Sveučilište u Zagrebu

Fakultet elektrotehnike i računarstva

STEGANOGRAFIJA

Dokumentacija

Marko Arsenović

Alan Avanić

Denis Kunšt

Tomislav Kranjčec

Zagreb, siječanj 2011.

Uvod

Steganografija je znanost skrivanja i slanja informacija na prividno bezazlen način kako bi se sakrilo samo postojanje te informacije. Steganografija je vrlo slična kriptografiji, obje znanosti se koriste kao sredstva koja prikrivaju informaciju. No, za razliku od kriptografije, steganografija ne mijenja samu informaciju, nego ju „kamuflira“ i samim time ne privlači pažnju na nju. Kriptirana informacija, koliko god dobro kriptirana, vidljivo postoji, te budi sumnju i radoznalost. Cilj kriptografije je promijeniti informaciju do te mjere da je ona nerazumljiva trećoj strani, a cilj steganografije je učiniti informaciju nevidljivom trećoj strani. Steganografija se koristi još od vremena Antičke Grčke, no razvojem računalne znanosti poprimila je novu dimenziju. Dotad su se koristile skrivene tetovaže, nevidljive tinte, mikrotoćke, beznačajne (null) šifre, a otada se informacije skrivaju unutar tekstova, slika, audia, videa, mrežnog prometa i protokola i sl.

Metoda primjene steganografije je jednostavna. Informaciju sakrivamo pomoću određenog stego-ključa unutar nekog medija (najčešće slike ili audio datoteke) te tako dobivamo stego-medij. Najčešće ključem zamjenjujemo nepotrebne bitove unutar slike ili zvuka sa porukom koju prikrivamo. Zbog toga je veličina te poruke ili informacije relativno ograničena. Dvije najčešće metode su LSB (least significant bit) i injektiranje.

Steganografija se legalno koristi kada kriptografija nije dopuštena, ili češće, kao dodatak kriptografiji; kriptirana poruka se sakriva unutar medija kako bi se sakrilo njeno postojanje.
Njena primjena je raznolika. Može se koristiti kako bi spojila slike i tekstualne bilješke vezane uz sliku (nešto poput post-it bilješkama na papirima) ili kako bi održala povjerljivost značajnih informacija čuvajući ih od sabotaže, krađe ili nedopuštenog gledanja. Također, steganografija ima i nelegalnu svrhu u špijuniranju, dječjoj pornografiji i teoretski terorizmu (2001. godine su mainsream novine nedokazano i neprovjereno gurali vijest da su teroristi koristili steganografiju u svojoj komunikaciji). Najznačajnija i najčešća upotreba je u digitalnim vodenim žigovima koji služe za zaštitu prava.

Postoje više različitih programa koji sakrivaju digitalnu informaciju, poput Blindsidea, Digital Picture Envelopea, Gifshuffle, Hide4PGP, JPHIDE and JPSEEK, MP3Stego, OutGuess, Snow, Steganos, Stego, StegParty i F5-a. Također postoje i vrlo slični programi za stegoanalizu, koji pokušavaju detektirati steganografiju i uništiti sakrivenu poruku.

U ovom praktičnom radu skrivali smo vodeni žig različitim metodama skrivanja u sliku, te isti otkrivali iz slike. Pri tome smo uspoređivali otpornost pojedine metode skrivanja na različite operacije nad slikom.

Digitalni vodeni žig

Prelaskom analize i obradbe podataka (slika, video, audio, tekst) iz analogne u digitalnu domenu postalo je nemoguće razlikovati izvorne podatke od kopija. Samim time zaštita autorskih prava i vlasništva postala je poprilično otežana. Javila se potreba za mogućnošću razlikovanja izvornog podatka od kopiranih i tu na scenu stupa digitalno označavanje podataka. Digitalno označavanje je pojam koji označava postupak umetanja digitalnog žiga u digitalni dokument s namjerom kasnijeg detektiranja ili vađenja žiga.

Iako je područje digitalnih vodenih žigova još uvijek slabo istraženo, danas postoje algoritmi za zaštitu svake vrste digitalnih medija: tekstualnih dokumenata, slika, video i audio signala, 3D modela, mapa i kompjutorskih programa. Zanimljivo je da tehnika vodenih žigova nije ograničena samo na digitalne medije, već se može primijeniti i na, primjerice, kemijske podatke kao što je struktura proteina.
Žig se može umetati u bilo koji dokument pomoću algoritma kodiranja, dok se algoritmom dekodiranja žig vadi iz označenog dokumenta i jednoznačno se određuje vlasnik i integritet dokumenta.
Prema „vizualnoj“ percepciji razlikuju se četiri skupine vodenih žigova. Kod vidljivog vodenog žiga na izvornom dokumentu je vidljiv žig u obliku logo oznake. Robustan nevidljiv vodeni žig je vizualno nevidljiv, ali ga dekoder može detektirati, a uz to je otporan na napade. Kod lomljivog nevidljivog žiga žig je također nevidljiv, ali se može detektirati i nije otporan ni na jednu vrstu napada. Dvostruki vodeni žig je kombinacija vidljivog i nevidljivog vodenog žiga.

Digitalni vodeni žigovi mogu se koristiti za dokazivanje autentičnosti podataka. Za to se najčešće koriste nevidljivi lomljivi vodeni žigovi. Digitalni žigovi su korisni i pri praćenju emitiranja programa na televiziji, radiju i sličnim uređajima. Žig se dodaje u sadržaj emitiranja i može poslužiti kao identifikator određenog sadržaja. Ta funkcija žiga je, primjerice, korisna kod prebrojavanja emitiranih reklama čime se oglašivači osiguravaju da su platili samo emitirane reklame.
Postoje određene primjene u kojima dodatna informacija o digitalnom sadržaju treba

sadržavati informacije o krajnjem korisniku, a ne o vlasniku sadržaja. Problem identificiranja izvora curenja informacija može se riješiti distribuiranjem neznatno različitih kopija svakom primatelju. Svaka kopija jedinstveno je vezana uz osobu koja ju treba primiti. Primjer takve zaštite može se pronaći u filmskoj industriji kod distribucije filmova različitim kinima. Svako kino dobije svoju kopiju filma i ako piratska inačica filma izađe u javnost može se otkriti iz kojeg je kina potekla.

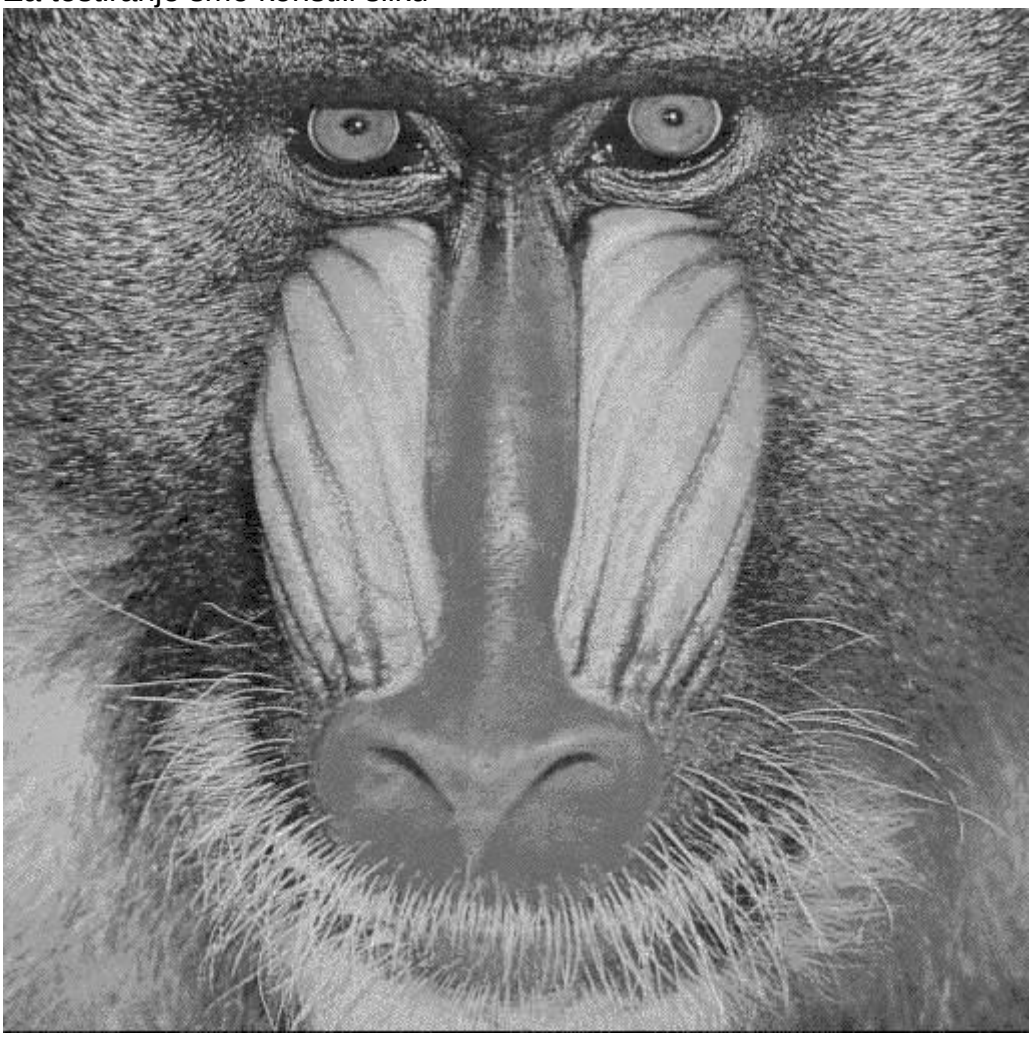
Sigurnost digitalnih vodenih žigova govori koliko su oni otporni na razne vanjske napade. Napadi su različite prirode, a neki od njih su JPEG kompresija, geometrijske transformacije (rotacija, odrezivanje, skaliranje, …) te operacije za poboljšanje kvalitete slike.

Modifikacija sa bitom najmanjeg značaja

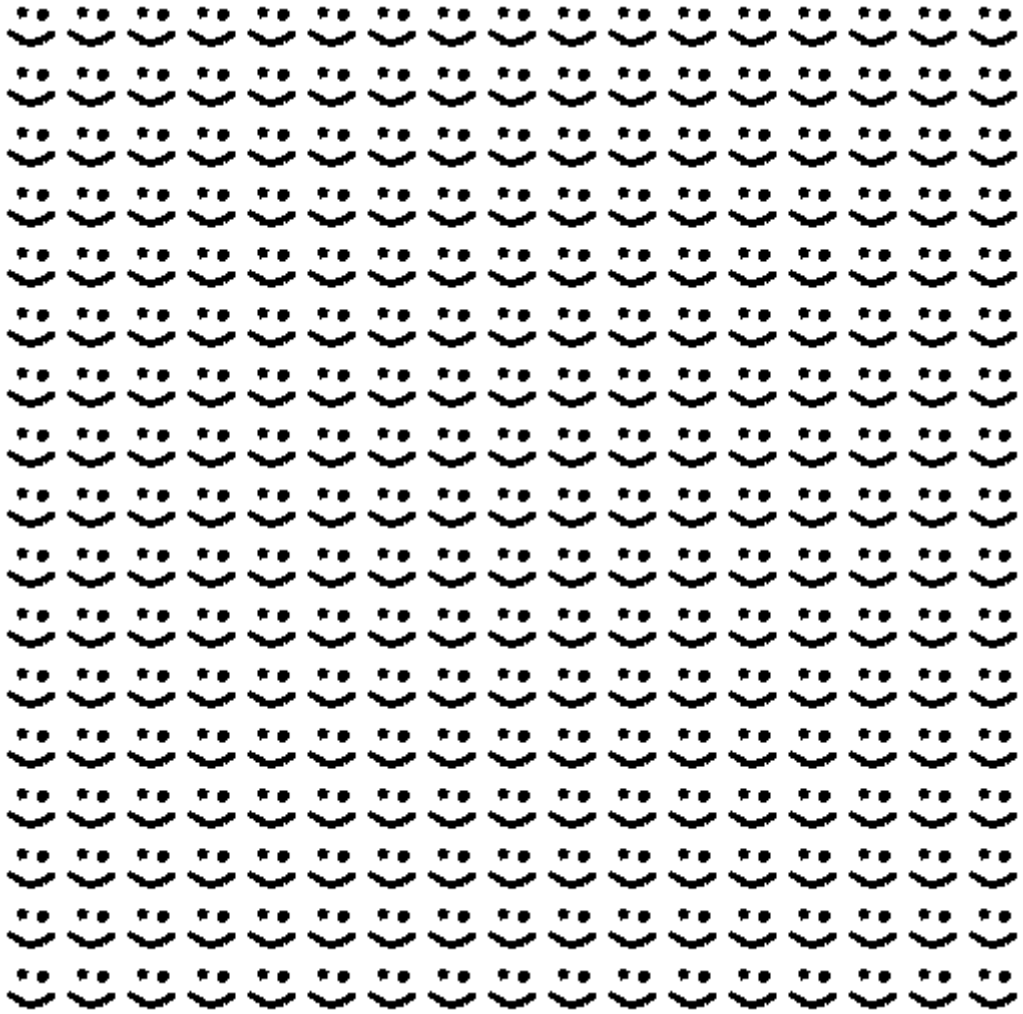
LSB (*least significant bit*) supstitucija jedna je od najčešćih steganografskih tehnika - najmanje značajni bitovi odabrane prikrivne datoteke zamijene se bitovima tajne poruke. Ova tehnika se lako primjenjuje na slikovne datoteke. Velika količina informacija može se sakriti malim ili potpuno neuočljivim utjecajem na datoteku nositelja skrivene informacije. Na primjer, želimo li sakriti poruku u svaki bajt 24-bitne slike, možemo spremiti 3 bita u svaki piksel (1 bit u kanal svake boje). Slika dimenzija 1024x768 piksela može sakriti $1024 \cdot 768 \cdot 3 = 2359296$ bitova informacija. To je 294912 bajta ili 288 kilobajta informacija. To je velika količina, no *stegoslika* ljudskom oku izgleda identično kao i original.
Ako želimo sakriti tajnu poruku unutar slikovne datoteke, prvi korak je odabir prikrivne datoteke. Nakon što su prikrivna datoteka i tajna poruka odabrane, bira se podskup najmanje značajnih bitova prikrivne datoteke (skup prikrivnih bitova). Broj bitova u odabranom skupu odgovara broju bitova tajne poruke. Tada se nekim redoslijedom svaki prikrivni bit zamjenjuje bitom tajne poruke, sve dok svi nisu zamijenjeni. U najjednostavnijem slučaju LSB supstitucije tajni se bitovi pohrane u najmanje značajni bit (LSB) svakog piksela po redu.

Da bi rekonstruirao poruku, primatelj mora znati podskup najmanje značajnih bitova u koje je poruka skrivena. Tehnikom obrnutom od umetanja "izvlači" najmanje značajne bitove, slaže ih pravim slijedom i dobiva poruku.
Kada bismo tajnu poruku ovom metodom skrivali u 2, 3 ili 4 najmanje značajna bita elemenata prikrivne datoteke, još uvijek bi ljudsko oko teško moglo primijetiti razliku u odnosu na original.

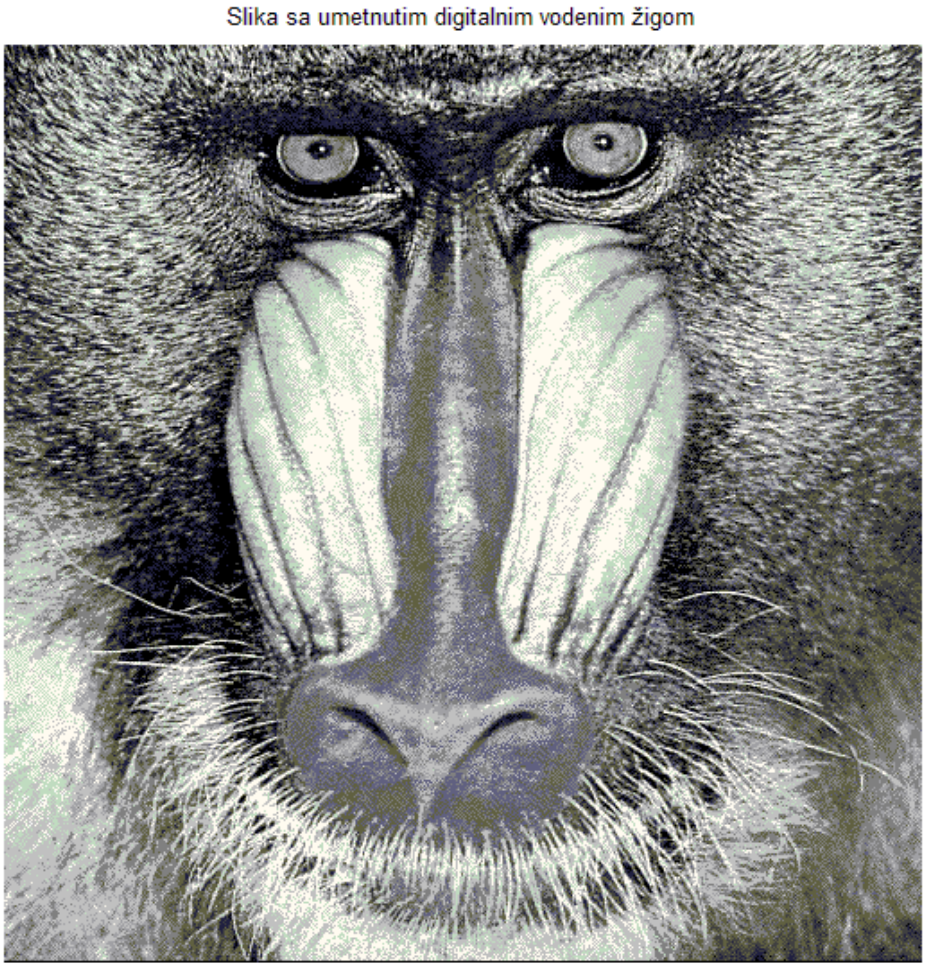
Za testiranje smo koristili sliku



I unutar nje smo sakrili vodeni žig

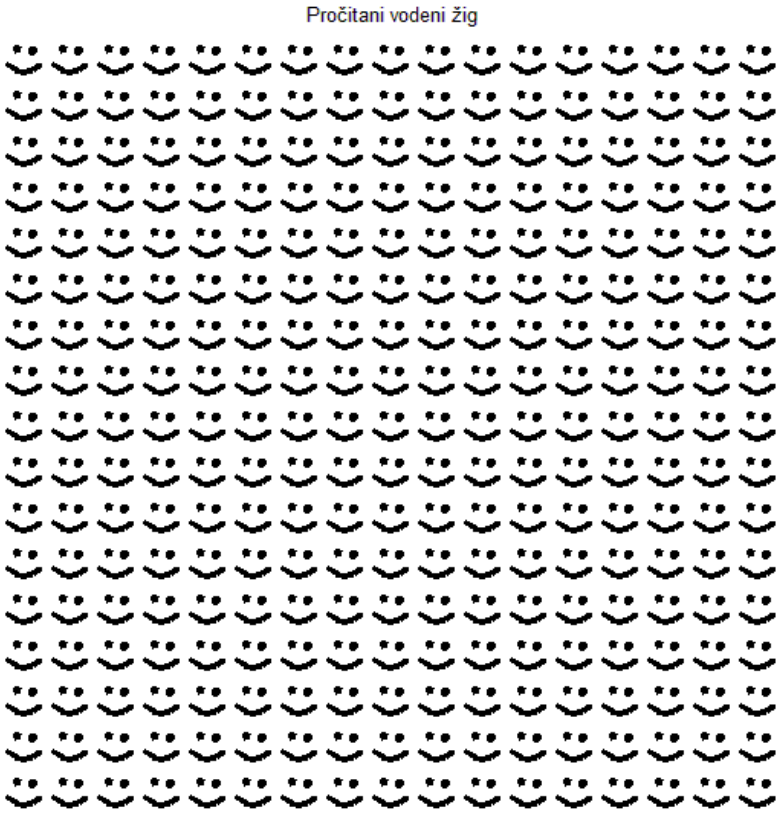


Slika sa sakrivenim vodenim žigom izgleda

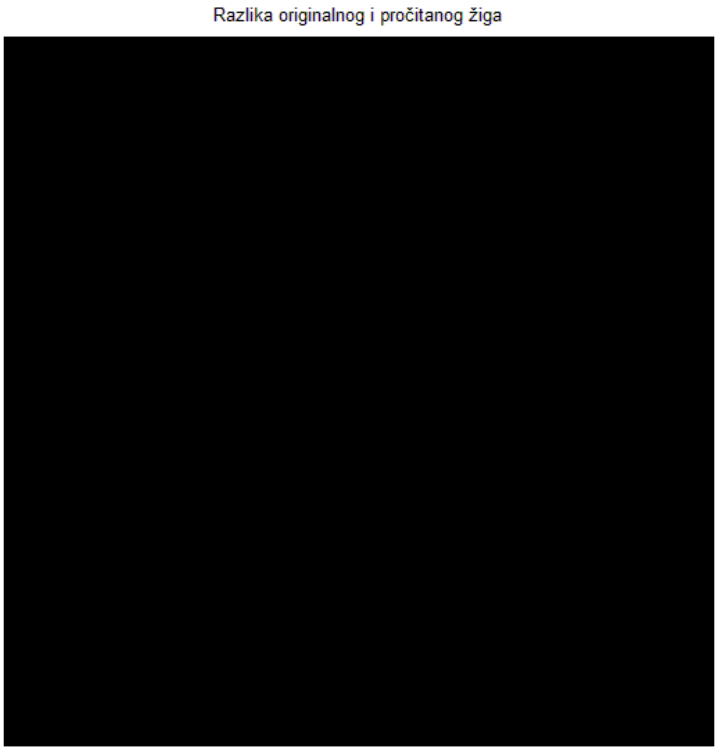


Slika 1

Skrivanje žiga trajalo je 1.2168s , a PSNR (engl. Peak signal-to-noise ratio - omjer najviše vrijednosti signala i razine šuma) je iznosio 1.0181e+004.
Iz te slike smo očitali vodeni žig. Očitavanje je trajalo 0.7488s. A rezultati se nalaze na slijedećim slikama.



Slika 2 – pročitani vodeni žig



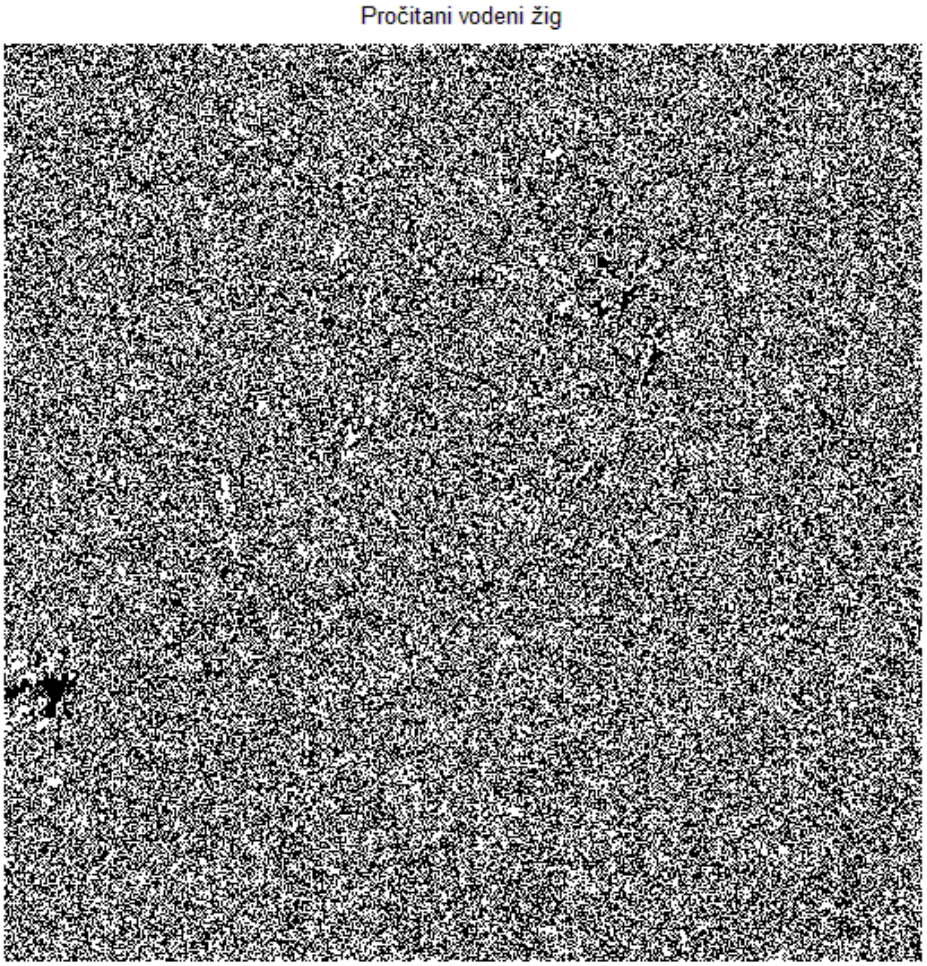
Slika 3 – razlika originalnog i pročitanog vodenog žiga

Zatim smo napravili različite modifikacije na slici koja je u sebi sadržavala vodeni žig i pokušali iz modificirane slike očitati vodeni žig kako bismo procijenili koliko je LSB metoda dobra za različite slučajeve.

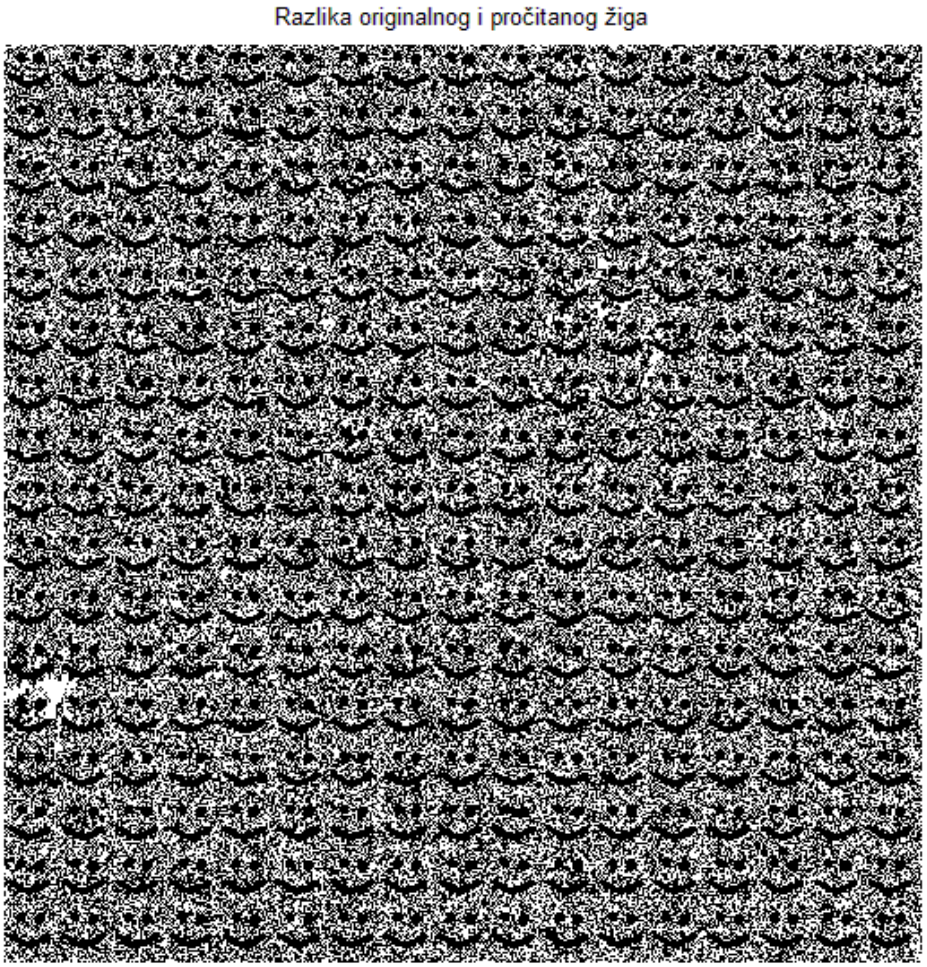
Prvo smo:

1) Dodali smo Gaussian Blur (odgovara niskopropusnom filtriranju) u najmanjoj vrijednosti od 3x3

Te smo dobili slijedeće rezultate



Slika 4

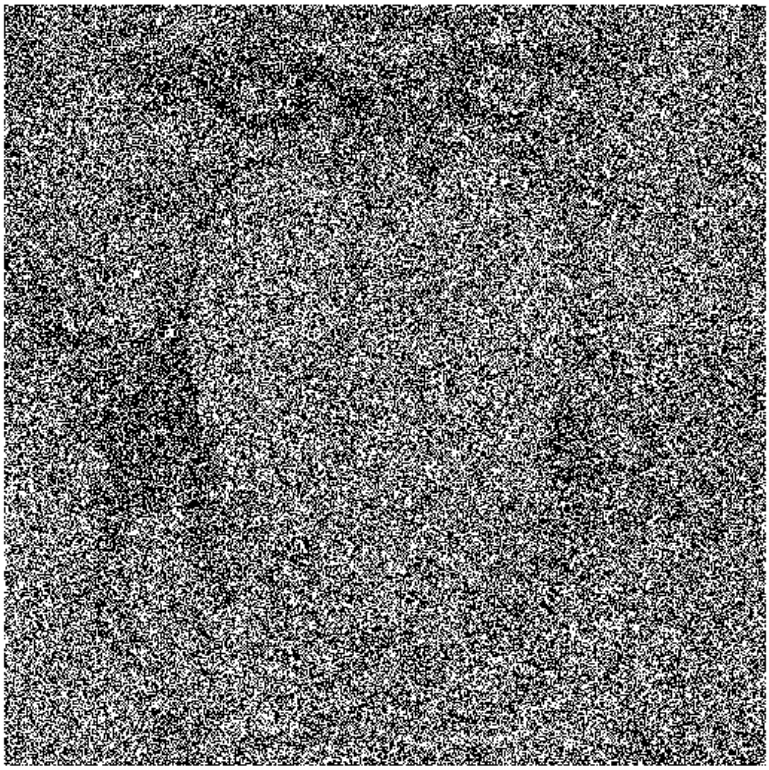


Slika 5

otkrivanje je trajalo 0.5928s te možemo vidjeti da je žig potpuno izgubljen kao što smo i očekivali.

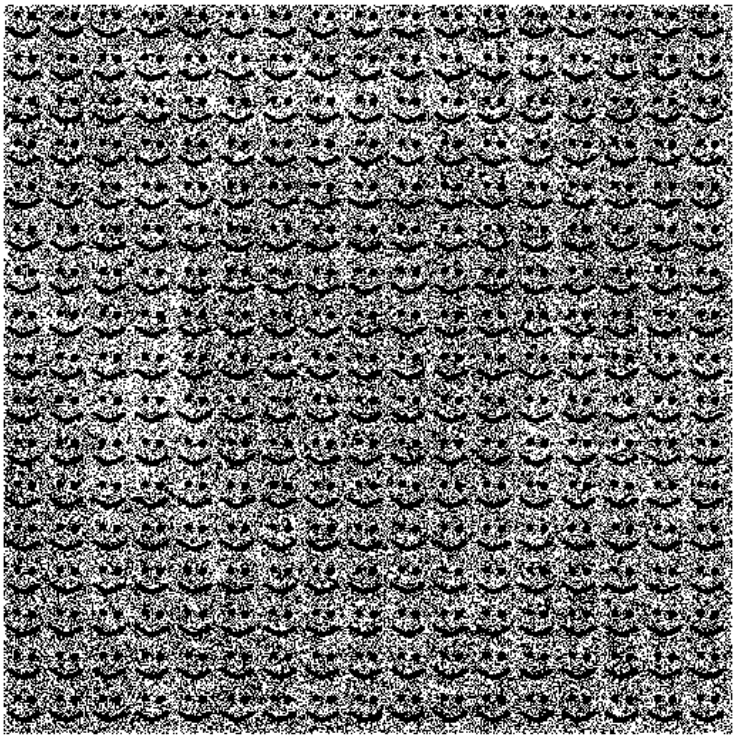
2) Dodali smo Gaussian Noise (Gaussov šum) također u najmanjoj vrijednosti od 1%, te smo očitali slijedeće slike. Otkrivanje je trajalo 0.6240s. vidimo da je žig u potpunosti izgubljen.

Pročitani vodeni žig



Slika 6

Razlika originalnog i pročitanog žiga

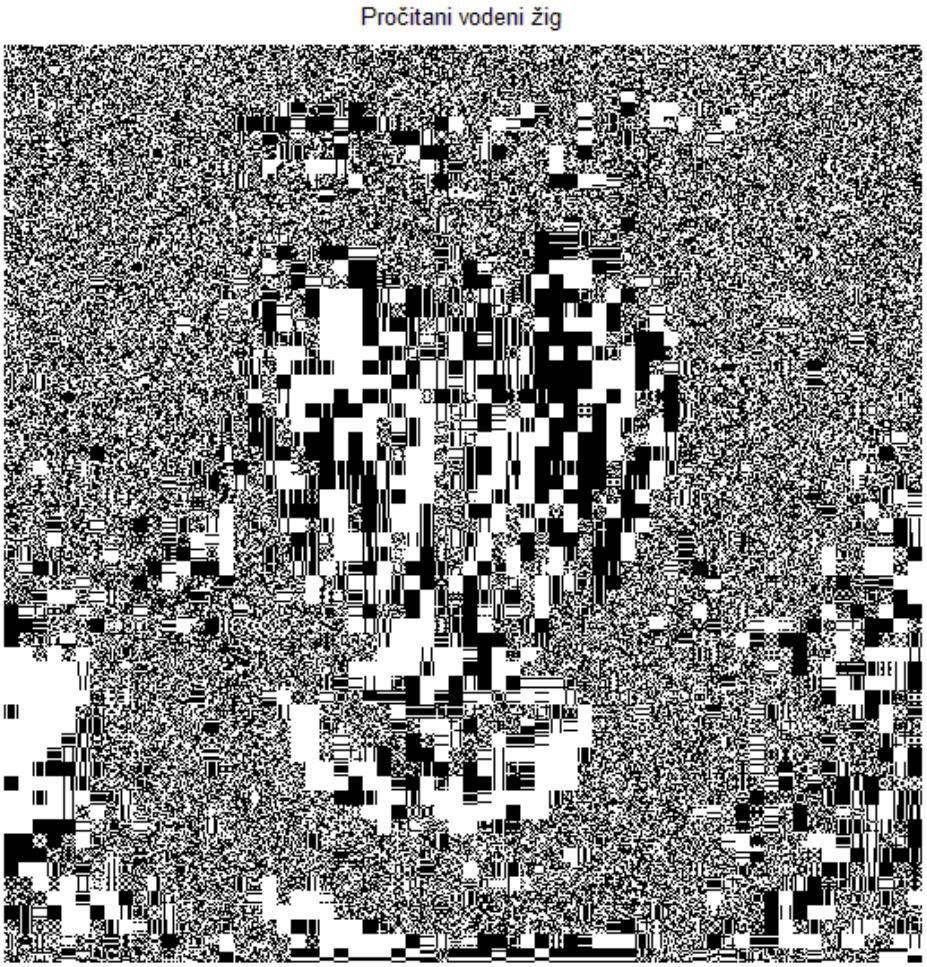


Slika 7

3) Spremali smo sliku s različitim stupnjevima jpeg kompresije. Rezultati se nalaze u slijedećoj tablici.

Stupanj kompresije	Vrijeme otkrivanja [s]	Vidiljivost žiga
20%	0.5928	nečitljiv
10%	0.5460	nečitljiv
0.1%	0.4836	nečitljiv

Izgled očitanog vodenog žiga nakon svih stupnjeva kompresije je približno jednak, tako da zaključujemo da primjena kompresije na ovoj metodi u potpunosti uništava sakrivenu tajnu poruku u slici.



Slika 8 –očitani vodeni žig nakon kompresije

4) Rotacija slike
Zarotirali smo sliku za 0.5°, rezultat je opet bio nečitljiv vodeni žig. Čitanje je trajalo 0.5976s.

5) Rezanje piksela
Sliku smo odrezali za 10 piksela vodoravno i vertikalno, te smo bez problema za 0.6214s pročitali vodeni žig.

Možemo zaključiti kako je LSB metoda jako osjetljiva na bilo kakvu promjenu nad slikom, te se iznimno lako može uništiti bez ikakvih vidljivih promjena na slici u koju je postavljen. Jedna od dobrih osobina kod LSB-a je kapacitet koji ima omjer 1:1 u korelaciji s veličinom slike u koju postavljamo vodeni žig.

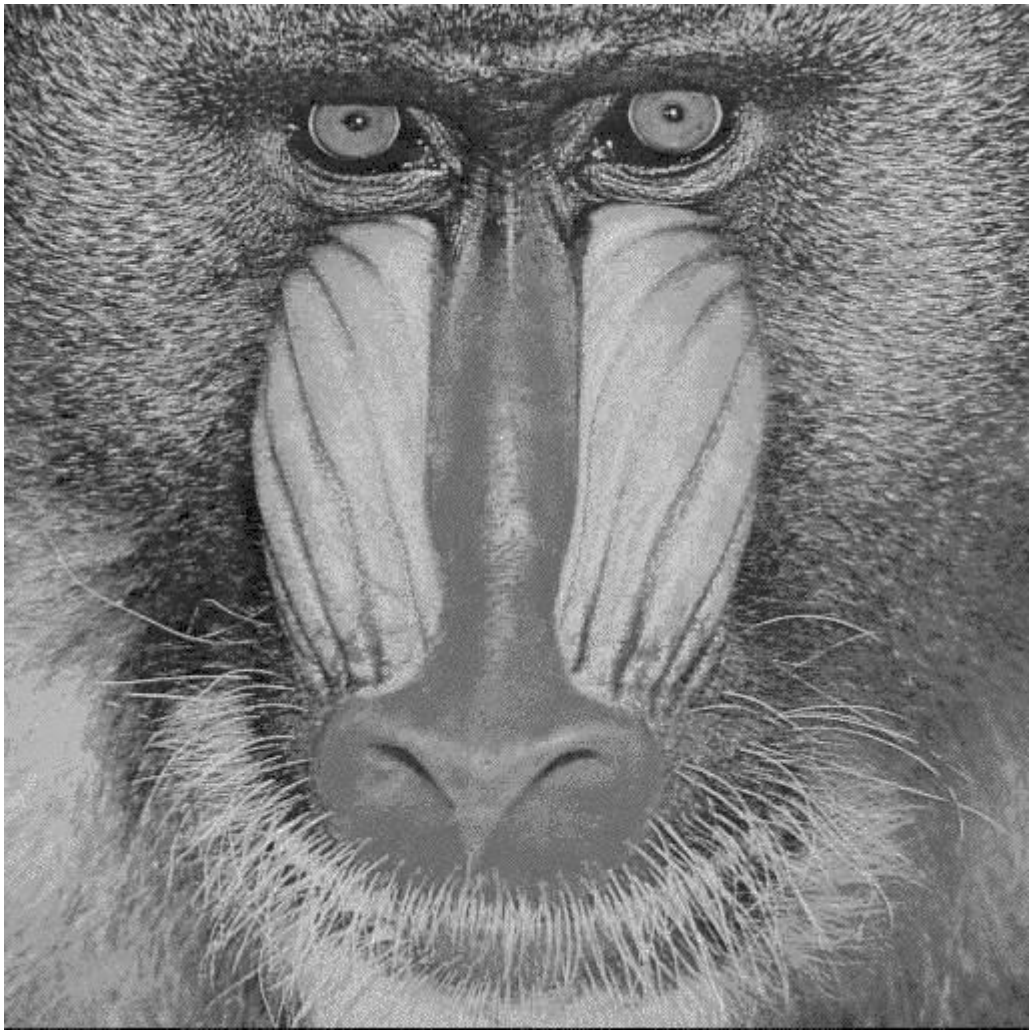
Modifikacija bazirana na korelaciji

Još jedna tehnika za ugradnju vodenog žiga je vrednovanje korelacijskih svojstava dodanog pseudoslučajnog šuma.
Da bismo preuzeli vodeni žig, koristimo algoritam sa generatorom pseudo-slučajnog šuma te ga punimo sa istim ključem, izračunavamo korelaciju između šuma i eventualnog uzorka sakrivenog u slici. Ako korelacija prelazi određeni prag T, vodeni žig se otkriva, a jedan bit se postavlja. Ova metoda se može lako proširiti podjelom slike u blokove, te obavljanjem prije navedenog postupka za svaki blok nezavisno. Ovaj osnovni algoritam može se poboljšati na nekoliko načina. Prvo, pojam praga se koristi za utvrđivanje logičke "1" ili "0" te se može eliminirati korištenjem dva odvojena pseudo-slučajna uzoraka. Jedan uzorak je određen logičkom "1" i drugi "0". Gornja procedura se tada izvodi jednom za svaki uzorak, a uzorak s višim rezultatom

korelacije se koristi. To povećava vjerojatnost točne detekcije, čak i nakon što je slika bila izložena napadu. Možemo i dodatno unaprijediti metodu predfiltriranja slike prije primjene vodenog žiga. Ako možemo smanjiti korelaciju između slike i PN sekvence, možemo povećati imunitet vodenog žiga na dodatni šum. Primjenom filtra za povećanje ruba robusnost vodenog žiga se može poboljšati bez gubitka kapaciteta i sa vrlo malim smanjenjem kvalitete slike.
Umjesto određivanja vrijednosti vodenog žiga iz "blokova" u prostornoj domeni, možemo koristiti CDMA sa raspršenim spektrom tehniku za raspršenje svakog od bitova nasumično kroz glavnu sliku, čime se povećava kapacitet i poboljšava otpornost na rezanje slike. Vodeni žig se prvobitno formira kao duga linija, a ne kao 2D slika. Za svaku vrijednost vodenog žiga, PN niz je generiran pomoću nezavisnih ključeva. Ovi ključevi ili mogu biti pohranjeni, ili se generiraju kroz PN metode. Zbrajanje svih tih PN sekvence predstavlja vodeni žig, koji je tada skalira i dodaje na glavnu sliku. Da bi smo otkrili vodeni žig, svaki ključ se koristi za generiranje svoje PN sekvence, koja se zatim korelira sa cijelom slikom. Ako je visoka korelacija, taj bit se u vodenom žigu postavlja na "1", inače na "0". Proces se zatim ponavlja za sve vrijednosti vodenog žiga. CDMA značajno poboljšava robusnost vodenog žiga, ali zahtijeva nekoliko redova više izračuna time i više vremena za njegovo postavljanje i otkrivanje.

Za testiranje metode korelacije, koristiti ćemo vodeni žig prikazan na slici

Slika 9 - Vodeni žig



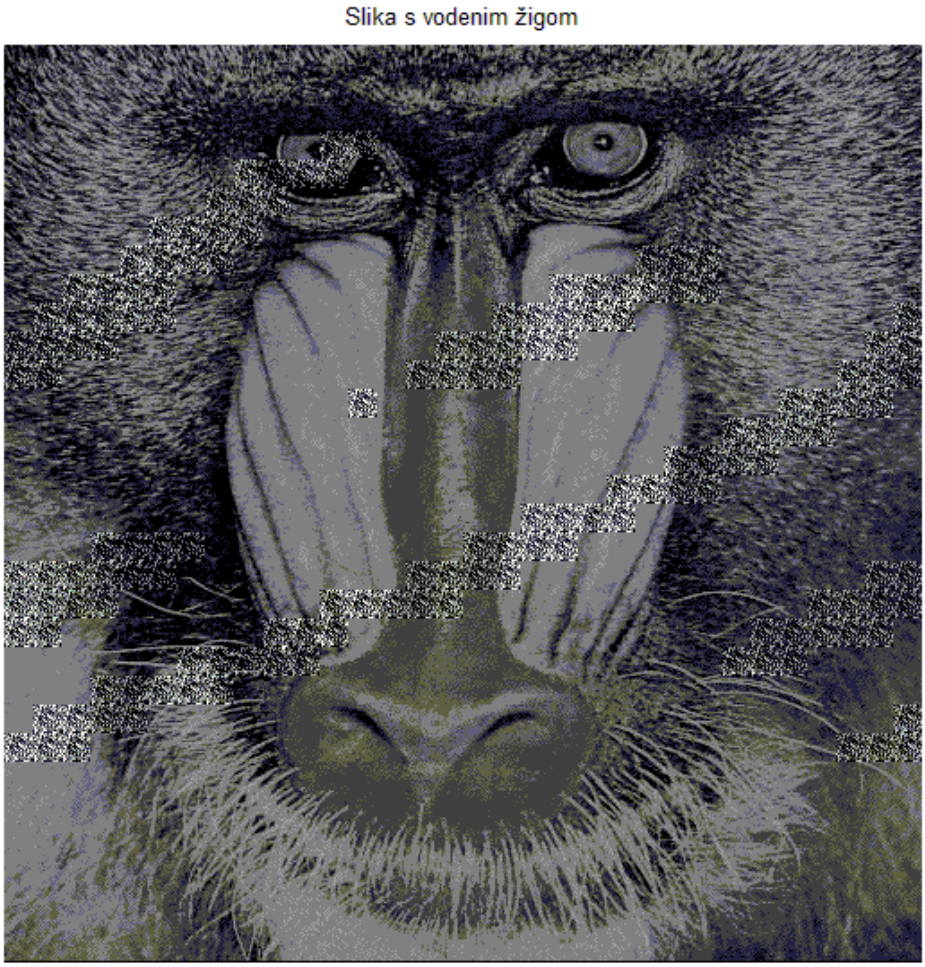
Slika 10

U sliku smo umetnuli vodeni žig i to smo učinili četiri puta za različite veličine faktora pojačanja.

Rezultati umetanja i zatim ponovnog otkrivanja vodenog žiga prikazani su u tablici

Pojačanje (k)	Trajanje sakrivanja	Trajanje otkrivanja	PSNR
5	0.3276	2.3244	3.0669e+003
10	0.2496	2.0280	798.3068
20	0.3270	1.9344	186.2746
50	0.2496	5.4912	33.3377

Očekivano je bilo da će pri najslabijem pojačanju od k=5 vodeni žig očitati najlošije, kao što je i očitano. Isto tako, očekivalo se da će najlošija slika biti ona sa najvećim pojačanjem, kao što se i dobilo.



Slika 11 - slika sa skrivenim vodenim zigom pri pojačanju k=50

Slika 12- otkriveni vodeni žig pri pojačanju k=5

U nastavku je metoda testirana na razne modifikacije:

1) Testirajući ovu metodu s Gaussian Blur 3x3 efektom, uočili smo da pri malim faktorima pojačanja nije moguće očitati vodeni žig. Međutim pri velikim faktorima pojačanja ga je moguće očitati, ali uz prisutstvo šuma. Pri faktoru pojačanja k=50, trajanje otkrivanja ovedenog žiga trajalo je 2.5740s i očitani vodeni žig se nalazi na slijedećoj slici

Slika 13 -očitani vodeni žig pri faktoru pojačanja k=50 i korištenju Gaussian Blur efekta

2) Dodajući Gaussian Noise od samo 1% na pojačanja k=5, k=10 i k=20, nije moguće iščitati žig iz slike. Međutim, s faktorom pojačanja k=50, žig postaje jasan. Povećavajući količinu šuma koju dodajemo, žig se može jasno iščitati iz slike koja ima do 50% Gaussian Nosie-a. Uočavamo da se dobivaju slični rezultati kao i prilikom korištenja Gaussin Blura.

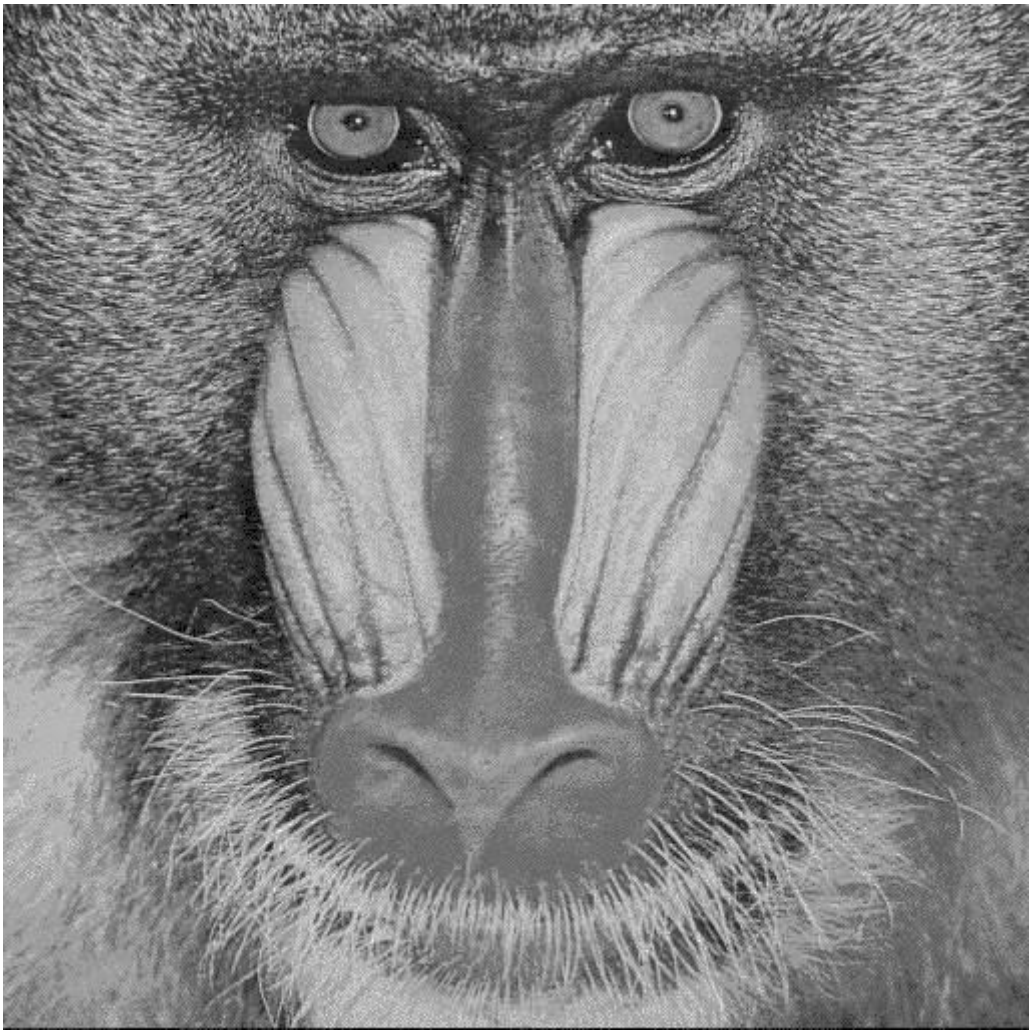
3) Rotacija slike. Sliku sa sakrivenim vodenim žigom uz pojačanja k=5, k=20, k=50 smo rotirali za 0.5 stupnjeva. Uočili smo da neovisno o faktoru pojačanja, šum se pojavljuje na očitanom vodenom žigu. Zaključujemo da metoda kompresije nije otporna na rotaciju.

4) JPEG kompresija napravljena je za dva faktora pojačanja, k=5 i k=50. Kod faktora k=5, za iznimno dobru kvalitetu Q=7, umjesto vodenog žiga, dobivamo samo šum. Povećanjem faktora pojačanja stvar se mijenja. Za Q =7 dobivamo čitljiv vodeni žig s malo šuma, no smanjujući faktor kvalitete Q, gubimo na čitljivosti žiga, te ispod faktora Q=5, više ga ne možemo razabrati.

CDMA metoda

Za sliku baboon.

U sliku

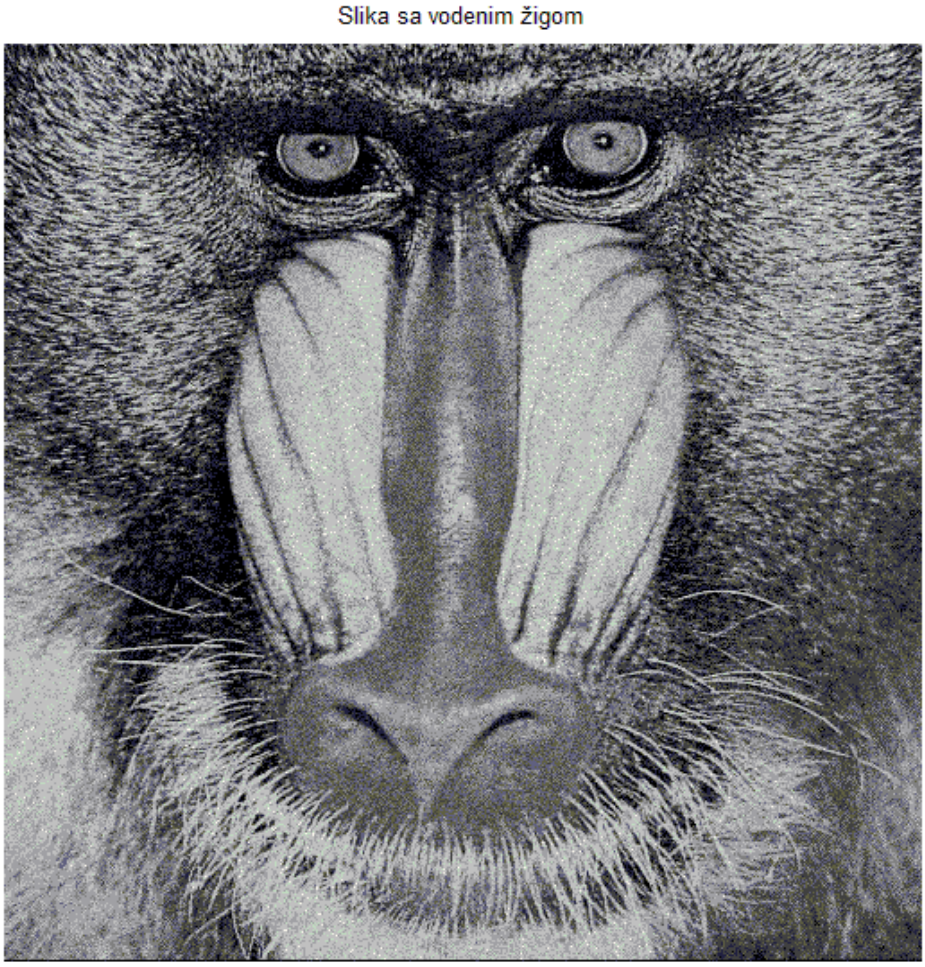


Slika 14

Ubacili smo tajnu poruku uz pojačanje k=2

Slika 15

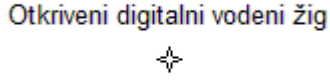
I dobili sliku



Slika 16

Skrivanje podataka je trajalo 5.6004s i PSNR=83.5902.
Vidimo da se vidi razlika u slici nakon sto je umetnuti vodeni zig.

Zatim vadimo podatke. Uspjeli smo očitati:

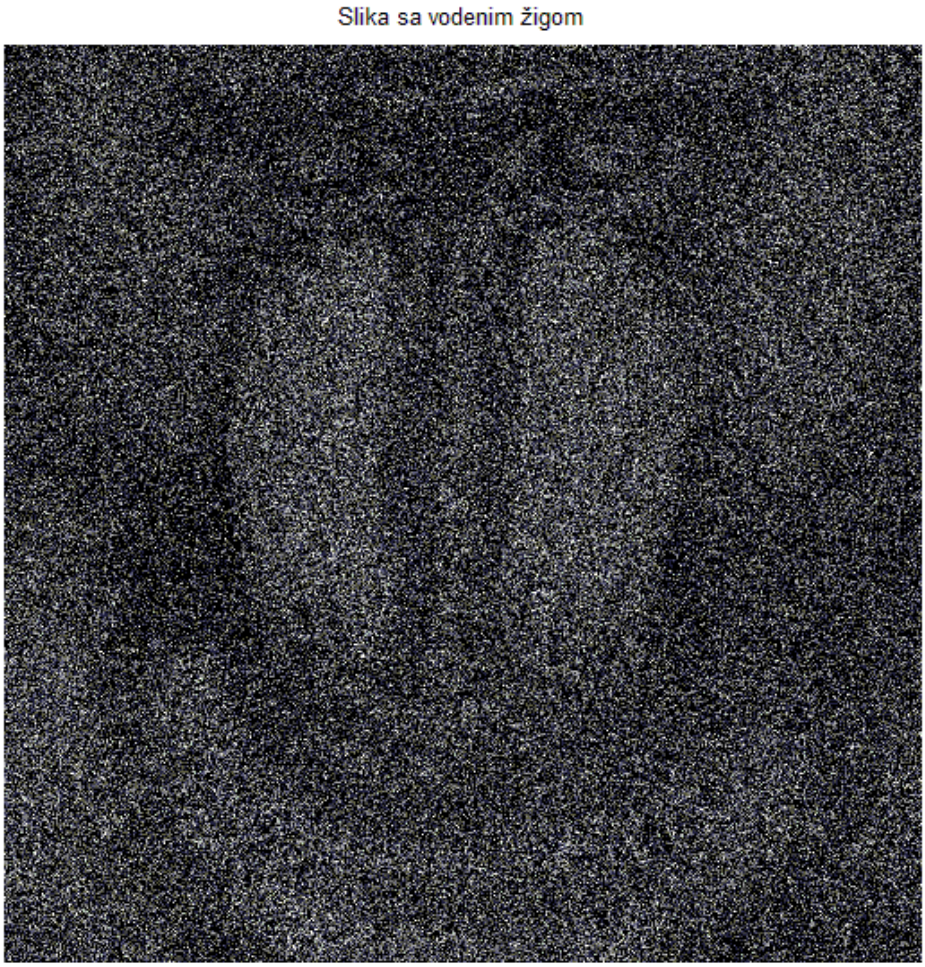


Slika 17

Trajanje je trajalo 22.2301s
Zatim smo testirali uz razna pojačanja.

Pojačanje k	Trajanje vremena otkrivanja (s)	PSNR (dB)
2	19.785	83.8526
5	19.2193	14.5998
10	19.4065	4.3737
20	19.4533	1.3706

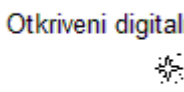
Slika 18 - Uz faktor pojačanja k=10



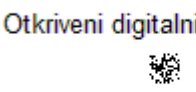
Slika 19 - Uz faktor pojačanja 20

Zatim smo sliku koja je sadrzavala u sebi vodeni žig podvrgnuli raznim modifikacijama kao:

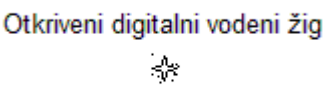
1) Dodali smo Gaussian Blur (odgovara niskopropusnom filtriranju) u vrijednosti od:
   - 3x3 uz k=2, trajanje=19.7809s (slika 20)
   - 5x5 uz k=2, trajanje=21.4501s (slika 21)
   - 7x7 uz k=10, trajanje=19.4845s (slika 22)



Slika 20



Slika 21

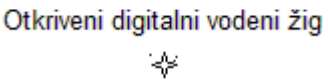


Slika 22

2) Dodali smo različite količine Gaussian Noise-a (Gaussov šum) te dobili rezultate prikazane u tablici

Količina Gaussian Noise (%)	Faktor pojačanja k	Trajanje (s)
10	2	19.8121
50	2	20.5670
100	2	35.3186

Vidimo da je skriveni žig citljiv i pri najvećem Gaussian Noisu uz najmanji faktor pojačanja (slika 23) i time zaključujemo da je postupak CDMA jako otporan na izobličenja gaussovog šuma.



Slika 23 – skriveni žig

3) Skraćivanju slike za određen broj piksela.

Prvo smo sliku odrezali za 2 piksela u vodoravnom smjeru pri pojačanju k=2 i nismo uspjeli očitati vodeni žig. Zatim smo to isto pokušali napraviti pri pojačanju od k=10 i također nismo uspjeli očitati vodeni žig. Zaključujemo da je ova tehnika u potpunosti neotporna na rezanje piksela.

4) Rotaciju slike.

Vodeni žig je nečitljiv za bilo koji kut rotacije.(slika 24).zaključujemo da ova metoda nije otporna na rotaciju. Očitani vodeni žig :

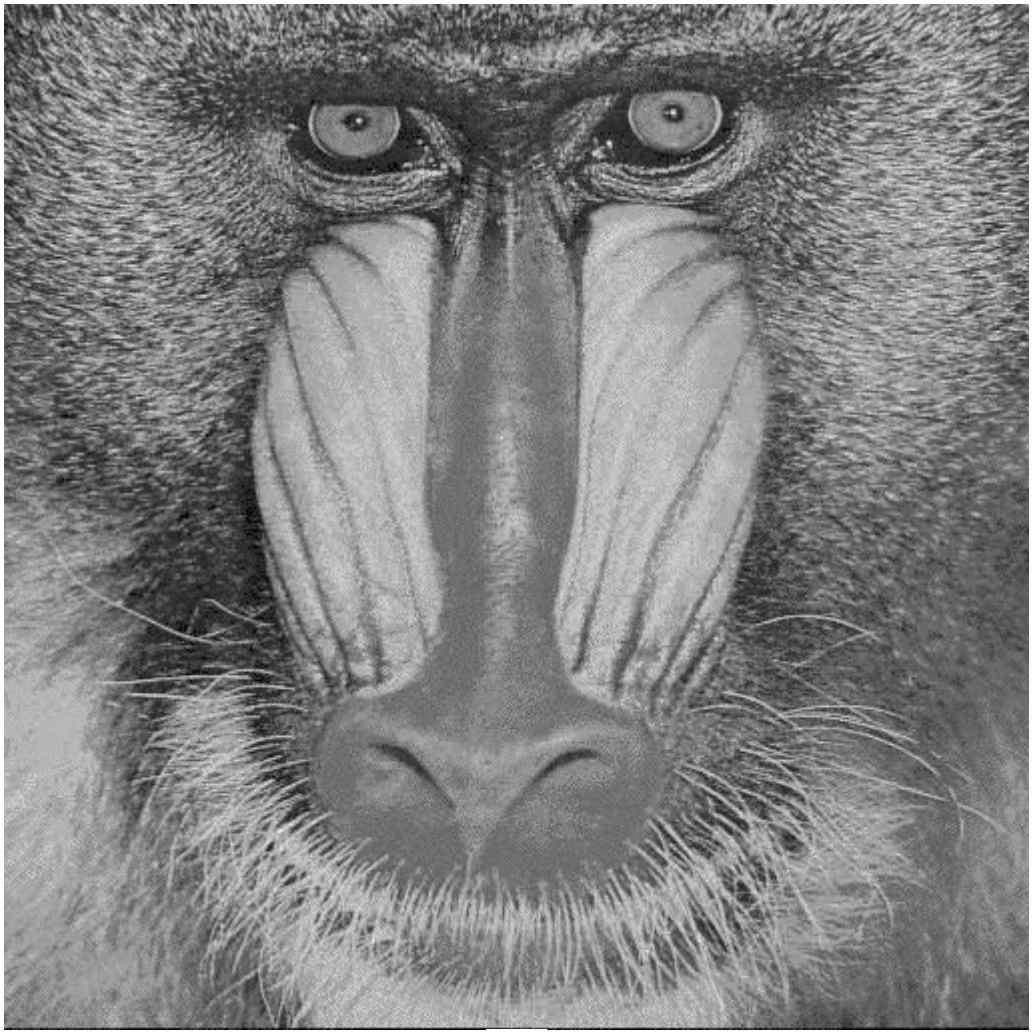
Slika 24

5) JPEG kompresija

Sliku smo kompresirali pomoću jpeg kompresije pri kvaliteti Q=5 i Q=7 i uspjeli očitati vodeni žig uz nešto veće vremena očitavanja. Zaključujemo da je ova metoda dobra za korištenje uz ovaj način kompresije.

Skrivanje u DCT domeni

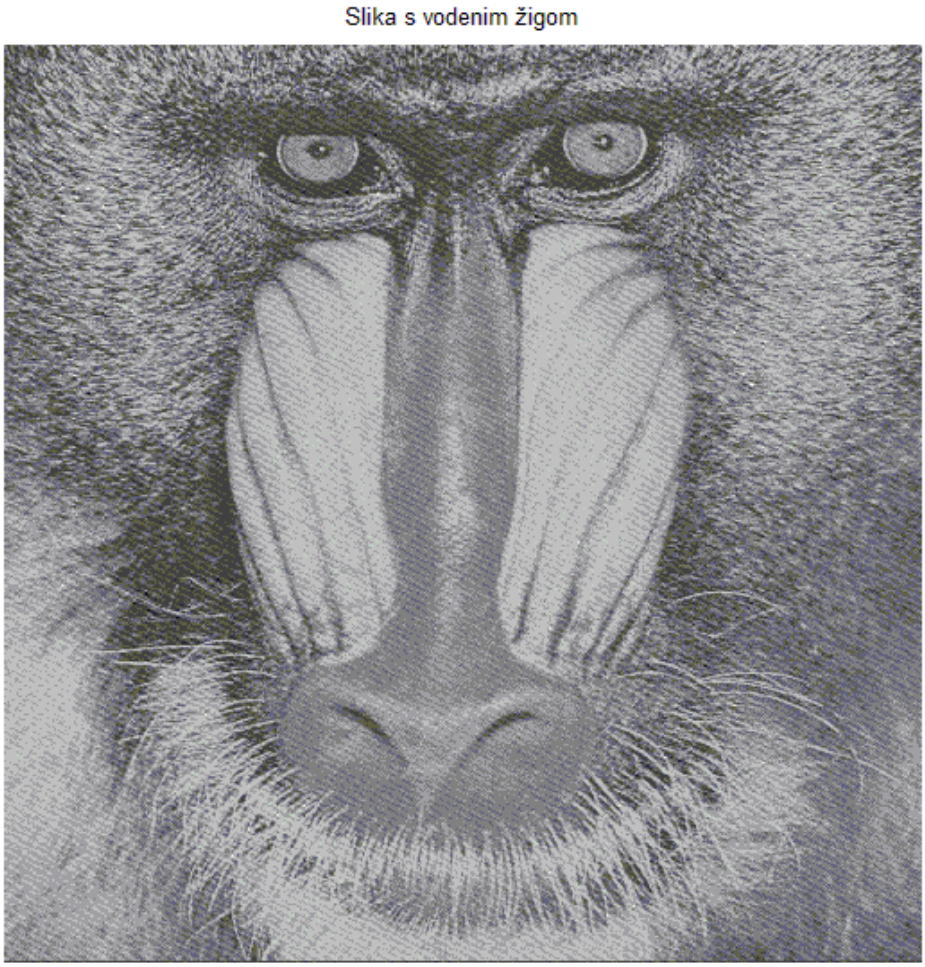
Steganografske metode koje skrivaju poruku u prostornoj domeni nisu pogodne za rad s formatima slika koje koriste postupak kompresije s gubitkom podataka. Stoga su razvijeni steganografski algoritmi prilagođeni JPEG formatu slika. Specifičnost tih algoritama se ogleda u tome što oni operiraju u DCT domeni pa ih se može svrstati u steganografske tehnike transformacije domene. U principu se za skrivanje koristi JPEG koder pri čemu se između koraka kvantizacije i kompresije bez gubitaka vrši skrivanje tajne poruke. Drugim riječima, poruka se skriva u kvantizirane DCT koeficijente.
U postupku dohvaćanja je dovoljno koristiti Huffmanov dekoder kojim se dobivaju DCT koeficijenti u kojima je skrivena poruka. Steganografski algoritmi implementirani u sklopu rada za skrivanje poruke koriste samo komponentu koja definira osvijetljenost slike, tj. Y komponentu. Naime, zbog procesa kodiranja opisanog u prethodnom poglavlju, veći dio kapaciteta predviđenog za skrivanje poruke se nalazi upravo u Y komponenti. Stoga se ne gubi puno na kapacitetu ukoliko se Cb i Cr komponente zanemare pri samom skrivanju.
Za korištenje dct metode koristili smo slijedeću sliku i vodeni žig:



Testiranje je urađeno s četiri različita faktora pojačanja k i dobiveni rezultati prikazani su u slijedećoj tablici:

Pojačanje (k)	Trajanje sakrivanja	Trajanje otkrivanja	PSNR
5	1.6848	0.6552	697.3389
10	1.5912	0.7800	639.5496
20	1.6692	0.655	458.4682
50	1.6692	0.7162	147.3650

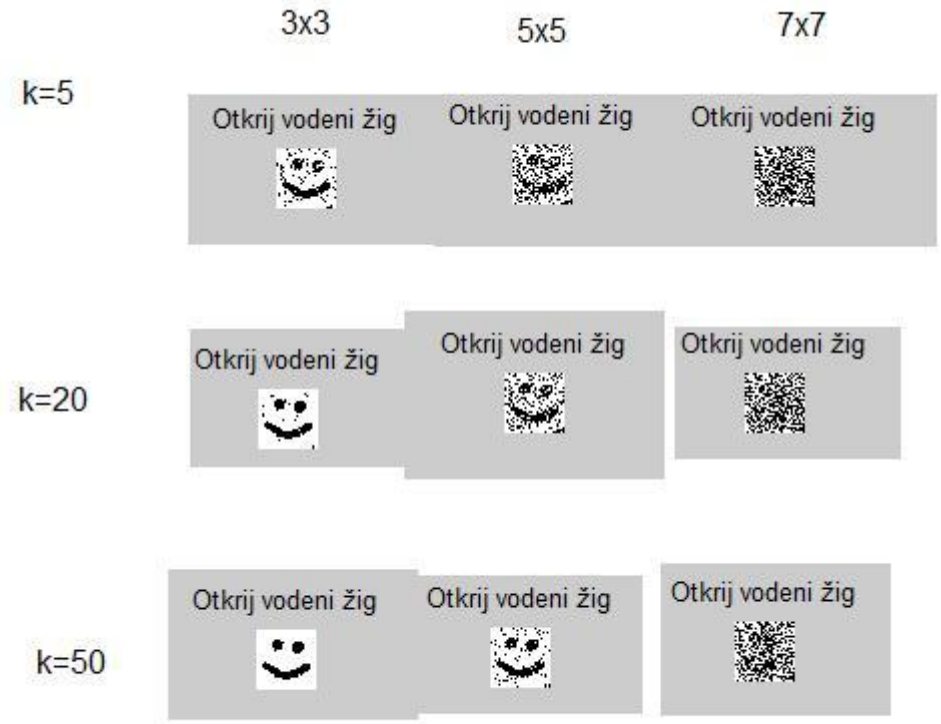
Pri faktoru pojačanja k=50 slika dobivena slika sa skrivenim vodenim žigom :



Slika 25 - slika sa skrivenim vodenim žigom pri faktoru pojačanja k=50

Očitavanje vodenog žiga je u potpunosti uspješno pri svim vrijednostima faktora pojačanja. Međutim, kvaliteta slike proporcionalno pada sa porastom faktora pojačanja, što se uostalom može i primjetiti pomoću PSNR vrijednosti.
Zatim smo slike sa sakrivenim vodenim zigom podvrgnuli razlicitim modifikacijama:

1) Gaussian Blur
Slikama smo dodavali Gaussian Blur 3x3, Gaussian Blur 5x5 i Gaussian Blur 7x7. Dobiveni rezultati su prikazani na slici 26.

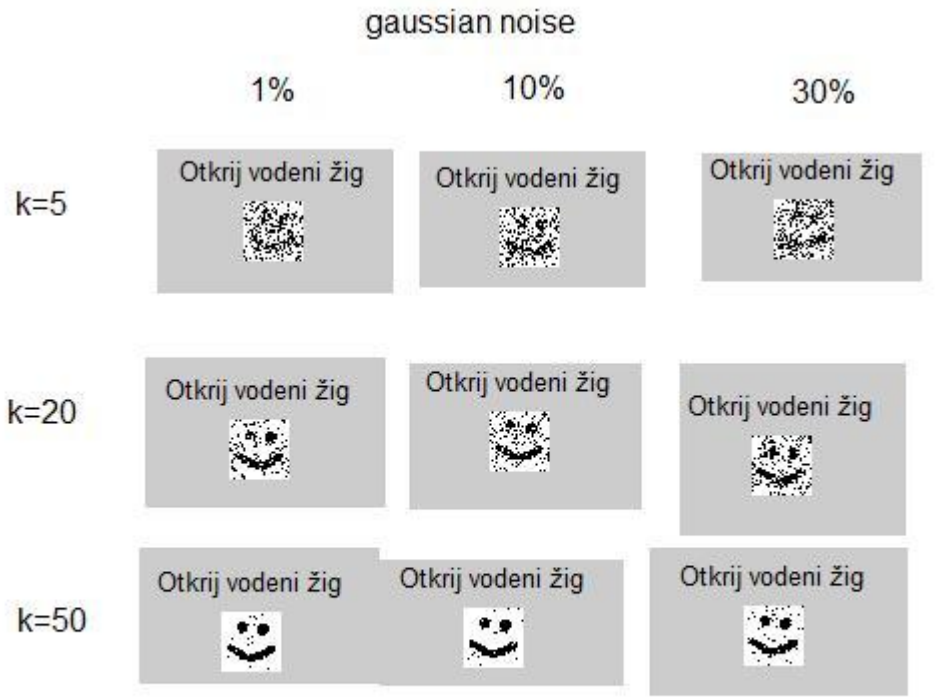


Slika 26 – Vodeni žigovi uz različita pojačanja i različiti Gaussian Blur

Kod male količine Gaussian Blur-a, moguće je iščitati vodeni žig za bilo koje pojačanje. Pomoću većih faktora pojačanja, možemo dobiti čitljiv vodeni žig i uz malo veći Gaussian Blur. Za velike količine zamućenja, ova metoda ne daje zadovoljavajuće rezultate čak i pri velikim faktorima pojačanja. Kod ovakvih modifikacija, metoda CDMA pokazala se pouzdanijom.

2) Gaussina Noise

Slikama smo dodavali različite količine Gaussian Noise-a (1%, 10%, 30%). Na slici su prikazani rezultati na temelju kojih zaključujemo da se i u ovom slučaju CDMA pokazala boljom metodom. Uočavamo da je potrebno velik faktor pojačanja da bi se tek uz malu količinu šuma razabrao čitljiv žig, no čim se taj šum poveća na 30%, više ne raspoznajemo žig.



Slika 27

3) Rotacija

Sliku u kojoj je umetnut vodeni žig (k=5) smo zarotirali za 1° te zatim pokušali zatim otkriti vodeni žig tako modificirane slike. Uočili smo da se vodeni žig uopće ne nazire. Potom smo pokušali isto uz veći faktor pojačanja (k=50), no razlike nema. Dakle, metoda diskretne kosinusne transformacije nije otporna na rotaciju.

4) Kompresija

Sliku s umetnutim vodenim žigom prebacili smo iz BMP formata u JPEG s različitim kvalitetama. Testiranje se radilo za nekoliko različitih faktora k koji označavaju razliku između dva odabrana koeficijenta srednjih frekvencija DCT matrice. Za mali k, uz kvalitetu JPEG formata 6, vidljiv je samo šum. No kada se taj k poveća (k=50), za istu kvalitetu dobije se jasno čitljiv vodeni žig bez imalo šuma. Smanjivali smo kvalitetu i uočili da za sliku niske kvalitete (Q=3) i dalje dobivamo čitljiv vodeni žig. Time smo potvrdili da je DCT metoda iznimno otporna na JPEG kompresiju.

Zaključak

Steganografija predstavlja alternativu kriptografiji. Kako je uobičajeno veliki broj slika koje kolaju komunikacijskim kanalom, napadač teško može svaku sliku analizirati. U tom pogledu je steganografski sustav u prednosti pred kriptografskim sustavom jer napadač teško dolazi u doticaj s tajnom porukom. Posebice su zanimljivi steganografski sustavi koji koriste kriptirane poruke čime se dodatno poboljšava sigurnost sustava: čak i ako se izdvoji poruka ona je i dalje kriptirana i napadaču nerazumljiva. Negativna strana steganografije leži u činjenici što je za skrivanje poruke potrebno koristiti objekt nositelj koji uobičajeno nosi veću količinu podataka nego li sama poruka. Tehnike steganalize nastoje otkriti postoji li skrivena poruka unutar bezazlene informacije. Posebice su bitne tehnike steganalize koje kao podlogu koriste statističke testove. Takve tehnike, osim same detekcije skrivene poruke, često mogu odrediti i približnu veličinu poruke.

LSB je najjednostavnija metoda koja ne pruža mnogo sigurnosti. Odlikuje se tek velikim kapacitetom u koji se može koristiti za umetanje vodenoga žiga, no svaka neznatna operacija urađena na slici, onemogućava otkrivanje vodenoga žiga. Iako postoje neka poboljšane verzije te metode, ona definitivno ne omogućava robusnost kakva je potrebna u zaštiti vodenog žiga.

Metoda korelacije pokazuje daje bolje rezultate od LSB metode, pogotovo kad je u pitanju šum, zamućenje i sl. Međutim, ta poboljšanja imaju za posljedicu jako lošu kvalitetu slike gdje je oku vidljiva podjela slike na blokove. Bolja verzija ove metode je CDMA metoda gdje je šum jednoliko raspoređen po cijeloj slici,a ne po blokovima. Uz to, CDMA daje još bolje rezultate pri utjecaju šuma i zamućenja od metode korelacije, ali ponovno kao posljedicu ima još manje kvalitetu slike odraženu objektivnom mjerom PSNR. Obje metode neotporne su na rotaciju slike.

Međutim, DCT metoda pokazala je iznimnu otpornost JPEG kompresiju te na značajnu količinu zamućenja i šuma. Inače, ova metoda vrlo je popularna u svijetu digitalne tehnologije i to velikim dijelom zbog otpornosti na JPEG kompresiju, ali isto zato što se unosi vrlo mala disperzija u sliku jer se područja odabiru prediktivnim

kodiranjem te zbog mogućnosti detektiranja watermarka direktno u transformiranoj domeni, što utječe na brzinu detekcije.
Danas ovim metodama konkuriraju neka nova rješenja kao što su transformacije u wavelet domeni te geometrijske transformacije. Također, budući koraci uključuju razmatranje drugih oblika steganografije i steganalize, poput upotrebe tehnika raspršenog spektra u steganografiji ili tehnika nadziranog učenja u steganalizi. No, ovisno o zahtjevima, svaka metoda će naći primjenu.

Literatura

http://e.math.hr/old/stegano/index.html , Sanja Zeljković, Hrvatski matematički elektroniskičasopis, Broj 5, lipanj 2005

http://www.vu.union.edu/~shoemakc/watermarking/watermarking.html , Chris Shoemaker, Independent Study, EER-290, proljeće 2002

http://sigurnost.lss.hr/documents/LinkedDocuments/CCERT-PUBDOC-2006-04-154.pdf, CARNet CERT, *Steganografija*, CCERT-PUBDOC-2006-04-154, Revizija v1.0, 2006.