CARNet

HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Digitalni vodeni žigovi

NCERT-PUBDOC-2010-08-310

Nacionalni CERT

u suradnji s

LSS

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem Nacionalni CERT kontinuirano radi.

Rezultat toga rada je i ovaj dokument, koji je nastao suradnjom Nacionalnog CERT–a i LS&S–a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

Nacionalni CERT, www.cert.hr

Nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.LSS.hr

Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Brzim razvojem informacijskih sustava i sve većeg broja korisnika Interneta došlo je do promjena u bankarskim poslovima (elektronički novac), znanosti i sličnim područjima, a promijenile su se i društvene prilike. Dokumenti koji su bili na papiru u arhivama sada prelaze u digitalni oblik na računalima. Digitalna tehnologija je postala popularna i proširila se na sve vrste analognih podataka: audio i video zapise, fotografije i sl. Pretvaranjem analognih podataka nastaju digitalni multimedijski dokumenti koji se sve više distribuiraju preko Interneta. Kopiranje digitalnih dokumenata ne narušava kvalitetu (za razliku od analognih) pa se postavlja pitanje što je izvornik, a što kopija. Time se narušava i pitanje pravog i prvog vlasnika dokumenta. Kriptiranjem podataka omogućena je njihova tajnost prilikom distribucije putem javnog kanala (npr. Interneta ili bilo koje računalne mreže). Kada je izvornik dekriptiran i informacije su lako čitljive, zaštita podataka se obavlja korištenjem digitalnih vodenih žigova (eng. Digital watermark). Ideja takve zaštite podataka je skrivanje podataka (informacije) u izvornom dokumentu, bilo da je riječ o fotografiji ili kojem drugom multimedijskom dokumentu. Načini skrivanja informacije u dokumentu su digitalni potpis (eng. Digital signature), pravo imena (eng. Copyright label) i digitalni žig. Pohranjivanjem takve informacije u izvornik, on postaje intelektualno vlasništvo osobe koja je unijela podatak. Digitalno označavanje je pojam koji predstavlja postupak umetanja digitalnog žiga u dokument s namjerom kasnijeg detektiranja ili vađenja žiga za razliku od klasičnih vodenih žigova koji su bili otisnuti na papiru (novčanice, čekovi itd.) i vidljivi pod određenim uvjetima (ultraljubičasto svjetlo).

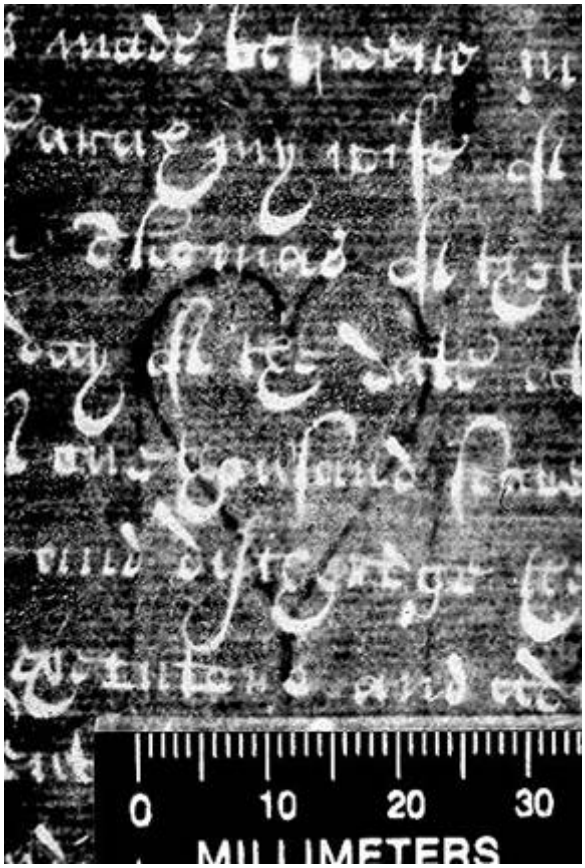
Digitalni vodeni žigovi koriste se za različite vrste označavanja digitalnih dokumenata kao što su:

- **Digitalni potpis** - vlasnik dokumenta stavljanjem vodenog žiga potvrđuje svoje vlasništvo nad dokumentom.
- **Otisci prstiju** - kupci dokumenta stavljanjem svog vodenog žiga u dokument pomažu u praćenju izvora nelegalnih kopija dokumenta.
- **Autentikacija** - korištenjem tzv. "lomljivih žigova" utvrđuje se autentičnost sadržaja dokumenta. Lomljivi vodeni žigovi imaju svojstvo da svaka promjena na dokumentu uzrokuje njihov lom, odnosno kasnije je nemoguće izdvojiti iz dokumenta izvorni žig. Ako se izdvojeni žig poklapa sa sadržajem dokumenta, tada je to znak da sadržaj dokumenta nije mijenjan.
- **Kontrola kopiranja** - vodeni žigovi mogu sadržavati informacije o pravilima upotrebe i kopiranja sadržaja dokumenta. Ta pravila mogu biti oblika "zabrani kopiranje" ili "dozvoli stvaranje samo jedne kopije".
- **Tajna komunikacija (steganografija)** - umetnuti signal vodenog žiga može se iskoristiti i kao nositelj tajne informacije. Skrivanje jedne informacije unutar druge je tipičan primjer steganografije. Upotreba ove tehnologije je savršena za bilo kakvu vrstu špijunaže jer zakonska ograničenja nad alatima za kriptiranje ovdje ne vrijede.

Slika 1. Vodeni žig na novčanici od 100$
Izvor: iTestCash

2. Povijest digitalnih vodenih žigova

Povijest vodenih žigova seže još iz 13. stoljeća. U gradiću Fabriano (Italija), pronađen je najstariji označeni papir koji datira iz 1292. godine i igra važnu ulogu u razvoju papirne industrije. U tom gradu je pri kraju 13. stoljeća tržište dijelilo čak četrdesetak tvornica koje su proizvodile papire različitih oblika, kvalitete i, naravno, cijene. S obzirom na to da je proizvedeni papir imao vrlo grubu površinu koja nije bila pogodna za pisanje, bilo ga je potrebno proslijediti zanatlijama na daljnju obradu. Nakon izglađivanja, papir je bilo potrebno prebrojati, složiti i prodati veletrgovcima. Veliki broj tvornica i zanatlija koji su omekšavali površinu papira i veletrgovaca uzrokovao je potrebu za identifikacijom izvora proizvoda. Tako je došlo do izuma vodenog žiga koji se vrlo brzo proširio po cijeloj Italiji i dalje po Europi. Iako mu je prvotna namjena bila prepoznavanje marke ili tvornice papira, uskoro je služio i za prepoznavanje formata, kvalitete i čvrstoće papira te označavanje datuma proizvodnje i autentičnosti.



Slika 2. Vodeni žig u obliku srca iz 1656. godine
Izvor: os2.zemris.fer

Globalna digitalizacija potaknula je prijelaz žigova s papira na digitalne sadržaje. Vodeni žigovi na novčanicama i poštanskim markama inspirirali su prvu upotrebu termina "*water mark*" u digitalnom kontekstu. Prvu publikaciju s temom digitalnih vodenih žigova objavio je Tanaka 1990. godine, a nju su slijedile publikacije Caronnija i Tirkela 1993. odnosno 1995. godine. nakon ovih publikacija digitalnim vodenim žigovima se počelo pridodavati mnogo više važnosti nego prije i tada je započeo njihov ubrzani razvoj.

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.

3. Digitalni vodeni žigovi

Digitalni vodeni žigovi su novo područje u računalnoj znanosti, kriptografiji, digitalnoj obradi signala i komunikacijama. Svrha postojanja ovog novog područja je omogućiti zaštitu multimedijskih dokumenata u smislu autorskog prava, zaštite kopiranja (eng. C*opyright protection*) i sl. Postupak digitalnog označavanja ili *„Digital Watermarking"* temelji se na umetanju podatka, vodenog žiga (eng. *Watermark*), u izvorni dokument u svrhu njegove ponovne detekcije. Dokument koji se označava može biti bilo koja vrsta informacije: multimedijski dokument, video, slika, zvuk, tekst i sl. Žig može sadržavati bilo koju informaciju, kao na primjer identifikaciju kupca, prodavača ili nešto drugo. Algoritam ili shema koja opisuje postupak označavanja dokumenata digitalnim žigom sastoji se od tri komponente:

1. **vodeni žig**,
2. **koder** – algoritam korišten za umetanje žiga te
3. **dekoder i komparator** – algoritam koji služi za izdvajanje žiga i verifikaciju.

Svaki korisnik ima samo jedan žig koji ga na jedinstven način identificira. Žig se može umetati u bilo koji dokument pomoću algoritma kodiranja, dok se algoritmom dekodiranja on vadi iz označenog dokumenta i jednoznačno se određuje vlasnik i integritet dokumenta.

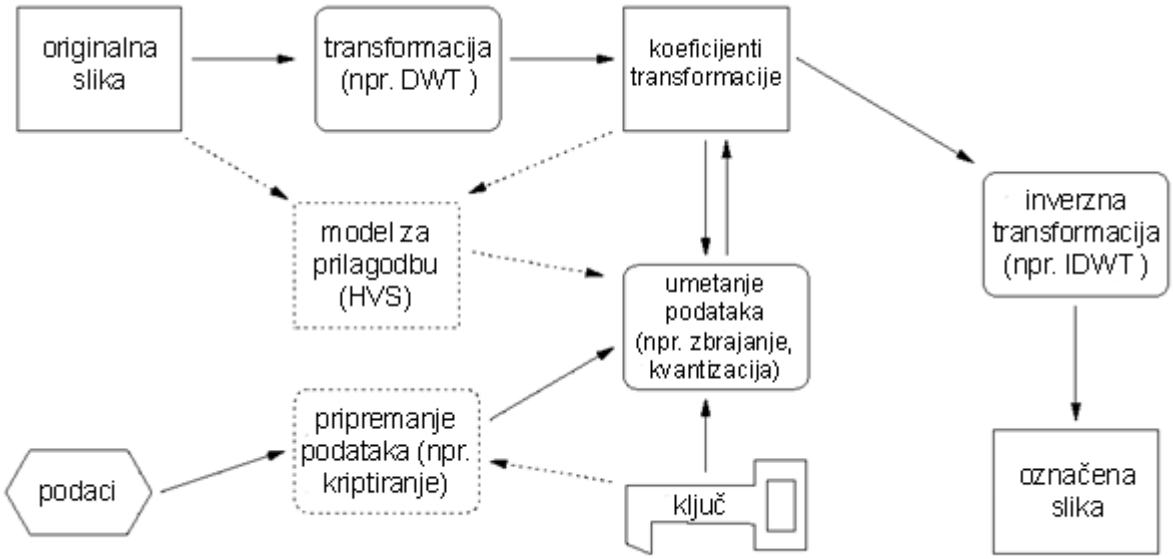
Slika 3. Fotografija označena digitalnim vodenim žigom
Izvor: Wikipedia

3.1. Umetanje digitalnog vodenog žiga

U ovom će se poglavlju na jednostavan način opisati postupak kodiranja digitalnim vodenim žigom uzimajući kao dokument sliku. Ako se izvorna slika označi kao ***I***, „digitalni potpis" kao ***S = s1, s2, ...***, sliku označenu vodenim žigom s ***Î*** i algoritam kodiranja s ***E***, matematički se može opisati postupak kodiranja formulom:

$$E(I, S) = \hat{I}$$

Bitno je napomenuti da „digitalni potpis" ***S*** ovisi o ulaznom dokumentu, tj. o slici. Ovaj koder može se prikazati i grafički kao na slici 4. Ulazni podaci za koder su dokument (slika) i digitalni vodeni žig, a kao izlaz se dobiva nova označena slika (eng. *watermarked image*).



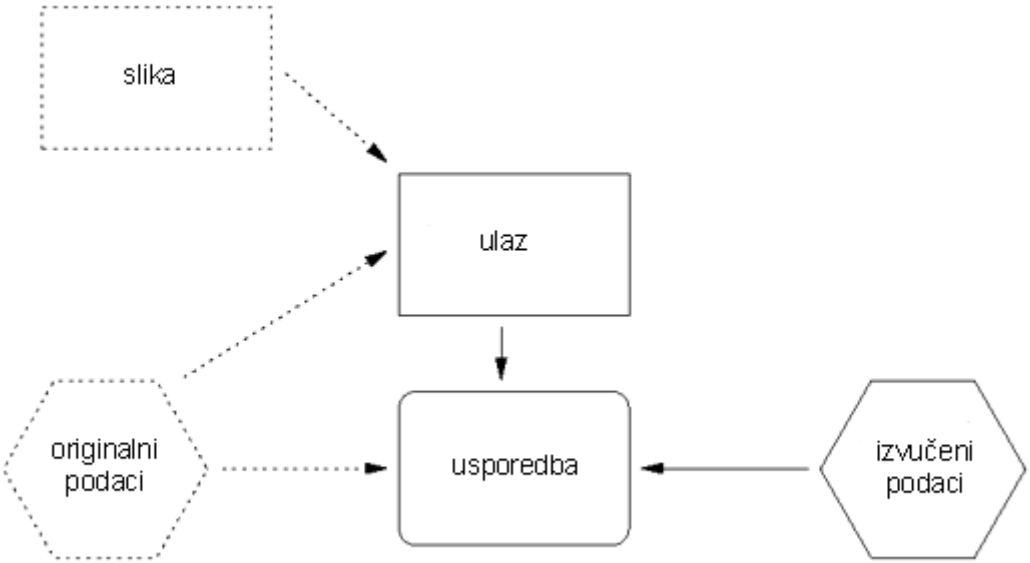
Slika 4. Postupak umetanja digitalnog vodenog žiga u sliku

3.2. Detekcija digitalnog vodenog žiga

Postupak dekodiranja, za razliku od kodiranja, ima dvije faze. Prva je samo dekodiranje, tj. izdvajanje žiga, a druga je verifikacija tj. uspoređivanje žiga s postojećim radi utvrđivanja identiteta korisnika. Kod postupka dekodiranja dekoder je označen slovom ***D***, ulazna slika slovom ***J***, gdje ***J*** može biti označena ili neoznačena (namjerno promijenjena označena) slika kako bi se teže detektirao žig, dok je detektirani žig oznake $\hat{S}$. Neki algoritmi detektiranja vodenog žiga trebaju izvornu sliku, dok kod nekih nije potrebna.

Postupak se matematički može opisati na sljedeći način:

$$D(J, I) = \hat{S}$$



Slika 5. Postupak detekcije i uspoređivanja digitalnog vodenog žiga

Nakon toga izdvojeni žig $\hat{S}$ se uspoređuje u komparatoru $C\delta$ s izvornim žigom i određuje se sličnost. Uz određeni prag sličnosti (korelacije) δ, izlaz iz dekodera je ***1*** ili ***0*** što označava podudaranje žigova (***1***) ili nepodudaranje (***0***).

Matematička formulacija je sljedeća:

$$C\delta(\hat{S}, S) = \{ 1 \text{ za } c \leq \delta \text{ ili } 0 \text{ za ostalo}$$

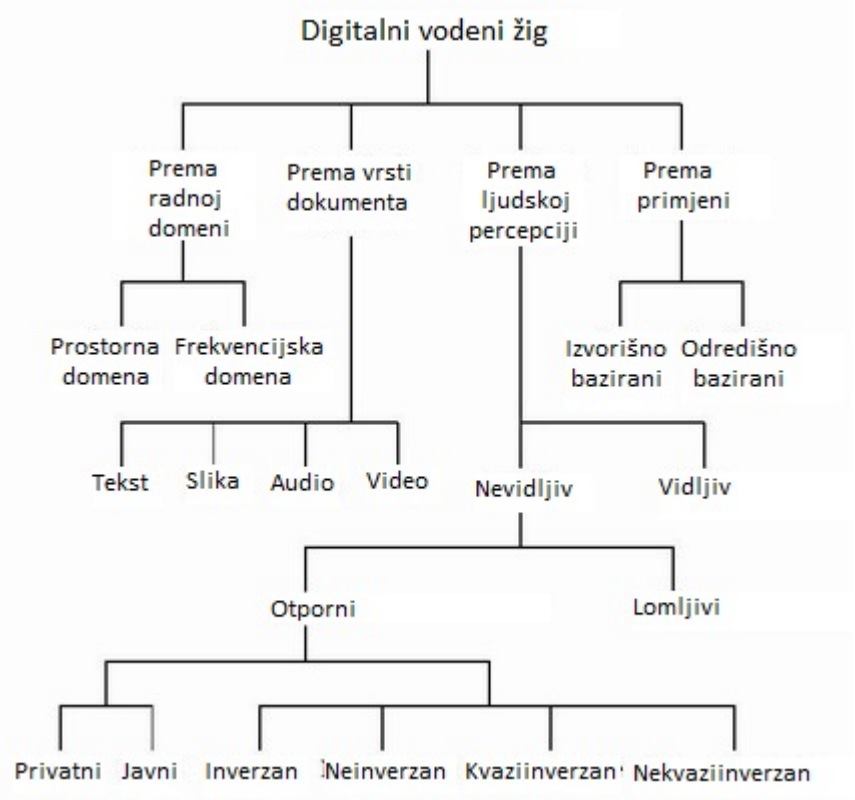
C je korelator, dok je c vrijednost korelacije za dva žiga koja se uspoređuju, $x = C\delta(\hat{S}, S)$, gdje x definira izlaz iz dekodera.

Matematički definirano, algoritam digitalnih vodenih žigova (eng. *watermarking scheme*) je uređena trojka (***E, D, C***δ). Glavno svojstvo algoritma za označavanje jest da umetnuti žig mora biti sigurno detektiran i izvađen. Ovisno o svojstvima žiga algoritama i primjene, postoje *watermarking* sheme koje omogućavaju samo detekciju ili omogućavaju i vađenje žiga. Tako algoritmi imaju nazive *„watermark extraction"* ili *„watermark detection"*.

4. Podjela digitalnih vodenih žigova

Digitalni vodeni žigovi i tehnike označavanja vodenim žigovima podijeljeni su na različite načine. Žigovi se mogu unositi u prostornoj domeni (*eng. spatial domain*) ili u nekoj od frekvencijskih domena (*eng. frequency domain*). U prostornoj domeni digitalni vodeni žig se dodaje direktno slici, dok se u frekvencijskoj domeni radi sa spektrima slike i žiga, tj. spektar žiga se dodaje spektru 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 promjeni sadržaj. Kod prostorne domene promjena se očituje samo u jednom dijelu dokumenta. Ako se taj dio „izreže", kod prostorne domene žig je uništen, dok je kod frekvencijske žig postojan i detektira se iz preostalog dijela dokumenta.

Ostale podjele vodenih žigova prikazane su na sljedećoj slici.



Slika 6. Vrste označavanja digitalnim vodenim žigovima

Tehnike vodenih žigova mogu se, prema tipovima dokumenata, podijeliti u četiri skupine:

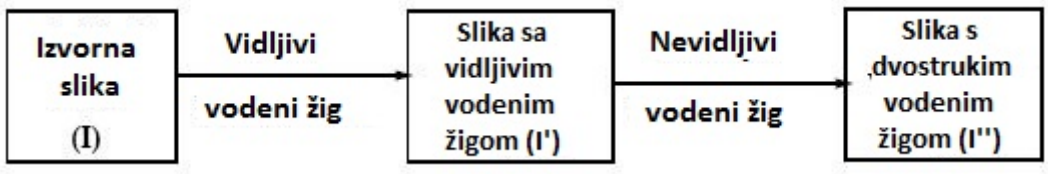
- označavanje **slike,**
- označavanje **videa,**
- označavanje **audio zapisa i**
- označavanje **teksta**.

Iz same podjele može se zaključiti namjena pojedine vrste vodenih žigova.

Podjela prema „vizualnoj" percepciji također sadrži četiri skupine:

- **vidljiv** vodeni žig,
- **robustan nevidljiv** vodeni žig,
- **lomljiv nevidljiv** vodeni žig i
- **dvostruki** vodeni žig .

Samo ime vodenog žiga ne daje jasnu sliku primjene i svojstva vodenog žiga. Kod vidljivog vodenog žiga (eng. *Visible watermark*) na izvornom dokumentu je vidljiv žig u obliku logo ili slične oznake. Robustan nevidljiv vodeni žig (eng. *Invisible – Robust watermark*) je vizualno nevidljiv, ali ga detektira dekoder. Uz to, otporan je na napade (npr. JPEG kompresija ne može uništiti žig). Kod lomljivog nevidljivog žiga (eng. *Invisible – Fragile watermark*) žig je također nevidljiv, ali se može detektirati i nije otporan ni na jednu vrstu napada (npr. ne prolazi JPEG kompresiju). Dvostruki vodeni žig (eng. *Dual watermark*) je kombinacija vidljivog i nevidljivog vodenog žiga (Slika 7).



Slika 7. Shematski prikaz dvostrukog digitalnog vodenog žiga

U podjeli prema robusnosti digitalni vodeni žigovi se dijele na dva načina. To su:

- javne sheme i
- tajne sheme.

Osim toga, dijele se i na:

- inverzne sheme (eng. Invertible watermarking scheme),
- neinverzne sheme (eng. Non invertible watermarking scheme),
- poluinverzne sheme (eng. Quasi invertible watermarking scheme) i
- nepoluinverzne sheme (eng. Nonquasi invertible watermarking scheme).

Tajne sheme vodenih žigova (*eng. Private watermarking scheme*) trebaju kod detekcije žiga izvornu „sliku", a javne sheme žigova (*eng. Public watermarking scheme*) je ne zahtijevaju. Svojstvo sheme inverznog vodenog žiga je temeljeno na matematičkoj notaciji i glasi:

$$1.\ E^{-1}(\hat{I}) = (I', S')$$

$$2.\ E(I', S') = (\hat{I})$$

$$3.\ C\delta(D(\hat{I}), S') = 1$$

Prvo svojstvo ukazuje na to da je inverzni algoritam kodiranja slike s digitalnim žigom funkcija originalne slike i digitalnog žiga. Drugo svojstvo kaže da se kodiranjem originalne slike i digitalnog žiga dobije slika s digitalnim žigom, a treće svojstvo govori da su dekodirana slika s žigom i digitalni žig identični. Ako prethodna svojstva ne vrijede shema je neinverzna.

Svojstvo poluinverzne sheme također je definirano matematičkom notacijom i glasi:

$$1.\ E^{-1}(\hat{I}) = (I', S')$$

$$2.\ C\delta(D(\hat{I}), S') = 1$$

Dakle, poluinverzne sheme su one koje zadovoljavaju dva od tri uvjeta inverzne sheme. Shema koja ne ispunjava prethodno svojstvo je nepoluinverzna.

Podjela na temelju primjene ima dvije vrste, a to su:

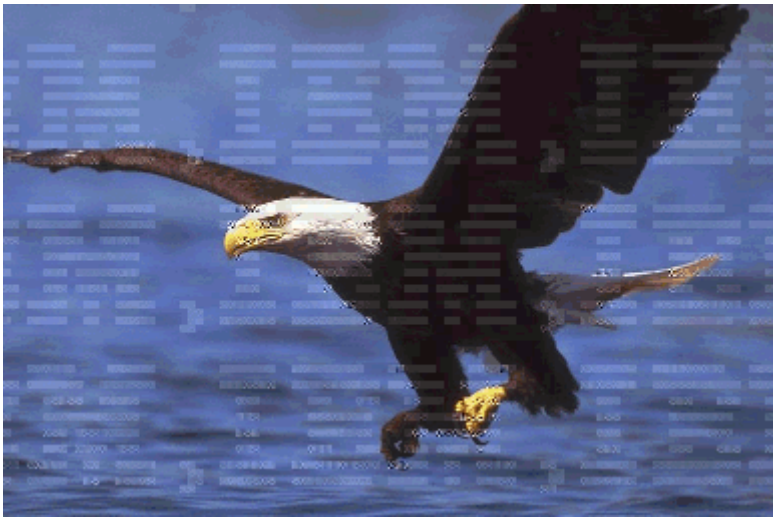
- **izvorišno** zasnovane i
- **odredišno** zasnovane sheme.

Izvorišno zasnovane (eng. *Source based*) sheme temelje se na principu autorskog prava (eng. *Ownership*) i autentikacije, tj. žig se unosi u izvornik i pri svakoj distribuciji u izvorniku se nalazi identifikacija vlasnika (intelektualno vlasništvo). Za odredišno zasnovane sheme (eng. *Destination based*) žig se unosi kod svake kopije izvornika, a time se postiže da svaki vlasnik (kupac) ima jedinstveni „vlastiti izvornik". Kod kopije se može pratiti čija se nelegalna kopija proširila u tuđe ruke i određenim sankcijama teretiti pravog vlasnika. Tim načinom rješava se problem prava kopiranja (eng. © *Copyright*).

5. Primjena digitalnih vodenih žigova

Vidljivi vodeni žig

- Koristi se za naprednu zaštitu od kopiranja. Primjer je slika koja se nalazi na Internetu i na njoj se nalazi vidljivi vodeni žig (slika 8). Njime se označava da se slika ne može koristiti u komercijalne svrhe bez naplate.
- Koristi se za zaštitu autorskog prava. Primjer toga je da fakultet izdaje knjige na kojima se nalazi njegov logo. Knjige se slobodno koriste za osobne potrebe, ali se ne mogu iskoristiti u komercijalne svrhe.



Slika 8. Fotografija označena vidljivim vodenim žigom
Izvor: IBM

Robusni nevidljivi vodeni žigovi

- Koriste se za detektiranje nelegalnih dokumenata. Primjer toga je slika koju prodavač, koji ima licencu, proda osobi koja je javno postavi na Internet. S tim je prodavač zakinut za prihod.
- Koriste se za evidentiranje autorskog prava. Primjer toga je da prodavač uvidi da je neka slika nastala mijenjanjem njegova izvornika. On provjeri je li na toj slici njegov žig tj. je li on vlasnik promijenjenog izvornika.

Lomljivi nevidljivi vodeni žigovi

- Koriste se kao nevidljivi žigovi za pouzdane (sigurne) kamere. Primjer toga je da se kod snimanja trgovine žig unosi u trenutku snimanja u kameri. Pregledavanjem snimke s žigom može se utvrditi je li snimka mijenjana.
- Koriste se kao nevidljivi žigovi za detekciju promjene slike u digitalnoj knjižnici. Primjer toga je baza podataka ljudskih otisaka prstiju. Prilikom snimanja u bazu na sliku se stavlja žig. Svaka promjena otiska može se detektirati jer je žig uništen i otisak nije valjan.

Primjene digitalnih vodenih žigova mogu se klasificirati na više različitih načina (ovisno o mediju, poruci itd.). Klasifikacija koja slijedi temelji se na otpornosti vodenog žiga na napade.

5.1. Dokazivanje autentičnosti sadržaja

Postoje različiti programski sustavi za uređivanje digitalnog sadržaja. S obzirom da je jednostavno mijenjati digitalni sadržaj bitno je naći način za dokazivanje integriteta i autentičnosti sadržaja. Rješenje ovog problema može se posuditi iz kriptografije, gdje se digitalni potpis koristi za dokazivanje autentičnosti. U slučaju označavanja digitalnim vodenim žigom digitalni potpis može biti vodeni žig koji će se ugraditi u sadržaj. Za dokazivanje autentičnosti preporuča se korištenje lomljivog vodenog žiga jer lomljivi vodeni žig mora postati nevažeći u slučaju izmjena te se njegovim korištenjem može saznati kako je digitalni sadržaj izmijenjen ili koji je dio izmijenjen.

5.2. Praćenje emitiranja

Mnoštvo multimedijskih proizvoda svakodnevno se emitira preko televizijske mreže: vijesti, filmovi, sportska događanja, reklame, itd. Emitiranje je vrlo skupo i oglašivači moraju izdvajati značajna financijska sredstva za svako emitiranje kratkih reklama koje se pojavljuju za vrijeme pauza popularnih filmova, serija ili sportskih događaja. Mogućnost precizne naplate vrlo je bitna. Oglašivači žele biti sigurni da plaćaju samo za reklame koje su se emitirale.

Praćenje emitiranja (eng. *Broadcast Monitoring*) obično se koristi za prikupljanje informacije o sadržaju koji se emitira. Prikupljene informacije koriste se za naplaćivanje i druge potrebe. Jednostavan način praćenja je korištenje ljudskih promatrača koji prate i bilježe sve što vide. Ova vrsta praćenja je skupa i sklona greškama. Automatizirano praćenje je očito bolji izbor. Postoje dvije vrste sustava za automatizirano praćenje: pasivni i aktivni. Pasivni sustav prati sadržaj koji se emitira i pokušava ga povezati s poznatim sadržajem pohranjenim u bazi. Implementacija pasivnih sustava nije jednostavna iz nekoliko razloga. Usporedba odaslanih signala sa sadržajem baze nije jednostavna. Održavanje velike baze sadržaja za usporedbu je skupo. Aktivni sustavi za praćenje oslanjaju se na dodatnu informaciju koja identificira sadržaj. Dodatna informacija emitira se zajedno sa sadržajem. Jedno od rješenja za aktivno praćenje je i označavanje digitalnim vodenim žigom. Vodeni žig koji sadrži informaciju za identifikaciju emitiranja ugrađuje se u sam sadržaj. Za ovu primjenu vodeni žigovi moraju biti otporniji na napade od lomljivih žigova te ih se mora moći lagano očitati.

5.3. Ostavljanje otisaka

Postoje određene primjene u kojima dodatna informacija o digitalnom sadržaju treba sadržavati informacije o krajnjem korisniku, a ne o vlasniku sadržaja. Primjer toga je okruženje u kojem se stvaraju filmovi. Za vrijeme produkcije filma manji dijelovi rada na filmu obično se svaki dan distribuiraju određenom broju ljudi uključenom u stvaranje filma. Ti dnevni dijelovi filmova su povjerljivi te, ako određena inačica procuri, studio želi imati mogućnost identificirati uzročnika curenja informacija. 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.

Drugi primjer primjene je distribucija filmova kinima u digitalnom formatu umjesto korištenja poštanskih usluga i celuloidnih formata. Iako je ovakva distribucija prilagodljivija, učinkovitija i jeftinija, producenti i distributeri je ne prihvaćaju jer se boje potencijalnog novčanog gubitka uzrokovanog ilegalnim kopiranjem i redistribucijom filmova. Rješenje ovog problema je da svako kino primi kopiju koja se jedinstveno veže uz kino. U slučaju pojave ilegalnih kopija, može se saznati koje je kino odgovorno te poduzeti potrebne pravne akcije protiv istog.

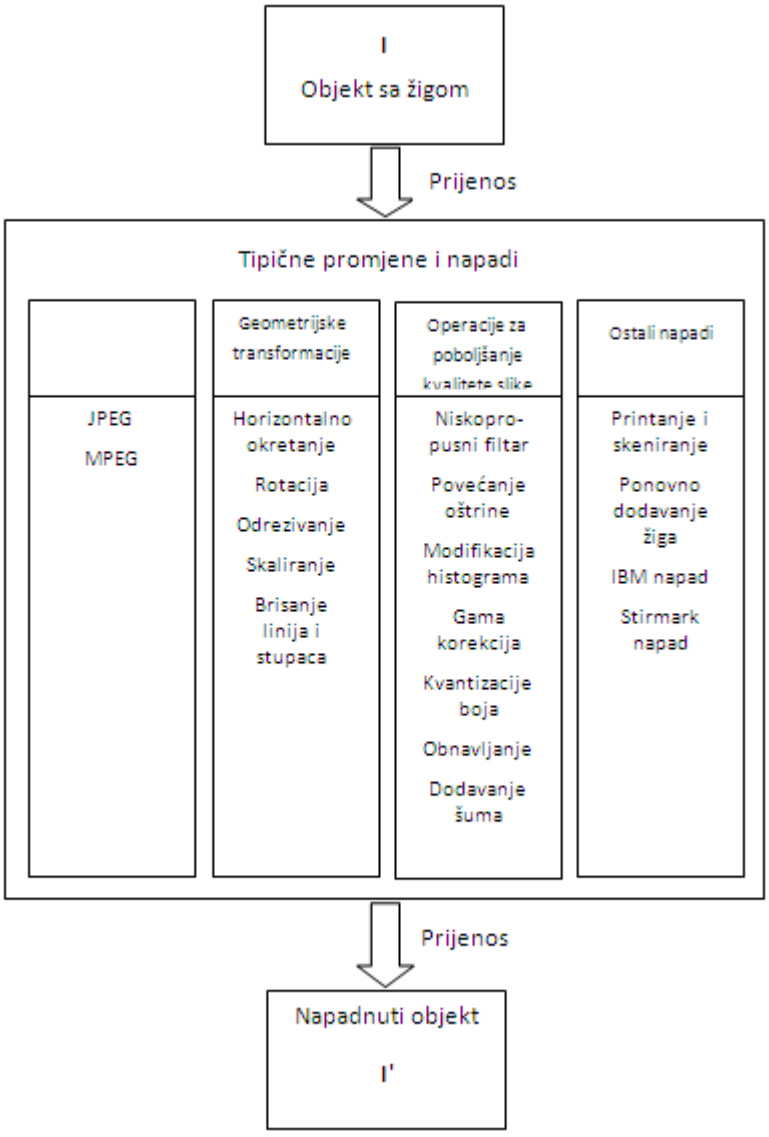
Povezivanje jedinstvene informacije o svakoj distribuiranoj kopiji digitalnog sadržaja zove se ostavljanje otisaka (eng. *Fingerprinting*). Označavanje vodenim žigovima je odgovarajuće rješenje za ovu primjenu jer je nevidljivo i nedjeljivo od sadržaja. Ovaj je tip primjene poznat i pod imenom *praćenje izdajica* (eng. *Traitor tracing*) jer je korisno kod praćenja ilegalno proizvedenih kopija digitalnog sadržaja. Ova primjena zahtijeva visoku razinu otpornosti vodenog žiga od različitih vrsta obrade podataka i zlonamjernih napada.

5.4. Zaštita autorskih prava

Zaštita autorskih prava jedno je od prvih područja za koja je označavanje digitalnim vodenim žigom namijenjeno. Vodeni žig, u ovom slučaju, sadrži informaciju o vlasniku autorskog prava i neprimjetno se ugrađuje u za to namijenjeni sadržaj. Ako korisnici digitalnog sadržaja imaju lagani pristup detektorima vodenog žiga mogu prepoznati i interpretirati ugrađeni vodeni žig te tako identificirati vlasnika autorskog prava.

6. Sigurnost digitalnih žigova

Svrha napada na vodene žigove je uništavanje vodenog žiga s ciljem ukidanja zabrane kopiranja, brisanja vlasnika dokumenta i ostalih nelegalnih radnji. Druga svrha je da neki žigovi moraju biti otporni na osnovne operacije kao što su pojačavanje kontrasta, svjetline, kompresija videa, slike i sl.



Slika 9. Napadi na digitalne vodene žigove
Izvor: os2.zemris.fer

JPEG kompresija je vrsta napada na digitalne vodene žigove i trenutno jedan od najraširenijih formata zapisa slika. Bilo koji sustav vodenih žigova mora biti otporan na promjene unesene JPEG kompresijom. Pod promjenama unesenim JPEG kompresijom smatra se smanjenje broja piksela unutar slike.

Geometrijske transformacije su operacije koje se primjenjuju na geometrijski opis objekta. Također, one mijenjaju sliku pa se smatraju i vrstom napada na vodene žigove. Neke od geometrijskih transformacija su:

- Horizontalno okretanje (eng. *Horizontal flip*) - Mnoge slike mogu se okrenuti oko horizontalne osi bez gubljenja informacije. Iako je otpornost na ovu operaciju lako izvesti, malo sustava vodenih žigova ju preživljava.
- Rotacija (eng. *Rotation*) - Rotacija za „mali" kut, posebno u kombinaciji sa odrezivanjem, obično ne mijenja komercijalnu vrijednost slike, ali može učiniti žig neprepoznatljivim. Rotacija je jako česta operacija u procesu skeniranja slika.
- Odrezivanje (eng. *Cropping*) - U nekim slučajevima napadači su zainteresirani samo za neki (npr. središnji) dio slike, štoviše mnoge web stranice koriste segmentaciju slike. Segmentacija slike je osnova za tzv. "*Mosaic*" napad [3]. "*Mosaic*" napad može se opisati kao ekstreman slučaj odsijecanja slike.
- Skaliranje (eng. *Scaling*) - Jako česta operacija koja se obavezno događa kad se otisnuta slika skenira. Isto tako gotovo je obavezna u pripremi slika za web izdavaštvo. Postoje dva osnovna tipa skaliranja: uniformno i neuniformno. Uniformno skaliranje je ono kod kojeg se zadržava omjer veličina stranica slike. Kod neuniformnog skaliranja taj se omjer ne čuva. Mnogi žigovi otporni su samo na uniformno skaliranje.
- Brisanje linija ili stupaca - Ovaj napad je vrlo učinkovit protiv jednostavnih implementacija žigova koji rade na principu raspršenog spektra u prostornoj domeni (eng. *Spread spectrum in spatial domain*).
- Opće geometrijske transformacije – Nastaje kao kombinacija neuniformnog skaliranja, rotacije i razmućivanja.

Operacije za poboljšanje kvalitete slike

- Niskopropusni filtar - Uključuje linearne i nelinearne filtre. Često korišteni filtar je Gaussov filtar. Niskopropusni filtri mijenjaju sliku tako da omekšavaju oštre rubove slika, a time utječu i na digitalni vodeni žig unutar slike.
- Povećanje oštrine - Već je dugo standardna funkcija u programu za obradu slika. Ovi filtri su jako dobri za napade na neke tipove žigova jer vrlo uspješno pronalaze i uklanjaju visokofrekvencijski šum koji takav tip žiga unosi u sliku. Suptilniji napadi zasnovani su na Laplace-ovom operatoru.
- Modifikacija histograma - Uključuje rastezanje i izravnavanje histograma (stupčasti graf za prikazivanje podataka raspoređenih u određene kategorije i grupe) kao česte operacije kojima se kompenziraju loši uvjeti osvjetljenja.
- Gama korekcija - vrlo česta operacija za poboljšanje kvalitete slika.
- Kvantizacija boja - Operacija koja se često koristi u pretvorbi slika u GIF format zapisa za prikazivanje na web stranicama.
- Obnavljanje - Ove tehnike se obično koriste da bi se smanjili efekti određene degradacije slika, ali bi se mogli upotrijebiti i za uklanjanje degradacije koju je unio vodeni žig, čime bi se uklonio i sam vodeni žig.
- Dodavanje šuma - aditivni šum i nekorelirani multiplikativni šum se često spominju u literaturi o teoriji komunikacija i obradi signala. Autori žigova često tvrde da njihovi žigovi preživljavaju ovakav šum, ali mnogi ne napomenu koliku amplitudu šuma može njihov žig podnijeti.

7. Algoritmi za ubacivanje i detekciju digitalnih vodenih žigova

Iako se digitalnim vodenim žigovima mogu zaštititi raznovrsni podaci, zaštita slika je najraširenija i najjednostavnija za objašnjavanje algoritama. Upravo zbog toga će se u nastavku poglavlja kao primjer uzeti zaštita slika digitalnim vodenim žigovima. Razvijeni su brojni algoritmi digitalnih vodenih žigova s ciljem zaštite autorskih prava digitalnih slika i provjere integriteta podataka. Kod većine algoritama obavlja se transformacija *slike domaćina* (originalne slike) u domenu koja omogućuje umetanje otpornih i nevidljivih digitalnih žigova. Većina pristupa uključuje diskretnu kosinusnu transformaciju, no noviji zahtjevi nalažu istraživanja i drugačijih (kompleksnijih) pristupa.

7.1. Podjela algoritama

Algoritmi digitalnog vodenog žiga mogu se podijeliti s obzirom na:

- Domenu u kojoj se obavlja umetanje/izvlačenje žiga:
  - prostorna domena,
  - diskretna kosinusna domena,
  - diskretna Fourierova domena,
  - diskretna domena valića i
  - Fourier-Mellinova domena.
- Dostupnost referentnih podataka (npr. slike domaćina) za izvlačenje žiga:
  - slijepe,
  - poluslijepe i
  - neslijepe.
- Metodu modifikacije slike domaćina:
  - linearno zbrajanje signala raspršenog spektra,
  - stapanje slika (prilikom umetanja loga) i
  - postupak nelinearne kvantizacije i zamjene.
- Strategiju perceptualnog modeliranja:
  - bez modeliranja,
  - implicitno modeliranje pomoću osobina domene transformacije i
  - eksplicitno modeliranje pomoću modela ljudskog vizualnog sustava.
- Namjenu:
  - zaštita autorskog vlasništva, praćenje cirkulacije podataka,
  - verifikacija i autentikacija slika s detekcijom neovlaštenih izmjena sadržaja te
  - skrivanje podataka i imenovanje slika.
- Oblik medija domaćina:
  - slike,
  - video i
  - posebni multimedijalni formati kao što su crtane slike i mape.

Svi opisani algoritmi su namijenjeni označavanju sivih slika. Slike u boji se mogu označavati tako da se prvo prebace u YUV područje boja [6] i zatim se označuje komponenta osvjetljenja Y. Ostale komponente se najčešće ne koriste jer imaju premaleni raspon i kapacitet za potrebe digitalnog vodenog žiga. Drugi način označavanja slika u boji je označavanje svake RGB komponente posebno, ili pak samo jedne, najčešće plave jer se za plavu boju smatra da ljudski vizualni sustav njene promjene najslabije detektira.

Sljedeće poglavlje u kratkim će crtama opisati tri najraširenija algoritma za ubacivanje i detekciju digitalnog vodenog žiga.

7.2. Coxov algoritam

Coxov algoritam je, uz Kochov, najpoznatiji algoritam koji koristi diskretnu kosinusnu transformaciju. Autori ovog algoritma su Ingemar J. Cox, Joe Kilian, Tom Leighton i Talal G. Shamoon s NEC Research Instituta. Kao digitalni vodeni žig uzima se Gaussov niz od 1000 pseudo-slučajnih brojeva koji se zatim zbraja s 1000 najvećih koeficijenata DCT-a (eng. Discrete cosine transform). Na slici 10. prikazana je smanjena crno-bijela slika prije umetanja digitalnog vodenog žiga Coxovim algoritmom, a na slici 11. nakon umetanja. Izvorne dimenzije slike su 512x512 piksela. Usporedbom digitalnog vodenog žiga izvučenog iz označene slike i umetnutog žiga dobije se Hammingova udaljenost, tj. mjera sličnosti između početne slike i slike s digitalnim žigom. U ovom primjeru ona iznosi d = 0.999999.

Slika 10. Slika prije umetanja digitalnog vodenog žiga Cox-ovim algoritmom

Slika 11. Slika nakon umetanja digitalnog vodenog žiga Cox-ovim algoritmom

7.3. Algoritam Corvi

Algoritam Corvi su razvili Marco Corvi i Gianluca Nicchiotti s Elsag-Bailey Research istraživačkog laboratorija iz Genove (Italija). Digitalni vodeni žig je Gaussov niz pseudoslučajnih realnih brojeva dužine 32x32 (sveukupno 1024 realna broja). Algoritam sliku domaćina prebacuje u diskretnu domenu valića i samo se niskofrekvencijski koeficijenti zbrajaju s žigom. Na slici 12. prikazana je crno-bijela slika prije umetanja digitalnog vodenog žiga algoritmom Corvi, a na slici 13. nakon umetanja. Usporedbom digitalnog vodenog žiga izvučenog iz označene slike i umetnutog žiga dobije se Hammingova udaljenost d = 0.950000.

Slika 12. Slika prije umetanja digitalnog vodenog žiga algoritmom Corvi

Slika 13. Slika nakon umetanja digitalnog vodenog žiga algoritmom Corvi

7.4. Algoritam Xia

Algoritam Xia je još jedan od algoritama koji koristi diskretnu domenu valića. Razvili su ga Xiang-Gen Xia, Charles G. Boncelet i Gonzalo R. Arce s odjela za Električni i kompjuterski inženjering Sveučilišta u Delawareu, Newark, USA. Kao digitalni vodeni žig koristi se Gaussov niz pseudoslučajnih realnih brojeva. Autori preporučuju prijelaz u diskretnu domenu valića dvorazinskom strukturom rastava uz upotrebu Haarovog filtra [7]. Digitalni vodeni žig se umeće u velike koeficijente visokih i srednjih frekvencijskih pojaseva (detaljnih podpojaseva) pa se, za razliku od algoritma Corvi, digitalni vodeni žig uopće ne nalazi u niskofrekvencijskom podpojasu. S obzirom na to da veliki koeficijenti u detaljnim podpojasevima najčešće predstavljaju rubove, ovim algoritmom se najviše energije digitalnog vodenog žiga koncentrira u područja rubova i tekstura. Time se postiže dobra nevidljivost umetnutog žiga jer je ljudsko oko je manje podložno primjećivanju promjena kod rubova i tekstura, za razliku od promjena uzrokovanima u području niskih frekvencija. Na slici 14. prikazana je slika prije umetanja digitalnog vodenog žiga, a na slici 15. nakon umetanja. Usporedbom digitalnog vodenog žiga izvučenog iz označene slike i umetnutog žiga dobije se Hammingova udaljenost d = 0.997599.

Slika 14. Slika prije umetanja digitalnog vodenog žiga algoritmom Xia

Slika 15. Slika nakon umetanja digitalnog vodenog žiga algoritmom Xia

Iz dobivenih rezultata može se zaključiti da je algoritam Cox učinkovit za teksturirane slike sa što manje ploha jednake svjetline. Za razliku od njega, algoritam Corvi se najbolje ponaša kod se radi o slici sa što manje tekstura, a digitalni vodeni žig ubačen algoritmom Xia najmanje je vidljiv na slikama koje sadrže određeni dio tekstura.

8. Zaključak

Suština digitalnih vodenih žigova je zaštita vlasništva od izrade ilegalnih kopija. Bilo bi korisno kada bi se ugrađeni vodeni žig mogao koristiti i kao dokaz vlasništva. Moguć je i sljedeći scenarij: vlasnik autorskog prava distribuira svoj digitalni sadržaj s ugrađenim vlastitim nevidljivim vodenim žigom. U slučaju spora oko vlasništva autorskog prava, legalni vlasnik bi trebao moći dokazati svoje vlasništvo. To se ostvaruje tako da stvarni vlasnik predoči izvorni dokument i detektor vodenog žiga. Sporni sadržaj je izvorni dokument u koji je ugrađen vodeni žig. Detekcijom vodenog žiga vlasnika u spornom dokumentu dokazuje se vlasništvo nad dokumentom. Nažalost, gornji scenarij uz određene pretpostavke može biti pobijen, a i označavanje vodenim žigom još nije dovoljno pouzdano za dokazivanje vlasništva. Jedan potencijalni problem je povezan s dostupnosti detektora vodenog žiga. Ako je detektor dostupan većem broju ljudi ne može se očuvati sigurnost vodenog žiga. U tom slučaju uvijek je moguće detektirati i ukloniti vodeni žig. To se može napraviti većim brojem neprimjetnih izmjena na označenom sadržaju sve dok detektor više ne može detektirati vodeni žig. Jednom kada je vodeni žig uklonjen izvorni vlasnik ne može više dokazati svoje vlasništvo. Čak i ako se vodeni žig ne ukloni u nekim uvjetima moguće je dodati novi vodeni žig preko postojećeg i to za sve kopije dokumenta (uključujući izvorni dokument). Zbog toga je potrebno moći identificirati prvi, vodeni žig koji je stvarni vlasnik ugradio. Zbog svega toga za ovu primjenu potrebna je najviša razina otpornosti vodenog žiga. Unatoč tome, tehnika digitalnih vodenih žigova je vrlo mlada i u svojoj novijoj povijesti, posljednjih petnaestak godina, veoma je napredovala. Kako vrijeme bude prolazilo, žigovi će postajati sve otporniji i robusniji i samo je pitanje vremena kad će se digitalnim vodenim žigovima moći zaštititi bilo koji podatak bez straha od njegovog nelegalnog kopiranja i korištenja.

9. Reference

[1] Tihana Golub: Diplomski rad Zaštita teksta digitalnim vodenim žigom, http://os2.zemris.fer.hr/wm/2007_poljak/index.html, studeni 2007.

[2] Matija Podravec: Seminarski rad Digitalni vodeni žig, http://os2.zemris.fer.hr/wm/2002_podravec/index.html, ožujak 2002.

[3] Fabien A.P. Petitcolas, Ross J. Anderson, and Markus G. Kuhn: Attacks on Copyright Marking Systems,

[4] Tomislav Novosel: Diplomski rad Digitalni vodeni žig, http://os2.zemris.fer.hr/wm/2005_novosel/dvz.pdf, lipanj 2005.

[5] Rukavina Domagoj: Seminarski rad Algoritmi za označavanje crno bijelih slika digitalnim vodenim žigom, http://os2.zemris.fer.hr/wm/2008_rukavina/, ožujak 2008.

[6] YUV Colorspace, http://en.wikipedia.org/wiki/YUV , kolovoz 2010.

[7] Haar Wavelet Implementation, http://www.tomgibara.com/computer-vision/haar-wavelet, kolovoz 2010.