SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

DIPLOMSKI RAD BR. 789

Steganografija i vodeni žig u zaštiti digitalnih fotografija

Sandra Šumiga

Zagreb, lipanj 2014.

Sadržaj

Uvod 2
1. Steganografija 3
2. Primjena steganografije u digitalnoj fotografiji 5
2.1. Digitalni potpis 6
2.2. Zaštićene oznake 8
2.3. Digitalni vodeni žig 11
3. Metode steganografije 15
3.1. Metoda injektiranjem 16
3.2. LSB (Least Significant Bit) metoda 17
3.3. Modifikacija bazirana na korelaciji 19
3.4. CDMA metoda 20
3.5. Sakrivanje u DCT domeni 21
4. Distorzije i napadi na vodeni žig 23
5. Implementacija i analiza u Matlabu 25
5.1. Injektiranje tajne poruke u originalnu sliku 26
5.2. LSB metoda 29
5.3. Modifikacija bazirana na korelaciji 37
5.4. CDMA metoda 43
5.5. Sakrivanje u DCT domeni 50
Zaključak 56
Literatura 57
Sažetak 58
Abstract 59
Privitak 60

Uvod

Sve većim napretkom tehnologije u području komunikacija i IT sektora, dolazi do jačanja veze između informatičkih područja i komunikacija, što nudi značajne nove mogućnosti obrade i distribucije raznog digitalnog sadržaja poput e-mailova, audio zapisa, slika i videa. Istovremeno, ukoliko netko želi pristupiti podacima koji nisu njemu namijenjeni, nove metode i tehnologije daju mu sve jednostavniji pristup i omogućuju nelegalno kopiranje sadržaja i korištenje piratskog materijala preko interneta. U svrhu zaštite autorskog sadržaja koriste se različite tehnike kriptiranja i načelo autorskog prava kako bi samo autorizirani korisnici mogu pristupiti podacima. Digitalni vodeni žig općeniti je i najrašireniji naziv koji obuhvaća bilo kakvu vrstu zaštite ili sakrivanja informacija. Konkretnije, znanost prijenosa tajnih informacija pod krinkom drugih, koja se koristi od najranijeg doba, naziva se steganografija. Najčešće primjene digitalnog vodenog žiga su praćenje emitiranja, identifikacija vlasnika, kršenje autorskih prava, online i offline financijske transakcije, kontrola kopiranja zaštićenog sadržaja i sl.

Pojavom digitalnog doba pa sve do današnjeg dana, metode steganografije razvijaju se na različite načine i u različitim domenama. Od onih najjednostavnijh do najsloženijih, svaka metoda ima svoje pozitivne i negativne strane te područje primjene. U ovom radu biti će opisane i implementirane dvije jednostavnije i tri složenenije tehnike što se tiče algoritama i vremena izvođenja. Rezultati svih testiranja prikazani su slikama i numeričkim mjerenjima. Korišteno programsko okruženje je Matlab 2013b.

1. Steganografija

Steganografija je znanost sakrivanja i prijenosa informacija sa ciljem da se tajna poruka prikrije tako da je u potpunosti nevidljiva trećoj strani ili tijekom transfera do primatelja. Riječ steganografija dolazi iz grčkih riječi *steganos* (pokriveno, skriveno, zaštićeno) i *graphein* (pisati) tako da je njezino doslovno značenje „sakriveno pisanje informacija“. [1] Jednako kao i kriptografija, steganografija se koristi kako bi se očuvala tajnost podataka. Glavna razlika između njih je što se nakon enkripcije jasno vidi kako dvije strane pokušavaju komunicirati u tajnosti dok steganografija sakriva postojanje tajne poruke te u najboljem slučaju tajna komunikacija između pošiljatelja i primatelja uopće nije vidljiva. Dakle, cilj kriptografije je izmijeniti poruku do te mjere da je ona skroz nerazumljiva, a cilj steganografije sakriti poruku da je u potpunosti sakrivena trećoj strani. [2]

Jednostavne tehnike steganografije koriste se već stotinama godina, no povećano korištenje datoteka u elektroničkom obliku omogućilo je razvoj novih metoda sakrivanja informacija. U digitalnom svijetu i kriptografija i steganografija odlično su sredstvo za zaštitu podataka od neželjenih strana ali nijedna tehnika sama nije savršena i može biti „probijena“ te zbog toga većina stručnjaka sugerira korištenje obje vrste zaštite kao višeslojnu sigurnost. [3]

Povijest steganografije

Najraniji zapisi korištenja steganografije nalaze se u kronikama grčkog povjesničara Herodota pod imenom „Povijesti“, a datiraju oko 440. godine prije Krista. Herodot je zabilježio dvije priče u kojima se koriste steganografske tehnike u tom vremenu. U prvoj priči navodi kako je kralj Darius obrijao glavu jednom od svojih robova i tetovirao mu tajnu poruku na skalp. Kada je robu kosa natrag narasla i prekrila kraljevu poruku, Darius ga je poslao svom zetu Aristagoru u Milet sa sakrivenom porukom. U drugoj Herodotovoj priči vojnik

imena Demarat je trebao poslati poruku u Spartu da Kserkso namjerava napasti Grčku. U to vrijeme podloga za pisanje bile su voskom prekrivene drvene pločice, no Demarat je uklonio vosak sa pločice, upisao skrivenu poruku u drvo te ju natrag prekrio sa voskom kako bi izgledala kao prazna pločica. Konačno, tajna poruka je bila sigurno prenesena.

Rimljani su za sakrivanje informacija koristili nevidljive tinte, koje su se bazirale na prirodnim supstancama poput voćnih sokova ili mlijeka. Čitanje poruke se postiže zagrijavanjem skrivenog teksta i tada se prikazuje njegov sadržaj. Nevidljive tinte se naprednijim metodama i u ograničenoj uporabi koriste i danas. [3]

Tijekom Prvog svjetskog rata i Drugog svjetskog rata dogodio se značajan napredak u staganografskim tehnikama. Razvijene su metode „null šifre“ (čitanje trećeg slova u svakoj riječi u naizgled bezazlenoj poslanoj poruci), sakrivanje Morseove abecede u slova i, j, t i f, zamjena slika, tajne poruke ispod markice na poslanim pismima, metoda „točkice“ itd. Nijemci su u Drugom svjetskom ratu sakrivali podatke tako da su tajnu poruku fotografirali i smanjili ju u tolikoj mjeri da bi unutar nekog poslanog dokumenta izgledala kao točka (interpunkcijski znak, „ . “). [2]

Prelaskom u digitalno doba, odnosno od 1985. godine do danas, steganografija se koristi diljem cijelog svijeta u računalnim sustavima, koristeći metode daleko naprednije i razvijenije od upravo opisanih. U nastavku rada slijede opisi najpoznatijih i najraširenijih tehnika steganografije te njihova praktična primjena.

2. Primjena steganografije u digitalnoj fotografiji

Moderna steganografija pojavila se u svijetu 1985. godine kada se počinju primjenjivati osobna računala za rješavanje klasičnih steganografskih problema. Digitalna steganografija prikriva informacije unutar računalnih datoteka. Elektroničke komunikacije mogu sadržavati steganografsko kodiranje unutar transportnog sloja kao što su dokumenti, slikovne datoteke, program ili protokol. Multimedijske datoteke su idealne za steganografski prijenos zbog svoje veličine.

Tehnike digitalne steganografije uključuju:

- Sakrivanje poruke unutar slikovne ili zvučne datoteke
- Sakrivanje poruke unutar šifriranih podataka ili u okviru slučajnih podataka. Tajna poruka se prvo posebno kriptira i zatim ubacuje u puno veći blok šifriranih ili slučajnih podataka za prijenos
- Sakrivanje poruke u izmjenjene izvršne datoteke
- Slike sakrivene u video materijal (detekcija moguća uz bržu ili sporiju reprodukciju videa)
- Unošenje neprimjetnog kašnjenja paketa poslanih preko mreže. Kašnjenje paketa u aplikaciji može se koristiti za kodiranje podataka
- Neprimjetnu promjenu redoslijeda unaprijed definiranih stavki u nekom dokumentu [4]

Svakodnevnim porastom korisnika elektroničkih sustava pa tako i njihove komunikacije i razmjene informacija, motivacija za korištenje steganografije u svrhu zaštite privatnosti i autorskih prava nameće se sama od sebe. U nastavku teksta slijedi opis najčešćih područja primjene digitalnih steganografskih tehnika.

2.1. Digitalni potpis

Jedan od osnovnih načina zaštite vjerodostojnosti informacije je potpis. Potpis treba biti jedinstven i služi prilikom identifikacije i provjere pojedinca. Kod elektroničke informacije, koncept potpisa se mijenja – potpis više ne smije biti nezavisan o informaciji koja se potpisuje. Naime, elektronička kopija potpisa jednaka je originalu i označavanje neovlaštenih dokumenata time postaje trivijalno. Nezaštićene elektroničke poruke moguće je relativno jednostavno presresti, neovlašteno čitati, mijenjati i proslijeđivati. Za digitalno nepotpisani e-mail nemoguće je dokazati izvornost a niti integritet, jer se svatko može krivo predstaviti. Iz tog razloga dokumenti se zaštićuju digitalnim potpisom koji uspostavlja identitet pošiljatelja i osigurava integritet podataka. Drugim riječima, digitalni potpis služi za utvrđivanje autentičnosti informacije i za identifikaciju pošiljatelja, ali ne osigurava tajnost informacije.

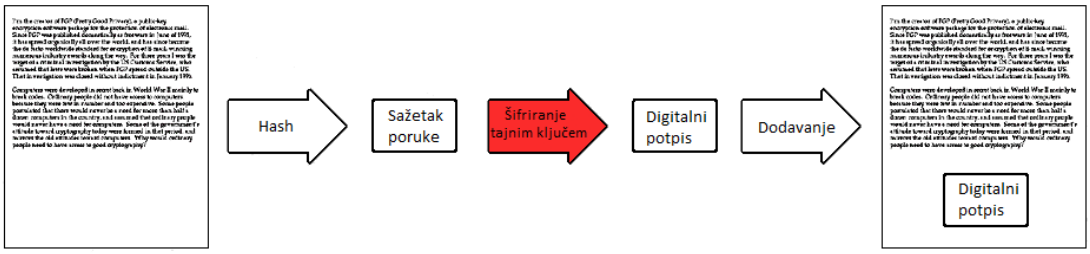
Digitalni potpisi koriste asimetričnu kriptografiju i sastoje se uglavnom od tri algoritma: generiranje privatnog i odgovarajućeg javnog ključa, kreiranje potpisa koristeći sadržaj poruke i privatni ključ, te provjera autentičnosti pošiljatelja pomoću poruke, pripadajućeg javnog ključa i potpisa. [5]

Kriptiranje privatnim ključem znači da svako računalo ima ključ (kod) za šifriranje koji koristi za kriptiranje paketa podataka prije nego pošalje poruku preko mreže drugom računalu. Za uspješnu komunikaciju nužno je da oba računala (i pošiljatelj i primatelj) znaju tajni ključ ili način kodiranja.

Kriptiranje javnim ključem koristi kombinaciju privatnog i javnog ključa. Privatni ključ je poznat samo računalu pošiljatelja a javni ključ računalo šalje bilo kojem računalu sa kojim želi sigurno komunicirati. Da bi primatelj dekodirao primljenu poruku mora koristiti dobiveni javni ključ pošiljatelja i svoj vlastiti privatni ključ. Javni ključ se temelji na hash[1] vrijednosti tajne poruke i gotovo je nemoguće izvesti izvornu ulaznu vrijednost bez poznavanja sadržaja poruke.

[1] Vrijednost dobivena sažimanjem sadržaja

Osnovu digitalnog potpisa čini sadržaj same poruke. Pošiljatelj najprije primjenom kriptografskih algoritama iz svoje poruke proizvoljne duljine izračunava sažetak (*message digest*) fiksne duljine koristeći hash funkciju. Dobiveni zapis dalje se šifrira privatnim ključem pošiljatelja i tako nastane digitalni potpis koji se dodaje izvornoj poruci. Postupak dobivanja i dodavanja digitalnog potpisa prikazan je na slici 2.1. Kada primatelj dobije poruku sa digitalnim potpisom, pomoću javnog ključa pošiljatelja dešifrira potpis u skraćeni zapis poruke. Taj zapis uspoređuje sa zapisom koji osobno izračuna iz primljene poruke koristeći isti matematički algoritam kao i pošiljatelj (slika 2.2). Time primatelj može utvrditi autentičnost (identitet pošiljatelja utvrđuje se dešifriranjem sažetka poruke), integritet (provjerom sažetka poruke utvrđuje se je li se poruka mijenjala na putu do primatelja) i neporecivost (pošiljatelj ne može poreći sudjelovanje u transakciji jer jedino on ima pristup do svojeg ptivatnog ključa kojim je potpisao poruku).



Slika 2.1 Kreiranje digitalnog potpisa

Slika 2.2 Čitanje poruke sa digitalnim potpisom

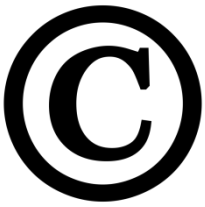
Prvi praktični digitalni potpis bio je na bazi RSA algoritma. Godine 1991. usvojen je i prvi standard digitalnog potpisa i bazirao se na RSA simetričnom algoritmu. 2000. godine, NIST (National Institute of Standards and Technology) objavio je da se u okviru DSS (Digital Signature Standard) standarda mogu koristiti tri algoritma: DSA (Digital Signature Algorithm, baziran na ElGamalovom kriptosistemu), RSA digitalni potpis i ECDSA (Elliptic Curve Digital Signature Algorithm) – digitalni potpis koji kao osnovu koristi eliptičke krivulje. [6]

2.2. Zaštićene oznake

Zaštićene oznake (*copyright labels*) služe za zaštitu autorskih prava te kopiranja kreatorovog oblika izražavanja. Autorsko pravo je pravni pojam, donesen od strane većine vlada, koji daje kreatoru izvornog djela ekskluzivna prava na korištenje i distribuciju, obično na ograničeno vrijeme, sa namjerom omogućavanja tvorcu intelektualnog vlasništva (npr. autoru fotografije ili knjige) primanja naknade za svoj rad. Oznaka autorskog prava nalazi se na originalnom primjerku i važna je jer informira javnost o zaštiti djela, identificira vlasnika autorskih prava i prikazuje godinu prve objave. Vlasnik autorskih prava ima isključivo pravo činiti i dopuštati drugima sljedeće: reproducirati rad u kopijama ili zvučnim snimkama, izrađivati izvedena djela po uzoru na original, distribuirati kopije ili zvučne snimke originala u javnosti u svrhu prodaje, iznajmljivanja, pozajmljivanja ili licenciranja, javno izvoditi original digitalne audio snimke te javno prikazivati originalno djelo. Uporaba zaštićene oznake odgovornost je vlasnika autorskih prava i ne zahtijeva prethodnu dozvolu ili registraciju Ureda za autorska prava.

Pravilan oblik zaštićenih oznaka mora sadržavati tri elementa: Copyright simbol © (slovo C u krugu), ili riječ „Copyright“ ili kraticu „Copr.“, godinu prve objave djela i ime vlasnika autorskih prava ili kraticu kojom ime može biti prepoznato ili opće poznatu alternativnu oznaku vlasnika. [7]

Kako bi zaštićena oznaka bila učinkovita i poslužila svrsi u svijetu multimedija, ne smije biti lako uklonjiva i mora biti otporna na različite obrade podataka. To obuhvaća širok raspon mogućnosti uključujući konverzije formata, kompresije podataka i filtriranje. Uz obilježavanje autorskih prava na slikama za emitiranje, područja primjene steganografije uključuju i označavanje podataka sigurnosnim zapisima u elektroničkom izdavaštvu, znanstvenoj obradi slike i medicinskim slikama.



Slika 2.3 Zaštićena oznaka autorskog prava

Za pretpostaviti je da glavna svrha elektroničkog napada na autorsku datoteku je ukloniti zaštićenu oznaku i/ili dokazati da nije verificirajuća. U osnovi postoje dva načina kako bi se oznaka učinila nevažećom. Prvi je promjena podataka u slici kako oznaka ne bi bila uopće čitljiva, dok je drugi način dokazati kako pročitana oznaka nije pouzdano sredstvo identifikacije. Dodatno, na integritet zaštićene oznake i autorskog djela mogu utjecati osnovna svojstva digitalnih multimedijskih podataka kao što su kreiranje identičnog koda za zaštićenu oznaku, niskopropusno filtriranje, transformiranje u drugi format ili drugi prostor boja, komprimiranje bez vidljivih degradacija u odnosnu na izvornu datoteku. Rješenja za ove navedene napade su: tajni ključ za kriptiranje kreiran koristeći jedinstvenu identifikaciju rada koji se onda koristi za umetanje zaštićene oznake; zaštićena oznaka koja se kamuflira vizualno i statistički u podatke koji se prenose kako ne bi bila vidljiva i doimala se kao dio datoteke; signali korišteni za umetanje zaštićene oznake moraju sadržavati rubni šum kako bi se oduprli šteti ako je datoteka obrađivana ili komprimirana te se lokacije sakrivanja oznaka i korišteni kodovi ne smiju ponavljati zbog moguće usporedbe datoteka istog pošiljatelja. [8]

Obilježavanje dokumenata zaštićenom oznakom provodi se tehnikom digitalnog vodenog žiga (*watermarking*). Vodeni žig u svrhu zaštite može biti vidljiv i nevidljiv, a često se u praksi koriste oba načina zaštite istovremeno kako bi se naglasilo vlasništvo originalnog dokumenta i sačuvala autorska oznaka u slučaju nelegalne distribucije ili izmjene sadržaja dokumenta. Pomoću sakrivenog vodenog žiga autor originalnog djela može pratiti daljnje korištenje tog sadržaja te otkriti neautorizirano korištenje i umnažanje istog. Slika 2.4 prikazuje fotografiju označenu zaštićenom oznakom dodanom kao digitalni vodeni žig.

Slika 2.4 Zaštićena oznaka na fotografiji

Glavna razlika između zaštićene oznake i digitalnog vodenog žiga je namjena zaštićene oznake da informira javnost o autorskom pravu na određeni dokument i otkad to pravo vrijedi, dok je vodeni žig sredstvo kojime se zaštićena oznaka prikazuje (ili sakriva, ovisno o namjeni).

2.3. Digitalni vodeni žig

Klasični vodeni žig oznaka je utisnuta na papiru dizajnirana tako da se vidi samo pod određenim kutom gledanja. Koristi se u štampanju novčanica, putovnicama, kao i u štampanju poštanskih marki kako bi se tiskovine zaštitile od mogućeg krivotvorenja. Prvi vodeni žigovi pojavili su se već davne 1292. u Italiji kako bi označili podrijetlo papira, tj. označili iz koje tvornice je stigao.

U digitalnom svijetu, vodeni žig ima jednaku svrhu i zadaću, samo elektronički implementiranu i primjenjenu na digitalne dokumente. Digitalni vodeni žig mogu sadržavati svi multimedijalni sadržaji - slike, glazba i video, no najčešća im je primjena u zaštiti sadržaja fotografije pa će u daljenjem tekstu biti naglasak na vodeni žig u domeni slike.

Digitalni vodeni žig informacija je koja se određenim metodama sakriva u originalni signal (multimedijalni zapis). Dodana informacija mora biti „sakrivena“, tj. signal dodavanjem vodenog žiga ne smije biti značajnije promjenjen. Također, vodeni žig mora biti otporan na razne modifikacije i kompresije signala kroz koje prolazi tijekom prijenosa na stranu primatelja te se mora moći detektirati (sve dok te modifikacije u potpunosti ne izmijene signal).

Osnovni zahtjevi digitalnog vodenog žiga su dakle transparentnost (sadržaj označen vodenim žigom mora biti upotrebljiv primatelju bez primjetnih smetnji, a vodeni žig se pojavljuje samo nakon ciljane detekcije), robusnost na bilokakve operacije obrade signala i sigurnost (samo vlasnik autorskog prava i osobe sa njegovom dozvolom smiju mijenjati sadržaj označen vodenim žigom). [9]

Ovisno o primjeni i potrebnoj razini sigurnosti zaštite podataka digitalni vodeni žigovi mogu se podijeliti prema vidljivosti, prema otpornosti, prema domeni primjene. U nastavku poglavlja slijedi detaljnije objašnjenje za pojedinu vrstu digitalnog žiga.

Vrste vodenih žigova

- Vidljivi i nevidljivi

Vidljivi vodeni žigovi danas imaju puno manju primjenu od nevidljivih, a najčešće se koriste na dokumentima u obliku loga. Vodeni žig se jednostavnom metodom zbrajanja dodaje na originalnu sliku dok je reverzibilan postupak moguć uz poznavanje točnog formata žiga ili uz trud i vještinu pomoću nekog programa za složeniju obradu slike. Nedostaci vidljivih žigova su degradacija kvalitete slike i detekcija samo vizualnim putem (pošto žig postaje dio slike algoritmi ne prepoznaju anomalije u digitalnom zapisu datoteke). [2] Na slici 2.5 prikazan je vidljivi vodeni žig na fotografiji.

Nevidljivi vodeni žigovi sakriveni su unutar sadržaja slike, nevidljivi ljudskom oku i moguće ih je detektirati programima sa tom namjenom. Koriste se za dodatnu zaštitu i autentifikaciju autorskih prava, detektiranje neovlaštenog kopiranja i distibuiranja te nelegalnih dokumenata.

Slika 2.5 Primjer vidljivog digitalnog vodenog žiga

- Otporni (robusni) i lomljivi

Robusni vodeni žigovi sakriveni su u sliku i otporni su na različite obrade slike i napade (najčešći primjer je JPEG kompresija). Iako niti jedan vodeni žig nije u potpunosti otporan, sustav se može smatrati robusnim ukoliko je za uklanjanje žiga potrebno unositi tolike promjene tako da originalna datoteka postane neupotrebljiva. Koriste se za zaštitu autorskih prava, detektiranje nelegalnih dokumenata i potvrdu vlasništva.

Lomljivi vodeni žigovi koriste se u svrhu detektiranja promjena u digitalnim podacima zbog svojeg svojstva velike osjetljivosti na obradu izvornog sadržaja i nisu otporni na JPEG kompresiju. Lomljivi žigovi mogu se usporediti sa pečatom u vosku na pismima koji su korišteni u prošlosti. Na slici 2.6 vidljivo je kako ukoliko lomljivi žig stigne do primatelja netaknut, garantirano nije bilo nikakvih promjena na originalnom dokumentu.

Slika 2.6 Pečat od voska kao primjer lomljivog žiga

- Prostorna i frekvencijska domena

Tehnike vodenog žiga u prostornoj domeni uglavnom dijele sljedeće karakteristike: vodeni žig se primjenjuje u domeni piksela slike, tijekom dodavanja vodenog žiga ne primjenjuju se nikakve transformacije na originalnu datoteku, kombinacija žiga sa originalnim signalom se bazira na jednostavnim operacijama sa pikselima te se vodeni žig se može detektirati korelacijom očekivanog uzorka sa primljenom porukom. [10] Najčešće korišten algoritam u prostornoj domeni je LSB (*Least Significant Bit*, umetanje digitalnog žiga na pozicije najnižih bitova u slici kako se ne bi narušila kvaliteta prikaza). Metoda LSB-a relativno efikasno sakriva vodeni žig u originalnoj slici no poprilično je neotporna na najčešće vrste manipulacija i degradacija slike.

Frekvencijska domena umetanja žiga ima prednosti pred prostornom jer je robusnija, tj. otpornija na napade. Promjenom jednog parametra u frekvencijskoj domeni, promjena se očituje tako da se cijelom dokumentu promijeni sadržaj. Kod prostorne domene promjena se dogodi u samo jednom segmentu i ako se taj segment izdvoji, kod prostorne domene žig u potpunosti nestaje dok je kod frekvencijske žig i dalje postojan i može se detektirati iz ostatka dokumenta. Zbog svojstva kompresije koja najčešće zanemaruje visoke frekvencije tokom prijenosa, vodeni žig se postavlja u značajnije frekvencije originalnog dokumenta. Postupak nalaže prvo transformaciju originalne slike u frekvencijsku domenu i zatim dodavanje vodenog žiga odabranom metodom. Sljedeće poglavlje bavit će se najčešće korištenim tehnikama steganografije i umetanja vodenog žiga u prostornoj i u frekvencijskoj domeni.

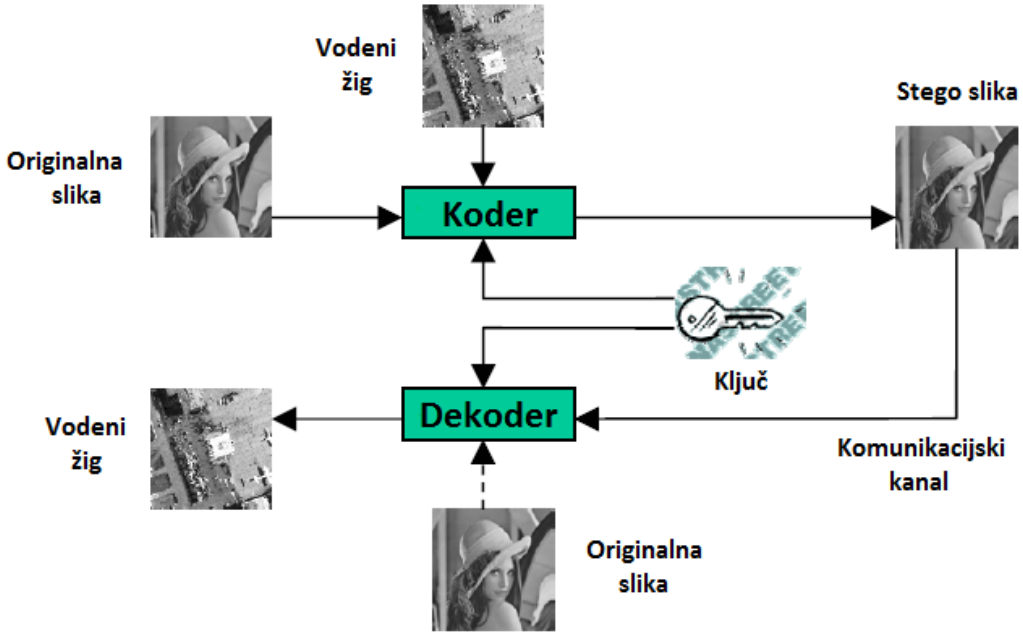
3. Metode steganografije

Iako se metode steganografije prilično razlikuju, po načinu kriptiranja ili u domeni primjene, svaka od njih mora zadovoljavati temeljne zahtjeve kako bi se mogla smatrati važećom:

- Integritet sakrivene poruke mora biti očuvan nakon dodavanja originalnoj slici. Tajna poruka se ne smije promijeniti ni na koji način, poput nadopunjavanja, mijenjanja ili gubljenja informacija.
- Stego slika (naziv za originalnu sliku sa dodanom tajnom porukom) mora ostati jednaka ili gotovo jednaka originalnoj slici. Promjene ne smiju biti vidljive golom oku kako neželjene strane ne bi primjetile razmjenu tajnih podataka.
- Bilo kakva promjena ili manipulacija podataka u stego slici ne smije utjecati na sakriveni žig. Sakriveni vodeni žig mora biti otporan na izrezivanje, rotiranje ili komprimiranje stego slike.

Na slici 3.1 prikazana je pojednostavljena shema steganografskog procesa. U ovom primjeru tajna poruka, tj. vodeni žig koji se sakriva u originalnu sliku je također slika. U prvom koraku originalna slika i tajni vodeni žig ulaze u koder. U koderu mogu biti implementirani različiti algoritmi i metode sakrivanja vodenog žiga u originalnu poruku. Vrlo često koder koristi kao dodatnu zaštitu i tajni ključ za kriptiranje žiga, sa odgovarajućim javnim ključem kojim tada primatelj slike dekodira sakrivenu poruku. Na izlazu iz kodera nalazi se stego slika, originalna slika sa dodanim i sakrivenim vodenim žigom, koja se zatim šalje pomoću nekog komunikacijskog kanala, npr. e-mailom. Primatelj mora stego sliku dekodirati kako bi pročitao sakrivenu poruku. Proces dekodiranja reverzibilan je procesu kodiranja – radi se ekstrakcija tajne poruke. Ukoliko je za kodiranje korišten javni ili tajni ključ dekodira se pomoću njega, a u nekim metodama je potrebno poznavanje i same originalne slike, bez ubačenog

digitalnog žiga. Nakon dekodiranja, vodeni žig se može izdvojiti iz stego slike i biti prikazan u odgovarajućem formatu. [2]



Slika 3.1 Pojednostavljena shema steganografskog procesa

3.1. Metoda injektiranjem

Metode bazirane na injektiranju tajne poruke sakrivaju podatke u područja datoteke koja se ne mijenjaju u procesima obrade ili kompresije bitova koji određuju sadržaj datoteke bitan krajnjem korisniku. Jedan od primjera algoritma injektiranjem je upisivanje sakrivene poruke u bloku za komentare HTML dokumenta. Gotovo svaki tip podataka ili program sadrži EOF (*end of file*) marker kako bi se obilježio kraj datoteke. Podaci upisani u datoteku iza EOF markera efektivno za sadržaj te datoteke nemaju značenje, no iz pogleda steganografije oznaka kraja korisne informacije može označavati početak sakrivenog sadržaja. [10]

Koristeći tehniku injektiranja na mjesto zaglavlja ili drugih „neiskorištenih“ područja koja se zanemaruju od strane preglednika slika, izbjegava se

degradacija na samoj slici, no ukupna veličina datoteke povećat će se sukladno veličini dodane poruke. U svrhu otkrivanja potencijalne stego slike, datoteka veličine veće nego očekivane može biti indikator da u njoj postoji skrivena poruka, a korisno je i provesti analizu toka podataka i provjeriti CRC (*cyclic redundancy check*) koji se mora poklapati sa CRC vrijednosti originalne slike.

3.2. LSB (Least Significant Bit) metoda

Najraširenija i jedna od jednostavnijih metoda sakrivanja informacije u slike je tzv. LSB metoda, modifikacija sa bitom najmanjeg značaja. Svaki piksel u slici sivih tonova može imati vrijednost od 0 (crna boja) do 255 (bijela boja) i predstavljen je nizom od 8 bitova. Sakrivanje vodenog žiga provodi se zamjenom najnižih bitova originalne slike sa bitovima tajne poruke. Ako bi se recimo promijenila zadnja 2 bita u pikselu vrijednosti 157, što je binarno 10011**01**, nova vrijednost piksela bila bi 10011**11**, tj. 159, a takva promjena ljudskom oku ne bi bila vidljiva. Ako se zbog vrijednosti piksela u vodenom žigu bitovi originalne slike značajnije promjene moguća je određena vidljiva distorzija, koja se može pripisati smanjenju kvalitete u prijenosu (šum, kompresija itd.) ali može biti i znak trećoj strani da su na slici obavljane određene modifikacije. Metoda ne koristi tajni ključ kod sakrivanja ali potrebno je obavijestiti primatelja stego slike koliki broj LSB-ova je korišten za kodiranje tajne poruke. Ukoliko je vodeni žig manji od originalne slike, preporučljivo je umetnuti ga u sliku više puta kako bi bio otporniji na kompresiju ili izrezivanje stego slike. [11, 12]

Postupak sakrivanja vodenog žiga LSB metodom započinje učitavanjem originalne slike i žiga u odabrani program za steganografiju i stegoanalizu. Zatim je potrebno odlučiti o količini najnižih bitova originalne slike koji će biti zamijenjeni najvišim bitovima tajne poruke. Broj bitova korišten za sakrivanje vodenog žiga obrnuto je proporcionalan kvaliteti izlazne stego slike, što bi značilo – bolje sakrivena tajna poruka, veća distorzija originalne slike. Odabrani

broj bitova u svakom pikselu originalne slike mijenja se sa jednakim brojem najznačajnijih bitova vrijednosti piksela u vodenom žigu. Nakon modifikacije svih bitova najmanjeg značaja u originalnoj slici (kao što je ranije spomenuto, zbog redundancije se žig dodaje koliko god je puta moguće), datoteka se sprema u željenom formatu i spremna je za prijenos.

Na strani primatelja provodi se stego analiza i postupak ekstraktiranja vodenog žiga jednostavnim postupkom suprotnim od sakrivanja žiga. Za uspješnu detekciju sakrivene poruke potrebno je znati koliki broj bitova originalne poruke (N) je korišteno za kodiranje. Iz vrijednosti svakog piksela stego slike, koji su također predstavljeni sa 8 bitova, redom se čitaju zadnjih N bitova te se pomoću njih rekonstruira sakriveni vodeni žig. [2]

Primjer LSB metode na jednom pikselu:

1. Originalni piksel – 10000111 (135)
2. Piksel vodenog žiga – **0100**1010 (74)
3. Stego piksel – 1000**0100** (132)
4. Korišteno bitova, N = 4
5. Rekonstruirani piksel – **0100**0000 (64)

Zbog jednostavnosti implementacije i lokacije vodenog žiga u stego slici, LSB metoda je poprilično neotporna na napade. Promjenom bilo kojeg broja najnižih bitova nasumičnim vrijednostima žig se automatski gubi, a velike su šanse i da će nakon kompresije poprilični dio skrivene poruke biti odbačen.

3.3. Modifikacija bazirana na korelaciji

Metoda bazirana na korelaciji prilikom kodiranja stego slike koristi generirani pseudo-slučajni šum te na temelju sadržaja vodenog žiga kreira masku koja se zatim dodaje originalnoj slici. Za detekciju žiga primatelj mora znati seed[2] pomoću kojeg je šum generiran te korištenu steganografsku metodu.

Postupak kodiranja započinje odabirom seed vrijednosti kojom se zatim generira pseudo-slučajni binarni šum. Dobiveni šum se množi sa gain vrijednosti k o kojoj ovisi kvaliteta rekonstruiranog vodenog žiga, odnosno količina distorzije u stego slici. Maska koja se dodaje originalnoj slici kreira se na sljedeći način: ukoliko je vrijednost vodenog žiga (koji je također preveden u binarnu sliku ili binarni niz) jednaka 0, u masku se dodaje vrijednost originalne slike. Ako je vrijednost vodenog žiga jednaka 1, taj bit u maski se postavlja na vrijednost šuma. Maska se na kraju pridodaje originalnoj slici operacijom zbrajanja. Izraz (1) opisuje upravo definiran postupak.

$$I_w(x,y) = I(x,y) + k * W(x,y) \tag{1}$$

$I(x,y)$ – originalna slika

$W(x,y)$ – generirana maska

k - gain

$I_w(x,y)$ – stego slika

Kod detekcije vodenog žiga generira se jednak pseudo-slučajni šum kao u algoritmu sakrivanja. Primljena potencijalna stego slika se za svaki piksel korelira sa dobivenim šumom i uspoređuje sa nekim postavljenim pragom (treshold, T). Ukoliko vrijednost korelacije slike i generiranog šuma prelazi prag, vodeni žig je na promatranom pikselu detektiran. [12, 13]

[2] Vrijednost korištena za inicijaliziranje generatora pseudo-slučajnih brojeva

3.4. CDMA metoda

CDMA (Code Division Multiple Access) metoda koristi tehniku raspršenosti spektra. Prijenosna uskopojasna tajna poruka raspršuje se po frekvencijskom pojasu stego slike koji je puno širi od potrebnog kako bi vodeni žig bio što robusniji na različite manipulacije podacima i kompresiju. Signali za raspršivanje bitova vodenog žiga generiraju se kao pseudo-slučajni šum. Zbog naizgled nasumične raširenosti na stego slici i odgovarajućih statističkih svojstava ova tehnika otporna je na izrezivanje slike, nelinearne degradacije i aditivni šum. [14]

Prednosti korištenja CDMA metode, unatoč korištenju apsolutno cijelog spektra, očituju se u sljedećem:

- Otpornost na šum i višepojasne distorzije
- Sakrivanje i šifriranje vodenog žiga
- Više poruka mogu se neovisno jedna o drugoj umetnuti u originalnu sliku, sa vrlo malom razinom interferencije
- Niske vrijednosti autokorelacije i kroskorelacije pseudo-slučajnih šumova garantiraju efikasno sakrivanje vodenog žiga [15]

U ovoj tehnici, pošiljatelj za kodiranje digitalnog vodenog žiga koristi određeni ortogonalni pseudo-slučajni generirani šum koji svojstvima odgovara bijelom šumu. Na odredištu poruke primatelj generirajući jednak šum kao pošiljatelj iz stego slike dekodira sakrivenu poruku. Značajno za CDMA metodu je mogućnost generiranja šuma na neograničeni broj načina što kodiranje, pa tako i samo dekodiranje, poruke čini toliko zamršenije.

Za generiranje pseudo-slučajnog šuma odabire se inicijalna seed vrijednost. Za svaku vrijednost bita u vodenom žigu posebno se generira novi šum, a nakon svake sekvence se vrijednost početnog seeda mijenja na zadani način u algoritmu. Zatim se provjerava je li piksel vodenog žiga jednak 0 ili 1 te se na temelju toga u stego sliku spremaju vrijednosti šuma ili

vrijednosti originalne slike. Šum je prije dodavanja stego slici pomnožen sa konstantom (gain, k) koju odabire pošiljatelj ovisno o potrebama kvalitete rekonstruiranog žiga.

Detekcija vodenog žiga također započinje generiranjem pseudo-slučajnih šumova koji se koriste za izračun korelacije sa primljenom stego slikom. Kao i na pošiljateljevoj strani, za svaki piksel sakrivene poruke generira se novi šum sa promijenjenim seed-om. Ako korelacija na promatranom pikselu prelazi srednju vrijednost svih korelacija, označava se da je na tom mjestu detektiran vodeni žig. [12]

Modifikacija bazirana na korelaciji i CDMA metoda naizgled se čine gotovo podjednakima, no CDMA je nekoliko redova složenija za implementaciju i izračun, a samim time i robusnija kod očuvanja i rekonstrukcije sakrivenog vodenog žiga. Za još učinkovitije rezultate, algoritmi se odmah implementiraju u frekvencijskoj domeni.

Budući da je CDMA jedna od najkvalitetnijih tehnika raspršenog spektra danas, koja se koristi u navigaciji i mobilnim komunikacijama za sigurno slanje i primanje informacija, preferira se i u svrhu steganografije.

3.5. Sakrivanje u DCT domeni

Metode ubacivanja vodenog žiga u transformacijskim domenama sakrivaju poruku u energetski značajan dio originalne slike. Iz tog razloga stego slika ne gubi informaciju o žigu prolazeći kroz različite obrade i kompresiju, a promjene koje se događaju u sadržaju slike neprimjetne su ljudskom oku. Postoji mnogo različitih metoda sakrivanja vodenog žiga u transformacijskim domenama. Kodiranje tajne poruke može se provoditi preko cijele originalne slike, na blokovima podataka određene veličine, i sl. Većina algoritama ne ovisi o izvornom formatu originalne slike i vodenog žiga te su otporni na konverzije sa gubicima i bez gubitaka.

DCT se uglavnom koristi za kompresiju podataka sa gubicima zbog svog svojstva „zbijanja energije“ u koeficijentima koji odgovaraju niskim frekvencijama u originalnoj slici. Niskih frekvencija je, kad se radi o prirodnim slikama sa blagim prijelazima kontura i površina, značajno više nego visokih. DCT metode vodeni žig sakrivaju u perceptivno značajnije dijelove slike koji se pri kompresijama ne odbacuju kao npr. visoke frekvencije.

Dvodimenzionalna DCT transformacija temelj je danas najviše korištene kompresije i formata za prikaz slika – JPEG formata. JPEG radi na način da prvo originalnu sliku podijeli u 8 x 8 blokove piksela te nad njima provodi RGB u YCbCr konverziju, zatim DCT transformaciju, kvantiziranje koeficijenata i konačno Huffmanovo entropijsko kodiranje za kompresiju dobivenih DCT koeficijenata. Kod dekodiranja, svi DCT koeficijenti prolaze postupak obrnute kvantizacije (množe se sa vrijednostima s kojima su bili podijeljeni u kodiranju) i inverzne DCT transformacije, i obnovljena slika se može prikazati. Ukoliko su vrijednosti u kvantizacijskoj tablici ispravno postavljene, kompresija ne bi smjela utjecati na kvalitetu slike vidljivu ljudskom oku. [16]

Opisane metode najčešće su korištene tehnike steganografije te će u nastavku ovog rada biti implementirane i testirane na različite vrste distorzija i kompresiju. U sljedećem poglavlju, prije izlaganja i usporedbe rezultata, nabrojane su vrste distorzija i napada koji mogu utjecati na stego sliku u procesu prijenosa.

4. Distorzije i napadi na vodeni žig

Postoji nekoliko vrsta namjernih distorzija i napada na kodiranu stego sliku zbog koje vodeni žig nakon rekonstrukcije nije čitljiv ili ne može uopće biti dekodiran. Napadi mogu biti sljedeći: [16]

- Aktivni napadi

  Presretač stego slike pokušava namjerno ukloniti vodeni žig ili učiniti da ga se ne može detektirati. Ovakvi napadi predstavljaju veliki problem u zaštiti autorskih prava, *fingerprint* metodi te zaštiti od nedozvoljenog kopiranja zaštićenog sadržaja.

- Pasivni napadi

  Vodeni žig se ne pokušava ukloniti nego samo dokazati njegova prisutnost u stego slici. U tajnim komunikacijama zaštita od pasivnih napada jednako je bitna jer i sama prisutnost žiga bi trebala ostati neotkrivena.

- Napadi nedopuštenim radnjama

  Cilj napada je isti kao i kod aktivnog, no primjenjujući drugačiju metodu. Kako bi se uklonio vodeni žig, napadač koristi nekoliko kopija jednakih stego datoteka, od kojih svaka sadrži drugačiji žig koje zatim kombinira u jednu datoteku bez oznake autorskog vlasništva ili *fingerprint*-a. Ova metoda uglavnom se koristi u filmskoj industriji no zbog česte nemogućnosti nabavljanja više različitih kopija nije široko raširena.

- Napadi krivotvorenjem

  Vrsta napada koja najviše utječe na autentifikaciju podataka. Cilj napada je ugraditi u stego sliku novi, naizgled važeći vodeni žig bez uklanjanja originalnog. Postavljajući i novi ključ umjesto originalnog koji je vjerojatno oštećen, promijenjena stego slika ne izgleda modificirano.

Nenamjerne ili namjerne distorzije i napadi tijekom prijenosa u komunikacijskom kanalu mogu biti JPEG kompresija, aditivni šum, geometrijske deformacije, uklanjanje šuma, median filtriranje i zamućivanje, promjene signala u svrhu izoštravanja i pojačavanja kontrasta.

Kompresija slike je najčešći uzrok unesene distorzije na stego sliku. Kako je u današnje vrijeme internet glavni prijenosni medij, slanje datoteka u originalnom formatu može biti vrlo sporo i neefikasno. Ovisno o formatu i načinu komprimiranja podataka treba uzeti odgovarajuću stego metodu za sakrivanje tajne poruke.

Aditivni šum je nasumični signal sa određenom distribucijom. Uglavnom se dodaje na stego sliku prilikom A/D i D/A pretvorbe ili tijekom prijenosa. Ukoliko je dodani šum većeg intenziteta može otežati detekciju vodenog žiga kod metoda koje koriste tehnike usporedbe.

Geometrijske deformacije vrlo su efektivan napad u smislu nemogućnosti detekcije vodenog žiga. Statistički se svojstva stego slike ne mijenjaju jer se pikseli samo premještaju na druge lokacije pa nema očitih indikacija da se dogodila distorzija. Najčešće deformacije su translacija, rotacija, izrezivanje i skaliranje cijele ili samo dijela stego slike.

Uklanjanje šuma provodi se pod pretpostavkom da je digitalni vodeni žig aditivni šum na stego slici. U tom slučaju provodi se filtriranje visoko propusnim filtrima i nisko propusnim filtrima, Gaussovim filtrom, filtrom za izoštravanje itd. Ako se aditivni šum gleda kao bijeli šum primjenjuju se i metode lokalnog medijana, Wienerovog filtra i usrednjavanja.

5. Implementacija i analiza u Matlabu

Metode steganografije opisane u 3. poglavlju ovog rada implementirane su u programskom okruženju Matlab. Uz prikaz slikovnih rezultata, kao objektivna mjera korišten je PSNR (*Peak Signal-to-Noise Ratio*). Vršna vrijednost odnosa signala i šuma (PSNR) daje omjer maksimalne snage signala i snage šuma u njoj. Kako većina signala ima vrlo veliki dinamički raspon (raspon između najveće i najmanje vrijednosti), PSNR se izražava u logaritamskom mjerilu. PSNR se za dvije monokromatske slike (I i K, dimenzija m x n) definira prema:

$$PSNR = 10log\frac{(2^n-1)^2}{MSE} \tag{2}$$

gdje je n broj bitova korištenih pri uzorkovanju izvorne slike. MSE predstavlja srednju kvadratnu pogrešku između uzoraka originalne (nekomprimirane, bez vodenog žiga) slike I i stego slike (sa umetnutim žigom) K, a definirana je relacijom:

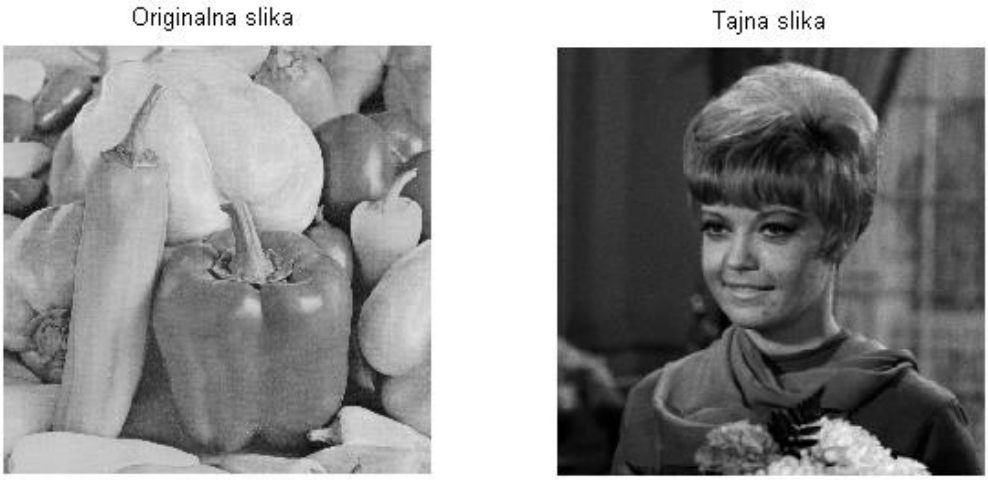
$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\|I(i,j)-K(i,j)\|^2 \tag{3}$$

Broj $(2^n-1)^2$ predstavlja maksimalnu vrijednost koju element slike može postići a ona ovisi o broju bitova s kojima je postojeća slika uzorkovana. Za standardnih 8 bitova ta vrijednost iznosi 255.

5.1. Injektiranje tajne poruke u originalnu sliku

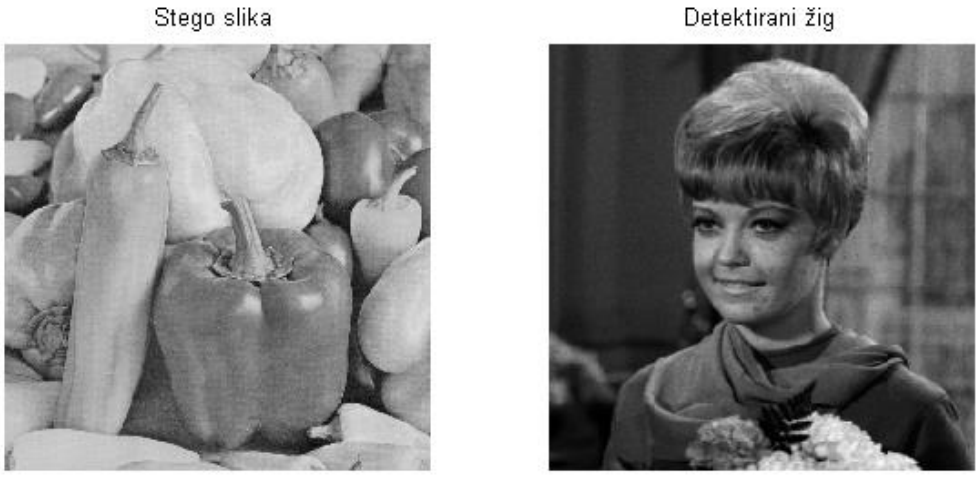
Proces umetanja sakrivene poruke u sliku metodom injektiranja koja je opisana u poglavlju 3.1. izveden je u binarnom zapisu originalne slike. Koraci algoritma implementiranog u Matlabu su:

Učitavanje originalne slike i vodenog žiga ili tajne poruke prikazano je na slici 5.1. Određuje se duljina poruke za kasniju rekonstrukciju.



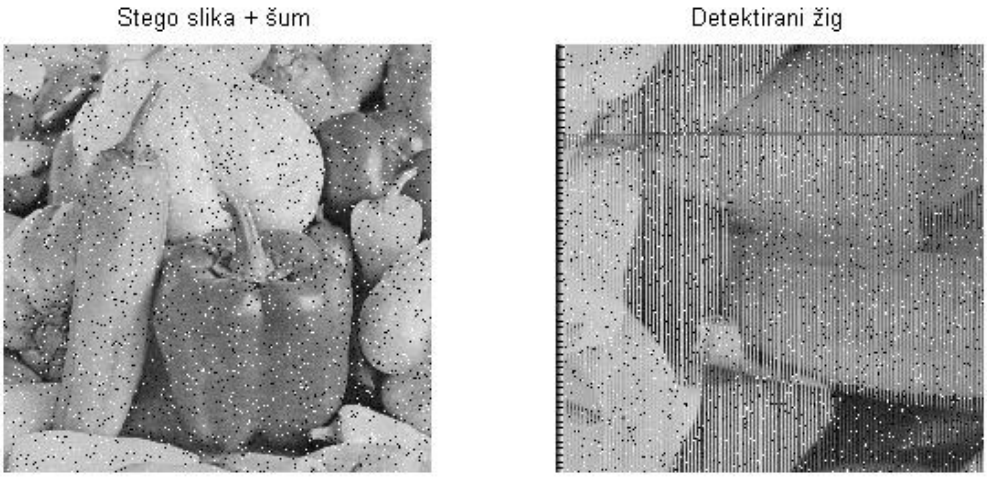
Slika 5.1 Originalna slika Peppers.tiff i tajna slika Girl.tiff

Originalna slika se otvara kao binarni file sa dozvolom čitanja i pisanja te se pozicionira na kraj tražeći oznaku EOF (*end of file*). Na kraju datoteke dodaje se sakrivena slika te se datoteka zatvara i sprema kao stego slika. Na primateljevoj strani stego slika se otvara kao binarni file te se postavlja na mjesto koje bi trebalo odgovarati kraju zapisa originalne slike. Od te pozicije čitaju se podaci tajne poruke do stvarnog kraja datoteke te se detektirani vodeni žig može prikazati. Rezultat čitanja skrivene poruke prikazan je na slici 5.2.

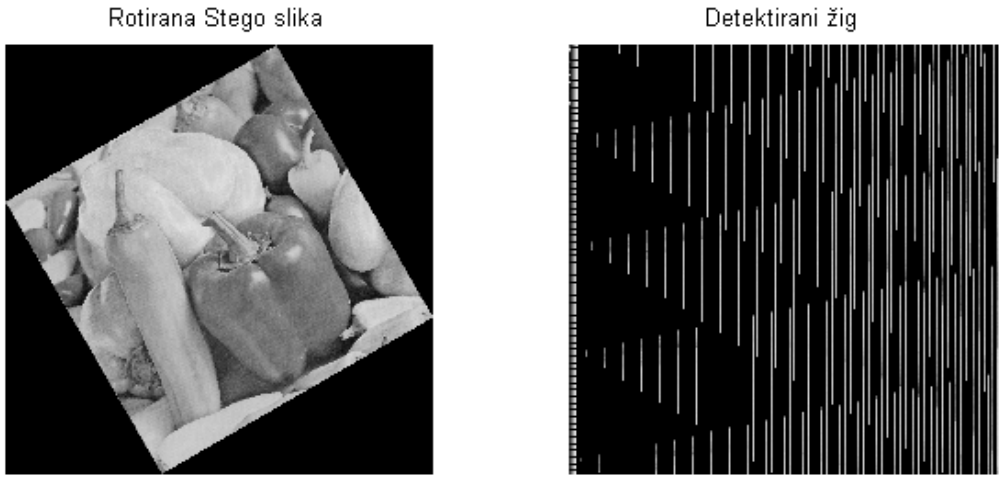


Slika 5.2 Stego slika i detektirani vodeni žig

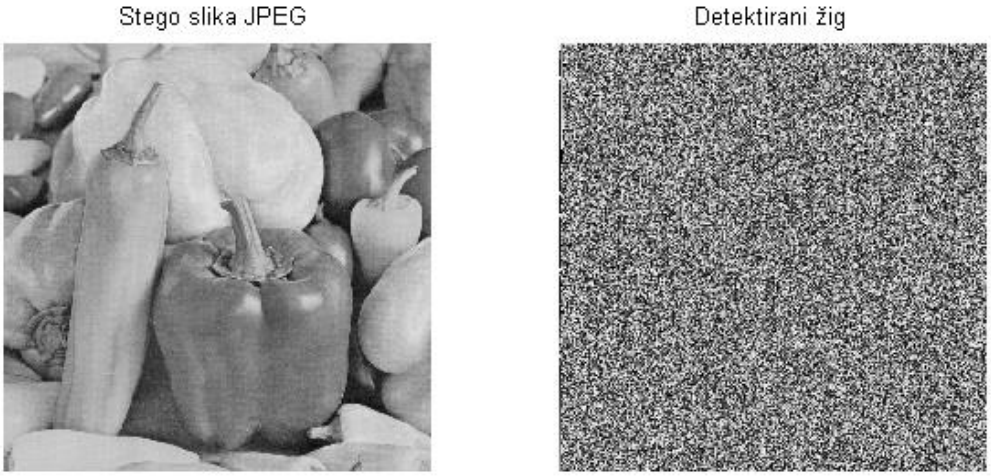
Nakon sakrivanja poruke u originalnu sliku i spremanja u formatu stego slike, dodane su različite vrste distorzija na nju. Prva od njih je u obliku aditivnog šuma Salt & pepper (d=0,05). Kao što je vidljivo na slici 5.3, vodeni žig nije dobro detektiran. U ovom slučaju radi se o ograničenju Matlab programa i korištenih funkcija za spremanje i učitavanje formata slike. Jednaki problem javlja se i kod rotacije stego slike za 30° te kod testa JPEG kompresijom. Rezultati i tih distorzija prikazani su na slikama 5.4 i 5.5.



Slika 5.3 Stego slika sa dodanim aditivnim šumom i detektirani vodeni žig



Slika 5.4 Stego slika rotirana za 30° i detektirani vodeni žig

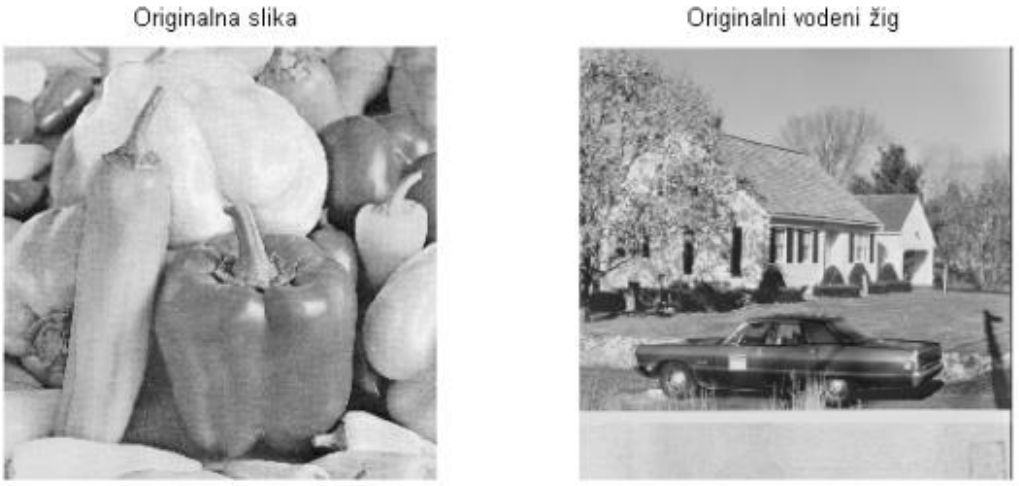


Slika 5.5 Stego slika nakon JPEG kompresije i detektirani vodeni žig

Na temelju prikazanih rezultata vidljivo je kako su za manipulaciju binarnim datotekama, njihovo pohranjivanje u formate za prikaz slike i distribuciju potrebni dodatni algoritmi koji će u standardnom koderu modificirati način spremanja podataka iz slike te uzeti u obzir i naknadno dodane vrijednosti vodenog žiga.

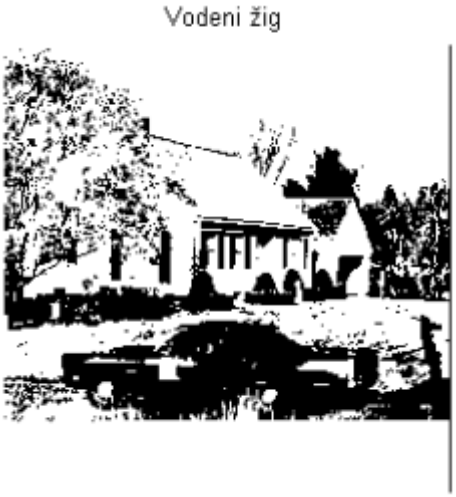
5.2. LSB metoda

Modifikacija originalne slike sa bitom najmanjeg značaja također započinje učitavanjem originalne slike i vodenog žiga u radno okruženje. Ukoliko slika i žig nisu jednakih dimenzija, vodeni žig se skalira na dimenzije originalne slike što ujedno služi i za zalihost sakrivene poruke. Slika 5.6 prikazuje učitane slike.



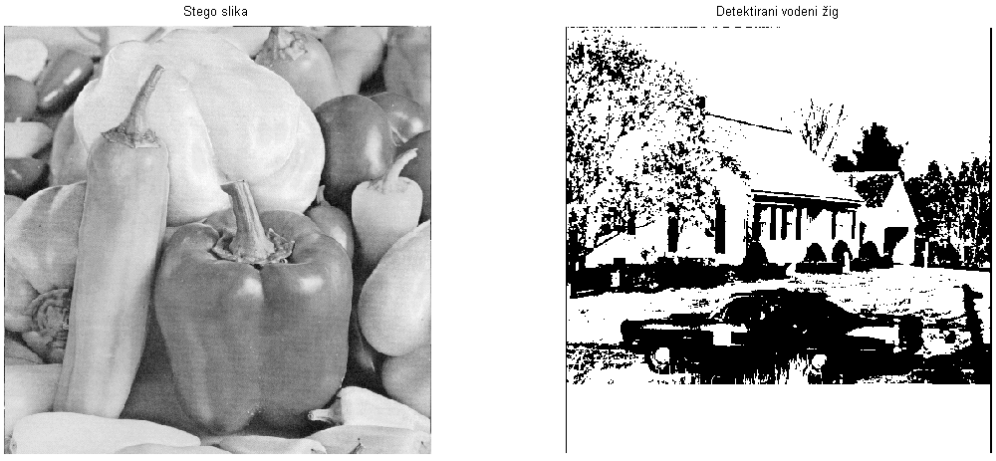
Slika 5.6 Originalna slika Peppers.tiff i vodeni žig House.tiff

Kako bi se složenost izvođenja algoritma optimizirala učitani vodeni žig konvertira se u binarnu sliku sa pragom izračunatim za svaki žig posebno. Na slici 5.7 nalazi se binarni vodeni žig spreman za ubacivanje u originalnu sliku.



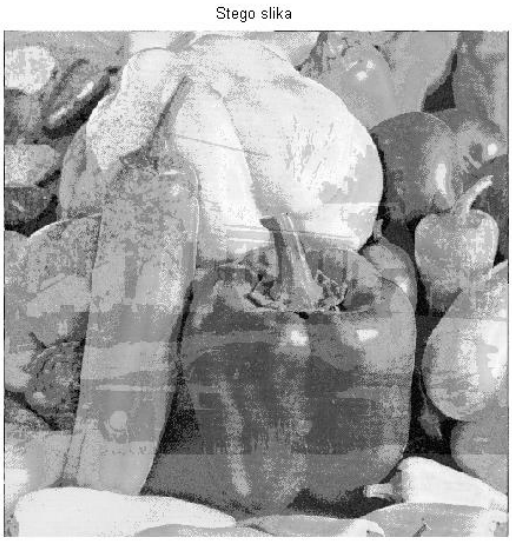
Slika 5.7 Binarni vodeni žig

Matlabovim funkcijama bitset i bitget, uz na početku definiran broj bitova koji će se koristiti za sakrivanje žiga (bitToSet), generira se stego slika koja u najnižih bitToSet bitova sadrži informaciju o vodenom žigu dok u ostalima, bitovima višeg značaja, ostaju podaci originalne slike. Za funkciju detektiranja žiga dovoljno je znati koliko bitova je korišteno u procesu kodiranja. Na slici 5.8 prikazani su rezultati generiranja stego slike sa vodenim žigom u 3 najniža bita originalne slike.



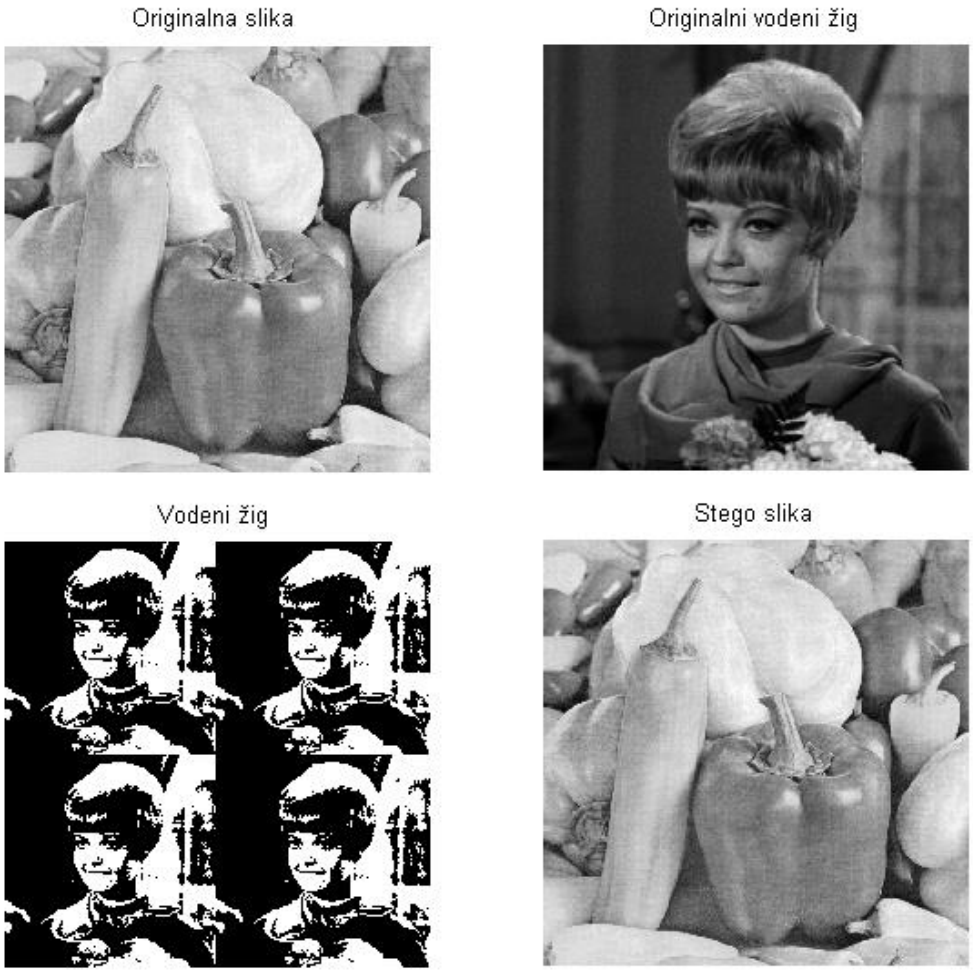
Slika 5.8 Stego slika i detektirani vodeni žig, bitToSet=3

Korištenjem veće količine bitova za skrivanje vodenog žiga dolazi do degradacije originalne slike te se na stego slici mogu vidjeti obrisi sakrivene poruke. Primjer takve stego slike je na slici 5.9.



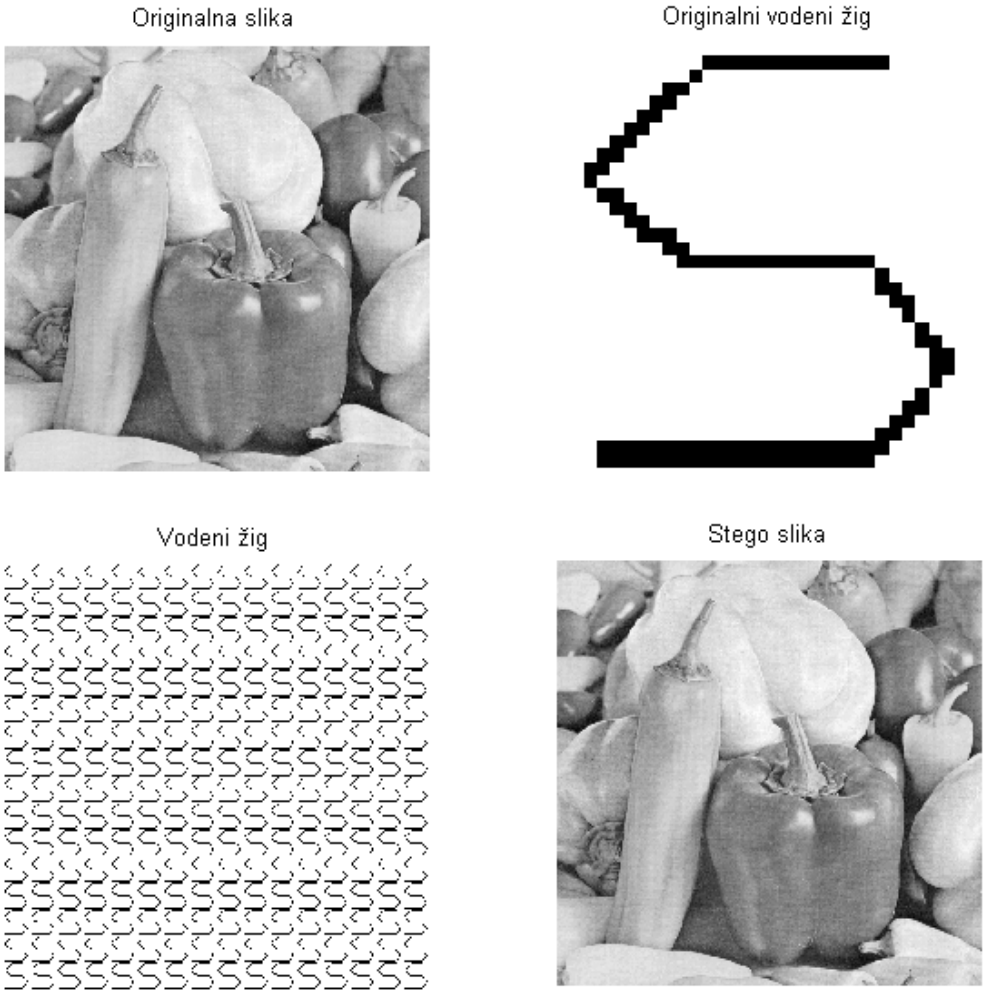
Slika 5.9 Stego slika, bitToSet=6

Kao što je ranije spomenuto, ukoliko vodeni žig nije jednakih dimenzija kao originalna slika prije ubacivanja se skalira. Na sljedećim slikama prikazani su rezultati sakrivanja i detekcije vodenih žigova različitih dimenzija.

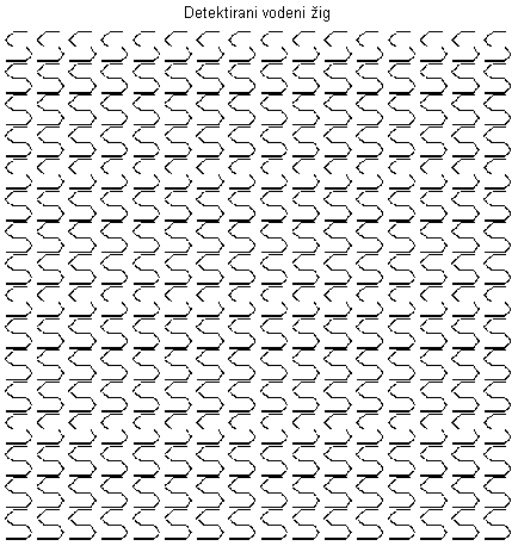


Slika 5.10 Originalna slika Peppers.tiff i vodeni žig Girl.tiff, bitToSet=3

Slika 5.11 Detektirani vodeni žig



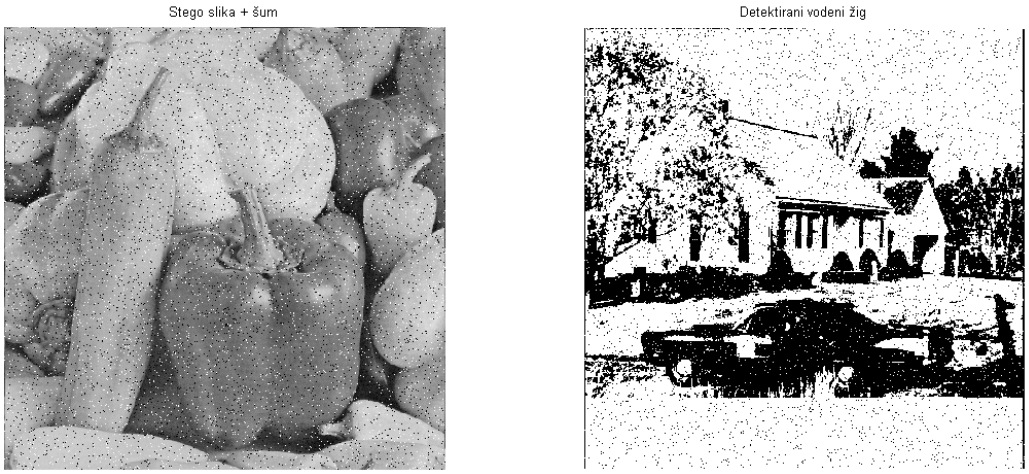
Slika 5.12 Originalna slika Peppers.tiff i vodeni žig S.bmp, bitToSet=3



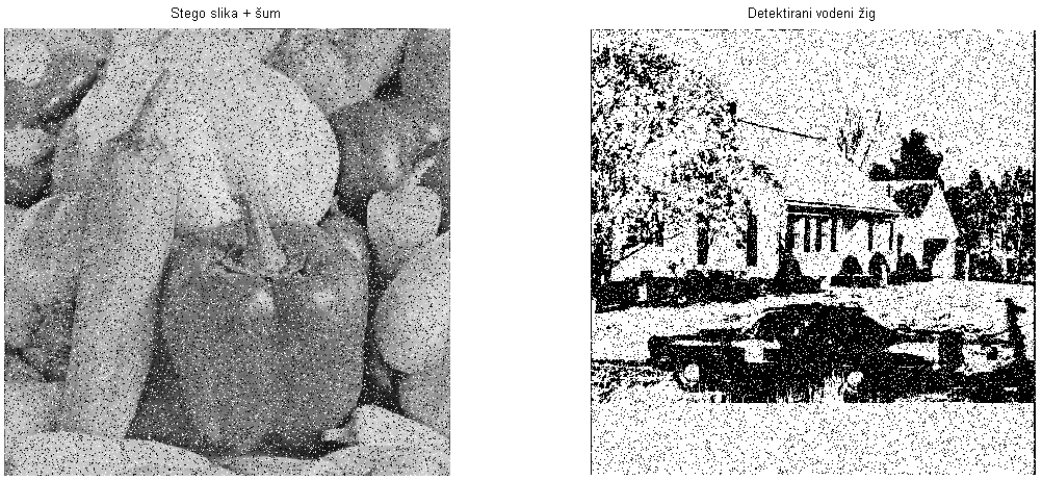
Slika 5.13 Detektirani vodeni žig

Sukladno intenzitetu distorzije na stego slici detekcija vodenog žiga provodi se više ili manje uspješno. Sljedeće slike prikazuju rezultate ekstrakcije žiga nakon utjecaja aditivnog šuma, rotacije i JPEG kompresije na stego sliku.

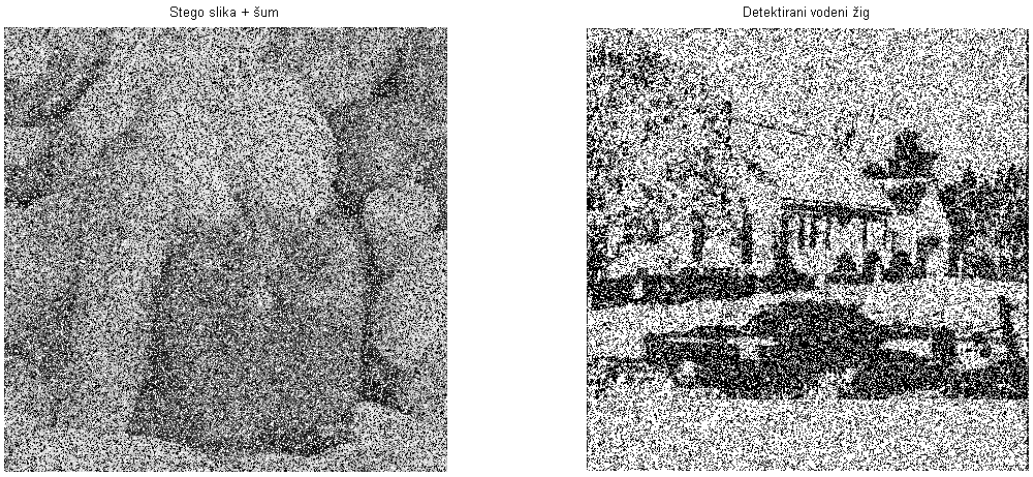
Vrijednosti PSNR mjere dane su u tablici 1. Tipične vrijednosti PSNR-a nakon kompresije s gubicima kreću se između 30 i 50 dB, gdje veća vrijednost označava bolju kvalitetu slike. Pri usporedbi dvije identične slike, MSE će biti jednak nuli (jer nema razlika koje unosi kompresija) pa tada PSNR teži u beskonačno.



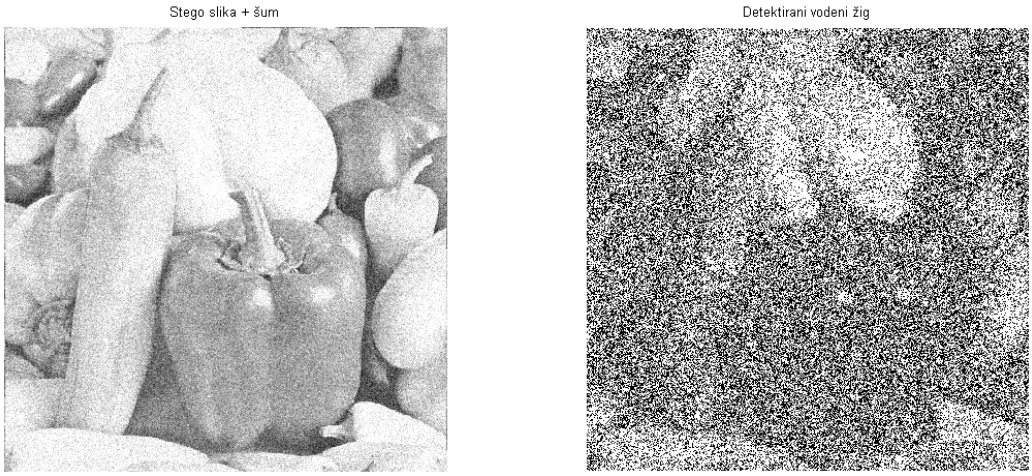
Slika 5.14 Salt & pepper šum (d = 0.05)



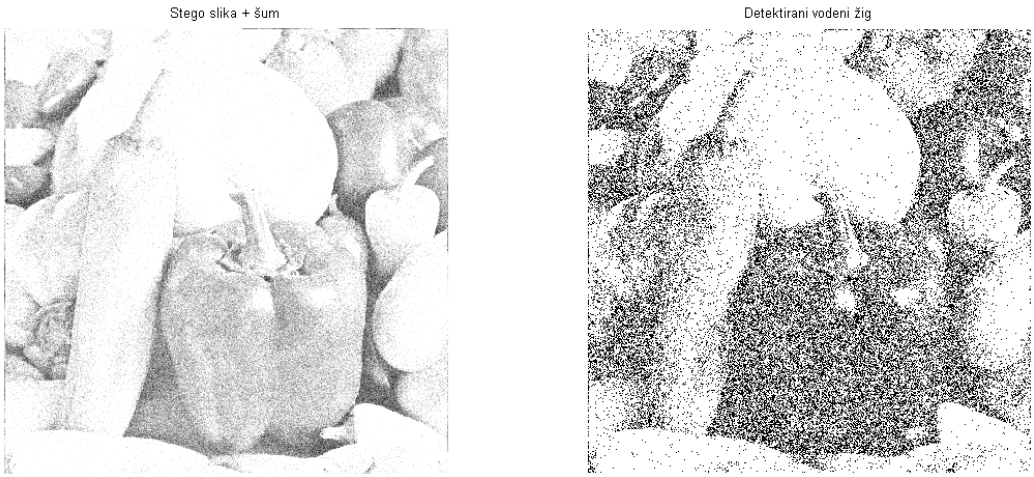
Slika 5.15 Salt & pepper šum (d = 0.15)



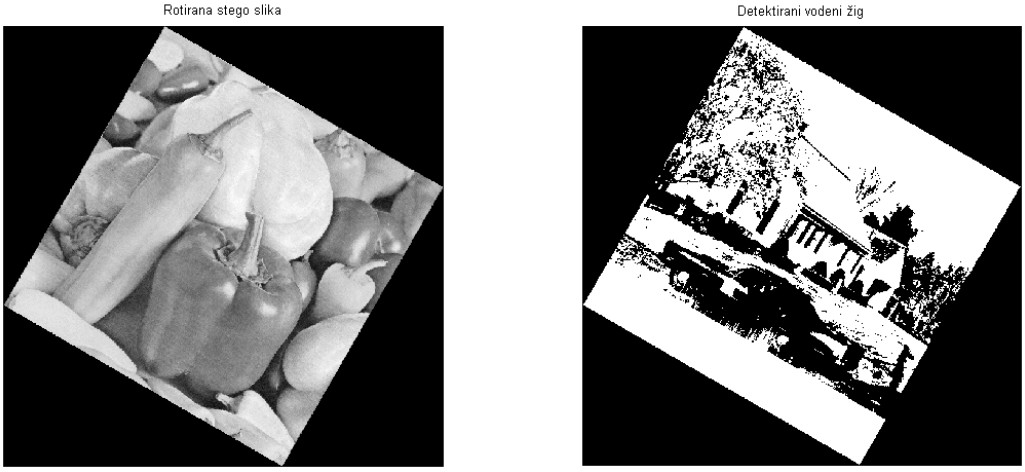
Slika 5.16 Salt & pepper šum (d = 0.5)



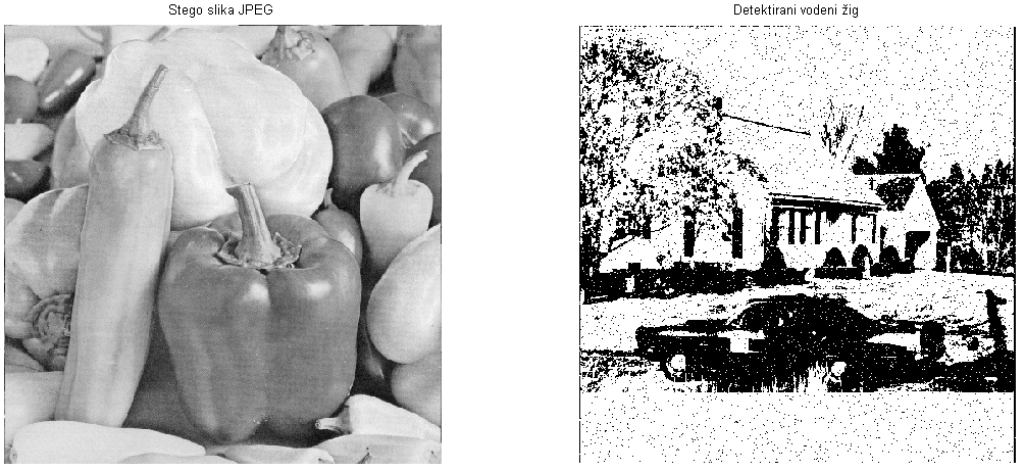
Slika 5.17 Gaussov šum (μ = 0.2, σ = 0.01)



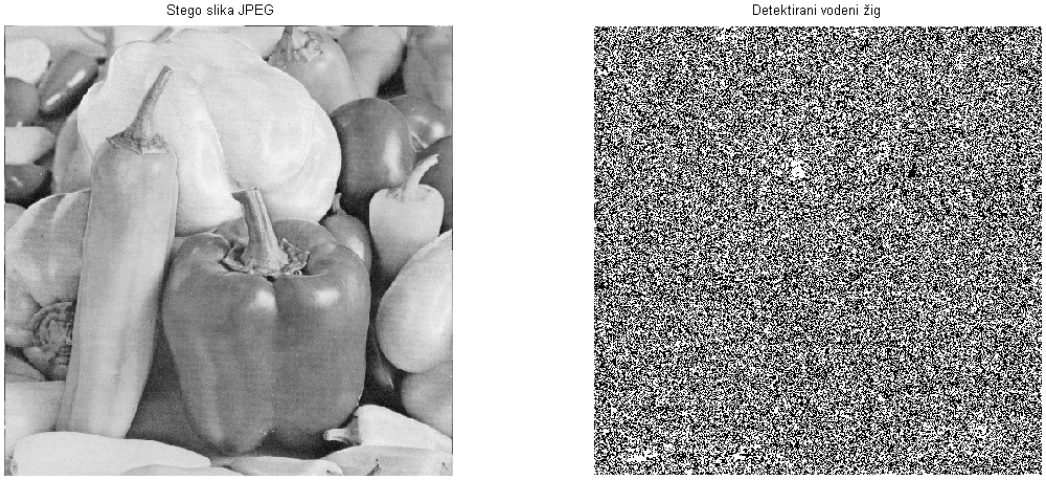
Slika 5.18 Gaussov šum (μ = 0.4, σ = 0.01)



Slika 5.19 Rotacija (30°)



Slika 5.20 JPEG kompresija, q=100



Slika 5.21 JPEG kompresija, q=90

Tablica 5.1 Utjecaj distorzija na kvalitetu slike u LSB metodi

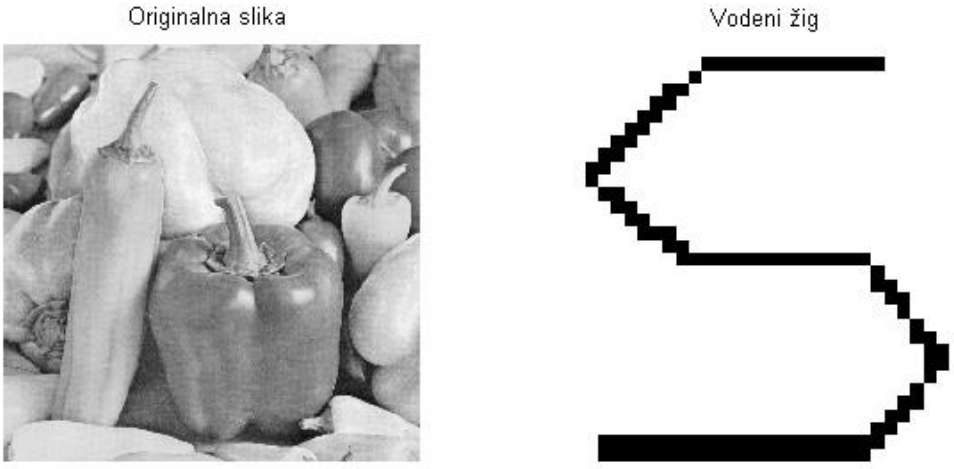
DISTORZIJA	PSNR
Bez distorzije	44.2476
Salt & pepper šum (d = 0.05)	37.4658
Salt & pepper šum (d = 0.15)	34.3682
Salt & pepper šum (d = 0.55)	29.8824
Gaussov šum (μ = 0.2, σ = 0.01)	24.3169
Gaussov šum (μ = 0.4, σ = 0.01)	24.0662
Rotacija (30°)	35.8166
JPEG kompresija, q=100	40.5800
JPEG kompresija, q=90	37.4122

Na temelju prikazanih rezultata kod unošenja distorzija kakve bi se mogle pojaviti u komunikacijskom kanalu na stego sliku, vidljivo je da LSB metoda u nekim slučajevima može sačuvati ugrađeni vodeni žig, dok su očekivano najlošiji rezultati kod JPEG kompresije koja radi na principu odbacivanja najmanje značajnih bitova – upravo onih gdje je vodeni žig LSB metodom utisnut te kod dodanog Gaussovog šuma na koji metoda nije nimalo otporna.

5.3. Modifikacija bazirana na korelaciji

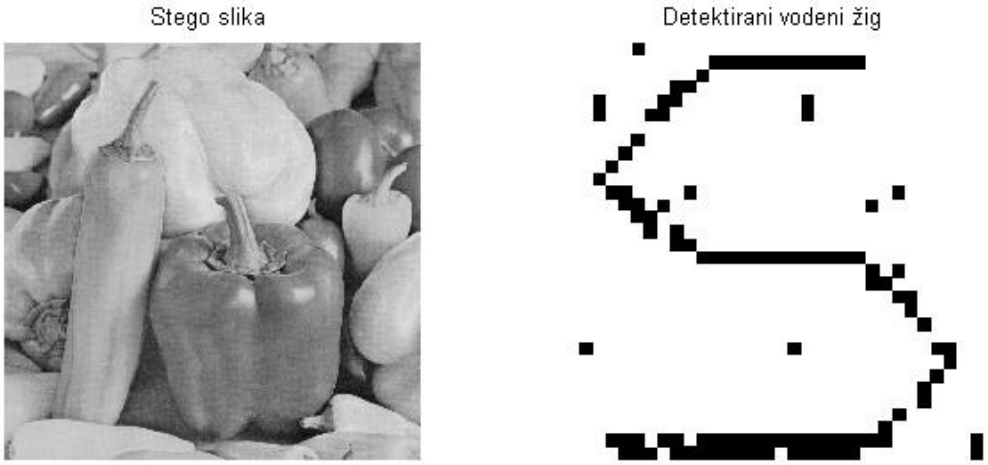
Kako bi sakriveni vodeni žig bio otporniji na napade i jednostavno uklanjanje, sadržaj vodenog žiga koristi se za oblikovanje generiranog slučajnog šuma dodanog na originalnu sliku. Nakon učitavanja originalne slike i vodenog žiga (slika 5.22), generira se pseudo-slučajni šum sa seed vrijednosti poznate samo pošiljatelju i primatelju kojem je tajna poruka namijenjena. Šum je zatim pomnožen sa odabranom gain vrijednosti o kojoj ovisi kvaliteta stego slike tj. uspješnost rekonstruiranja žiga. Ovisno o sadržaju vodenog žiga maska za stego sliku se izrađuje po sljedećem principu: ako je vrijednost vodenog žiga na trenutno promatranom pikselu jednaka 0, maska poprima vrijednost originalne

slike dok se u suprotnom slučaju u masku zapisuje vrijednost šuma. Postupak se provodi za cijeli vodeni žig te se na kraju maska zbraja na originalnu sliku prema izrazu (1). Za otkrivanje sadržaja vodenog žiga na strani primatelja potrebno je generirati identičan pseudo-slučajni šum (sa poznatom seed vrijednosti) te izračunati korelaciju piksela stego slike sa tim šumom. Ukoliko vrijednost korelacije prelazi određeni prag T, postavlja se bit za detektirani vodeni žig te ga se na kraju ispitivanja može prikazati.

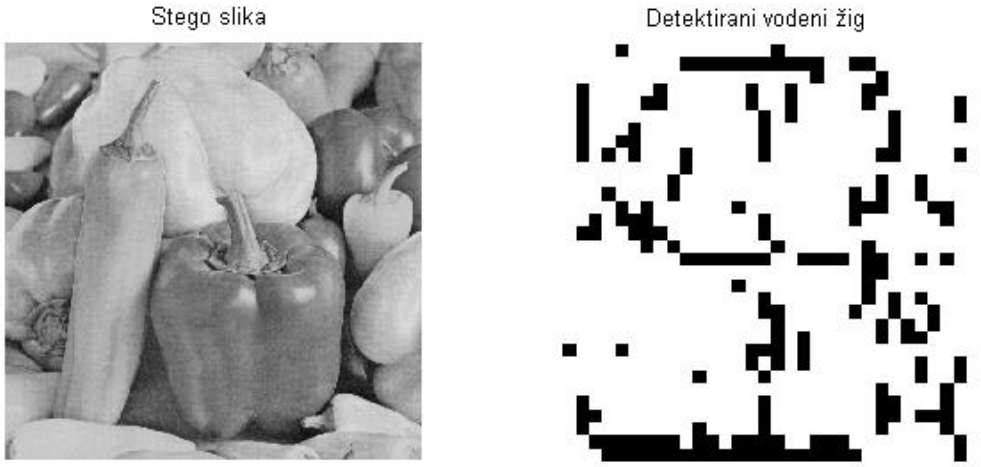


Slika 5.22 Originalna slika Peppers.tiff i vodeni žig S.bmp

Na slikama 5.23 i 5.24 prikazane su nastale stego slike i detektirani žigovi uz gain vrijednosti k=10 i k=1. Kod većeg gaina vidljiva je značajnija promjena originalne slike ali zato dobro rekonstruiran žig. Kada je gain vrijednost postavljena na 1, stego slika izgleda gotovo identično kao i originalna dok se na žigu pojavljuje poprilično pogrešaka.

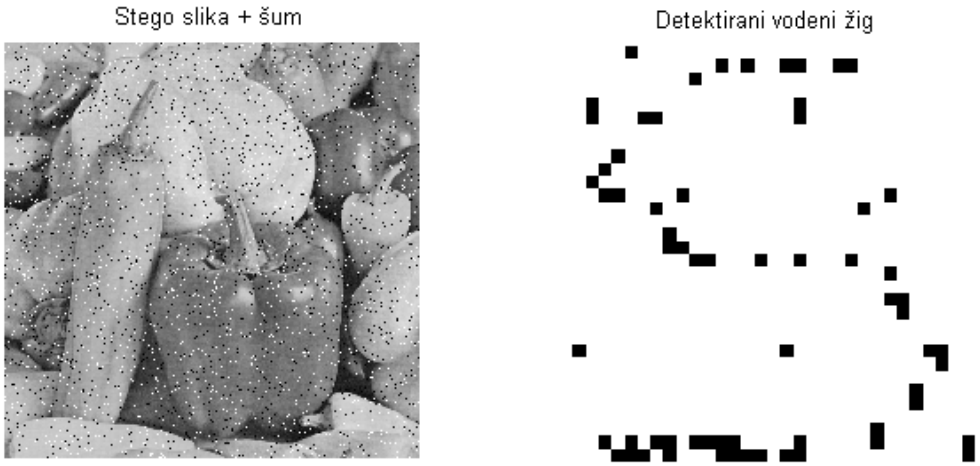


Slika 5.23 Stego slika i detektirani vodeni žig, gain=10

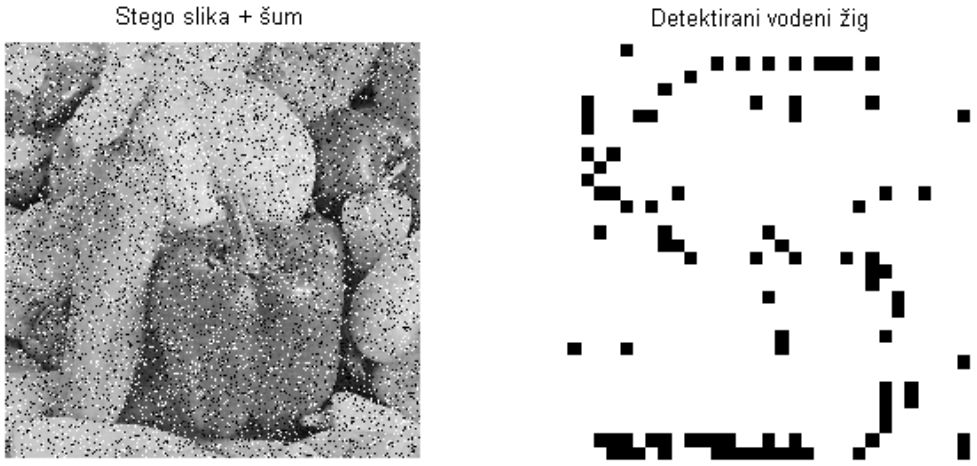


Slika 5.24 Stego slika i detektirani vodeni žig, gain=1

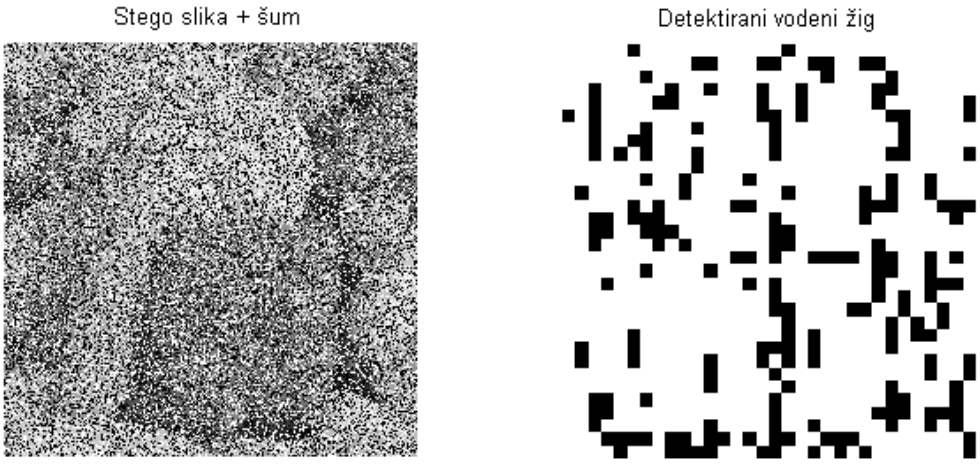
Na slikama 5.25 – 5.32 rezultati su detekcije vodenog žiga pod utjecajem već navedenih vrsta distorzija.



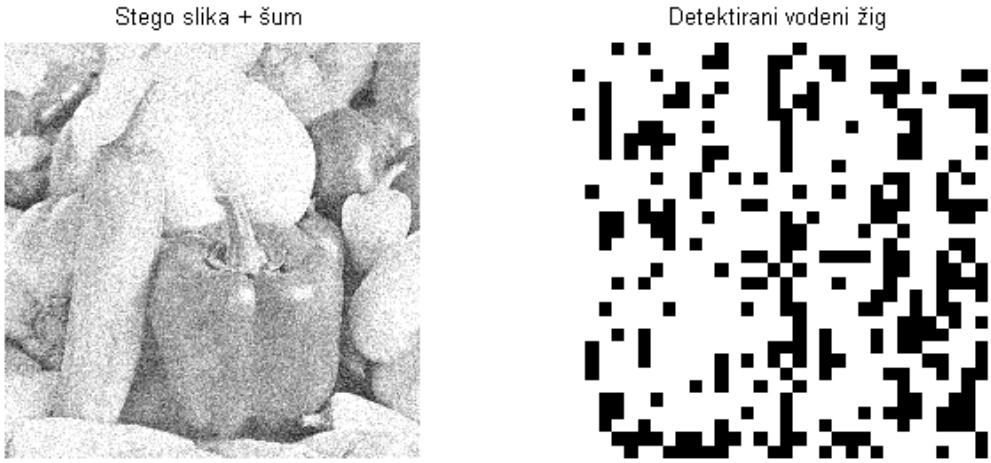
Slika 5.25 Salt & pepper šum (d = 0.05), gain=10



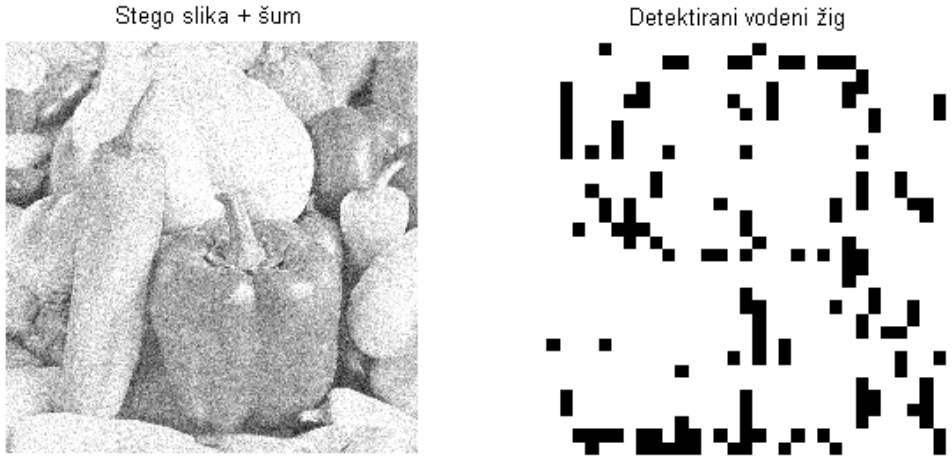
Slika 5.26 Salt & pepper šum (d = 0.15), gain=10



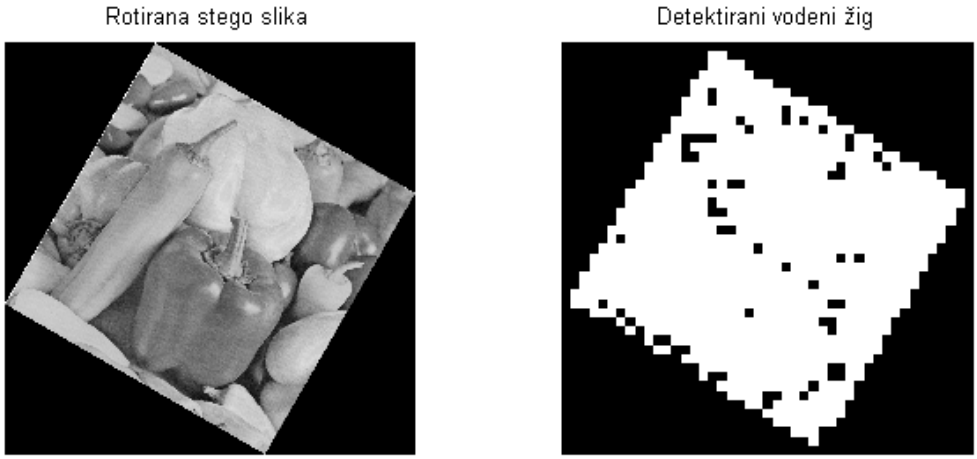
Slika 5.27 Salt & pepper šum (d = 0.5), gain=10



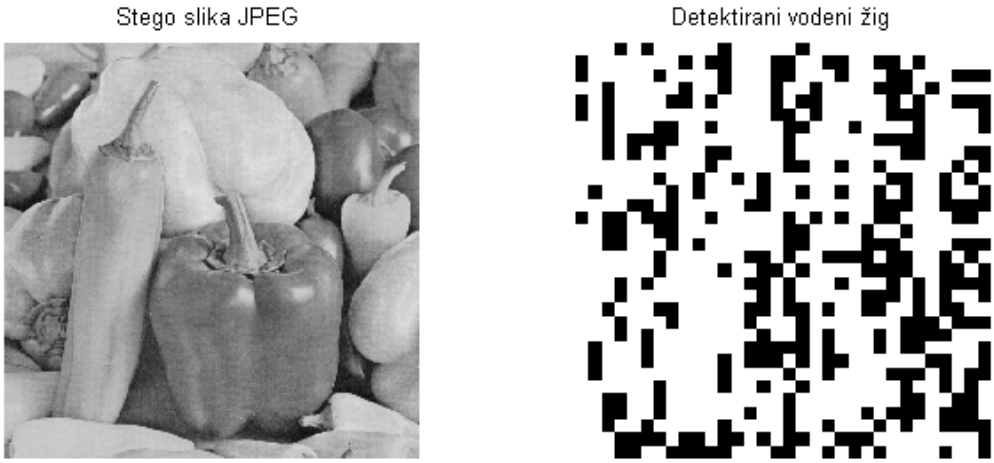
Slika 5.28 Gaussov šum (μ = 0.2, σ = 0.01), gain=10



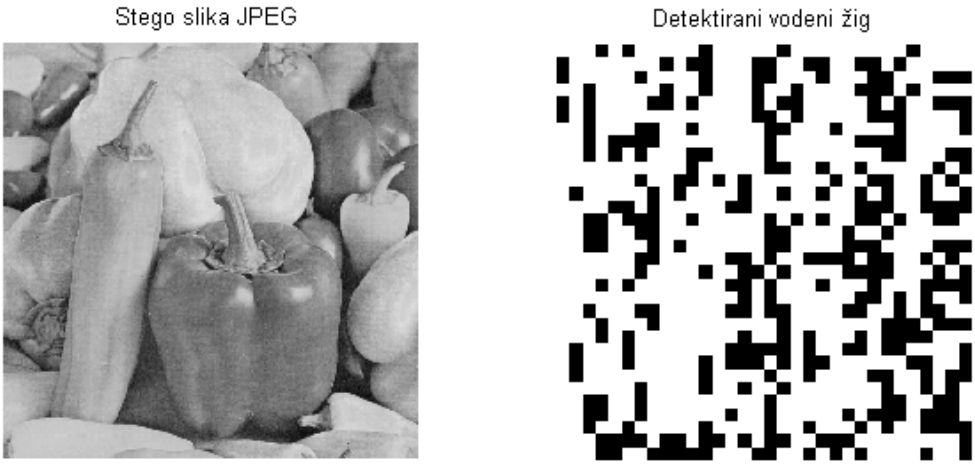
Slika 5.29 Gaussov šum (μ = 0.4, σ = 0.01), gain=10



Slika 5.30 Rotacija (30°), gain=10



Slika 5.31 JPEG kompresija, q=100, gain=10



Slika 5.32 JPEG kompresija, q=90, gain=10

Tablica 5.2 prikazuje odnos originalne slike i stego slike sa dodanim distorzijama.

Tablica 5.2 Utjecaj distorzija na kvalitetu slike u metodi korelacije

DISTORZIJA	PSNR
Bez distorzije, gain=10	55.7236
Bez distorzije, gain=1	75.4448
Salt & pepper šum (d = 0.05)	66.3455
Salt & pepper šum (d = 0.15)	61.7265
Salt & pepper šum (d = 0.55)	56.5297
Gaussov šum (μ = 0.2, σ = 0.01)	61.6557
Gaussov šum (μ = 0.4, σ = 0.01)	57.4998
Rotacija (30°)	53.4296
JPEG kompresija, q=100	80.4370
JPEG kompresija, q=90	79.3944

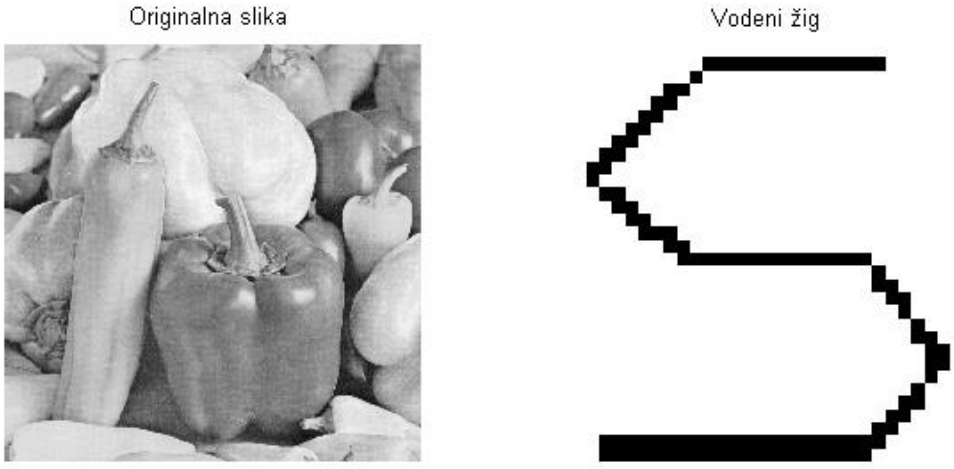
Zbog složenijeg načina sakrivanja vodenog žiga u originalnu sliku, PSNR vrijednosti pokazuju dobru kvalitetu stego slika. Rekonstrukcija žiga sa većom gain vrijednosti vidljivo je bolja nego sa manjom. Aditivni šumovi poprilično otežavaju detekciju žiga što bi se moglo poboljšati primjenom različitih filtara. Nakon JPEG kompresije vodeni žig se može prepoznati samo u tragovima.

5.4. CDMA metoda

Tehnika CDMA koristi prednosti raspršenosti spektra i broj šumova jednak broju uzoraka u vodenom žigu. Algoritam prolazi kroz svaki uzorak učitanog žiga te generira pseudo-slučajni šum koji množi sa nekom gain vrijednosti. U slučaju da je piksel vodenog žiga jednak 0, na originalnu vrijednost se dodaje trenutni šum, inače se ostavlja vrijednost originalne slike. U sljedećem koraku generira se novi šum i ponovno gleda vrijednost žiga i tako sve dok se ne prođe kroz svaki piksel. Za rekonstrukciju sakrivenog žiga primatelju kojem je stego

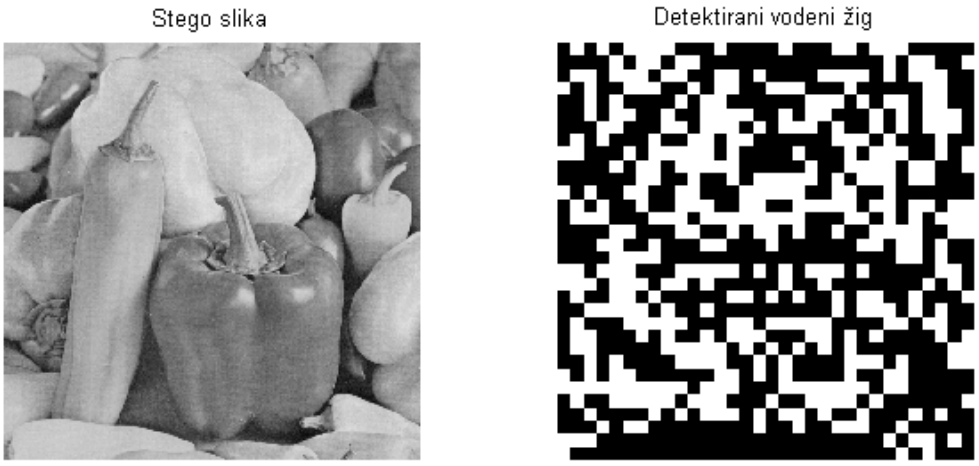
slika namijenjena je dovoljno znati inicijalnu seed vrijednost za generiranje pseudo-slučajnih šumova. Za svaki generirani šum računa se korelacija sa stego slikom te se svaka od vrijednosti uspoređuje sa srednjom vrijednosti korelacija. Ako je korelacija veća od prosječne vodeni žig je detektiran. Ova metoda je implementirana u frekvencijskoj domeni koristeći funkciju fft2 zbog veće robusnosti vodenog žiga.

Slika 5.33 prikazuje učitanu originalnu sliku i vodeni žig.

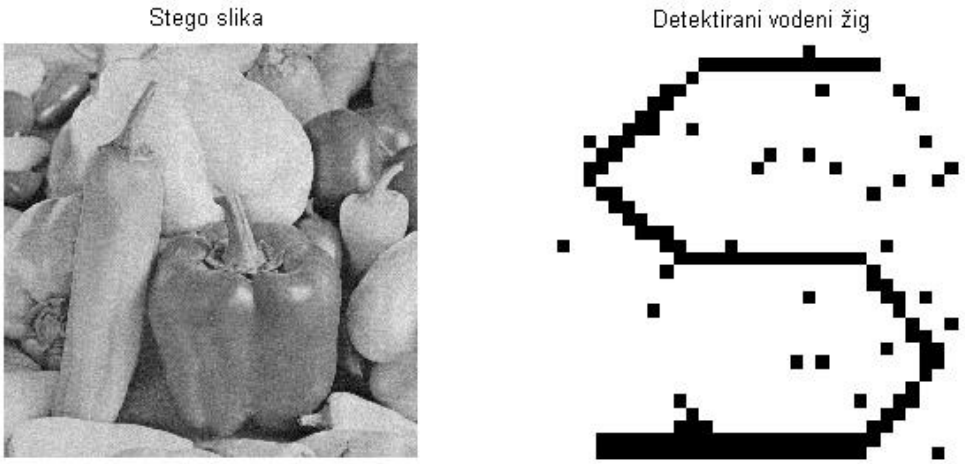


Slika 5.33 Originalna slika Peppers.tiff i vodeni žig S.bmp

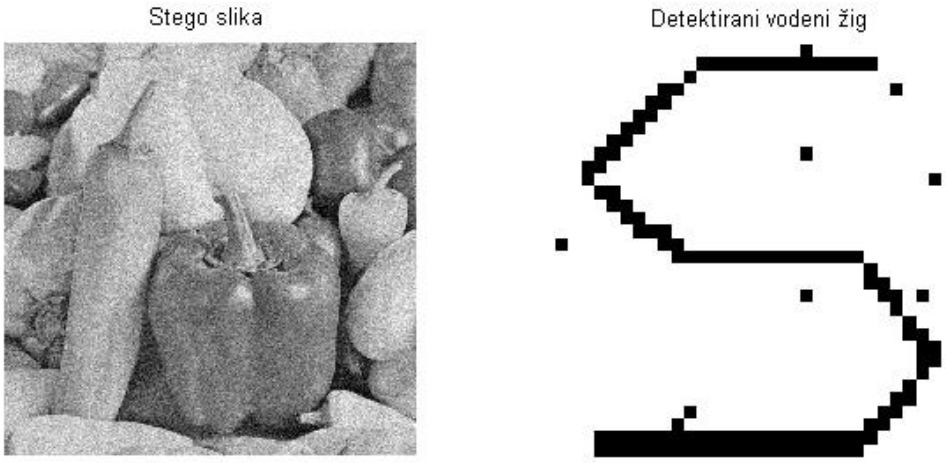
Na slikama 5.34 – 5.36 vidljiva je ovisnost kvalitete stego slike i detektiranog žiga o odabranoj gain vrijednosti. Na slikama 5.37 – 5.45 rezultati su detektiranja žiga sa dodanim distorzijama.



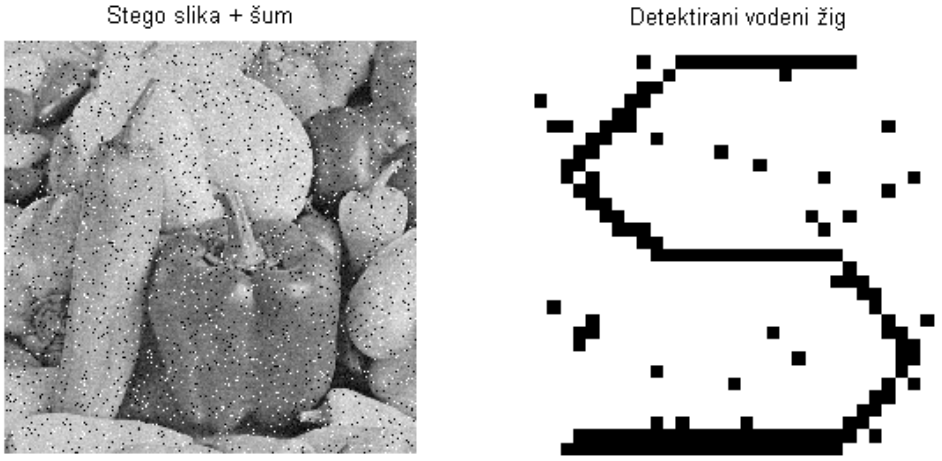
Slika 5.34 Stego slika i detektirani vodeni žig, gain=1



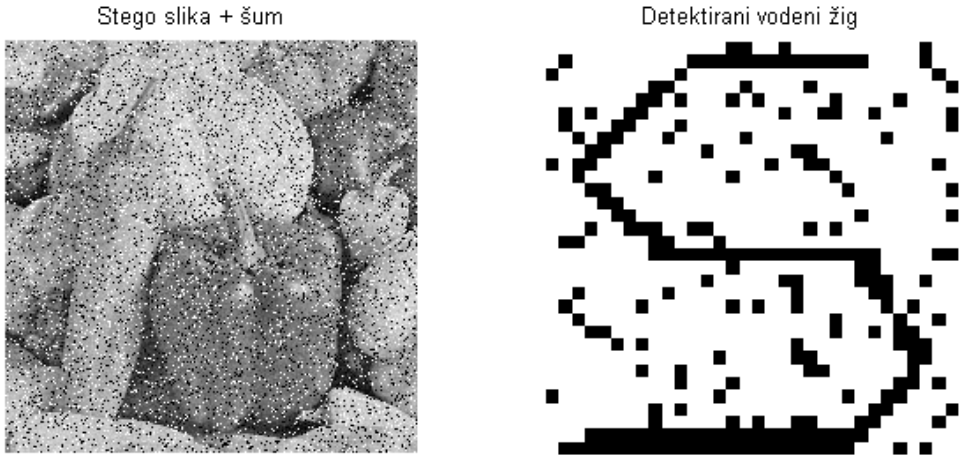
Slika 5.35 Stego slika i detektirani vodeni žig, gain=5



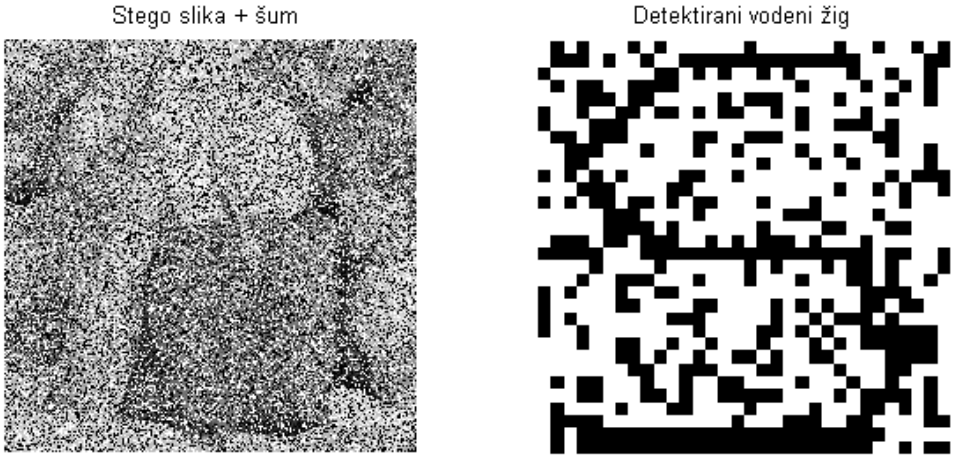
Slika 5.36 Stego slika i detektirani vodeni žig, gain=10



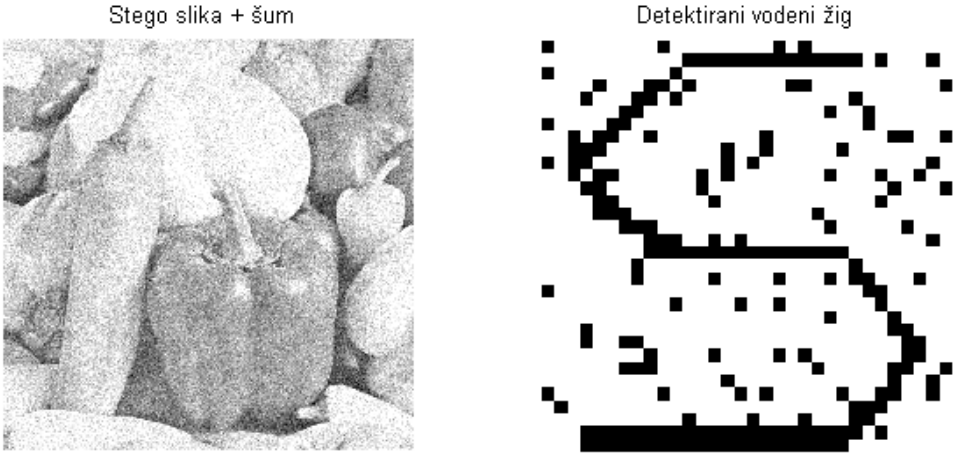
Slika 5.37 Salt & pepper šum (d = 0.05), gain=5



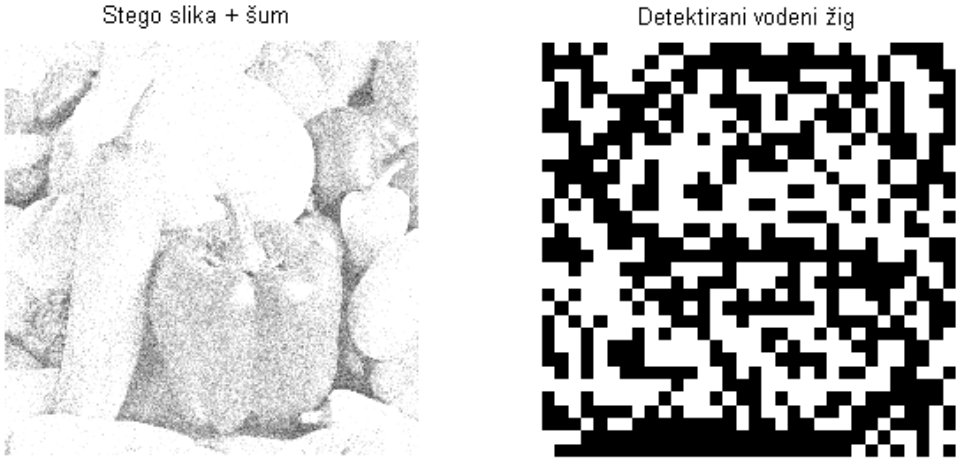
Slika 5.38 Salt & pepper šum (d = 0.15), gain=5



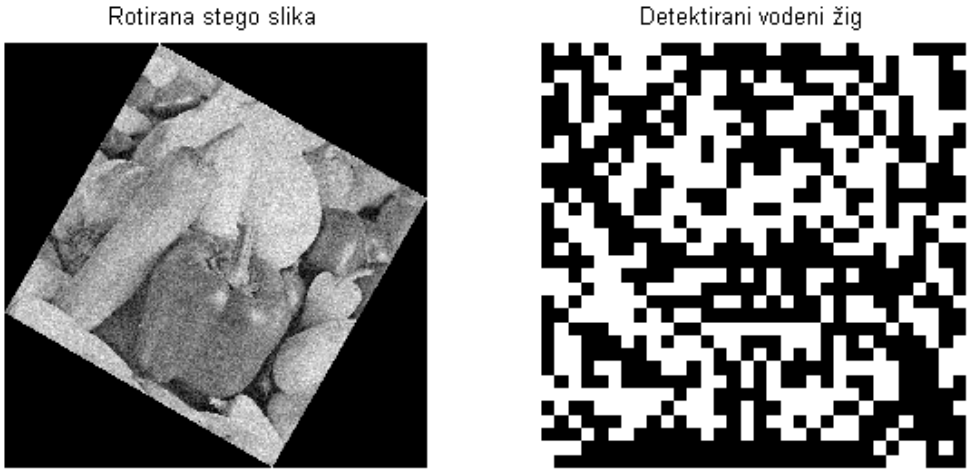
Slika 5.39 Salt & pepper šum (d = 0.5), gain=5



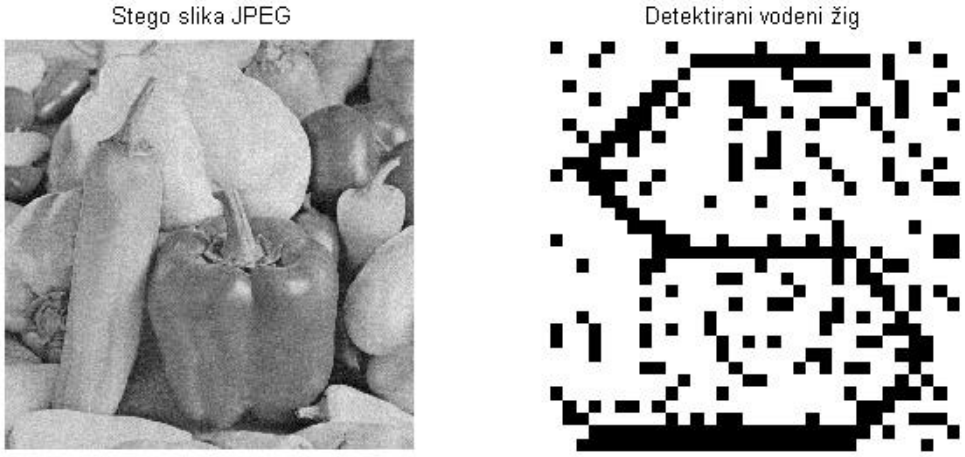
Slika 5.40 Gaussov šum (μ = 0.2, σ = 0.01), gain=5



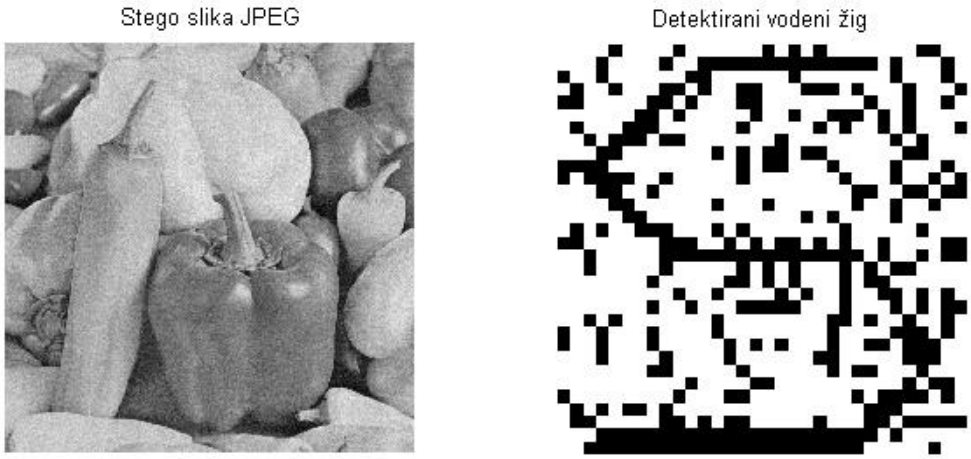
Slika 5.41 Gaussov šum (μ = 0.4, σ = 0.01), gain=5



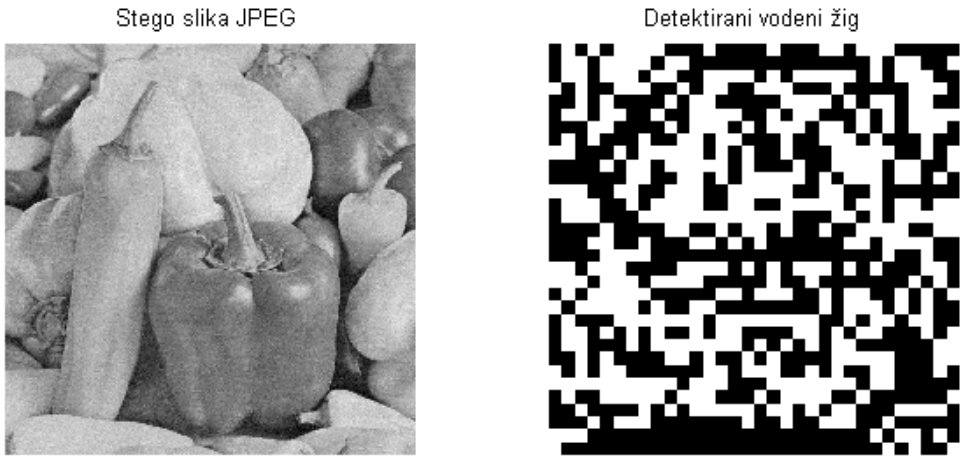
Slika 5.42 Rotacija (30°), gain=10



Slika 5.43 JPEG kompresija, q=100, gain=5



Slika 5.44 JPEG kompresija, q=90, gain=5



Slika 5.45 JPEG kompresija, q=70, gain=5

Tablica 5.3 prikazuje PSNR vrijednosti odnosa originalne i stego slike.

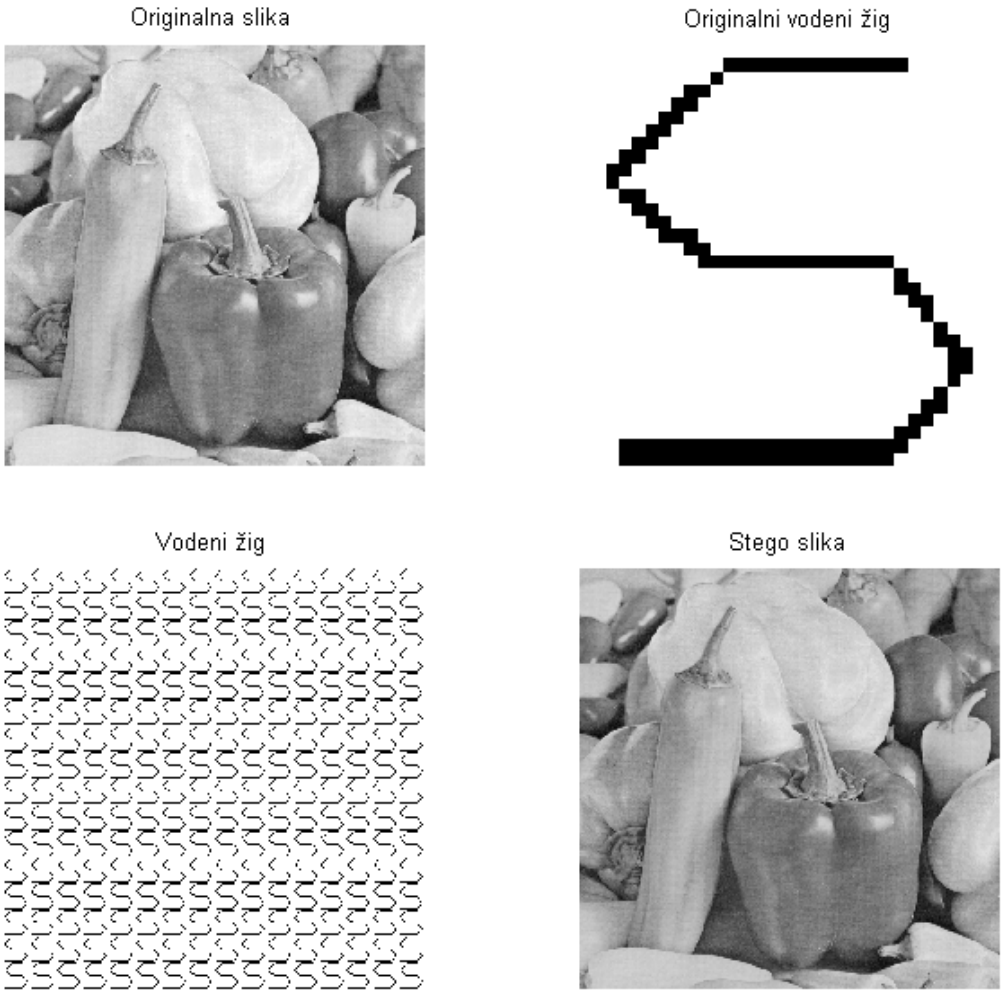
Tablica 5.3 Utjecaj distorzija na kvalitetu slike u CDMA metodi

DISTORZIJA	PSNR
Bez distorzije, gain=10	46.7172
Bez distorzije, gain=5	52.7378
Bez distorzije, gain=1	66.7172
Salt & pepper šum (d = 0.05)	65.7786
Salt & pepper šum (d = 0.15)	61.5457
Salt & pepper šum (d = 0.5)	56.4690
Gaussov šum (μ = 0.2, σ = 0.01)	61.5325
Gaussov šum (μ = 0.4, σ = 0.01)	57.4935
Rotacija (30°), gain=10	69.6509
JPEG kompresija, q=100	76.5034
JPEG kompresija, q=90	75.8752
JPEG kompresija, q=70	76.1986

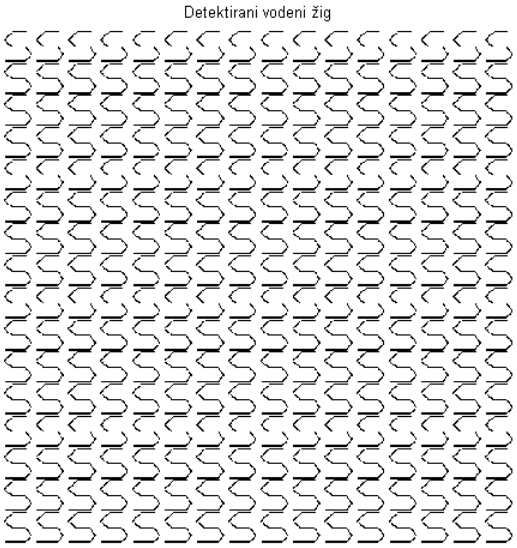
Na temelju prikazanih rezultata jasno je vidljiva kvaliteta i učinkovitost sakrivanja vodenog žiga CDMA metodom. Samo uz najizraženije distorzije dolazi do poteškoća sa čitanjem tajne poruke. Vizualne rezultate potvrđuju i PSNR vrijednosti koje odgovaraju standardim načinima kompresije koji se koriste pri slanju slikovnih datoteka.

5.5. Sakrivanje u DCT domeni

Posljednja metoda sakrivanja vodenog žiga u sliku također se izvodi u frekvencijskoj domeni, koristeći ugrađenu Matlab funkciju dct2. Nakon učitavanja, vodeni žig se skalira na veličinu originalne slike. Nad blokovima 8 x 8 provodi se DCT transformacija, koeficijentom a (služi za određivanje stupnja vidljivosti žiga u slici) skalira se DCT vrijednost žiga te se frekvencijski oblici originalne slike i vodenog žiga zbrajaju. Na strani primatelja potrebno je izračunati razliku između originalne i stego slike i tu razliku ponovno skalirati istom vrijednosti a kako bi žig postao vidljiv.

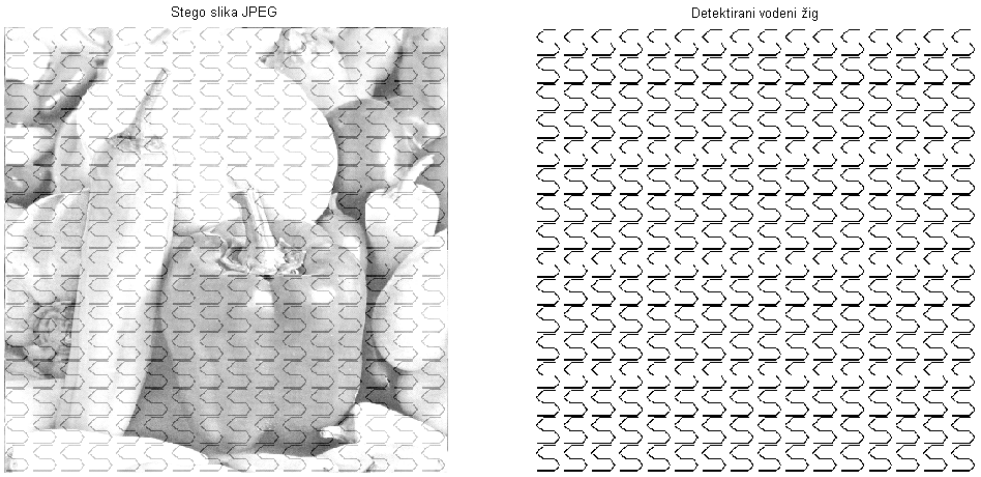


Slika 5.46 Originalna slika Peppers.tiff i vodeni žig S.bmp, a=0.01



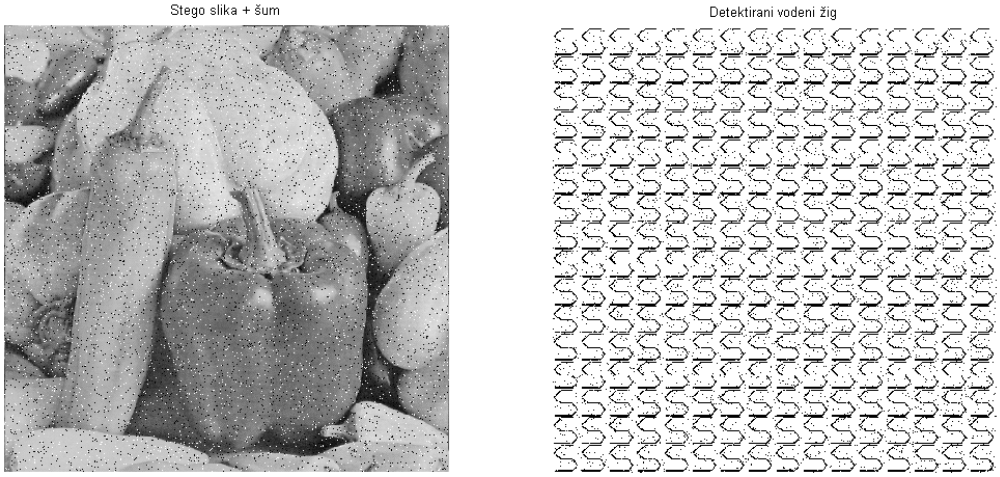
Slika 5.47 Detektirani vodeni žig

Slike 5.45 i 5.46 prikazuju originalnu sliku, skaliranje vodenog žiga, nastalu stego sliku i detektirani žig DCT metodom, a slika 5.47 slučaj kada je vrijednost skalirajućeg koeficijenta a=0.3.

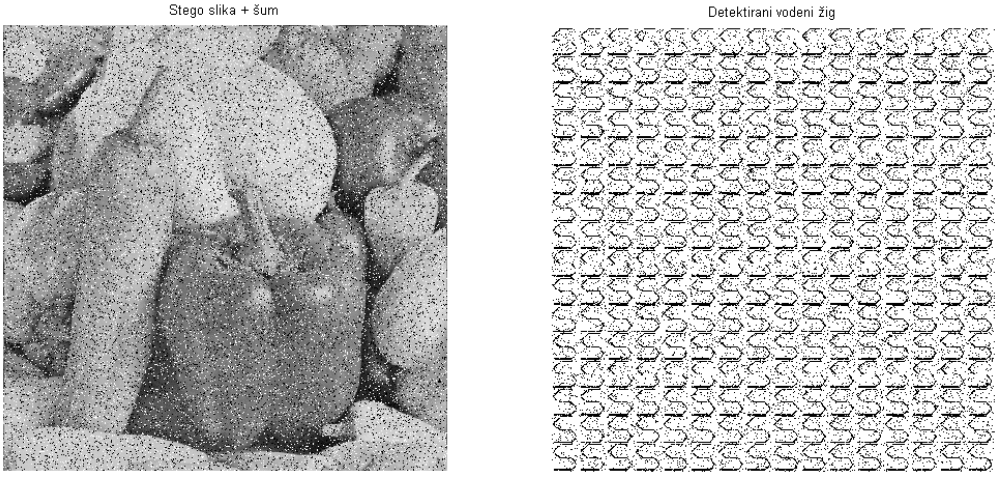


Slika 5.48 Stego slika i detektirani vodeni žig, a=0.3

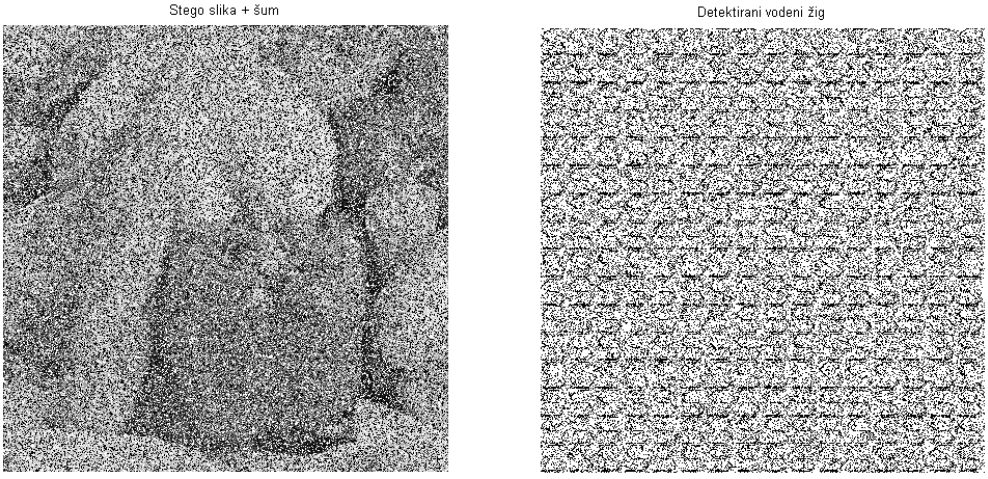
Na sljedećim slikama metoda je testirana na različite distorzije, a u tablici 5.4 dane su numeričke vrijednosti usporedbe originalne i stego slike.



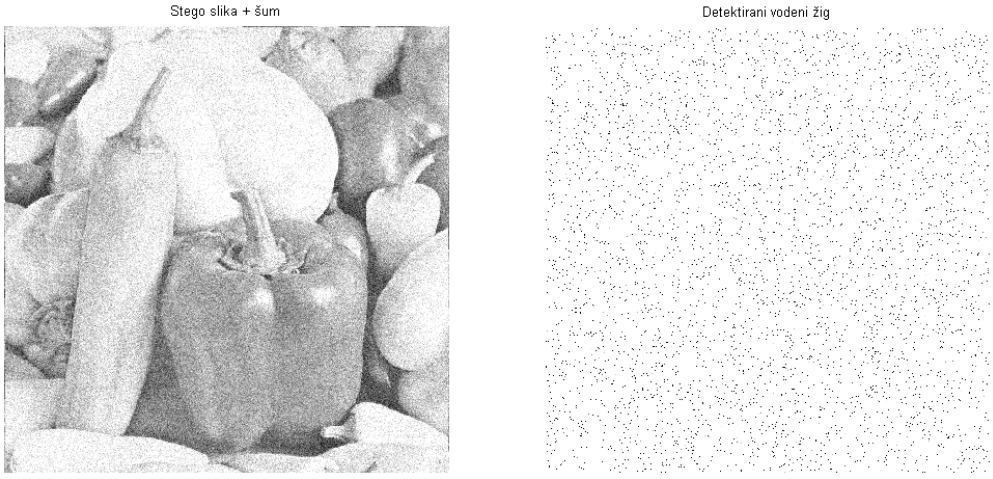
Slika 5.49 Salt & pepper šum (d = 0.05)



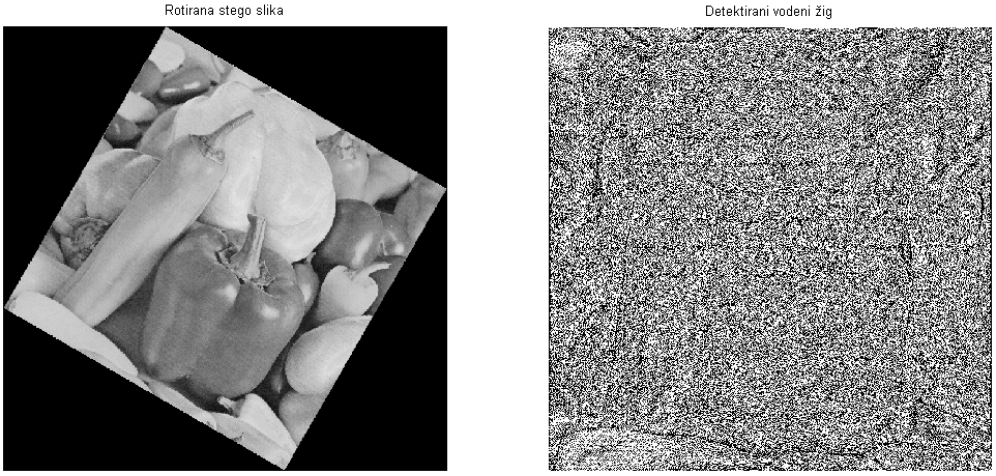
Slika 5.50 Salt & pepper šum (d = 0.15)



Slika 5.51 Salt & pepper šum (d = 0.5)

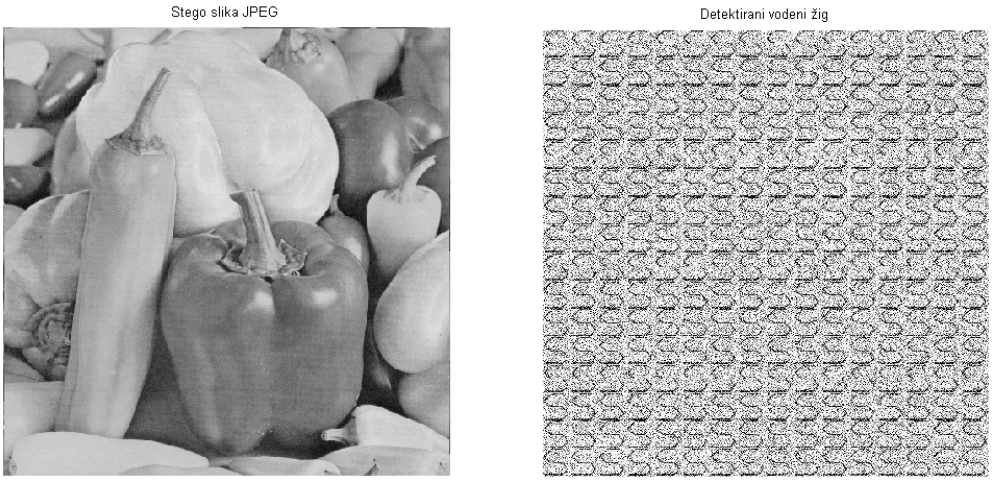


Slika 5.52 Gaussov šum (μ = 0.2, σ = 0.01)

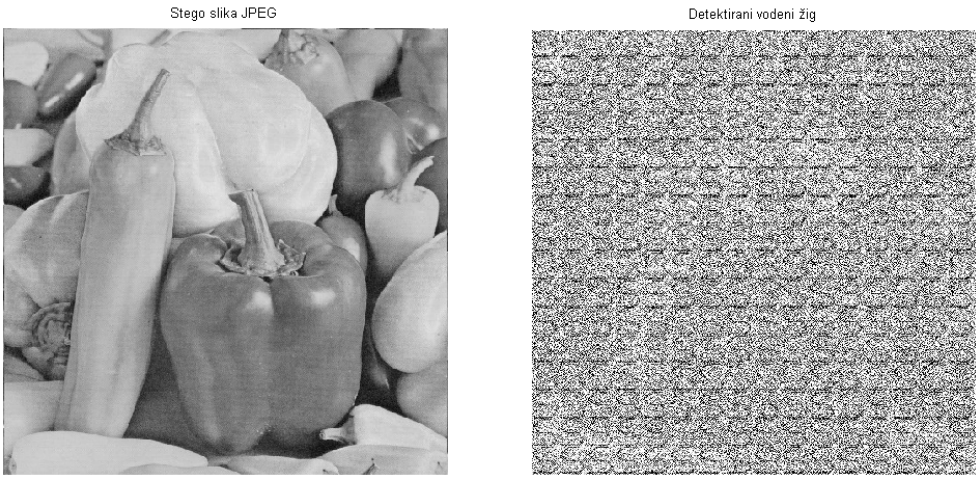


Slika 5.53 Rotacija (30°)

Slika 5.54 JPEG kompresija, q=100



Slika 5.55 JPEG kompresija, q=95



Slika 5.56 JPEG kompresija, q=90

Tablica 5.4 Utjecaj distorzija na kvalitetu slike u DCT metodi

DISTORZIJA	PSNR
Bez distorzije	88.6721
Bez distorzije, a=0.3	59.1297
Salt & pepper šum (d = 0.05)	66.4823
Salt & pepper šum (d = 0.15)	61.7532
Salt & pepper šum (d = 0.5)	56.5291
Gaussov šum (μ = 0.2, σ = 0.01)	61.4381
Rotacija (30°)	75.2567
JPEG kompresija, q=100	87.1978
JPEG kompresija, q=95	85.6100
JPEG kompresija, q=90	83.4603

U DCT metodi prisutstvo vodenog žiga vidljvim okom se ne može otkriti, a to i potvrđuju PSNR vrijednosti u gornjoj tablici. Nakon što je određena optimalna vrijednost skalirajućeg koeficijenta a, i sakrivanje i detekcija daju jako dobre rezultate. Na određene distorzije implementirana metoda nije otporna, dok kod JPEG kompresije žig može biti detektiran do određene granice.

Zaključak

Testiranjem različitih algoritama i tehnika steganografije, može se zaključiti kako su metode sakrivanja vodenog žiga u prostornoj domeni jednostavnije za implementaciju, no i poprilično neotporne na distorzije. Za JPEG kompresiju koja se u digitalnom svijetu trenutno najčešće koristi, rekonstruirane tajne poruke nisu davale dovoljno zadovoljavajuće rezultate. Sa druge strane, metode implementirane u frekvencijskoj domeni generirale su stego slike robusne na obradu i kompresiju te se preporuča njihovo korištenje u daljnjem radu. Uz razvoj i poboljšanje tehnika i metoda steganografije, paralelno napreduju i načini otkrivanja i uklanjanja kriptirane informacije u stego datotekama. Iz tog razloga istraživanja i novi načini sakrivanja vodenog žiga ili tajne poruke mogu (a i moraju) odvesti steganografiju kao znanost na jednu potpuno novu razinu.

_____

Sandra Šumiga, univ. bacc. ing. comp.

Literatura

[1] Wikipedia, Steganography, http://en.wikipedia.org/wiki/Steganography, 12.5.2014.

[2] Cummins, J., Diskin, P., Lau, S., Parlett, R., *Steganography And Digital Watermarking*

[3] Dunbar, B. *A Detailed look at Steganographic Techniques and their use in an Open-Systems Environment*

[4] *Digital signatures and steganography*, http://www.itandquran.com/8_6DigiSig.htm, 1.6.2014.

[5] Gite, B. B., Choksey, D., Jambhulkar, M., Ramath, R., Jhamvar, Y., *Data Hiding Using Steganography And Authentication Using Digital Signatures And Facial Recognition*

[6] Wikipedia, Digital signature, http://en.wikipedia.org/wiki/Digital_signature, 9.6.2014.

[7] http://inventors.about.com/od/copyrights/a/CopyrightNotice.htm, 9.6.2014.

[8] Koch, E., Zhao, J., *Towards Robust and Hidden Image Copyright Labeling*

[9] Horak, G., Murat, I., Domazet, M*., Digitalni vodeni žig*

[10] Weiss, M., *Principles of Steganography*

[11] Gurpreet, K., Kamaljeet, K., *Image Watermarking Using LSB*

[12] Bora, A., Dalshania, N., Bhongle, A., *Competitive Analysis of Digital Image Watermarking Techniques*

[13] Thanki, R., Kher, R., Vyas, D., *Robustness of Correlation Based Watermarking Techniques Using WGN against Different Order Statistics Filters*

[14] Fang, Y., Huang, J., Shy, Y., *Image Watermarking Algorithm Applying CDMA*

[15] Mandhani, N.K., *Watermarking Usign Decimal Sequences*

[16] Johnson, N., Katzenbeisser S., *A Survey of Steganographic tehniques*

[17] Vallabha, V.H., *Multiresolution Watermark Based on Wavelet Transform for Digital images*

Sažetak

Steganografija i vodeni žig u zaštiti digitalnih fotografija

U ovom radu su nakon općih definicija i pregleda povijesti i razvoja steganografije opisane najpoznatije i najčešće korištene metode sakrivanja digitalnog vodenog žiga te njihove primjene. Steganografija osim za tajnu komunikaciju služi i za zaštitu od ilegalnog korištenja autorskih djela te njihovo umnožavanje i distribuiranje. Zaštićena oznaka autorskog prava (*copyright*) može biti vidljiva ili nevidljiva korisniku. Vidljive vodene žigove je lako ukloniti no sakriveni moraju biti dodatno zaštićeni i otporni na različite distorzije koje bi mogle biti korištene u svrhu njegovog detektiranja ili uklanjanja.

U drugom dijelu rada implementirane su tehnike injektiranja informacije u sliku, LSB metoda, metoda bazirana na korelaciji i CDMA te korištenje DCT transformacije. Rezultati su prikazani slikama i tablicama i na temelju toga su doneseni zaključci. Korišteno programsko okruženje je Matlab 2013b.

KLJUČNE RIJEČI: steganografija, vodeni žig, zaštita, autorska prava, distorzije, JPEG kompresija, Matlab

Abstract

Steganography and digital watermarking for digital images

This thesis describes steganography, as its history, development and the most common and most widely methods of hiding watermarks in digital photography. Other than secret communication, steganography is used to protect copyrighted data against illegal use, reproduction and distribution. Copyright label can be visible or hidden inside the file. Visible watermarks can be easy to remove, so hidden ones have to be fully protected and robust to various distortions used for detecting or removing them.

The second part of the paper presents implementation in Matlab and test results based on the earlier described steganography methods (injection, LSB, correlation, CDMA and DCT transformation).

KEY WORDS: steganography, watermark, security, copyright, distortion, JPEG compression, Matlab

Privitak

[1] CD sa .zip datotekom koja sadrži:

- izvorni primjerak Diplomskog zadatka
- .pdf datoteku Diplomskog rada
- .docx datoteku Diplomskog rada
- Matlab skripte
- korištene slike