga diskretna Fourierova transformacija je vrlo pogodna za umetanje digitalnog vodenog žiga unutar slike.



Slika 4 - Shema umetanja digitalnog vodenog žiga korištenjem DFT

Diskretna kosinusna transformacija (DCT)

Diskretna kosinusna transformacija, kao i Fourierova, koristi frekvencijski, a ne amplitudni, prostor za prikaz podataka. To je korisno jer više odgovara načinu na koji ljudsko oko percipira svjetlost, tako da se dijelovi koji su manje primjetni ili neprimjetni mogu odbaciti. Metode bazirane na DCT su otpornije od metoda koje koriste prostornu domenu rada. Algoritmi koji koriste DCT otporni su na jednostavne manipulacije slike poput filtriranja niskopropusnim filtrom, promjena svjetline i kontrasta, zamučivanje i sl. S druge strane, teže ih je implementirati i računski su dosta kompleksniji, odnosno skuplji za izvedbu. U isto vrijeme nisu pretjerano otporni na geometrijske transformacije poput skaliranja, rotacije, translacije itd. Izvedba DCT može biti nad cijelom slikom ili blokovska [10].

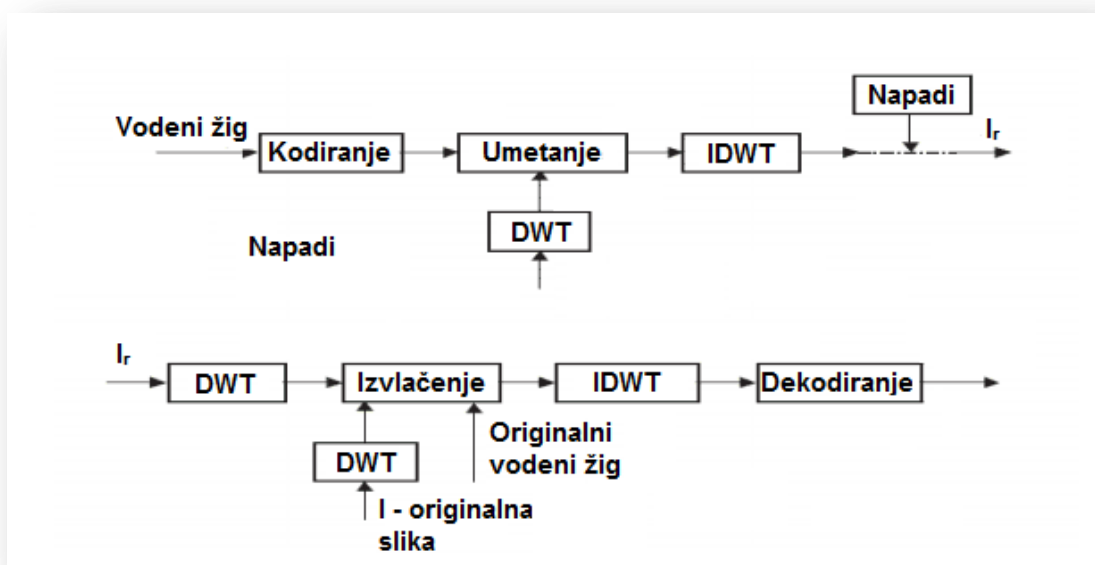


Slika 5 - Umetanje digitalnog vodenog žiga korištenjem DCT

Diskretna valična (wavelet) transformacija (DWT)

Diskretna valična transformacija trenutno je korištena u velikom broju primjena obrade signala, poput audio i video kompresije, uklanjanja šuma iz audio signala i simulacije distribucije bežičnih antena. Valići (waveleti) imaju energiju koncentriranu u vremenu, pa su iz tog razloga pogodni za obradu vremenski promjenjivih signala. Kako je veličina stvarnih signala po prirodi vremenski promjenjiva valići pronalaze primjenu u mnogim situacijama. Jedan od glavnih problema u tehnikama digitalnog vodenog žiga je postizanje dobre ravnoteže između otpornosti i mogućnosti percipiranja digitalnog vodenog žiga. Povećanje otpornosti moguće je postići povećanjem snage utisnutog vodenog žiga, ali se time povećava i vidljivi poremećaj uzrokovan vodenim žigom na slici. Zato je DWT vrlo korisna transformacija, jer istovremeno postiže prostornu lokalizaciju digitalnog vodenog žiga, kao i

njegovu raširenost u spektru unutar označene slike. Osnovna ideja valične transformacije u obradi slika je rastav slike na nekoliko područja različitih prostornih domena i nezavisnih frekvencija [11].



Slika 6 - Prikaz sheme sustava za umetanje i izvlačenje digitalnog vodenog žiga pomoću DWT

4. Implementacija i analiza u Matlabu

Za potrebe analiziranja uspješnosti umetanja i izvlačenja koristit će se dvije mjere kvalitete, od kojih je prva SNR (odnos signal šum), koja se koristi za objektivnu procjenu kvalitete slike:

$$SNR = \frac{\sum_{i=1}^M \sum_{j=1}^N [z(i,j)]^2}{\sum_{i=1}^M \sum_{j=1}^N [I(i,j) - z(i,j)]^2} \quad (1)$$

gdje z predstavlja sliku označenu vodenim žigom, nakon unošenja dodatne distorzije za potrebe testiranja, I označava originalnu sliku bez vodenog žiga, dok su M i N dimenzije slike.

Druga mjera će biti korištena za izračun sličnosti originalnog i izvučenog vodenog žiga i dana je sljedećom jednadžbom:

$$SF = \frac{\sum_{i=1}^M \sum_{j=1}^N [o(i,j) * e(i,j)]}{\sqrt{\sum_{i=1}^M \sum_{j=1}^N [o(i,j)^2 * e(i,j)^2]}} \quad (2)$$

gdje o predstavlja originalni vodeni žig, e izvučeni vodeni žig, a M i N su dimenzije vodenog žiga. Vrijednost SF (eng. *similarity factor*, faktor sličnosti) kreće se u rasponu $[0,1]$. Što je vrijednost bliže 1, to je bolja metoda izvlačenja vodenog žiga. Zadovoljavajućim se smatra ako je SF veći od 0.75.

4.1. Diskretna Fourierova transformacija

Fourierova transformacija je važan alat za obradu slike koji koristi rastav slike na njene sinusne i kosinusne komponente. Izlaz Fourierove transformacije predstavljaju komponente slike u frekvencijskoj domeni dok je ulazna slika njena reprezentacija u prostornoj domeni. U domeni Fourierove transformacije svaka točka slike predstavlja određenu frekvenciju sadržanu u slici u prostornoj domeni.

Fourierova transformacija se koristi za razne primjene poput obrade, filtriranja, rekonstrukcije, kompresije slike, te umetanje digitalnog vodenog žiga unutar slike.

Umetanje digitalnog vodenog žiga

Proces umetanja digitalnog vodenog žiga u sliku korištenjem Fourierove transformacije (Slika 4.) obavlja se u sljedećim koracima:

- Učitavaju se slika I (koju treba označiti), te slika W (vodeni žig), koje ne moraju nužno biti iste veličine
- Ukoliko je potrebno slika W (vodeni žig) se skalira na veličinu slike I
- Pronalaze se DFT (FFT) koeficijenti obje slike
- Određuje se vrijednost faktora umetanja (α) koji mijenja vidljivost vodenog žiga na slici
- FFT koeficijenti originalne slike i vodenog žiga mijenjaju se prema (3), te se računa IFFT označene slike

$$R = \sum_{i=1}^M \sum_{j=1}^N [X(i,j) + \alpha * K(i,j)] \quad (3)$$

gdje X predstavlja Fourierovu transformaciju originalne slike, a K predstavlja Fourierovu transformaciju digitalnog vodenog žiga, a M i N su dimenzije slike, odnosno vodenog žiga (R označava rezultat).

Izvlačenje digitalnog vodenog žiga

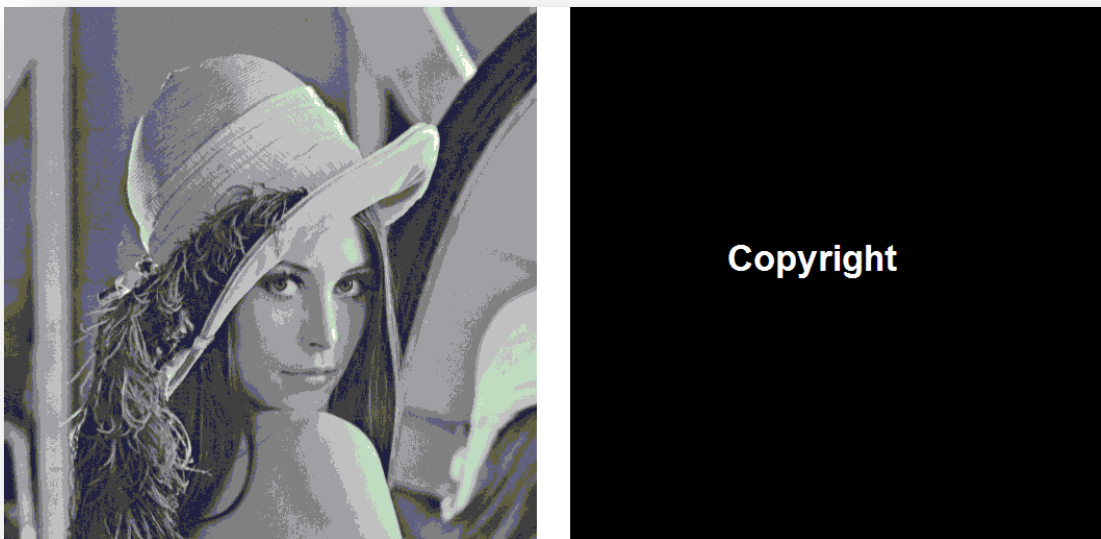
Izvlačenje digitalnog vodenog žiga iz označene slike odvija se prema sljedećoj jednadžbi:

$$R = \sum_{i=1}^M \sum_{j=1}^N \frac{[A(i,j)-I(i,j)]}{\alpha} \quad (4)$$

gdje A predstavlja označenu sliku nakon uvođenja dodatnih distorzija, a I predstavlja originalnu sliku bez vodenog žiga.

Analiza

Na sljedećoj slici (Slika 7.) prikazane su slika korištena za umetanje vodenog žiga, te vodeni žig:



Slika 7 - (a) Originalna slika

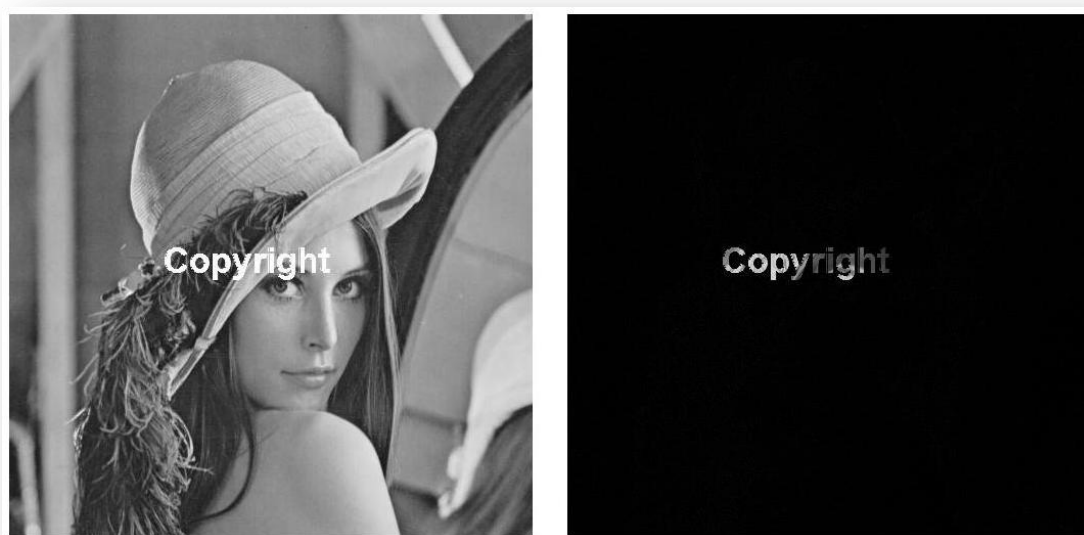
(b) Vodeni žig

Simulacija umetanja digitalnog vodenog žiga i uvođenja nekoliko vrsta distorzija pokretana je nekoliko puta do postizanja željenih rezultata.

Rezultati simulacije prikazani su na sljedećim slikama (Slika 8. – Slika 17.), gdje lijeva strana prikazuje označenu sliku s opisanom distorzijom, a desna izvučeni vodeni žig.



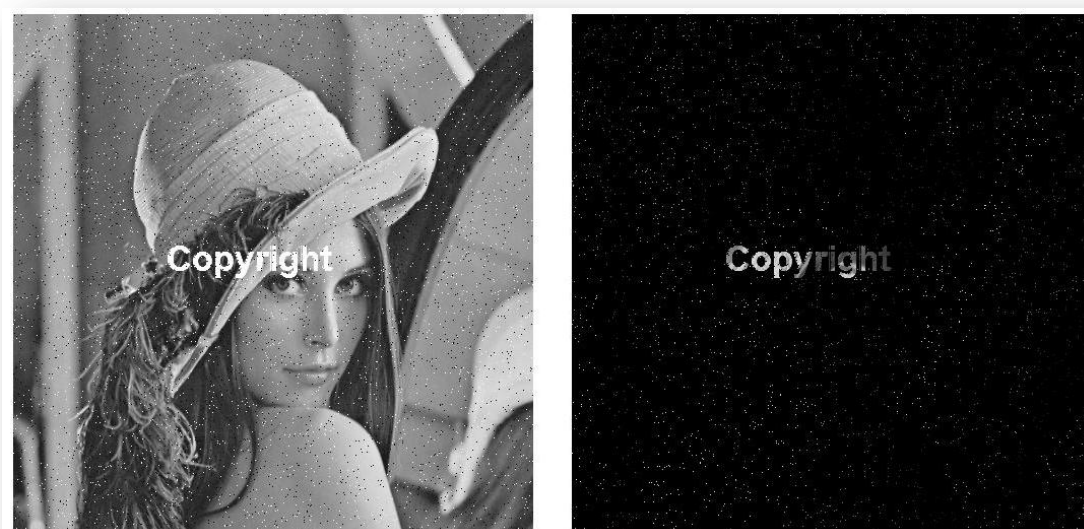
Slika 8 - JPEG kompresija uz $q = 15$, $\alpha = 0.5$



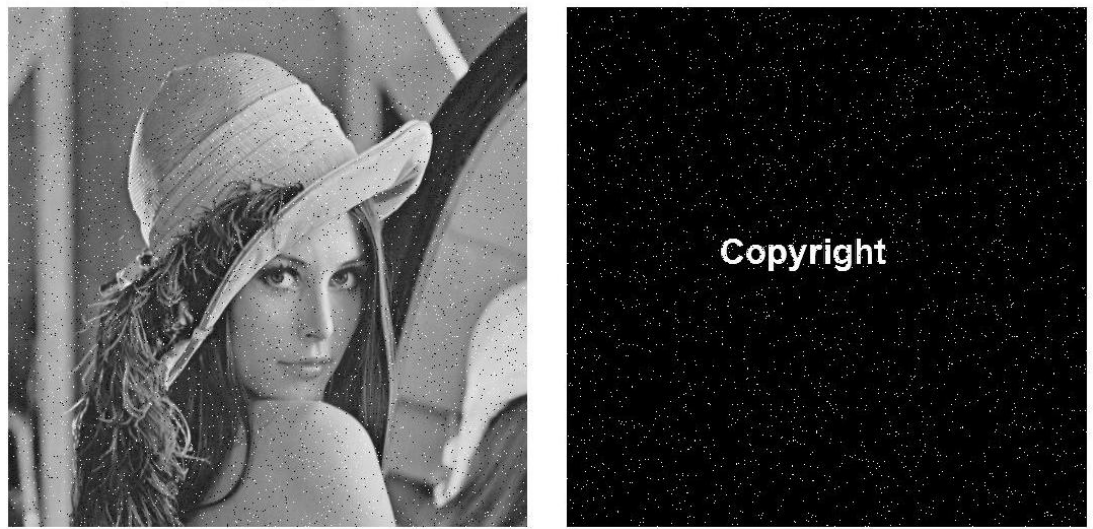
Slika 9 - JPEG kompresija uz $q = 75$, $\alpha = 1$



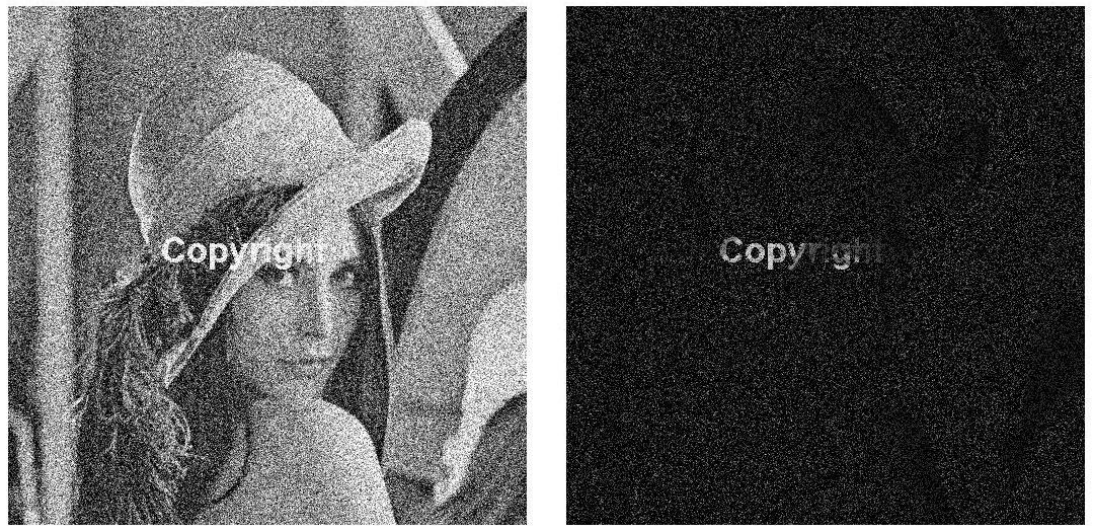
Slika 10 - JPEG kompresija uz $q = 30$, $\alpha = 0.02$



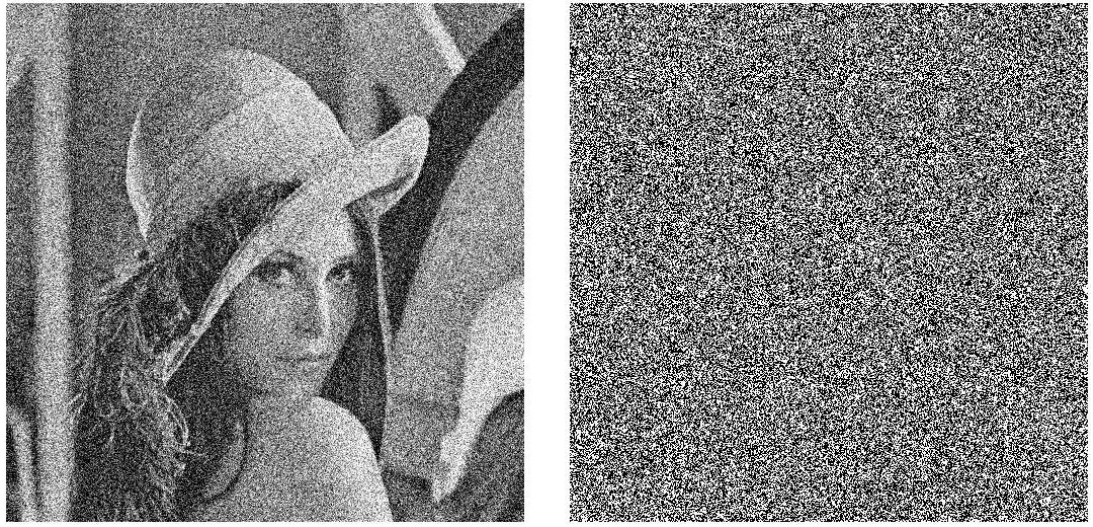
Slika 11 - Salt & pepper šum ($d = 0.02$) uz $\alpha = 1$



Slika 12 - Salt & pepper šum ($d = 0.02$) uz $\alpha = 0.02$



Slika 13 - Gaussov šum ($\mu = 0, \sigma = 0.05$) uz $\alpha = 1$



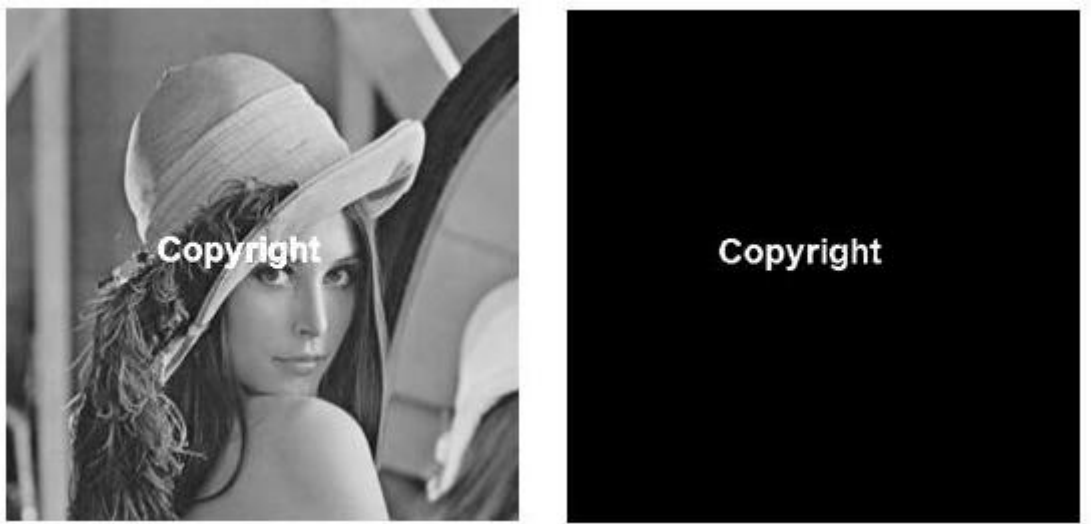
Slika 14 - Gaussov šum ($\mu = 0, \sigma = 0.05$) uz $\alpha = 0.02$



Slika 15 - Rotacija (30°) uz $\alpha = 1$



Slika 16 - Rotacija (30°) uz $\alpha = 0.02$



Slika 17 - Skaliranje (0.5) uz $a = 1$

Na prethodnim slikama vidljivo je da je metoda korištenjem DFT-a otporna na JPEG kompresiju do određenog stupnja kompresije naravno, te da vizualno možemo prepoznati digitalni vodeni žig nakon skaliranja, rotacije, dodavanjem salt & pepper šuma, dok dodavanje Gaussovog šuma gotovo u potpunosti uništava vodeni žig. Objektivniji način određivanja sličnosti dan je u sljedećoj tablici (Tablica 1.):

Tablica 1 - Utjecaj distorzija na kvalitetu slike (DFT)

Distorzija	SNR	SF
<i>JPEG kompresija</i> ($q=15, \alpha=0.5$)	21.8565	0.7573
<i>JPEG kompresija</i> ($q=75, \alpha=1$)	20.6007	0.8906
<i>JPEG kompresija</i> ($q=30, \alpha=0.02$)	28.5797	0.0753
<i>Salt & pepper</i> ($\alpha=1$)	15.4214	0.4869
<i>Salt & pepper</i> ($\alpha=0.02$)	16.8210	0.0225
<i>Gaussov šum</i> ($\alpha=1$)	8.4699	0.1766
<i>Gaussov šum</i> ($\alpha=0.02$)	8.5765	0.0090
<i>Rotacija 30°</i> ($\alpha=1$)	14.8610	$1.3104 * 10^{-17}$
<i>Rotacija 30°</i> ($\alpha=0.02$)	48.5557	$5.7611 * 10^{-16}$
<i>Skaliranje</i> ($\alpha=1$)	16.8652	$1.5839 * 10^{-18}$

Matlab kod:

```
close all; clc;

%Učitavanje slike
I = im2double(imread('bb.bmp'));
figure;
imshow(I);
title('Originalna slika');
X=fft(I);
alpha=1;

% Učitavanje vodenog žiga
o=im2double(imread('ba.bmp'));
figure;
imshow(o);
title('Vodeni žig');

% Umetanje vodenog žiga
r=fft(o);
K=r.*alpha;
X=X+K;
T=ifft(X);

% JPEG kompresija označene slike
q=input('Quality Factor q = ');
imwrite(T,'xyz.jpg','jpg','quality',q);
a=imread('xyz.jpg');

%a = imnoise(T, 'Salt & pepper', 0.02);
%a = imnoise(T, 'Gaussian', 0, 0.05);
%a = imrotate(T,30);
%I = imrotate(I,30);
%a = imresize(T,0.5);
%I = imresize(I,0.5);

a=im2double(a);
figure;
imshow(a);
title('Označena slika');
w1= (a-I)./alpha;
figure;
imshow(w1);
title('Detektirani vodeni žig');

% Izračun SNR
z1=double(a);
snr_num=0;
snr_den=0;
for i=1:512
    for j=1:512
        snr_num=snr_num+(z1(i,j)*z1(i,j));
        snr_den=snr_den+((I(i,j)-z1(i,j))*(I(i,j)-z1(i,j)));
    end
end

snr=10*log10(snr_num/snr_den)
```

```
% Izračun faktora sličnosti (SF)
sf_num=0;
sf_den=0;
a=0;
b=0;
for i=1:512
    for j=1:512
        sf_num=sf_num+(w1(i,j)*o(i,j));
        a=a+(o(i,j)*o(i,j));
        b=b+(w1(i,j)*w1(i,j));
        sf_den=sqrt(sf_den+a*b);
    end
end
sf=(sf_num/sf_den)
```

4.2. Diskretna kosinusna transformacija

Diskretna kosinusna transformacija reprezentira sliku kao sumu sinusoida varirajućih amplituda i frekvencija. DCT ima specijalno svojstvo da koncentrira percipijski bitne dijelove slike u vrlo malen broj DCT koeficijenata.

Kako DCT ima jako dobro svojstvo sažimanja energije, razvijeni su mnogi algoritmi za umetanje digitalnog vodenog žiga na bazi DCT transformacije. Jedini veći problem DCT-a je razdvajanje slike, pa i vodenog žiga na blokove što može dovesti do pojave diskontinuiteta u slici.

Umetanje digitalnog vodenog žiga

Koraci potrebni za umetanje digitalnog vodenog žiga koristeći DCT transformaciju (Slika 5.) su sljedeći:

- Učitavaju se slika I (koju treba označiti), te slika W (vodeni žig), koje ne moraju nužno biti iste veličine
- Ukoliko je potrebno slika W (vodeni žig) se skalira na veličinu slike I
- Pronalaze se DCT koeficijenti obje slike
- Određuje se vrijednost faktora umetanja (α) koji mijenja vidljivost vodenog žiga na slici
- DCT koeficijenti originalne slike i vodenog žiga mijenjaju se prema (5), te se računa IDCT označene slike

$$R = \sum_{i=1}^M \sum_{j=1}^N [X(i,j) + \alpha * K(i,j)] \quad (5)$$

gdje X predstavlja diskretnu kosinusnu transformaciju originalne slike, a K predstavlja diskretnu kosinusnu transformaciju digitalnog vodenog žiga, a M i N su dimenzije slike, odnosno vodenog žiga (R označava rezultat).

Izvlačenje digitalnog vodenog žiga

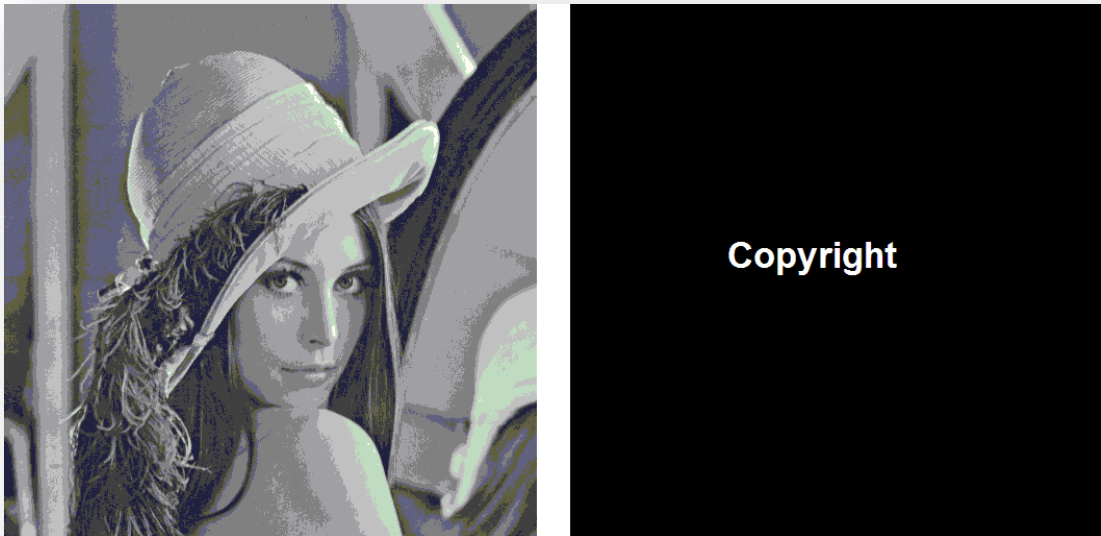
Izvlačenje digitalnog vodenog žiga iz označene slike odvija se prema sljedećoj jednadžbi:

$$R = \sum_{i=1}^M \sum_{j=1}^N \frac{[A(i,j)-I(i,j)]}{\alpha} \quad (6)$$

gdje A predstavlja označenu sliku nakon uvođenja dodatnih distorzija, a I predstavlja originalnu sliku bez vodenog žiga.

Analiza

Na sljedećoj slici (Slika 7.) prikazane su slika korištena za umetanje vodenog žiga, te vodeni žig:



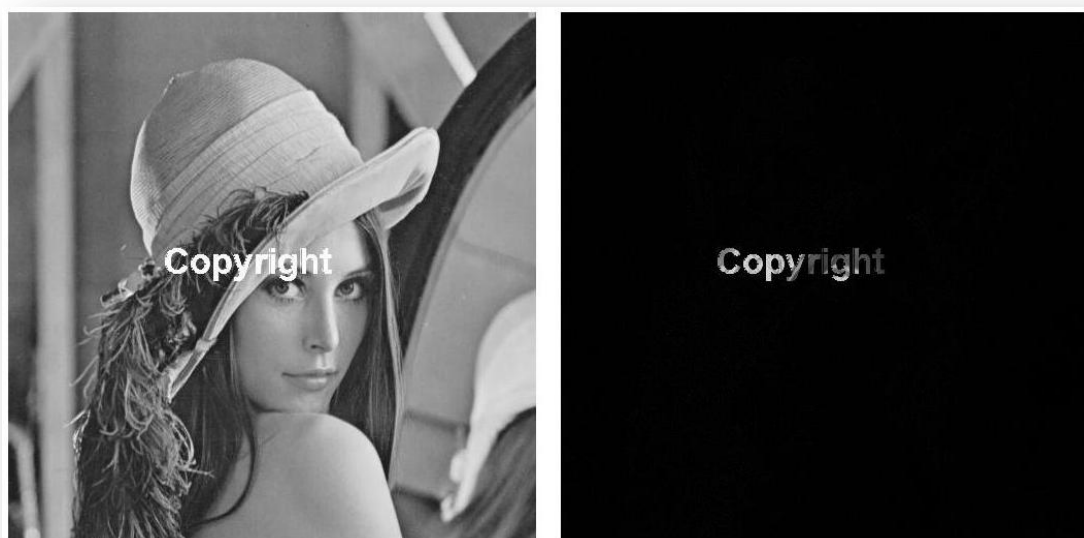
Slika 18 - (a) Originalna slika

(b) Vodeni žig

Simulacija umetanja digitalnog vodenog žiga i uvođenja nekoliko vrsta distorzija pokretana je nekoliko puta do postizanja željenih rezultata. Rezultati simulacije prikazani su na sljedećim slikama (Slika 19. – Slika 28.), gdje lijeva strana prikazuje označenu sliku s opisanom distorzijom, a desna izvučeni vodeni žig.



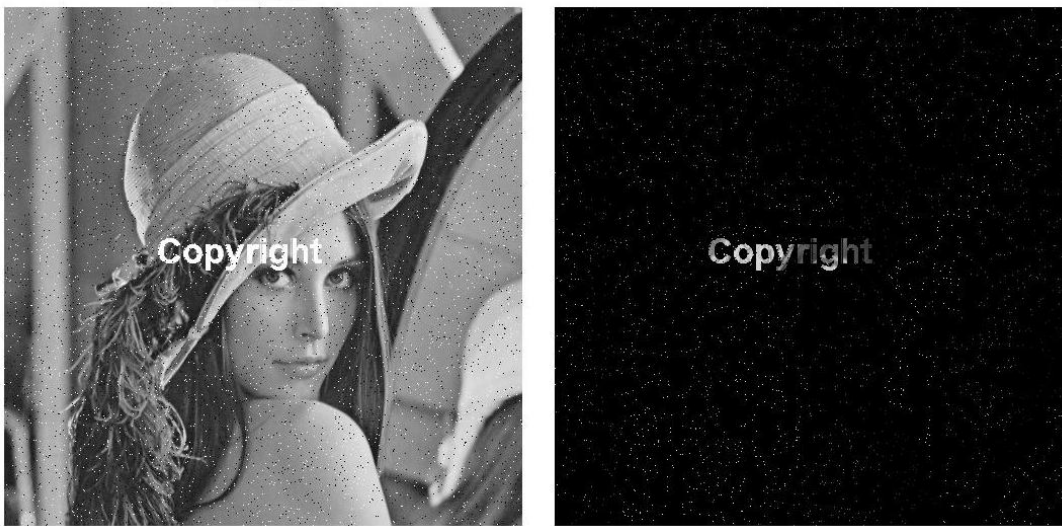
Slika 19 - JPEG kompresija uz $q = 15$, $\alpha = 0.5$



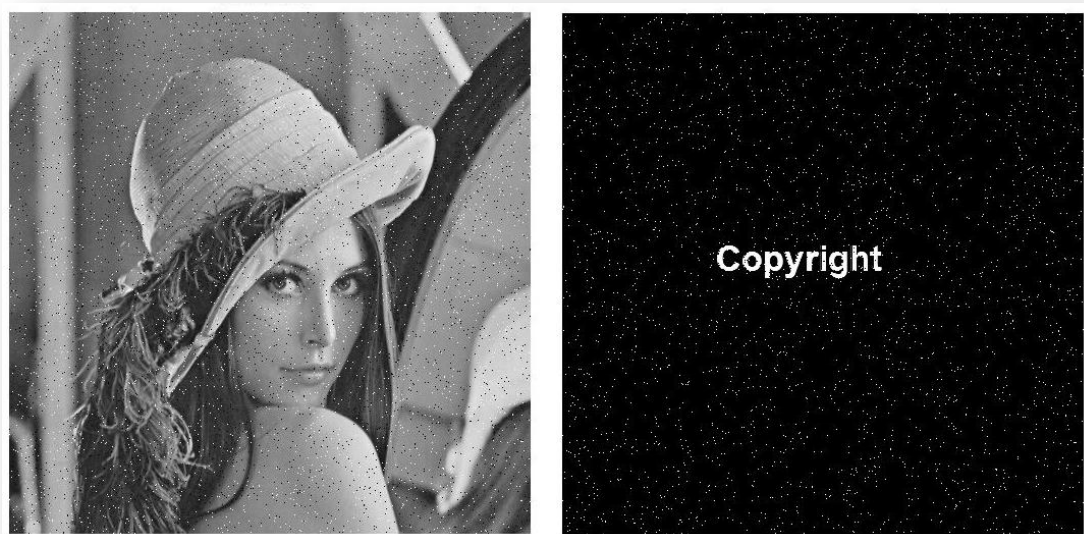
Slika 20 - JPEG kompresija uz $q = 75$, $\alpha = 1$



Slika 21 - JPEG kompresija uz $q = 30$, $\alpha = 0.02$



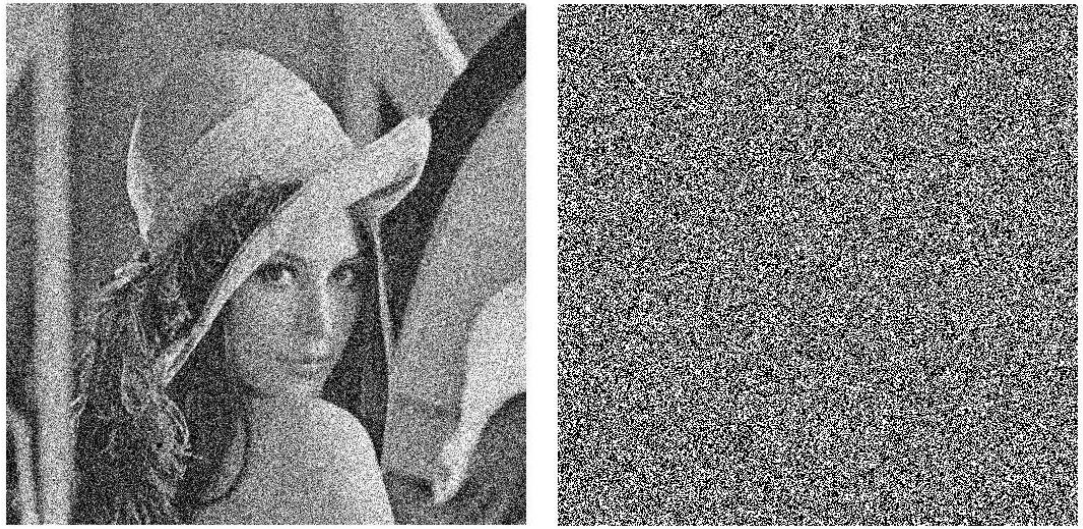
Slika 22 - Salt & pepper šum ($d = 0.02$) uz $\alpha = 1$



Slika 23 - Salt & pepper šum ($d = 0.02$) uz $\alpha = 0.02$



Slika 24 - Gaussov šum ($\mu = 0, \sigma = 0.05$) uz $\alpha = 1$



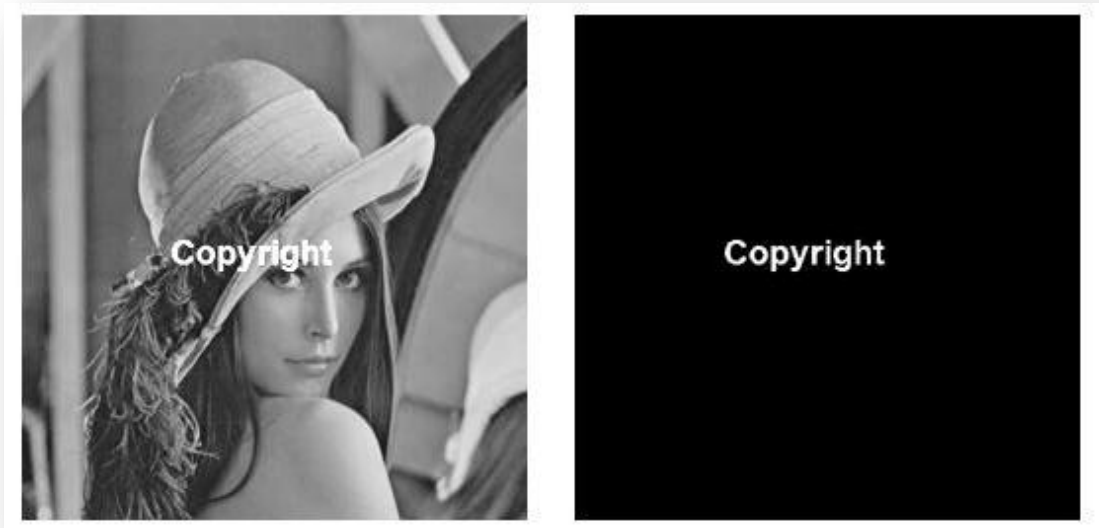
Slika 25 - Gaussov šum ($\mu = 0$, $\sigma = 0.05$) uz $\alpha = 0.02$



Slika 26 - Rotacija (30°) uz $\alpha = 1$



Slika 27 - Rotacija (30°) uz $\alpha = 0.02$



Slika 28 - Skaliranje (0.5) uz $\alpha = 1$

Iz dobivenih rezultata za metodu implementacije digitalnog vodenog žiga korištenjem DCT-a vidljivo je kako je ova transformacija pod uspješnosti vrlo slična Fourierovoj, uz vrlo male razlike u kvaliteti, te je otprilike jednako otporna na iste distorzije kao i metoda korištenjem DFT-a. Objektivnije procjene dane su u sljedećoj tablici (Tablica 2.):

Tablica 2 - Utjecaj distorzija na kvalitetu slike (DCT)

Distorzija	SNR	SF
<i>JPEG kompresija (q=15, $\alpha=0.5$)</i>	21.8703	0.7568
<i>JPEG kompresija (q=75, $\alpha=1$)</i>	20.6007	0.8906
<i>JPEG kompresija (q=30, $\alpha=0.02$)</i>	28.5797	0.0753
<i>Salt & pepper ($\alpha=1$)</i>	15.3741	0.4875
<i>Salt & pepper ($\alpha=0.02$)</i>	16.7927	0.0222
<i>Gaussov šum ($\alpha=1$)</i>	8.4748	0.1776
<i>Gaussov šum ($\alpha=0.02$)</i>	8.5574	0.0084
<i>Rotacija 30° ($\alpha=1$)</i>	14.8610	$8.5106 * 10^{-17}$
<i>Rotacija 30° ($\alpha=0.02$)</i>	48.5557	$6.0345 * 10^{-15}$
<i>Skaliranje ($\alpha=1$)</i>	16.8652	$1.0662 * 10^{-16}$

Matlab kod:

```
close all; clc;

%Učitavanje slike
I = im2double(imread('bb.bmp'));
figure;
imshow(I);
title('Originalna slika');
alpha=1;
X = dct2(I);

%Učitavanje vodenog žiga
o=im2double(imread('ba.bmp'));
figure;
imshow(o);
title('Vodeni žig');

%Umetanje vodenog žiga
r=dct2(o);
K2=r*alpha;
X=X+K2;
T = idct2(X);
w1=(T-I)./alpha;

%JPEG kompresija označene slike
q=input('Quality Factor q = ');
imwrite(T,'xyz.jpg','jpg','quality',q);
a=imread('xyz.jpg');
%a = imnoise(T, 'Salt & pepper', 0.02);
%a = imnoise(T, 'Gaussian', 0, 0.05);
%a = imrotate(T,30);
%I = imrotate(I,30);
%a = imresize(T,0.5);
%I = imresize(I,0.5);
a = im2double(a);
figure;
imshow(a);
title ('Označena slika');
w1=(a-I)./alpha;
figure;
imshow(w1);
title('Detektirani vodeni žig');

% Izračun SNR
z1=double(a);
snr_num=0;
snr_den=0;
for i=1:512
    for j=1:512
        snr_num=snr_num+(z1(i,j)*z1(i,j));
        snr_den=snr_den+((I(i,j)-z1(i,j))*(I(i,j)-z1(i,j)));
    end
end

snr=10*(log10(snr_num/snr_den))
```

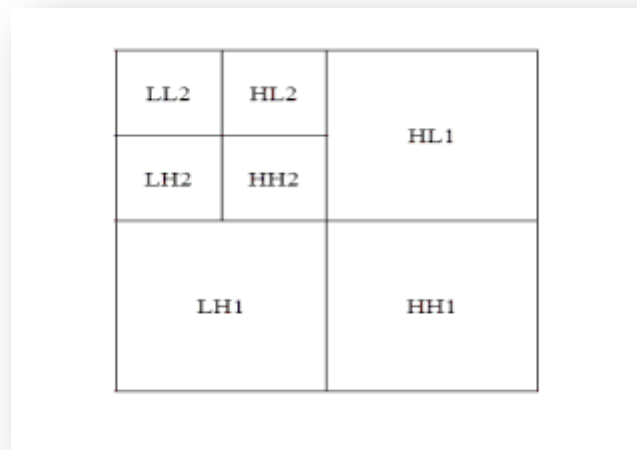
```
%Izračun faktora sličnosti (SF)
sf_num=0;
sf_den=0;
a=0;
b=0;
for i=1:512
    for j=1:512
        snr_num=snr_num+(z1(i,j)*z1(i,j));
        sf_num=sf_num+(w1(i,j)*o(i,j));
        a=a+(o(i,j)*o(i,j));
        b=b+(w1(i,j)*w1(i,j));
        sf_den=sqrt(sf_den+a*b);
    end
end

sf=(sf_num/sf_den)
```


4.3. Diskretna wavelet transformacija

Wavelet transformacija je metoda fiksnih veličina prozora, promjenjivih oblika, dobro lokalizirana u vremenu. DWT transformirani signali imaju jako dobro vremensku diferenciranost u području visokih frekvencija, odnosno jako dobru frekvencijsku diferenciranost u području nižih frekvencija. Osnovna ideja wavelet transformacije je raspodjela slike na različita područja prostorne domene nezavisnih frekvencija.

Nakon wavelet transformacije slika je podijeljena u 4 frekvencijska pojasa, i to jedan niže frekvencije (LL), te tri viših frekvencija (LH, HL, HH). Wavelet transformacija može se primjeniti i više puta, gdje svaki stupanj dekompozicije stvara 4 nova podpojasa podataka (Slika 29.). Za potrebe testiranja ove metode korišten je 'Daubechies' wavelet, s jednom razinom dekompozicije slike.



Slika 29 – Prikaz 2 stupnja dekompozicije DWT-a

Umetanje digitalnog vodenog žiga

- Koristeći dvodimenzionalnu separabilnu wavelet transformaciju, naći prvi stupanj dekompozicije slike

- Modificirati wavelet koeficijente u LL pojasu:

$$LL_w = \sum_i \sum_j [LL(i,j) + \alpha * w(i,j)] \quad (7)$$

- Upotrijebiti inverznu wavelet transformaciju za dobivanje zaštićene slike

U (7) LL predstavlja niskofrekvencijski pojas slike dobiven wavelet transformacijom, w predstavlja digitalni vodeni žig, a α je factor vidljivosti digitalnog vodenog žiga.

Izvlačenje digitalnog vodenog žiga

- Koristeći dvodimenzionalnu separabilnu wavelet transformaciju, naći prvi stupanj dekompozicije zaštićene slike
- Izvući digitalni vodeni žig iz LL pojasa pomoću:

$$w_e = \sum_i \sum_j \frac{LL_1(i,j) - LL(i,j)}{\alpha} \quad (8)$$

gdje w_e predstavlja izvučeni vodeni žig, LL_1 niskofrekvencijski pojas prvog stupnja wavelet dekompozicije zaštićene slike pod utjecajem distorzije, a LL niskofrekvencijski pojas prvog stupnja wavelet dekompozicije originalne slike.

Analiza

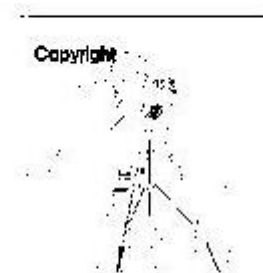
U nastavku će opet biti prikazano, kao i u prethodna dva dijela ovog poglavlja, utjecaj umetanja vodenog žiga unutar slike, te utjecaj distorzija na uspješnost njegovog izvlačenja (Slika 31. – Slika 40.).



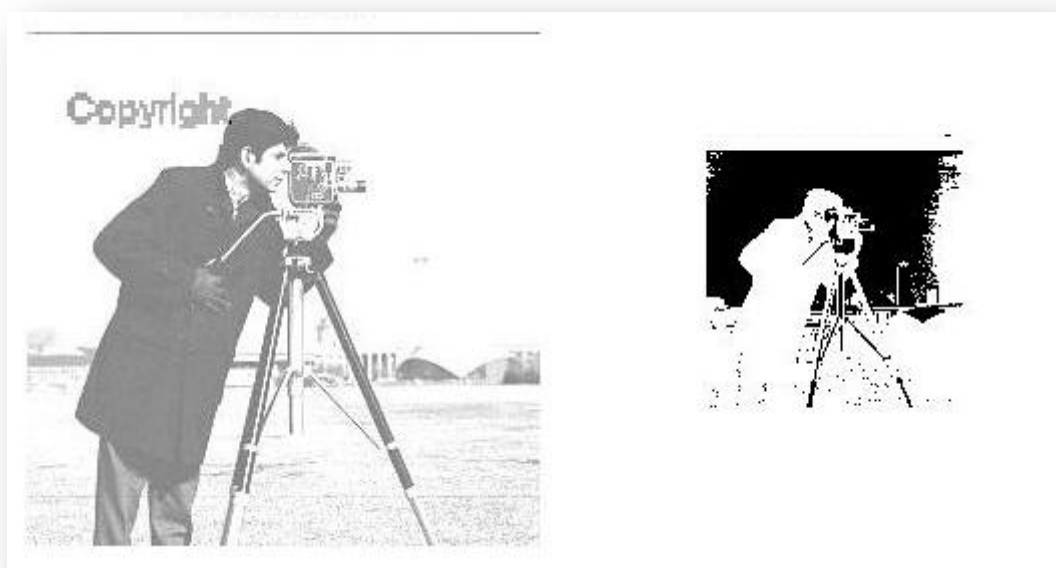
Copyright

Slika 30 - (a) Originalna slika

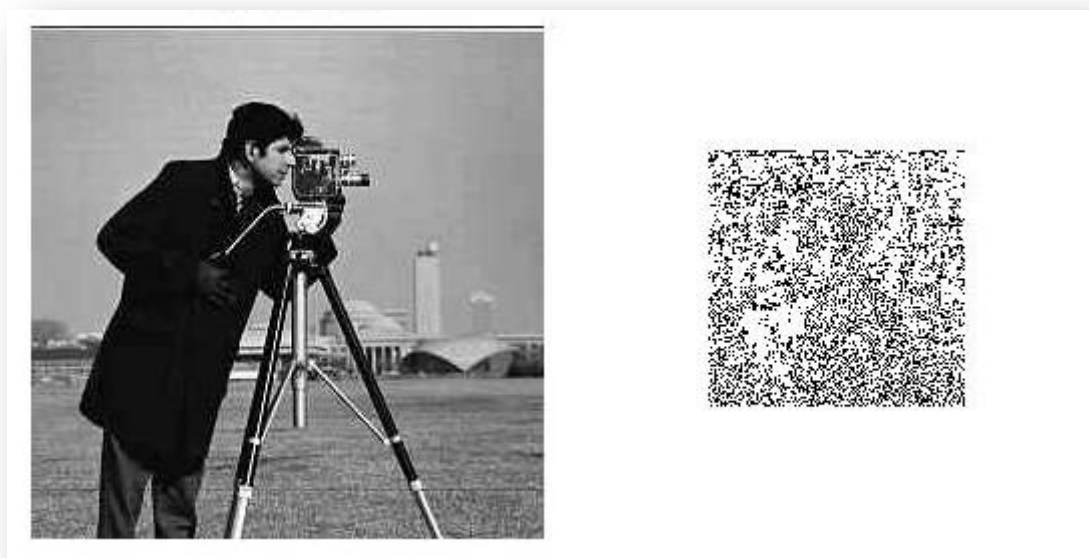
(b) Vodeni žig



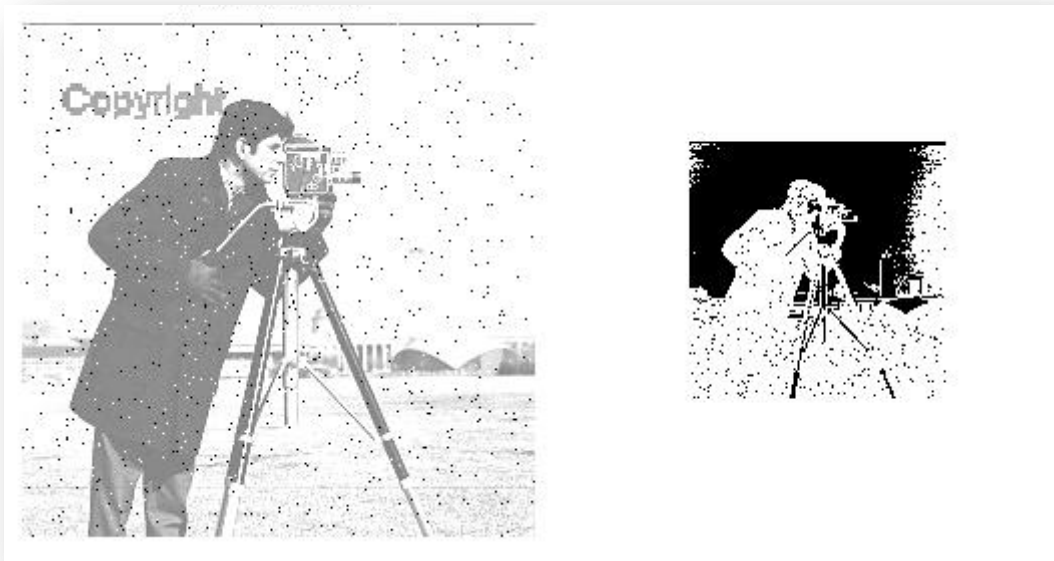
Slika 31 - JPEG kompresija uz $q = 15$, $\alpha = 0.5$



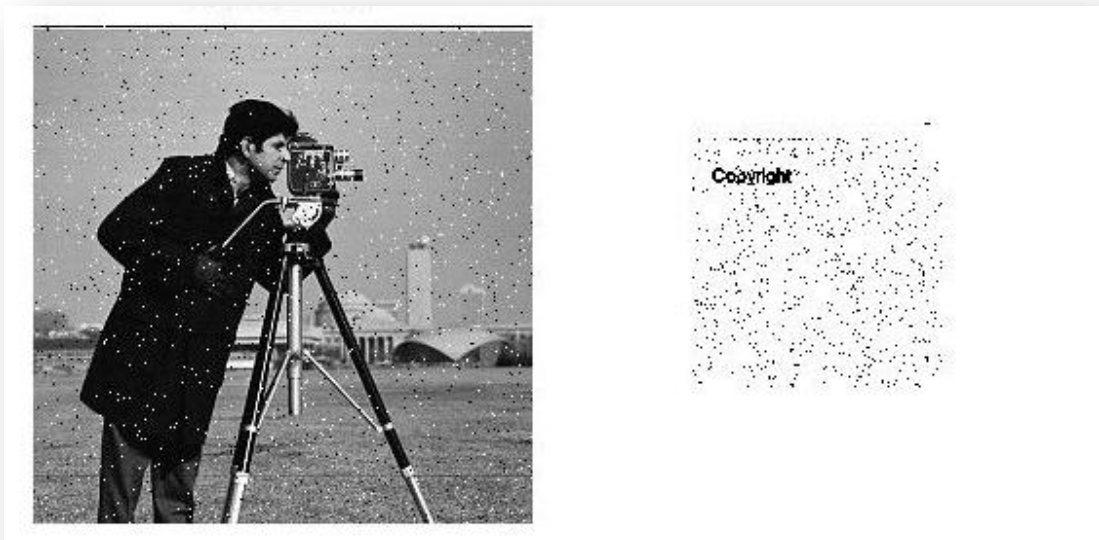
Slika 32 - JPEG kompresija uz $q = 75$, $\alpha = 1$



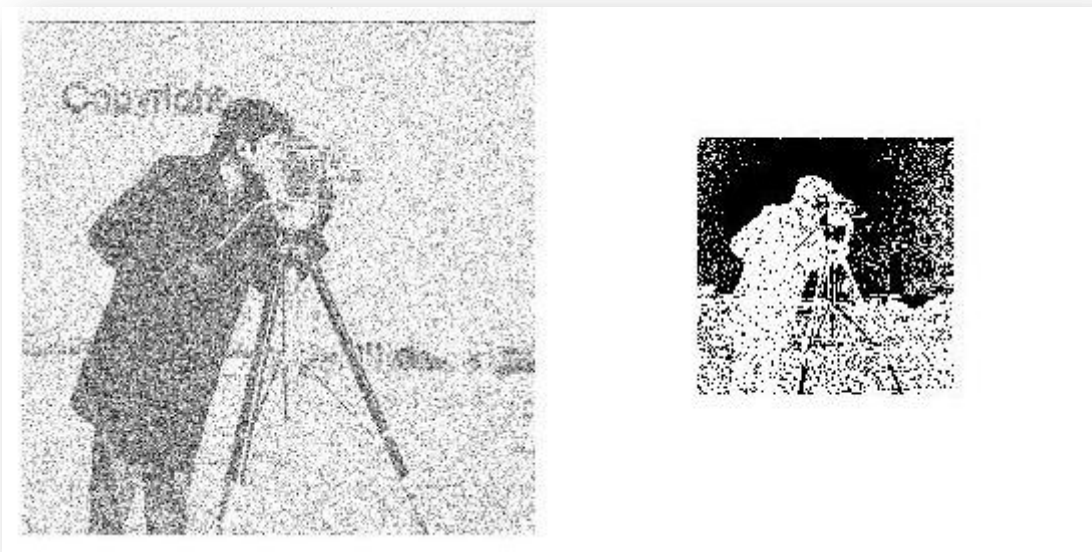
Slika 33 - JPEG kompresija uz $q = 30$, $\alpha = 0.02$



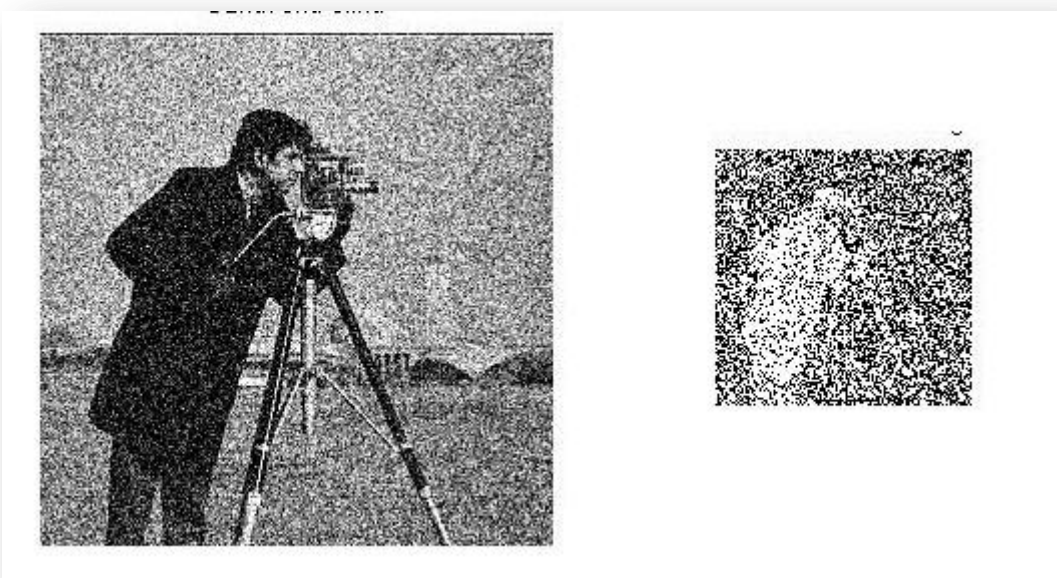
Slika 34 - Salt & pepper šum ($d = 0.02$) uz $\alpha = 1$



Slika 35 - Salt & pepper šum ($d = 0.02$) uz $\alpha = 0.02$



Slika 36 - Gaussov šum ($\mu = 0, \sigma = 0.05$) uz $\alpha = 1$



Slika 37 - Gaussov šum ($\mu = 0, \sigma = 0.05$) uz $\alpha = 0.02$



Slika 38 - Rotacija (30°) uz $\alpha = 1$



Slika 39 - Rotacija (30°) uz $\alpha = 0.02$



Slika 40 - Skaliranje (0.5) uz $\alpha = 1$

Korištenje wavelet transformacije pokazalo se vrlo efikasno kao metoda ubacivanja i izvlačenja digitalnog vodenog žiga u slikama. Većina objektivnih procjena pokazuje bolje rezultate nego što je to bilo kod DCT i DFT (Tablica 3.):

Distorzija	SNR	SF
<i>JPEG kompresija</i> ($q=15, \alpha=0.5$)	9.4492	0.9645
<i>JPEG kompresija</i> ($q=75, \alpha=1$)	6.4774	0.5944
<i>JPEG kompresija</i> ($q=30, \alpha=0.02$)	21.9109	0.8833
<i>Salt & pepper</i> ($\alpha=1$)	6.3910	0.5973
<i>Salt & pepper</i> ($\alpha=0.02$)	16.5611	0.9621
<i>Gaussov šum</i> ($\alpha=1$)	6.3502	0.9621
<i>Gaussov šum</i> ($\alpha=0.02$)	9.0284	0.8268
<i>Rotacija 30°</i> ($\alpha=1$)	4.8580	0.4930
<i>Rotacija 30°</i> ($\alpha=0.02$)	5.3014	0.4863
<i>Skaliranje</i> ($\alpha=1$)	5.1797	0.8228

Matlab kod:

```
close all; clc;

% Učitavanje originalne slike
X=imread('cameraman.jpg');
X=im2double(X);
X=rgb2gray(X);
figure;
imshow(X);
title('Originalna slika');
[F1,F2]= wfilters('db1', 'd');
[LL,LH,HL,HH] = dwt2(X,'db1','d');

% Učitavanje vodenog žiga
o=imread('watermark.bmp');
level=graythresh(o);
w=im2bw(o,level);
w=double(w);
alpha=1;

% Umetanje vodenog žiga
k=w*alpha;
LL_1=LL+k;
Y=idwt2(LL_1,LH,HL,HH,'db1','d');

% JPEG kompresija
q=input('Quality Factor q = ');
imwrite(Y,'xyz.jpg','jpg','quality',q);
Y=imread('xyz.jpg');
%Y = imnoise(Y, 'Salt & pepper', 0.02);
%Y = imnoise(Y, 'Gaussian', 0, 0.05);
%Y = imrotate(Y,30);
%X = imrotate(I,30);
%[LL,LH,HL,HH] = dwt2(X,'db1','d');
%Y = imresize(Y,0.5);
%X = imresize(I,0.5);
%[LL,LH,HL,HH] = dwt2(X,'db1','d');
Y=im2double(Y);
figure;
imshow(Y);
title ('Oznažena slika');

% Izvlačenje digitalnog vodenog žiga
[LL1,LH1,HL1,HH1] = dwt2(Y,'db1','d');
w1=(LL1-LL)./alpha;
level1=graythresh(w1);
w2=im2bw(w1,level1);
w2=im2double(w2);
figure;
imshow(w2);
title ('Detektirani vodeni žig');

% Izračun SNR
z1=double(Y);
snr_num=0;
snr_den=0;
```

```

for i=1:256
    for j=1:256
        snr_num=snr_num+(z1(i,j)*z1(i,j));
        snr_den=snr_den+((X(i,j)-z1(i,j))*(X(i,j)-z1(i,j)));
    end
end

snr=10*log10(snr_num/snr_den)

% Izračun faktora sližnosti (SF)
sf_num=0;
sf_den=0;
a=0;
b=0;
w2=imresize(w2,2);
for i=1:128
    for j=1:128
        sf_num=sf_num+(w2(i,j)*w(i,j));
        a=a+(w(i,j)*w(i,j));
        b=b+(w2(i,j)*w2(i,j));
        sf_den=sqrt(sf_den+a*b);
    end
end

sf=(sf_num/sf_den)

```

Zaključak

Od početka razmatranja korištenja tehnologije ubacivanja digitalnih vodenih žigova kao načina zaštite u digitalni sadržaj nije prošlo mnogo vremena, ali je napredak u mogućnostima i više nego vidljiv. Postoji mnogo metoda i tehnika kojima se digitalno vodeni žig može utisnuti unutar digitalnog sadržaja i dobar dio njih to solidno odrađuje. Iako je napredak velik postoji još mnogo prostora za daljnji napredak ovih tehnologija.

Što se tiče načina umetanja digitalnog vodenog žiga, metode koje to čine u frekvencijskoj domeni pokazuju bolje rezultate, veću otpornost, manje vidljive smetnje na slikama i općenito bolju zaštitu. Metode poput DFT-a, DCT-a, te DWT-a su budućnost ovakve vrste tehnologija, i njihovim daljnjim razvojem mogu se postići mnogo zapaženiji rezultati. Iako je ovim radim tek zagrebena površina ove problematike, može se vidjeti kako se ova vrsta tehnologija može koristiti u svojim brojnim primjenama.

Literatura

- [1] <http://www.scribd.com/doc/37021026/Project-Report-on-Digital-Watermarking>
- [2] <http://homepages.vub.ac.be/~andooms/research.html>
- [3] <http://www.alpvision.com/watermarking.html>
- [4] Edin Muharemagic and Borko Furht, "Survey Of Watermarking Techniques And Applications", Department of Computer Science and Engineering, Florida Atlantic University
- [5] Andreja Samčović, Jan Turan, "ATTACKS ON DIGITAL WAVELET IMAGE WATERMARKS", Journal of ELECTRICAL ENGINEERING.
- [6] Peining Taoa and Ahmet M. Eskicioglu, "A robust multiple watermarking scheme in the Discrete Wavelet Transform domain ", The Graduate Center, The City University of New York.
- [7] M. S. Sutaone , M.V. Khandare "Image Based Steganography Using LSB Insertion Technique", *IEEE WMMN* pp. 146-151, January 2008
- [8] Manpreet Kaur, Sonika Jindal & Sunny Behal " A Study of Digital Image Watermarking" Volume 2, Issue 2(ISSN: 2249-3905) ,February 2012
- [9] Dr. Vipula Singh "Digital Watermarking: A Tutorial", (JSAT), January Edition, 2011
- [10] Charles Way Hun Fung, Antonio Gortan & Walter Godoy Junior "A Review Study on Image Digital Watermarking" 2011.
- [11] Anuradha , Rudresh Pratap Singh "DWT Based Watermarking Algorithm using Haar Wavelet" ISSN 2277-1956/V1N1-01-06

Primjena digitalnog vodenog žiga u zaštiti vlasništva slika u digitalnom zapisu

Sažetak:

U prvim poglavljima ovog rada dan je kratki pregled digitalnog vodenog žiga, pokrivajući njegova svojstva, nedostatke, moguće primjene, zlouporabe, te napada i načina obrane od njih.

U sljedećim je poglavljima dana klasifikacija tehnika implementacije digitalnog vodenog žiga, te njihovi nešto detaljniji opisi, dok su tri tehnike koje koriste frekvencijsku domenu (DFT, DCT, DWT) još detaljnije obrađene.

Te tri tehnike su i testirane unutar programskog okruženja Matlab, pokazujući njihove dobre i loše strane, te mogućnosti daljnjih popravaka i ispravaka.

Ključne riječi: digitalni vodeni žig, DFT, DCT, DWT, dekompozicija, Matlab, slike u digitalnom zapisu, autorska prava

The use of digital watermarking in copyright protection of digital images

Abstract:

Within the first few chapters a brief general overview of digital watermarking was given, covering its performance, drawbacks, possible applications and attacks, as well as the defence methods against those attacks.

In the next chapters we gave the implementation technique classification of watermarking methods, along with a bit more detailed overview, while the three frequency domain techniques (namely DFT, DCT, DWT) were given a bit more detailed descriptions.

The three aforementioned techniques were tested and analyzed within Matlab, showing their qualities and shortcomings, with the addition of possible further corrections.

Keywords: digital watermark, DFT, DCT, DWT, decomposition, Matlab, digital images, copyright

Privitak

[1] CD sa .zip datotekom koja sadrži:

- .pdf datoteku s diplomskim radom
- Matlab kodove
- korištene slike