Sveučilište u Zagrebu
Grafički fakultet

Filip Lulić

Usporedba postojećih sustava za umetanje digitalog vodenog žiga u sliku

Završni Rad

Zagreb, 2021.

Sveučilište u Zagrebu
Grafički fakultet

Smjer: tehničko-tehnološki

Filip Lulić

Usporedba postojećih sustava za umetanje digitalog vodenog žiga u sliku

Završni Rad

Mentor:
Ante Poljičak

Student:
Filip Lulić

Zagreb, 2021.

Sažetak

Sveprisutnim razvojem digitalnih mreža omogućuje korisnicima beskrajno kopiranje i distribuiranje dokumenata velikom broju ljudi bez troškova. Zbog ovakvih razloga nastaje potreba za digitalnim vodenim žigom. Algoritmi digitalnih vodenih žigova u sliku ugrađuju digitalne podatke i/ili potpise kako bi dokazali identitet vlasnika, potom spriječili kršenje autorskih prava. Rad se sastoji od definicija i povijesti digitalnog vodenog žiga, te primjena i integracija digitalnog vodenog žiga kroz par primjera.

Cilj je ustanoviti prednosti i mane postojećih komercijalnih i nekomercijalnih sustava za zaštitu umetanja digitalnog vodenog žiga. Istraživanje će se izvoditi tako da se u 5 različitih slika ubaci digitalni vodeni žig, integriran pomoću 4 različita sustava, potom su slike povedene kroz niz osnovnih napadaja obrade slike. Analizirani rezultati testiranja stavljeni su u tablicu, te naposljetku uspoređeni detektira li se promjena digitalnog vodenog žiga na slici.

Sadržaj

1. Uvod

Najraniji oblici sakrivanja informacija mogu se smatrati vrlo grubim oblikom kriptografije. Grčke pismonoše bi imale poruke tetovirane na vrhu glave, sakrivajući poruku novo naraslom kosom. [1] Tijekom vremena ovakve primitivne kriptografske tehnike su se poboljšale u brzini, kapacitetu i sigurnošću poslane poruke.

U današnje doba informacije postaju široko dostupne putem globalnih mreža. Ove povezane mreže omogućuju uspoređivanje informacija između vise baza podataka. Dolaskom multimedija pojavljuju se različiti načini za korištenje tih podataka. Industrija teži potrošačima ponuditi što više opcija u elektronskom obliku. Zbog brzog napretka digitalnih medija velike korporacije prijelaze s analognog u digitalan format. Digitalni mediji imaju veću kvalitetu signala nego analogni, te sama kvaliteta digitalnih medija ne opada tijekom vremena. Analogni podaci zahtijevaju skupe i kompliciranе sustave za proizvodnju visoko kvalitetnih kopija dok se digitalni kopiraju s lakoćom. To je ujedno dvosjekli mač jer se kopije dragocjenih digitalnih podataka ne mogu razlikovati od originala. Dupliciranje digitalnih podataka bez tuđeg dopuštenja postaje neizbježno zato dolazi do podizanja svijesti o problemima zaštite autorskih prava. Pojavom digitalnog vodenog žiga se nastoje riješiti ti problemi. Moguće je sakriti neke informacije unutar digitalnih podataka na takav način da su te modifikacije nedetektabilne.

U radu će se zaštititi 5 fotografija u digitalnom formatu pomoću 4 komercijalna i nekomercijalna sustava za ubacivanje digitalnog vodenog žiga (digimarc, stagonline, mobilefish i manytools). Usporedba će se obraditi na takav način da će se zaštićene fotografije napasti sa 4 osnovne metode obrade slike (JPEG kompresija, blur, rotacija i skaliranje). Usporedbom zaštićenog originala i zaštićene obrađene fotografije utvrditi će se razlike u zaštiti fotografije između tih sustava.

Slika 1. Primjer tetovirane poruke na glavi

2. Teorijski dio

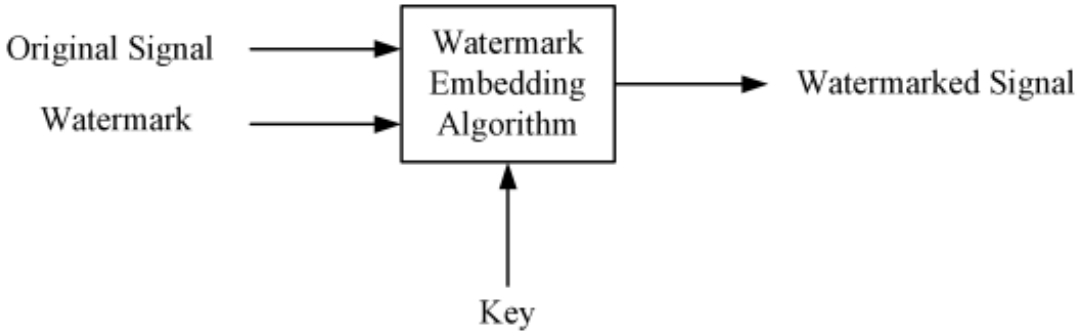
2.1. Vodeni žig

Prvi zapisani vodeni žig se pojavio u Italiji 1282. godine. Pomoću tanke žice na papir bi se ostavio trag. Njihovo značenje i svrha su do dan danas nepoznati, no pretpostavlja se da su se koristili kao zaštitni znak proizvođača papira ili kao način raspoznaje različite vrste papira. U 18. stoljeću vodeni žig dobiva novu funkciju u Europi i Americi. Koristio se kao način provjere krivotvorenog novca. Novi valovi krivotvorina su potaknuli razvoj tehnologije vodenog žiga. Englez William Henry Smith je izumio novi i praktičniji način umetanja vodenog žiga. Umjesto označivanja papira sa tankim žicama, William je pomoću plitke reljefne skulpture u papir utisnuo reljefni uzorak. Nastali uzorak bio je manje upadljiviji i teži za krivotvoriti. [2]

Slika 2. Primjer otisnutog vodenog žiga na novčanici

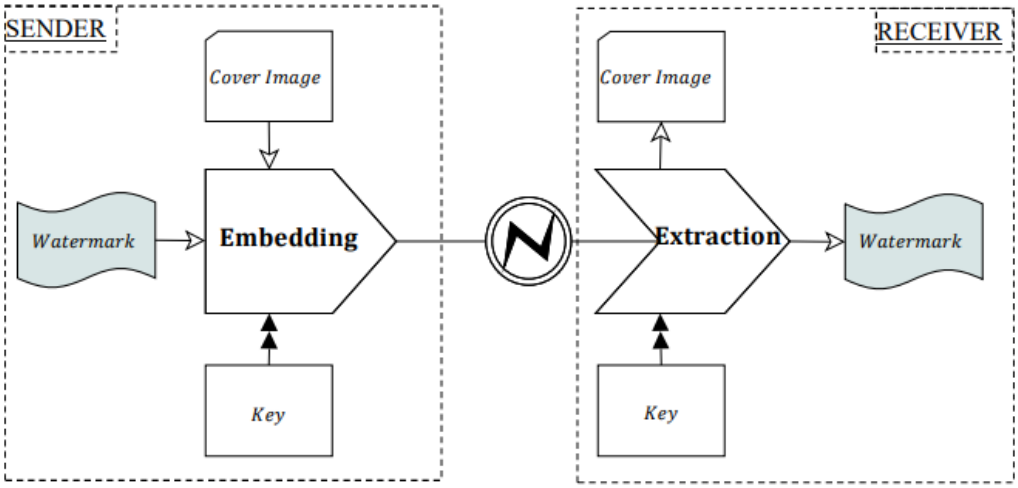
2.2. Digitalni vodeni žig

Digitalni vodeni žig je tehnika umetanja sakrivenog signala u digitalan sadržaj (slika, video, zvuk, tekst). Digitalni vodeni žig postupno se razvijao sve dok nije postao prihvaćen kao oblik zaštite autorskih prava. Digitalni sadržaj ima nekoliko prednosti nad analognim sadržajem. Obično ima veću kvalitetu koja se ne izgubi tijekom vremena. Digitalne datoteke se lako mogu uređivati. Osoba može uz veliku preciznost ubaciti ili izbaciti informaciju u datoteci. Osim toga digitalni sadržaj se s lakoćom može prenositi putem interneta. Međutim, ove prednosti izazivaju sve veću zabrinutost upravljanjem autorskih prava i zaštite privatnosti. Tradicionalni zaštitni sustavi utemeljeni na kriptiranoj vezi ne pružaju dovoljno dobru zaštitu jer ne zaustavljaju redistribuciju i modifikaciju već raskrivenog sadržaja. Jedna metoda za rješavanje ovog problema je digitalni vodeni žig, gdje se u zaštićenu datoteku ugradi neprimjetan znak. Digitalni vodeni žig može sadržavati u sebi informaciju za autentifikaciju autorskih prava, opis datoteke za otkrivanje neovlaštenog rukovanja ili tajnu informaciju za kontrolirani pristup.



Slika 3. Shema umetanja digitalnog vodenog žiga [3]

Tijekom ugrađivanja digitalnog vodenog žiga, koji uglavnom bude niz binarnih brojeva, digitalni vodeni žig se strateški ubaci u izvorni signal. Bitno je da signal sa umetnutim digitalnim vodnim žigom nema nikakve vidljive razlike od izvornog signala. Korištenjem privatnog ključa onemogućuje neovlaštenim korisnicima da generiraju legitiman signal sa digitalnim vodenim žigom.



Slika 4. Shema distribuiranja digitalnog vodenog žiga

2.3. Podjela digitalnog vodenog žiga

- Prema radnoj domeni.

  a) Prostorna domena - digitalni vodeni žig dodaje se izravno na sliku

  b) Frekvencijska domena - spektar žiga se dodaje spektru slike, domena je otpornija na napade

- Prema vrsti dokumenta

  a) Tekst

  b) Slika

  c) Audio

  d) Video

- Prema ljudskoj percepciji

  a) Vidljiv - žig u obliku logotipa je vidljiv na izvornom dokumentu

  b) Robustan nevidljiv - vizualno se ne vidi, decoder ga detektira, otporniji na napade

  c) Lomljiv nevidljiv - vizualno nije vidljiv, decoder ga detektira, nije otporan na napade

  d) Dvostruki – spoj nevidljivog i vidljivog

- Prema primjeni

  a) Izvorišno bazirani - žig se unosi u izvornik i pri svakoj distribuciji izvornik sadrži iformacije o vlasniku

  b) Odredišno bazirani - žig se unosi uz svaku kopiju izvornika, tako da svaki vlasnik (kupac) ima jedinstveni „vlastiti izvornik“. Kod kopije se nadzire čija nelegalna kopija se proširila u tuđe ruke i određenim sankcijama teretiti pravog vlasnika. Tim načinom se rješava problem kopiranja autorskih prava.

- Prema robusnosti

  a) Javne sheme – nije potrebna izvorna slika za detekciju

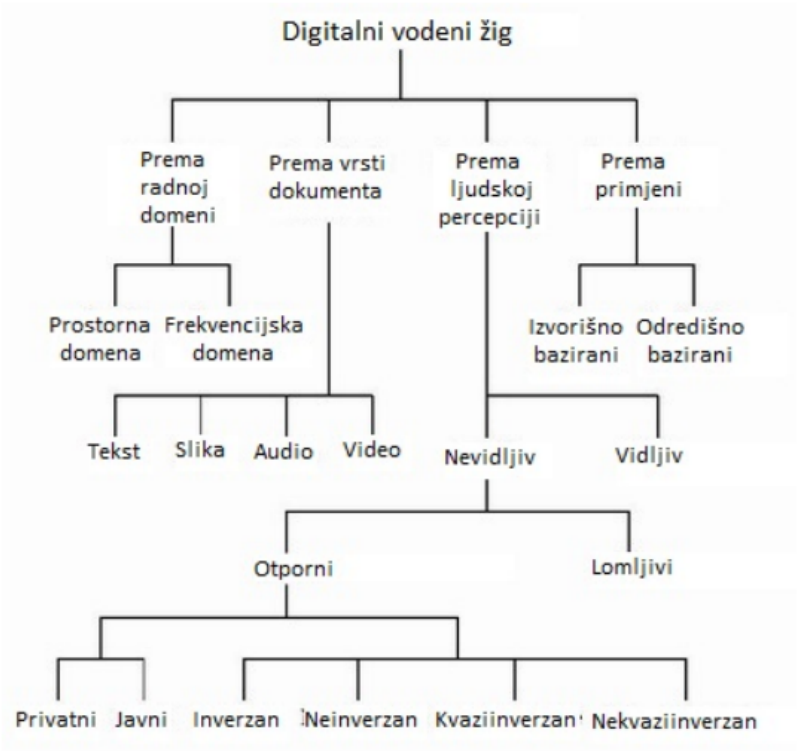
  b) Tajne sheme – potrebna izorna slika za detetekiju

  c) Inverzne sheme – ispunjava sve uvjete inverzne sheme

  d) Neinverzne seme – ne ispunjava niti jedan uvjet inverzne sheme

  e) Poluinverzne sheme – zadovoljavaju dva od tri uvjeta inverzne sheme

  f) Nepoluinverzne seme – ne ispunjava ni dva od tri uvjeta inverzne sheme [4]



Slika 5. Shema klasifikacija digitalnih vodenih žigova

2.4. Umetanje digitalnog vodenog žiga

Kod umetanja digitalnog vodenog žiga u sliku bitno je razumjeti piksele i modele boja. Piksel je najmanji dio slike i boje u svakom pikselu su funkcije kombinacije proporcija boja npr. RGB (crvena zelena, plava). Dakle piksel vrijednosti 0,0,1 (0 crvene, 0 zelene, 1 plave) boje prikazuje plavi piksel. U slučaju 8-bitnog sustava, piksel može primiti do 8 znamenki (nula ili jedinica). Najveći broj koji se može ubaciti u znamenki je 11111111 koji bi bio 255, dok najmanji broj bi se prikazao kao 00000000 i iznosio bi 0. Dakle svaki piksel u bitnom scenariju može prihvatiti bilo koju vrijednost između 0 i 255. Recimo da slučajna 8-bitna mreža ima 3 piksela, a svaki piksel ima donje vrijednosti za RGB.

	R (crveno)	G (zeleno)	B (plavo)
Piksel 1	00101101	00011100	11011100
Piksel 2	10100110	11000100	00001100
Piksel 3	11010010	10101101	01100011

Tablica 1. Prikaz 8-bitne mreže

Ako bismo ubacili na primjer broj 200, dobili bismo binarnu vrijednost tog broja tj. 11001000. Ovisno o svim brojevima te binarne vrijednosti će se zamijeniti najmanje bitan broj (uglavnom zadnji broj). Ovime bi se promijenile boje originalne slike u tri kanala za 3 piksela najmanje količine. Promjene na novonastaloj slici su gotovo nevidljive. Ovo je primjer Least Significant Bit (LSB) algoritma za ubacivanje digitalnog vodenog žiga u sliku.[5]

	R (crveno)	G (zeleno)	B (plavo)
Piksel 1	00101101	00011101	11011100
Piksel 2	10100110	11000101	00001100
Piksel 3	11010010	10101100	01100011

Tablica 2. Prikaz djelovanja Least Significant Bit algoritma

2.5. Detekcija digitalnog vodenog žiga

Tijekom detekcije slike žig se prvobitno analizira. Detekcija žiga ovisi o vrsti sustava te informacijama umetnutim u sliku. Kada se radi o aplikacijama gdje je cilj zaštita od neovlaštenog kopiranja lakše se može doći do rezultata jer odgovor na to pitanje može biti da ili ne. Mjera sličnosti između originalnog žiga W i izvađenog žiga W* je normalizirana korelacija za pseudo-slučajne nizove. [6]

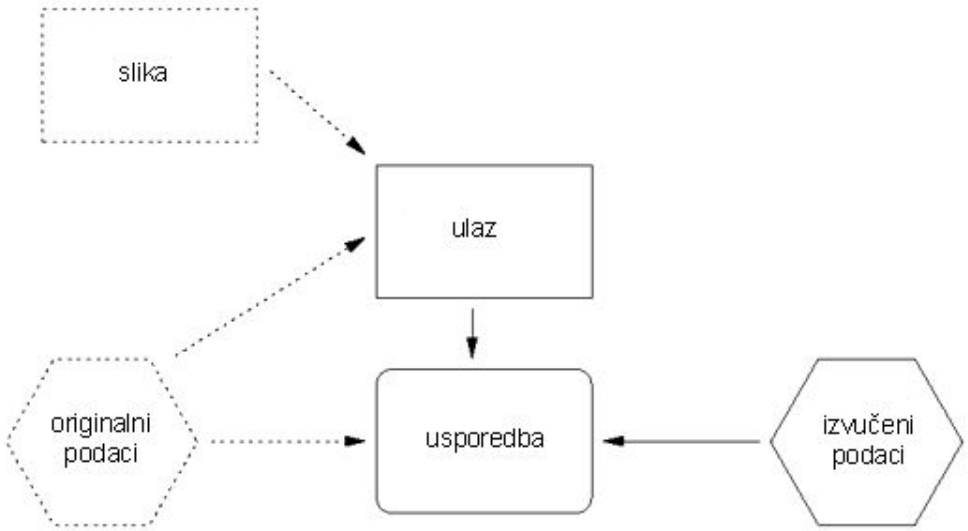
$$\delta = \frac{W^{\star} \cdot W}{\|W^{\star}\| \cdot \|W\|},$$

$$w_i \in \{-1, 1\} :$$

$$\delta = N - \sum^{N} w_i^{\star} \cdot w_i$$

Slika 6. Hammingova udaljenost za binarne poruke

Kod sustava koji u sliku ubacuju informacije koje opisuju sliku ili daju malo više od samog potpisa nije dovoljan odovor da/ne tijeko detekcije. U tom slučaju žig mora biti vidljiv u potpunosti nakon ekstrakcije. Takvi sustavi uglavnom sadrže kod koji pomaže pri ispravljanju grešaka.



Slika 7. Shematski prikaz detekcije digitalnog vodenog žiga

2.6. Vrste napadaja

Napadi digitalnog vodenog žiga usmjereni su na uklanjanje ili uništavanje bilo kakvog signala digitalnog vodenog žiga u podacima slike. Kako bi se osmislila bolja i snažnija tehnika umetanja digitalnog vodenog žiga važno je uzeti u obzir modele napadaja. Postoje 4 različite klasifikacije napada na digitalni vodeni žig (napad odstranjivanja, geometrijski napad, kriptografski napad i napad protokolom).

2.6.1. Napad odstranjivanjem

Cilj napada odstranjivanjem je da se umetnuti signal uspije iskrivit ili poništit bez provale sigurnosti algoritma digitalnog vodenog žiga. Međutim, ti napadaji znaju biti slučajni. Ako je samo iskrivljena slika dostupna, napad odstranjivanja se može smatrati slučajnim utjecajem. Zato je količina informacija potrebna za opis tog utjecaja jako velika. Najpoznatiji tip takvog napadaja je JPEG kompresija gdje se originalna slika i njezin umetnuti signal izgube ili oštete tijekom kompresije datoteke izmjenom u drugi format (npr. PNG u JPEG). U većini slučajeva signal digitalnog vodenog žiga će se teško uspjeti obnoviti. Ovakvi napadi se zbog njihove jednostavnosti lako mogu analizirati pomoću

srednje kvadratne pogreške. Osim kompresije u ovu kategoriju možemo svrstati još zamućenje, izoštravanje, šum i filtriranje.

2.6.2. Geometrijski napad

Učinkovitost geometrijskog napada uglavnom ovisi o kompenzacijskoj sposobnosti dekodera. Geometrijski napadi su u principu drugačiji od napada odstranjivanjem. Promjene na slici kod geometrijskih napada su teško uočljive. Zbog toga se teže analiziraju pomoću srednje kvadratne pogreške. Najčešći geometrijski napadi su rotacija, skaliranje, translacija i obrezivanje.

2.6.3. Kriptografski napad

Kriptografski napadi funkcioniraju na način da provale sigurnost digitalnog vodenog žiga. Za to je uglavnom potrebno pronaći ključ korišten za umetanje digitalnog vodenog žiga. Sa uspješnom provalom većina digitalnih vodenih žigova se s lakoćom mogu odstraniti bez oštećenja kvalitete slike. Osim toga, obmanjujući digitalni vodeni žig se može umetnuti na pozicije određene ključem.[7] Jedan tip ovakvog napadaja je baziran na brute-force napadu gdje se ključ nastoji dobiti na način da se velika količina mogućih rješenja testira sve dok se ne dobije traženi ključ. Drugi tip se zove Oracle napad i koristi se za stvaranje neoznačenog signala digitalnog vodenog žiga kada je dostupan dekoder digitalnog vodenog žiga.

2.6.4. Napad protokola

Kod napada protokola strategija je ta da se na sliku nadoda vlastiti signal digitalnog vodenog žiga. Time se vlasništvo slike prenosi na napadača a originalni signal bude zamaskiran novim. Još jedan napad protokola je napad kopiranjem. Umjesto maskiranja digitalnog vodenog žiga, iz podataka digitalnog vodenog žiga se napravi procijenjena kopija koja se kasnije prenosi u ciljane podatke. Procijenjena kopija digitalnog vodenog

žiga prilagođena je lokalnim značajkama ciljanih podataka kako bi se zadovoljio zahtjev transparentnosti. [8]

2.7. Adobe Photoshop

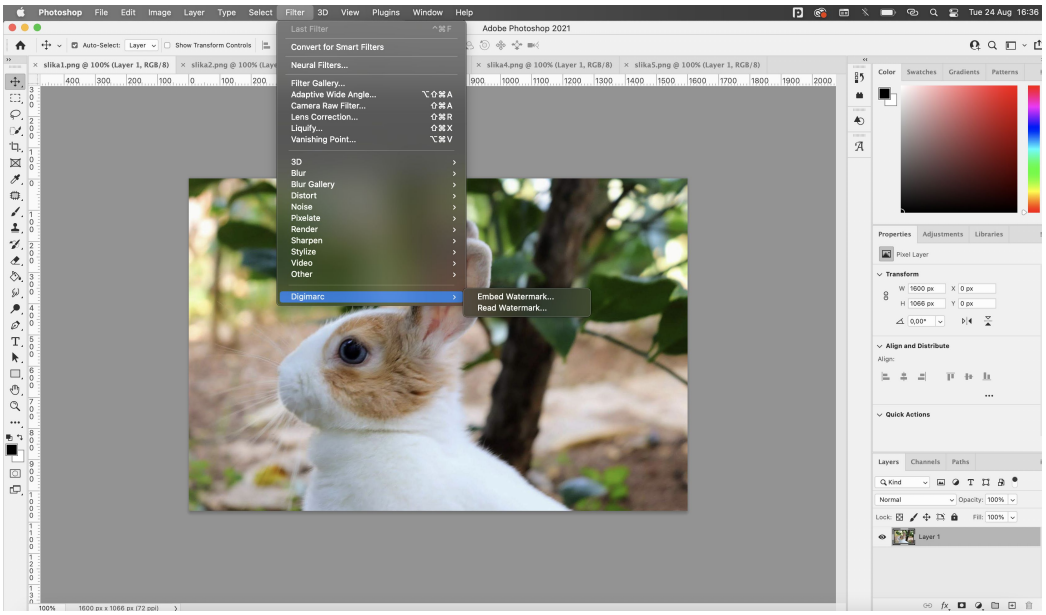
Tom Knoll je 1987.u Macintosh Plusu napravio prvu verziju programa Photoshop. Koristio se za prikazivanje grayscale slika na monokromatskom zaslonu. Tomov brat John je vidio potencijal u programu te je zajedno sa Tomom pretvorio photoshop u program za uređivanje slika. Braća Knoll su 1989. prodali Photoshop Adobeu. Prva službena verzija nastala je 1990. i zvala se Adobe Photoshop. S vremenom Adobe Photoshop bi dobivao nove verzije i nove mogućnosti. Razvojem programa Adobe Photoshop je postao jedan od najpopularnijih komercijalnih programa tadašnjice. 2003. godine se krenuo prodavati kao skup programa zvan Creative Suite. U njemu su se mogli pronaći svi potrebni programi vezani za grafički dizajn, fotografiju i film.

2.8. Sustavi za umetanje digitalnog vodenog žiga

U nastavku rada su prikazana 4 sustava za ubacivanje digitalnog vodenog žiga koja ćemo međusobno usporediti.

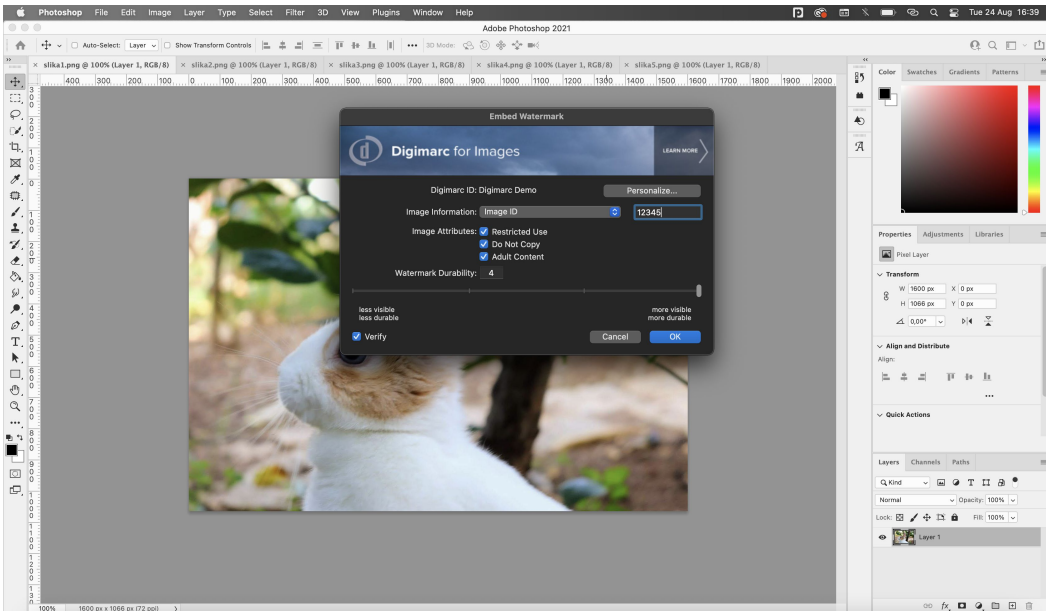
2.8.1. Digimarc

1996. u Adobe Potoshop se dodaje prvi third-party plug-in zvan Digimarc. Osnovao ga je astronom i poduzetnik Geoff Rhoads 1990. Omogućuje nam ubacivanje digitalnog potpisa i/ili informacija u sliku.



Slika 8. Pozicija Digimar plug-ina u Adobe Photoshopu

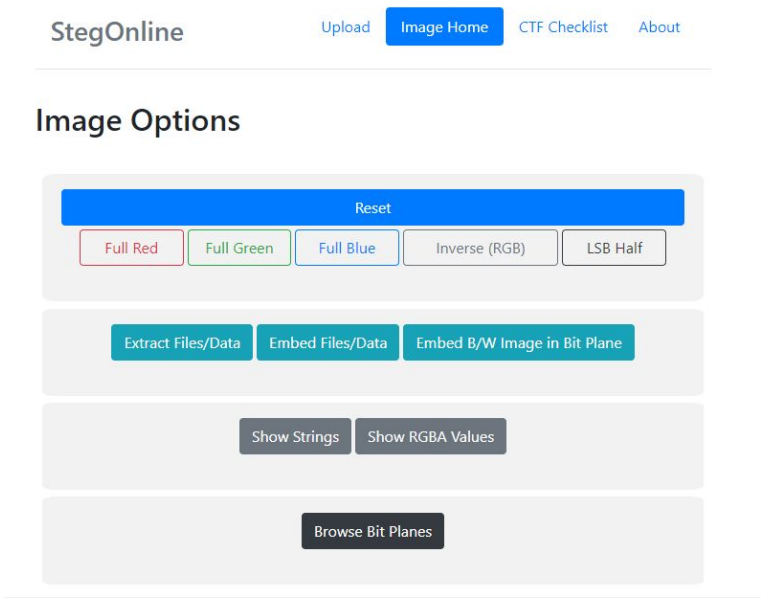
Sadrži opciju Embed Watermark pomoću koje ubacujemo digitalni žig u sliku. Pomoću opcije Read Watermark možemo očitati vidi li se digitalni vodeni žig na slici, te prikazati sve sakrivene informacije o slici. Obje opcije nam nakon korištenja prikazuju snagu zaštite digitalnog vodenog žiga. Digimarc sadrži patentiranu uslugu zvanu MarcSpider.[9] Ta usluga javlja korisnicima i vlasnicima gdje i kada je pronađena slika sa njihovim digitalnim žigom.



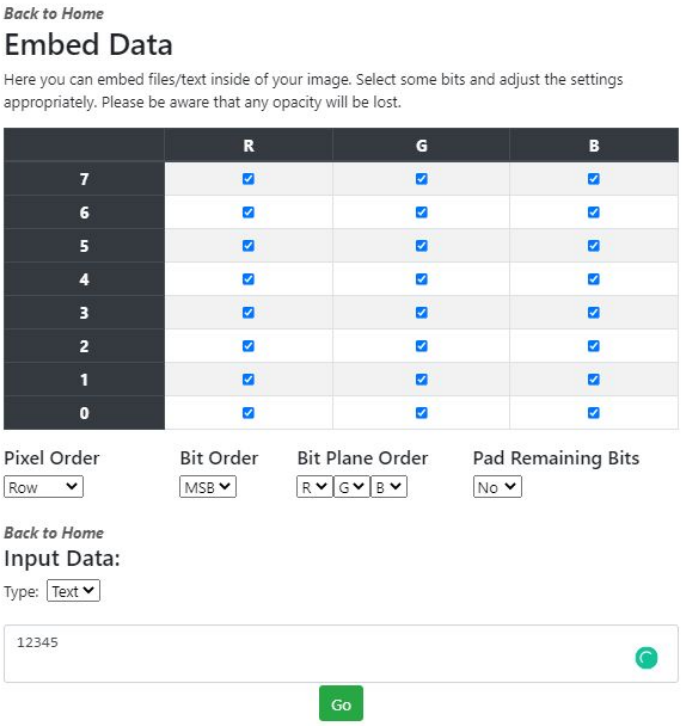
Slika 9. Opcija embed watermark

2.8.2. StegOnline

Poboljšani port StegSolve s otvorenim kodom na webu.[10] Stagonline sustavom za ubacivanje digitalnog vodenog žiga je moguće pregledavati 32 bitne ravnine slike, PNG Chuk informaciu te preuzeti RGBA vrijednosti slike. Podaci se umeću i izdvajaju pomoću LSB steganografskih tehnika. Može sakriti slike unutar drugih bitnih ravina slike i daje pregled palete boja. Za pregled PNGa koristi se PngToy koji omogučuje pregled drugih binih informacija kao chunk info i bitmap podaci.



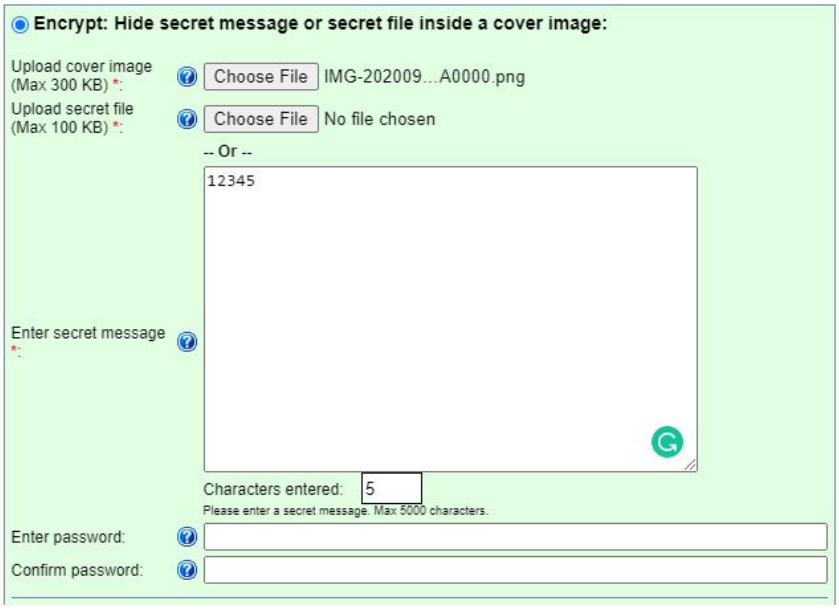
Slika 10. Prikaz sučelja StegOnline



Slika 11. Opcija embed watermark

2.8.3. Mobilefish

Mobilefish.com je osnovao Robert Lie 2002.[11] Cilj ove stranice je pružiti brže, jednostavne i praktične odgovore o internetu, web develepmentu, programiranju, te drugim tehnologijama. Stranica sadrži steganografski sustav za ubacivanje digitalnog vodenog žiga u sliku. Omogućuje ubacivanje digitalnog žiga u ovim formatima datoteke .bmp, .gif, .jpeg, .jpg, .png. Osim što može sakriti informacije u sliku može ih i izvaditi iz već sakrivene slike. Ima dodatnu opciju sigurnosti gdje se tijekom enkriptanja slike može umetnuti šifra koja je potrebna da bi se ta ista slika dekriptala.

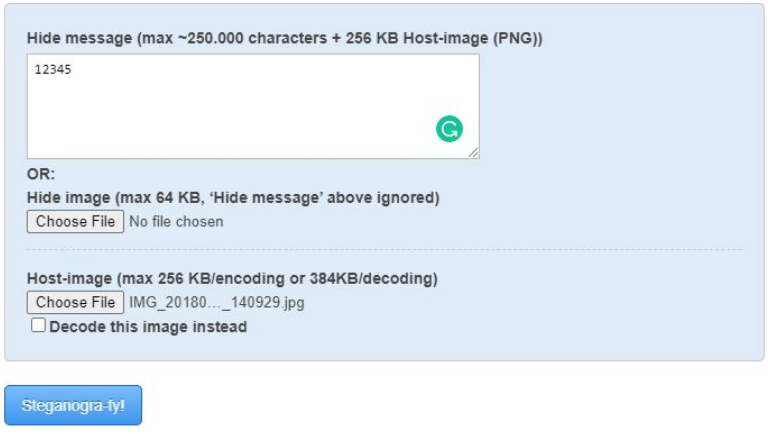


Slika 12. Prikaz sučelja Mobilefish

Slika 13. Opcija embed watermark

2.8.4. Manytools

Ovu stranicu se može gledati kao skupina alata potrebnih za automatiziranje repetitivnih poslova bilo u web dizajnu ili bilo kojem drugom poslu.[12] Jedan od tih alata je još jedan sustav za ubacivanje digitalnog vodenog žiga u sliku. Ima opcije za ubacivanje slike ili teksta u sliku, te dekodiranje iste slike.



Slika 14. Prikaz sučelja Manytools

3. Eksperimentalni dio

U radu se ispituju otpornosti 4 različita sustava za ubacivanje digitalnog vodenog žiga na napade u Adobe Photoshopu. Prije samog testiranja u slike smo ubacili digitalni vodeni žig, koristeći svaki sustav posebno.

Zaštićene slike napadamo sa 4 različita napada (JPEG kompresija, blur, rotacija i skaliranje). Svaki napad ćemo provesti kroz tri razine. Tijekom ispunjavanja tablice koristili smo 4 vrijednosti:

- 1 - Digitali vodeni žig se ne prepoznaje, kvaliteta slike se jako smanjila
- 2 - Digitalni vodeni žig se ne prepoznaje, kvaliteta slike se malo smanjila
- 3 - Digitalni vodeni žig se prepoznaje, kvaliteta slike se smanjila
- 4 - Digitalni vodeni žig se prepoznaje, kvaliteta slike ostala skoro identična

Slika 15. Slike korištene u istraživanju

Digimarc	JPEG kompresija			Blur			Rotacija			Skaliranje		
	25%	50%	75%	1px	3px	5px	45°	90°	135°	-50%	150%	250%
Slika 1	1	1	4	4	3	1	4	4	4	4	4	1
Slika 2	1	1	4	4	3	1	4	4	4	4	4	1
Slika 3	1	1	4	4	3	1	4	4	4	2	4	4
Slika 4	1	1	4	4	3	1	4	4	4	4	4	1
Slika 5	1	1	2	4	3	1	4	4	4	4	4	1

StegOnline	JPEG kompresija			Blur			Rotacija			Skaliranje		
	25%	50%	75%	1px	3px	5px	45°	90°	135°	-50%	150%	250%
Slika 1	1	1	2	2	1	1	2	4	2	1	4	1
Slika 2	1	1	2	2	1	1	2	4	2	1	4	1
Slika 3	1	1	2	2	1	1	2	4	2	1	4	1
Slika 4	1	1	2	2	1	1	2	4	2	1	4	1
Slika 5	1	1	2	2	1	1	2	4	2	1	4	1

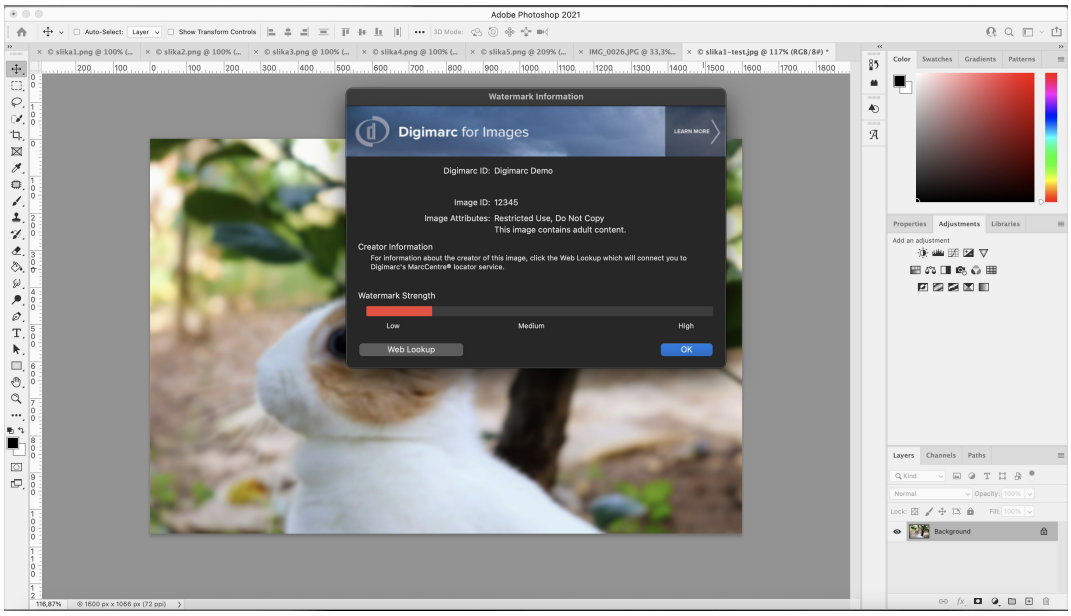
Mobilefish	JPEG kompresija			Blur			Rotacija			Skaliranje		
	25%	50%	75%	1px	3px	5px	45°	90°	135°	-50%	150%	250%
Slika 1	1	1	2	2	1	1	2	2	2	1	2	1
Slika 2	1	1	2	2	1	1	2	2	2	1	2	1
Slika 3	1	1	2	2	1	1	2	2	2	1	2	1
Slika 4	1	1	2	2	1	1	2	2	2	1	2	1
Slika 5	1	1	2	2	1	1	2	2	2	1	2	1

Manytools	JPEG kompresija			Blur			Rotacija			Skaliranje		
	25%	50%	75%	1px	3px	5px	45°	90°	135°	-50%	150%	250%
Slika 1	1	1	2	4	1	1	2	4	2	1	2	1
Slika 2	1	1	2	4	3	1	2	4	2	1	2	1
Slika 3	1	1	2	4	1	1	2	4	2	1	2	1
Slika 4	1	1	2	4	1	1	2	4	2	1	2	1
Slika 5	1	1	2	4	1	1	2	4	2	1	2	1

Slika 16. Rezultati mjerenja otpornosti digitalnog vodenog žiga pojedinih sustava

Kod JPEG kompresije slika nijedan sustav nije mogao očitati digitalni vodeni žig osim Digimarca i to samo kod minimalne kompresije slike. Izuzetak je bila slika 5 na kojoj se nije mogao učitati žig čak niti tijekom minimalne kompresije. Mogući razlog tom rezultatu može biti taj što slika pet sadrži puno crne u sebi zbog koje sliku možemo smatrati kao monokromatsku. Još jedan argument zašto digitalni vodeni žig nije moguće očitati je taj da slika sadrži puno detalja, samim time i izgubi vise detalja tijekom kompresije. Kod zamućenja slike Digimarc-ov digitalni vodeni žig se uspio očitati slike od

1px i 3px zamućenosti. Ostali sustavi nisu mogli pronaći digitalni vodeni žig u slikama osim Manytoolsa koji je mogao očitati svoj digitalni vodeni žig na svim slikama sa 1px zamućenosti i jednu sa 3px.



Slika 17. Očitavanje digitalnog vodenog žiga u Digimarcu nakon 5px blur napada.

Nakon rotacije slika digitalni vodeni žig mogao se očitati u potpunosti kod Digimarca nebitno o stupnju rotacije. StegOnline i Manytools su mogli očitati žig samo ako slika bude rotirana za 90 stupnjeva, dok Mobilefish nije uspio očitati žig nakon bilokakve rotacije slike.Skaliranjem slika žig se mogao očitati jedino kod Digimarca i Stegonlinea. Svi ostali sustavi bi nama davali neadekvatne rezultate. Stegonline može očitati digitalni vodeni žig jedino tijekom 150% skaliranja slike. Digimarc može tijekom -50% i 150% skaliranja. Slika 3 je izuzetak jer se kod nje žig može očitati sa skaliranjem od 150% i 250% dok sa -50% gubi jako u kvaliteti. Razlog zašto je to tako može biti taj da je slika 3 zapravo greyscale slika što znači da sadrži truecolor monokromatske boje. [13]

4. Zaključak

Po završetku eksperimenta analizom dobivenih rezultata možemo ustvrditi da od 4 testirana sustava za ubacivanje digitalnog vodenog žiga, Digimarc preostaje kao sustav sa najvise prednosti i najmanje mana.

Ostali sustavi su se predstavili kao izrazito nepouzdanima gdje jedino Stegonline i Manytools nude vrlo slabu zaštitu slike. Rezultati su bili podjednaki kod sviju slika osim slike 3 i slike 5. Razlog tome je to da su slika 3 i slika 5 monokromatske slike, te da su nam zbog toga dali drugčije rezultate. Ovime možemo zaključiti da boje u slici mogu utjecati na kvalitetu žiga u Digimarc sustavu.

Na kraju se iz eksperimenta može zaključiti kako nemaju svi sustavi za umetanje digitalnog žiga potrebnu razinu zaštite, dok oni koji je imaju poput Digimarca, nude dojmlive rezultate. Digimarc zadržava svoju poziciju kao jedna od vodećih tvtrki u zaštiti digitalnih podataka, te nastoji revolucionizirati zaštitu digitalnog vodenog žiga.

5. Literatura

[1] A. Mandal and M. K. Nigam, "E-R E-R E-R E-R," vol. 1, no. 10, pp. 46–54, 2018.

[2] A. A. Kamal, "Digital watermarking of still images A thesis submitted to the University of Manchester for the degree of Doctor of Philosophy in the Faculty of Engineering and Physical Sciences 2013 Kamal Ali Ahmed School of Electrical and Electronic Engineering," 2013.

[3] X. C. Guo, "Methodologies in Digital Watermarking : Robust and Reversible Watermarking Techniques for Authentication , by Copyright c 2008 by Xin Cindy Guo," 2008.

[4] G. Horak, I. Murat, and M. Domazet, "Digitalni Vodeni Žig," *Fer.Unizg.Hr*, 2010. [Online]. Available: https://www.fer.unizg.hr/_download/repository/Digitalni_Vodeni_Zig%5B1%5D.pdf

[5] "Image Steganography Explained | What is Image Steganography?" [Online]. Available: https://www.mygreatlearning.com/blog/image-steganography-explained/#Understandingimagesteganography

[6] S. Drobac, "ALGORITMI ZA UBACIVANJE I DETEKCIJU," 2005.

[7] Y. Zolotavkin, *New Methods for Digital Image Watermarking New Methods for*, 2015.

[8] C. F. Li, W. Hong, Z. C. Liu, and Y. T. Tian, *Active controllability of flocking behavior based on local interaction*, 2011, vol. 42, no. SUPPL. 1.

[9] "Copyright communication system marcspider."

[10] "StegOnline." [Online]. Available: https://stegonline.georgeom.net/upload

[11] "Mobilefish.com - Online steganography service, hide message or file inside an image." [Online]. Available: https://www.mobilefish.com/services/steganography/steganography.php

[12] “Online Steganography tool (embed/hide secret messages or images within a host-image).” [Online]. Available: https://manytools.org/hacker-tools/steganography-encode-text-into-image/

[13] D. Corporation and S. W. G. Drive, “Best Practices Guide Digimarc for Digital Images.”