Sveučilište u Zagrebu
Grafički fakultet

Završni Rad

Sebastian Wagner

Sveučilište u Zagrebu
Grafički fakultet

tehničko-tehnološki

Sebastian Wagner

Završni Rad
Digitalni Vodeni Žig

Klasifikacija metoda za označavanje slike digitalnim vodenim žigom

Mentor:
Ante Poljičak

Student:
Sebastian Wagner

Zagreb, 2021.

Sažetak

Ovaj će završni rad prikazati primjere nedopuštenog korištenja i otkrivanja vodenih žigova u autorskim djelima. S obzirom na postojeće metode primjene tradicionalnih i digitalnih vodenih žigova, rad će također diskutirati različita svojstva vodenih žigova. Također, u ovom će se radu obraditi i klasificirati moderne metode označavanja slike digitalnim vodenim žigom. Rad će ponuditi pregled i klasifikaciju postojećih metoda ovisno o domeni u kojoj se koriste, vrsti slika koje se označavaju, otpornosti vodenog žiga na različite namjerne i ne namjerne napade na sliku.

Sadržaj

1. Uvod/Introduction

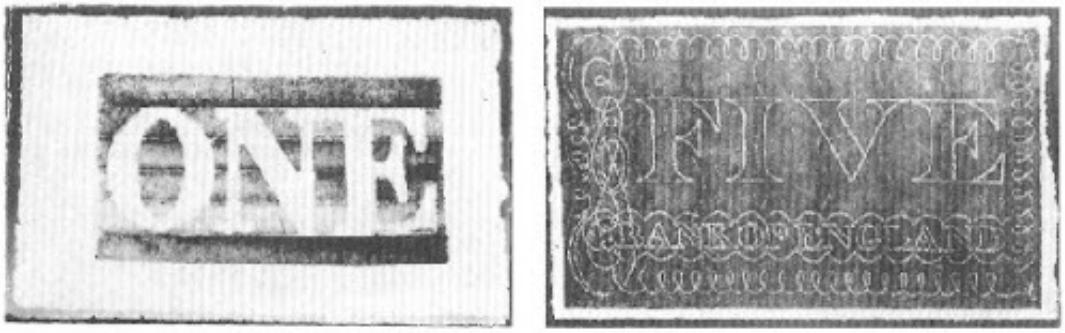
Umjetnost izrade papira je izmišljena u kini skoro prije tisuću godina. Prvi vodeni žigovi na papiru su se pojavili u Italiji 1282. godine [1]. Oznake prvih vodenih žigova su napravljene dodavanjem tankih žica savijenim u obliku uzorka te šablone koje su zatim dodane u kalupe papira. Papir bi bio tanji na mjestima gdje su dodani žičani uzorci te time bio transparentniji na tim dijelovima.

Značenje prvih vodenih žigova nije otkriveno, no pretpostavlja se da su bili korišteni u praktične svrhe poput identifikacije kalupa na kojima su se listovi papira izrađivali, i način na koji bi se utvrdili proizvođači papira. Pretpostavlja se da su možda ti vodeni žigovi predstavljali mitske znakove i bili korišteni u svrhu dekoracije papira.

Do 18-og stoljeća, vodeni žigovi na papiru se pojavljuju u Europi i Americi te se njihova upotreba postaje praktična. Korišteni su kao zaštitni znakovi, za evidentiranje datuma kada je papir proizveden i da indicira veličinu početnog papira. Vodeni žigovi počinju biti korišteni u svrhu zaštite protiv krivotvorenja novca i sličnih dokumenata od velike važnosti.

Izraz "watermark" je nastao krajem 18-og stoljeća te se pretpostavlja da je podrijetlo riječi potječe od njemačke riječi "wasser-marke". Izraz "watermark" je zapravo pogrešan naziv, voda nema nikakvog utjecaja prilikom stvaranja oznake u papiru, ali se pretpostavlja da je dobilo naziv jer izgled oznake nalikuje na reljef kakav voda ima kada se nalazi na papiru. U isto doba krivotvoritelji počinju razvijati tehnike kojima kopiraju šablone koje su korištene za sigurnost papirnatog novca. Krivotvorenje je potaknulo razvitak tehnologije vodenog žiga.

William Congreve, je Britanac koji je izumio tehniku obojenih vodenih žigova tako što je umetnuo obojeni materijal u sredinu papira prilikom procesa izrade papira.



Slika 1. Vodeni žig Williama Congreva

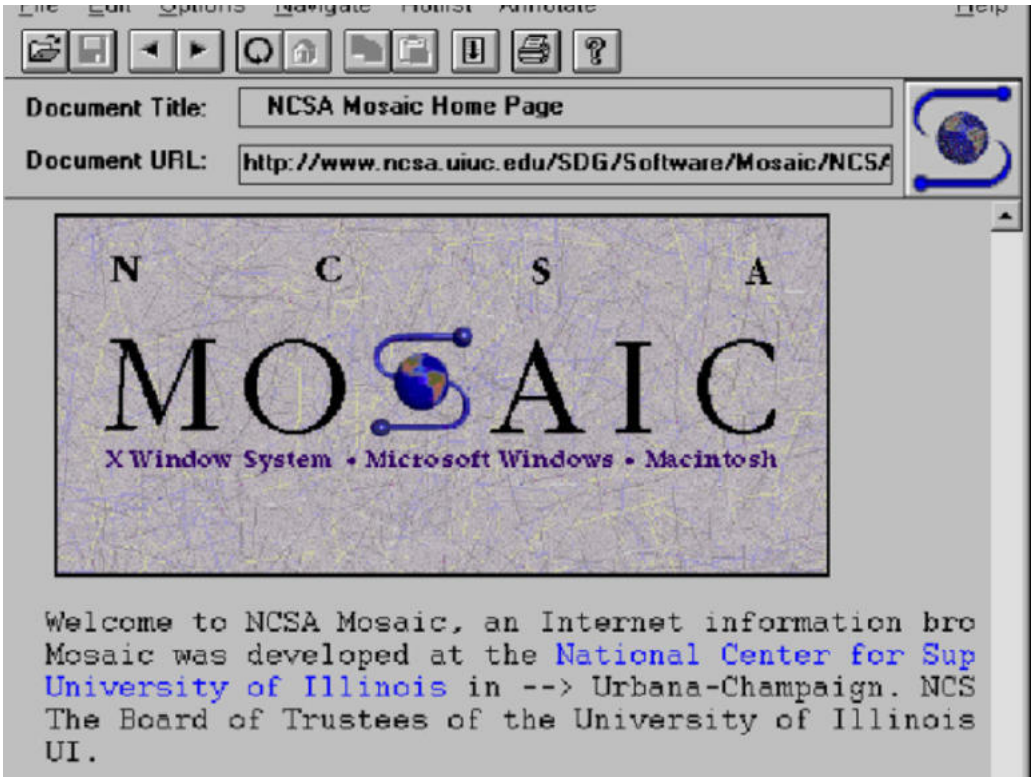
Izrada takvog vodenog žiga bio je toliko teška za reproducirati da ga je Engleska Banka odbila ih koristiti pri izradi novca. Praktičnija tehnika je razvijena od strane Williama Henrya Smitha [2]. Henry William Smith je zamijenio žičane uzorke sa plitkim reljefnim skulpturama, koje nakon što su bile utisnute u kalup papira ostavljaju predivne vodene žigove sa različitim tonovima sive.

Takve tehnike se koriste na jednoj od najjačih valuta na svijetu, američki dolar, Američki Dolar. Na novčanici od dvadeset dolara utisnut je portret sedmog američkog predsjednika Andrewa Jacksona.

Slika 2. Vodeni na novčanici od 20 Američkih Dolara

2. Digitalni vodeni žig

Iznenadni interes za digitalne vodene žigove je povezan sa povećanom brigom oko zaštite autorskih prava na materijale. Internet je postaje pristupačan korisnicima u Studenom 1993. godine dolaskom Marc Andereesenova preglednika pod imenom Mosaic, te brzo dolazi do izražaja da korisnici interneta žele skidati slike, muziku i video zapise [3]. Internet postaje odličan distribucijski sistem za digitalne medije zbog svoje cijene, praktičnosti (jer rješava probleme skladištenja i zaliha) te je dostava medija gotovo trenutna. Vlasnici medija vide potencijalne rizike "piratstva" (ilegalnog skidanja i distribucije medije bez ovlasti vlasnike).



Slika 3. Marc Andereesenov preglednik Mosaic

Rizici piratstva su pogoršani proliferacijom velike količine digitalnih sustava snimanja. Kada je za prosječnog kupca jedini način da snimi pjesmu ili film bila analogna traka, piratske verzije su većinom bile lošije kvalitete od originala, te kvaliteta druge generacije pritastva (kopija kopije) je bila veoma loša. Pojavom digitalnih uređaja za snimanje,

pjesme i filmovi mogu biti snimljeni sa vrlo malo, pa čak i bez bilo kakve degradacije u kvaliteti. Koristeći takve uređaje za i internet za distribuciju, krivotvoritelji mogu jednostavno snimiti i distribuirati materijale s zaštićenim autorskim pravima bez da vlasnik medija koji je zaštićen autorskim pravima bude plaćen. Stoga su vlasnici medija u potrazi za tehnologijom koja im osigurava zaštitu njihovih djela.

Prvi vlasnici tehnoloških sadržaja se počinju koristiti tehnikom zvanom kriptografija. Kriptografija je vjerojatno najčešća metoda zaštite digitalnog sadržaja. To je sigurno jedna od najbolje razvijenih znanosti [4]. Sadržaj je šifriran prije isporuke, a ključ za dešifriranje dostupan je samo onima koji su kupili legitimne kopije sadržaja. Šifrirana datoteka tada se može učiniti dostupnom putem Interneta, ali bi krivotvoritelju bila beskorisna bez odgovarajućeg ključa. Nažalost, šifriranje ne može pomoći prodavaču da nadgleda kako kupac obrađuje sadržaj nakon dešifriranja. Pirat ili krivotvoritelj zapravo može kupiti proizvod, upotrijebiti ključ za dešifriranje kako bi dobili nezaštićenu kopiju sadržaja, a zatim nastaviti sa distribucijom ilegalnih kopija. Drugim riječima, kriptografija može zaštiti sadržaj u prolazu, ali nakon dešifriranja, taj sadržaj nema daljnje zaštite.

Stoga postoji snažna potreba za alternativnom ili za procesom koji će nadopunjavati kriptografiju: tehnologijom koja može zaštiti sadržaj čak i nakon što se sadržaj dešifrira. Vodeni žigovi mogu ispuniti tu potrebu jer stavljaju informacije unutar sadržaja gdje se nikada ne uklanja tijekom uobičajene upotrebe. Dešifriranje, ponovno šifriranje, kompresija, digitalno-analogna pretvorba i formatiranje datoteke - vodeni žig može biti oblikovan da preživi sve naveden procese.

Vodeni žig razmatran je u mnogim aplikacijama za zaštitu od kopiranja i zaštitu autorskih prava. U prevenciji kopiranja može se koristiti vodeni žig kako bi informirali softver ili hardverske uređaje da kopiranje treba ograničiti. U aplikaciji za zaštitu autorskih prava, vodeni žig se može koristiti za identifikaciju nositelja autorskih prava i osigurati pravilno plaćanje tantijema (eng. royalties).

Iako je sprječavanje kopiranja i zaštita autorskih prava jedan od glavnih razloga zbog ko-

jeg su pokrenuta istraživanja na polju vodenih žigova, postoji niz drugih aplikacija za koje se koristi ili predlaže vodeni žig. Tu spadaju praćenje emitiranja, praćenje transakcija, provjera autentičnosti (e.g. novčanice od 20 Američkih Dolara), kontrolu kopiranja i kontrolu uređaja.

3. Aplikacije i svojstva

Vodeni žig se može koristiti u širokom spektru primjena. Općenito, ako je korisno povezati neke dodatne informacije s Djelom, primjerice, metapodaci s dodatnim informacijama o djelu mogu biti ugrađeni kao vodeni žig. Naravno, postoje i drugi načini povezivanja dodatnih informacija s dijelom. Na primjer: stavljanje zaštite u zaglavlje digitalne datoteke, kodiranje u vidljivi bar kod na slici ili izgovaranje naglas kao uvod u audio zapis. To dovodi do pitanje poput: "Kada je vodeni žig bolja alternativa?" te "Što može učiniti vodeni žig, a što se ne može učiniti jednostavnijim tehnikama?".

Vodeni žig razlikuje se od ostalih tehnika u tri važne značajke. Prvo, za razliku od barkodova, vodeni žigovi su neprimjetni i oni ne ometaju estetiku slike ili djela. Drugo, vodeni žigovi su neodvojivi od Djela u koja su ugrađena. Za razliku od polja zaglavlja, oni nisu uklonjeni kada se radovi prikažu ili pretvore u druge formate datoteka. Treće, vodeni žigovi prolaze iste transformacije kao i radovi. To znači da je ponekad moguće naučiti ponešto o tim transformacijama gledanjem nastalih vodenih žigova. To su tri atributa koja čine vodeni vodene žigove neophodnim za određene primjene.

Učinak određenog sustava vodenog žiga može se procijeniti na osnove malog skupa svojstava. Na primjer, robusnost opisuje koliko dobro vodeni žigovi preživljavaju uobičajene postupke obrade signala, opisuje vjernost neprimjetnosti vodenih žigova. Relativna važnost tih svojstava ovise o primjeni za koju je sustav dizajniran. Na primjer, u aplikacijama u kojima moramo otkriti vodeni žig u kopiji djela koje je emitirano preko analognog kanala, vodeni žig mora biti robustan protiv propadanja uzorkovanog tim kanalom. Međutim, ako možemo opravdano očekivati da se Djelo neće mijenjati između

ugradnje i kopiranja, robusnost vodenog žiga nije bitna.

3.1. Aplikacije vodenog žiga

Ispitivanih osam predloženih ili stvarnih primjena vodenog žiga: nadzor emitiranja, identifikacija vlasnika, dokaz o vlasništvu, praćenje transakcija, provjera autentičnosti, kontrola kopiranja, kontrolu uređaja i naslijeđena poboljšanja. Za svaku od ovih aplikacija pokušano je identificirati koje karakteristike problema čine vodeni žig prikladnim rješenjem. Da bismo to učinili moramo pažljivo razmotriti zahtjeve za prijavu i ispitati ograničenja alternativnih rješenja.

3.1.1. Nadzor emitiranja

1997. godine u Japanu je izbio skandal u vezi s televizijskim oglašavanjem. Barem su dvije televizijske stanice rutinski prebukirale vrijeme emitiranja reklama. Oglašivači su plaćali za tisuće reklama koje nikada nisu emitirane. Praksa je ostala uglavnom neotkrivena više od 20 godina, dijelom zato što nije postojao sustav za praćenje stvarnog emitiranja oglasa [5].

Postoje nekoliko vrsta organizacija i pojedinaca zainteresiranih za široko praćenje (BARB skraćeno od "Broadcasters' Audience Research Board" je kompanija koja prati reklame u Ujedinjenom Kraljevstvu, te Nielsen Media Research u Sjedinjenim Američkim Državama) . Oglašivači, naravno, žele osigurati da dobiju sve emitirano vrijeme koje kupuju od emitera, a emiteri zauzvrat žele osigurati da dobiju autorske naknade dobiju od oglašivačkih tvrtki. Nadalje, vlasnici dijela zaštićenog autorskim pravima žele osigurati da se njihova imovina ne emitira protuzakonito po piratskim web stranicama.

Niskotehnološka metoda praćenja emitiranja jest imati ljudske promatrače koji gledaju emisije te snimati ono što vide i čuju. Ova metoda je skupa i sklona pogreškama. Stoga je poželjno zamijeniti ga nekim drugim oblikom nadzora emitiranja. Pasivni nadzorni

sustavi pokušavaju izravno prepoznati emitirani sadržaj, te zapravo zamjeniti ljudske promatrače (premda su oni pouzdaniji i s nižim troškovima). Sustavi aktivnog nadzora oslanjaju se na povezane informacije koje se emitiraju zajedno sa sadržajem.

Pasivni sustav sastoji se od računala koje nadgleda emisije i uspoređuje primljene signale s bazom podataka poznatih Djela. Kada usporedba pronalazi podudaranje, pjesmu, film, TV program ili reklamne sadržaje emitirane koje je moguće identificirati. Ovo je najizravnija i najmanje nametljiva metoda automatiziranog praćenja emitiranja. Ne zahtijeva uvođenje bilo koje povezane informacije za vrijeme emitiranja, pa stoga nisu potrebne promjene u tijeku rada oglašivača. Zapravo ne zahtijeva nikakvu suradnju s oglašivačima ili emiterima.

Međutim, postoji niz potencijalnih problema s primjenom pasivnih sustava praćenja. Prvo, uspoređivanje primljenih signala s bazom podataka nije trivijalan. U principu, htjeli bismo podijeliti signale na prepoznatljive jedinice, poput pojedinačnih kadrova video zapisa, i potražiti ih u bazi podataka. Međutim, svaki kadar videozapisa sastoji se od nekoliko milijuna bitova informacija, i bilo bi nepraktično koristiti tako veliku seriju bitova kao indeks za pretraživanje baze podataka. Dakle, sustav prvo mora obraditi primljene signale u manji zapis koji je dovoljno bogat da se i dalje mogu razlikovati sva moguća djela, ali dovoljno malo da se koristi kao indeks u pretraživanju baze podataka. Nadalje, općenito samo emitiranje degradira signal, a ta degradacija može se mijenjati tijekom vremena, što će rezultirati time višestruki prijem istog djela u različito vrijeme može dovesti do različitih potpisa. To znači da sustav praćenja ne može tražiti točno podudaranje u svojoj bazi podataka. Umjesto toga, mora izvršiti pretragu najbližeg susjeda, za koji se zna da je znatno složeniji proces. Zbog poteškoće u izvođenju smislenih potpisa i traženja najbližih susjeda u velikoj bazi podataka teško je dizajnirati pasivni sustav praćenja koji ima pouzdanost od 100%.

Čak i ako je problem pretraživanje baze podataka riješen, spremanje i upravljanje bazom podataka može biti skupo jer je baza podataka velika. Nadalje, sustav bi trebao istodobno nadzirati nekoliko zemljopisnih mjesta. Svaka web lokacija mora pristupiti centralizi-

ranoj bazi podataka poznatih djela, pohraniti bazu podataka lokalno (s mogućnošću redovnog ažuriranja), ili prenijeti potpise natrag u središnju obradu.

Jedan od načina implementacije aktivnog sustava je smještanje identifikacijskih podataka u zasebno područje emitiranog signala. Na primjer, analogna televizija emisije omogućuju kodiranje digitalnih podataka u vertikalno prazno polje interval (VBI) video signala. Ovaj dio signala, koji se šalje između okvira, nema utjecaja na sliku. Informacije o titlovima distribuiraju se na ovaj način, kao što je to teletekst u Europi.

Za digitalna djela postoje slične aktivne tehnike koje pohranjuju identifikaciju kodova u zaglavljenim datotekama. Ove tehnike imaju iste probleme kao i oni pristup VBI, u kojem bi srednji rukovatelji i krajnji distributeri morali zajamčiti dostavu podataka sa zaglavljem ne promijenjenim. Naime malo je vjerojatno da će podaci preživjeti promjene formata bez izmjena na postojećim sustavima.

Digitalni vodeni žig očita je alternativna metoda kodiranja identifikacijskih informacija za aktivno praćenje. Prednost je to što postoji unutar sadržaja, umjesto iskorištavanja određenog segmenta emitiranog signala, stoga je potpuno kompatibilan s bazom opreme za emitiranje, uključujući digitalni i analogni prijenos. Primarni nedostatak je složeniji postupak ugrađivanja od postavljanja podataka u VBI ili u zaglavljima datoteka. Također postoji zabrinutost, posebno kod stvaratelja sadržaja, da vodeni žig može pogoršati vizualnu ili zvučnu kvalitetu djela. Ipak, postoji niz tvrtki koje pružaju usluge vodenih žigova sa praćenjem emitiranja. Na primjer, Teletrax nudi uslugu koja je zasnovana na tehnologiji video vodenog žiga tvrtke Philips.

3.1.2. Identifikacija vlasnika

Prema američkim zakonima, tvorac priče, slike, pjesme ili bilo kojeg drugog izvornog djela automatski zadržava autorska prava na njega onog trenutka kad je Djelo zabilježeno u nekom fizičkom obliku. I kroz 1988. godinu ako su nositelji autorskih prava htjeli distribuirati svoja Djela bez gubljenja prava, u svako djelo su morali uključiti obavijest

o autorskim pravima koji sada više nije potreban. Međutim, ako je Djelo koje je zaštićeno autorskim pravima zlouporabe a sudovi odluče dosuditi vlasniku autorskih prava naknadu štete, ta nagrada može biti značajno ograničena ako je obavijest o autorskim pravima prihvatljivog oblika i postavljanje nike pronađeno na distribuiranom materijalu.

Važan je točan oblik obavijesti o autorskim pravima. Za vizualna djela, ta obavijest mora biti prikazana u formatu "Djelo datum vlasnik autorskih prava", "Vlasnik © Datum" ili "Copr. vlasnik datum". Za zvučne snimke obavijest o autorskim pravima ima sličan oblik "p datum vlasnik" i mora se postaviti na površinu fizičkog medija, naljepnice, ili na ambalaži kako bi se korisnika "razumno obavijestilo o tužbi za autorska prava".

Tekstualne obavijest o autorskim pravima imaju nekoliko ograničenja kao tehnologija za identificiranje vlasnika djela. Kao prvo, lako ih je ukloniti iz dokumenta kada se kopira, čak i bez ikakve namjere da se protupravno postupi. Na primjer, profesor koji kopira stranice iz knjige (u okvirima poštene upotrebe) možda zanemarivanje fotokopiranja obavijesti o autorskim pravima na naslovnoj stranici. Umjetnik koji koristi legalno prikupljenu fotografiju u oglasu časopisa može odsjeći dio koji uključuje obavijest o autorskim pravima. Dakle, građanin koji poštuje zakon koji naknadno želi koristiti Djelo možda neće moći utvrditi da li Djelo je zaštićeno autorskim pravima. Čak i ako se pretpostavlja da je djelo zaštićeno, možda će biti teško pronaći identitet tvorca ili osobe koju se treba tražiti dozvolu uporabe djela.

Poznati slučaj u kojem je gubitak teksta na slici prouzročio upravo takve probleme je fotografija Lene Sjööblom [6]. Ovo je možda najčešća testna slika u istraživanju obrade slika i pojavila se u bezbroj članaka časopisa i konferencijskih zbornica - i sve bez ikakvog pozivanja na zakonitog vlasnika, Playboy Enterprises, Inc. Slika je započela kao Playboyev središnji preklop. Kada je ova slika skenirana za upotrebu kao probna slika, većina datoteke slika je bila odrezana, a ostalo je samo Lenovo lice i rame. Nažalost, u postupak, tekst koji je Playboy identificirao kao vlasnika također je izrezan. Slika se od tada distribuira u elektroničkom obliku u svijetu, a vjerojatno je i većina istraživača koji ga uključuju u

svoje radove nesvjesno da krše Playboyeva autorska prava. Playboy je to odlučio previdjeti široku upotrebu ove slike.

Drugi problem s tekstualnim obavijestima o autorskim pravima na slikama je taj što mogu biti estetski odbojne i mogu prekriti dio slike. Iako je obično moguće učiniti ih nenametljivim (npr. pozicioniranjem u nevažan kut slike), takva praksa čini ih osjetljivima na rezanje slike. Situacija je još gora u audio sastavu, gdje je obavijest o autorskim pravima postavljena na fizički medij (disk, kaseta, CD, DVD, zapis i tako dalje) i na ambalažama. Nijedna od ovih obavijesti ne bi se kopirala zajedno s audio sadržajem. Štoviše, za neke audio sadržaje koji postoje samo u elektroničkom obliku obrazac (E.g. na web mjestu), nijedan fizički medij ili pakiranje sa obavijest ne postojali.

Budući da se vodeni žigovi mogu učiniti neprimjetnim i neodvojivim od djela koje ih sadrži, ono je superiornije od fizičkog teksta za identifikaciju vlasnika. Ako se korisnici djela dobivaju detektorima vodenih žigova, oni bi trebali biti u mogućnosti identificirati vlasnika djela s vodenim žigom, čak i nakon što je djelo bilo modificirano na načine koji bi uklonili tekstualnu obavijest o autorskim pravima.

3.1.3. Dokaz o vlasništvu

Upotreba vodenih žigova se koristi ne samo da bi identificirali vlasništvo nad autorskim pravima već da zapravo dokaže vlasništvo. To je nešto što tekstualna obavijest može učiniti, jer se tako lako može krivotvoriti. Primjerice, pretpostavljamo da umjetnik (npr. Sara) stvori sliku i objavi je na svom web mjestu, uz obavijest o autorskim pravima ”© 2001 Sara.” Krivotvoritelj (Marko) zatim ukrade sliku i koristi znak program za obradu slika kojim zamjenjuje obavijest o autroskim pravima s ”© 2001 Marko” a zatim tvrdi da sam posjeduje autorska prava. Kako se spor rješava?

Jedan od načina rješavanja takvog spora jest upotreba središnjeg spremišta. Prije stavljanja svoje slike na web, Sara bi je mogla registrirati u Unitedu States Copyright Office-u tako što će im poslati kopiju. Ured arhivira sliku, zajedno s podacima o pravom vlasniku.

Onda, kad se spor između Sare i Marka nastaje, Sara kontaktira Ured za autorska prava da dokaže da je ona zakoniti vlasnik.

Međutim, Sara bi mogla odbiti registrirati svoju slike jer je preskupa. Registracija u Uredu za Autorska prava SAD-a košta približno 45 USD po dokumentu. S mnogo slika koje treba registrirati, to može stvoriti znatan trošak za umjetnika koji se bori. Ako si Sara ne može priuštiti taj trošak, ona bi se mogla zateći kako goni Marka bez koristi Ureda za autorskih prava na njezinoj strani.

U takvom slučaju Sara bi morala pokazati dokaze da je ona stvorila sliku. Na primjer, možda bi imala negativ filma ako je slika izvorno bila fotografija. Ili bi mogla imati rane skice ako je to umjetničko djelo. Nevolja je u tome ako Marko je uistinu odlučan da pobijedi u slučaju, takve dokaze može sam izmisliti. On može napraviti novi negativ iz slike ili lažno izraditi njegove rane skice. Još gore, da je slika stvorena digitalno, možda joj ne bi ni bilo negativa ili rane skice.

Može li Sara zaštiti svoja prava i izbjeći troškove registracije, primjenom vodenog žiga na njezinu sliku? U slučaju vodenog žiga Digimarc, odgovor je vjerojatno ne. Problem njihovog sustava je taj što detektor je lako dostupan svima. Svatko tko može otkriti vodeni žig može ga i ukloniti, isto tako Sarin vodeni žig nije siguran jer ga se može ukloniti i zamijeniti ga svojim.

Da bi se postigla razina sigurnosti potrebna za dokaz vlasništva, vjerojatno je potrebno ograničiti dostupnost detektora. Kad protivnik nema detektor, uklanjanje vodenog žiga može biti izuzetno teško. Stoga, Kad Sara i Marko izađu pred suca, Sara bi producirala njezin original i kopija slike ubacili bi u detektor vodenog žiga, a detektor bi otkrio Sarin vodeni žig.

Međutim, čak i ako se Sarin vodeni žig ne može ukloniti Marko bi to mogao učiniti da je potkopa. Kao što su istakli Craver i sur. Marko bi koristeći vlastiti vodeni žig, mogao učiniti da se čini kao da je njegov vodeni žig bio prisutan u Sarinog originalnoj kopiji slike.

Tako bi treće strana bila nesposobna procijeniti je li je Sarino ili Markovo djelo istinski izvorno.

Ovaj se problem može riješiti ako napravi promjena u izjavi problema. Umjesto da pokušamo izravno dokazati vlasništvo ugrađivanjem "Sara" u djelo u kojem je poruka s vodenim žigom, pokušat će to dokazati kako je jedna slika izvedena iz druge. Takav sustav pruža neizravne dokaze da je vjerojatnije je original u vlasništvu Sare prije nego Marka, jer je Sara ta koja ima izvornu inačicu iz koje se mogu stvoriti sva druga djela. Dokazi su slični pod uvjetom da Sara proizvodi negativ iz kojeg je slika stvorena, osim što je jača, u tome što Marko može izmisliti negativ ali ne mogu izraditi lažni original koji prolazi naš test.

3.1.4. Praćenje transakcija

U ovoj primjeni vodenog žiga, vodeni žig bilježi jednu ili više transakcija koje su se dogodile u povijesti kopije djela u kojem je ugrađen. Na primjer, vodeni žig može zabilježiti primatelja u svakom pravnom zakonu prodaje ili distribucije djela. Vlasnik ili producent djela bi u svaku kopiju stavio drugi vodeni žig. Ako se djelo naknadno zloupotrijebi (procuri u tisak ili se ilegalno preraspodjeli), vlasnik bi tako mogao saznati tko je odgovoran.

U literaturi o praćenju transakcijama osoba odgovorna za zloupotrebu djela ponekad se naziva izdajnikom, dok se osoba koja prima djelo izdajice naziva gusarom. Kako ta razlika nema smisla kada raspravljamo o drugim primjenama u kojima je piratstvo problem, ne koristimo ovu terminologiju. Umjesto toga, koristimo izraz protivnik da bismo opisali svakoga tko pokušava ukloniti, onemogućiti ili krivotvoriti vodeni žig u svrhu zaobilaženja njegovog vodenog žiga.

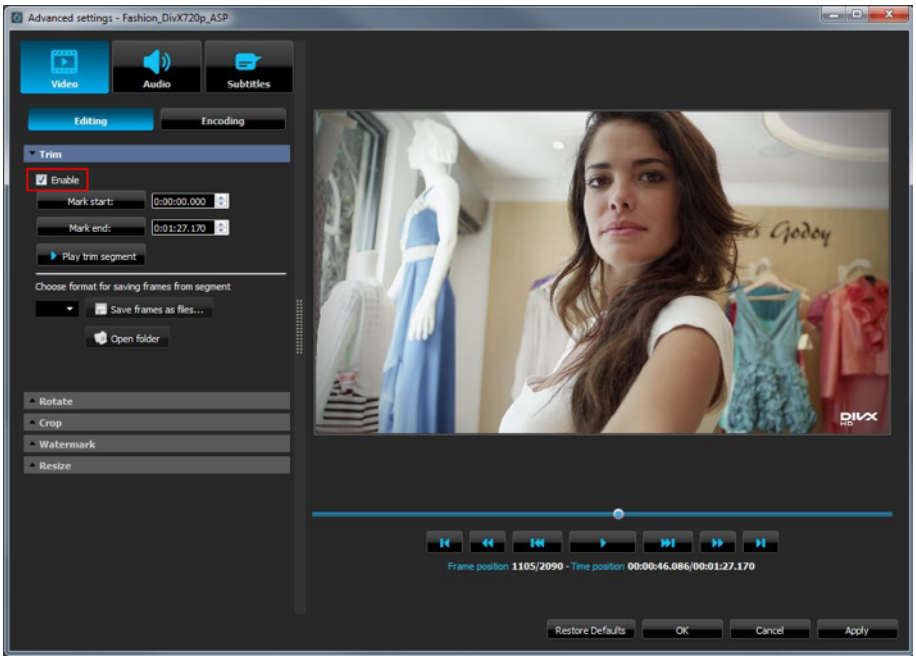
Praćenje transakcija češće se naziva Otiskom prsta (eng, fingerprint), kao i svaka kopija djelo se može jedinstveno prepoznati po vodenom žigu koji je analogan s ljudskim otiskom prsta koji jedinstveno identificira osobu. Da bismo izbjegli ove nejasnoće, koristi se izraz praćenje transakcija.

Malo je tehnologija za praćenje transakcija koje ne spadaju u definiciju vodenog žiga. Jedna od uobičajenih alternativa vodenim žigovima je uporaba vidljive oznake. Na primjer, vrlo osjetljivi poslovni dokumenti, poput poslovnih planova, ponekad se tiskaju na pozadinama koje sadrže velike sive znamenke, s različitim brojem za svaku kopiju. Zatim se vodi evidencija o tome tko ima koji primjerak. Ovi se znakovi često nazivaju "vodenim žigovima", jer imaju fizičku sličnost s vodenim žigovima na papiru. Međutim, oni nisu vodeni žigovi u smislu pojma, jer značajka koja definira vodeni žig jest neprimjetnost. Naravno, neprimjetni vodeni žigovi jesu poželjniji od vidljivih znakova iz istih razloga što su poželjni vidljivi vodeni žigovi na tekstualne obavijesti o autorskim pravima.

Primjer vodenog žiga za praćenje transakcija implementirao je sada ugašena DiVX Corporation [7]. DiVX je prodao poboljšani DVD uređaj koji implementirao poslovni model pay-per-view. Proveli su razne sigurnosne tehnologije za sprečavanje piratstva njihovih diskova, od kojih je jedna bila vodeni žig dizajniran za praćenje transakcija. Svaki player s uključenim DiVX bi stavio jedinstveni vodeni žig u svaki video zapis koji je reproducirao. Ako je netko tada snimio taj videozapis i započeo prodaju kopija na crnom tržištu, korporacija DiVX mogla je dobiti jednu od kopija i identificirati protivinika (ili, barem, protivnički DiVX player) dekodiranjem vodenog žiga. Prema našim saznanjima, DiVX vodeni žig nikada nije bio korišten za traženje protivnika prije nego je DiVX prestao s poslom.

Drugi primjer praćenja transakcija je u distribuciji filmova. Tijekom snimanja filma rezultat svakodnevne fotografije često se distribuira brojim ljudima koji su uključeni u njegovu proizvodnju. Ti su dnevni listovi vrlo povjerljivi, ali povremeno neki od njih procuri do novinara. Kada se to dogodi, studiji brzo pokušavaju identificirati izvor curenja. Studiji mogu upotrijebiti vidljivi tekst na rubovima zaslona za prepoznavanje svake kopije filma. Međutim, vodeni žigovi su poželjniji jer je tekst kao takav lako uklonjiv.

Akademija filmske umjetnosti i znanosti odgovorna je za poznate nagrade Oscar, koje



Slika 4. Primjer DiVX-ovog vodenog žiga

prepoznaju doprinos glumaca, glumica, redatelja i mnogih drugih za umjetnost i znanost snimanja filmova. U zaostatku na ceremonije dodjele Oscara, Akademija anketira svih svojih 5.803 članova koji imaju pravo glasa kako bi glasali za najboljeg glumca, najbolji film itd. Akademija osigurava svakog člana koji glasa s prikazima Oscara (tj kopijama svih razmatranih filmova u VHS ili DVD formatu), tako da članovi mogu gledati sve nominirane filmove. Međutim, mnogi od ovih filmove još nisu pušteni u video. Zapravo, u nekim slučajevima film možda čak nije dobio ni kino izdanje. U takvim okolnostima, može biti ekonomski vrlo štetno ako piratska kopija Oskara se pojavljuje u VHS ili DVD formatu ili na internetu.

2004. Godine Technicolor, odjel Thompsona, koristio je video vodene žigove tehnologijom licenciranom od Philipsa za pojedinačni vodeni žig svakog od 5.803 članova koji glasaju za Oscara. Nakon distribuiranja ovih kopija, piratski video filmova Posljednji samuraj, Something's Gotta Give, Big Fish i Mystic RIver pojavili su se na internetu. Otkrivena analiza ovih piratskih kopija je da su izvorni materijal nominiranih filmova Oscara koji su dobili glumac Carmine Caridi. Carmine Caridi obavijestio je istražitelje da je kopije dao svom prijatelju Russell Sprageu i da nije bio svjestan da je njegov prijatelj

Slika 5. Vodeni žig na filmu distribuiranog od strane Oscara

namjeravao napraviti ilegalne kopije. Ipak, 70 godišnji glumac bio je izbačen iz Akademije. Columbia Pictures i Warner Bros. Entertainment Ltd. je nakon toga tužio Carmine Caridi za naknadu štete. U studenom 2004. Warner Brosu je dodijeljena maksimalna zakonska odšteta od 150.000 USD po naslovu (tj. 300.000 USD) u građanskoj parnici. [8]

3.1.5. Provjera autentičnosti sadržaja

Sve je lakše i lakše izmijeniti digitalni zapisi na načine koji je teško otkriti. Na primjer, slika prikazuje izmjenu napravljenu na slici pomoću Adobe Photoshopa; slijeva je originalna slika; na desno je izmijenjena verzija. Kad bi ova slika bila kritičan dokaz u pravnom slučaju ili policijskoj istrazi, ovaj oblik neovlaštenog predstavljanja mogao bi predstavljati ozbiljni problem. Isti problem postoji sa zvukom i videom.

Problem autentifikacija poruka dobro je proučen u kriptografiji. Jedan od uobičajenih kriptografskih pristupa ovom problemu je stvaranje digitalnog potpisa, koji je u biti šifrirani sažetak poruke. Koristi se asimetrični algoritam šifriranja ključa, tako da je potreban ključ za šifriranje potpisa i razlikuje se od onoga potrebnog za njegovo dešifriranje.

Slika 6. Primjer uklonjenog lika sa slike

Samo ovlašteni kreator poruke zna ključ potreban za stvaranje potpisa.

Stoga, protivnik koji pokušava promijeniti poruku ne može stvoriti novi potpis. Ako netko naknadno usporedi izmijenjenu poruku sa izvornim potpisom, utvrdit će da se potpisi ne podudaraju i da će se znati da je poruka izmijenjena. Friedman je tehnologiju digitalnog potpisa primijenio na digitalne fotoaparate, koji predlažu stvaranje "pouzdane kamere" uračunavanjem potpisa unutar fotoaparata. Samo kamera bi imala ključ potreban za stvaranje potpisa. Stoga, ako utvrdimo da se kopija slike podudara s njegovim potpisom, možemo biti sigurni da je identičan originalu bit za bit. [9]

Ti su potpisi metapodaci koji se moraju prenijeti zajedno s dijelima te ih oni provjeravaju. Stoga je lako izgubiti potpise u uobičajenoj uporabi. Na primjer, razmotrimo sustav provjere autentičnosti slike koji pohranjuje metapodatke u JPEG polje zaglavlja. Ako se slika pretvori u drugi format datoteke koji nema prostor za potpis u zaglavlju, potpis će se izgubiti. Kada se potpis izgubi, djelo više ne može biti potvrđeno.

Poželjnije rješenje moglo bi biti ugrađivanje potpisa izravno u djelo pomoću vodenog žiga. Epson nudi takav sustav kao opciju za mnoge od svojih digitalnih fotoaparata. Pozivamo se na takav ugrađeni potpis kao oznaku za ovjeru. Oznake za provjeru identiteta dizajnirane su da postanu nevaljane nakon što se i najmanja preinaka djela naziva krhkim vodenim žigom.

Korištenje oznaka za provjeru autentičnosti eliminira problem osiguravanja potpisa da ostane uz djelo. Naravno, mora se paziti da se čin ugradnje vodenog žiga ne mijenja djelo dovoljno da bi se učinio nevaljanim u usporedbi s potpisom. To se može postići razdvajanjem djela na dva dijela: jedan na koji je uračunat potpis i jedan u koji je ugrađen potpis. Na primjer, nekoliko autora predlaže izračunavanje potpisa iz visokih bitova slike i ugrađivanje potpisa u bitove niskog reda.

Ako je djelo koje sadrži oznaku za provjeru autentičnosti izmijenjeno, oznaka se mijenja zajedno s njim. Ovo otvara mogućnost da saznate više o tome kako je Djelo bilo modificirano. Na primjer, ako je slika podijeljena u blokove, i svaki blok ima svoj vlastiti znak provjere autentičnosti, ugrađen je u njega, bili bismo sposobni steći grubu ideju o tome koji su dijelovi slike autentični, a koji dijelovi su izmijenjenu. Ovu i slične ideje predložili su mnogi istraživači.

Primjer gdje bi ova vrsta lokalizirane provjere autentičnosti mogla biti korisna bio bi u policijskoj istrazi zločina. Zamislite da policija prima nadzorni video koji je je izmijenjen. Ako je video zapis ovjeren s tradicionalnim potpisom, sve što bi policija znala jest da je videozapis neautentičan i da mu se ne može vjerovati. Međutim, ako koriste vodeni žig dizajniran da daju lokaliziranu provjeru autentičnosti, mogli bi otkriti da svaki kadar videozapisa je pouzdan osim za registarske tablice na automobilu. Ovo bi bio snažan dokaz da je s videozapisa uklonjen identitet nekoga tko je sudjelovao u zločinu.

Suprotno tome, možda nas ne bi zanimalo je li neko djelo komprimirano, i mogao bi se baviti samo značajnim promjenama napravljenim, kao što je naznačeno na slici 2.3. To dovodi do teme polu krhkih vodenih žigova i potpisa, koji preživljavaju manje transformacije, poput kompresije s gubitkom, ali su onesposobljene velikim promjenama.

3.1.6. Kontrola kopiranja

Većina dosadašnjih primjena vodenog žiga ima samo učinak u slučaju potvrde ili evidentiranja vlasništva. Na primjer, praćenje emitiranja pomaže uhvatiti nepoštene emitere

nakon što ne puste oglase koji su plaćeni, a praćenje transakcija identificira protivnike nakon što distribuiraju ilegalne kopije. Te tehnologije služe kao odvraćanje od takvih ne djela, ali korisnije je spriječiti nezakonitu radnju. U kontroli kopiranja aplikacija, cilj je spriječiti ljude da prave ilegalne kopije sadržaja zaštićenog autorskim pravima.

Prva i najsnažnija linija obrane od ilegalnog kopiranja je šifriranje. Šifriranje Djela prema jedinstvenom ključu možemo ga učinit neupotrebljivim svima koji nemaju taj ključ. Tada bi se dobio ključ podijelio legitimnim korisnicima tako da bilo tko bez tog ključa ima poteškoće kopiranja ili distribucije. Primjerice, mnogi satelitski televizijski programi su šifrirani. Ključevi za dešifriranje daju se svakom kupcu te svatko tko pokušava gledati ili snimati prijenos bez ključa vidio bi samo kodirani video.

Jedan od osnovnih načina na koja protivnik može pokušati prevladati sustav šifriranja. Prvo i najteže je dešifrirati podatke bez dobivanja ključa. To obično uključuje neki oblik pretraživanja, u kojem protivnik iscrpno pokušava dešifrirati signal s višestrukim kombinacijama. Ako je kriptografski sustav dobro dizajniran, protivnik će morati isprobati sve moguće ključeve. To je veoma nepraktično ako su šifre dulje od 50 bitova.

Budući da su vodeni žigovi ugrađeni u sam sadržaj djela, oni su prisutni u svakom predstavljanju sadržaja te se stoga može pružiti bolja metoda provođenja kontrole kopiranja. bi svi ugrađeni uređaji za snimanje imali ugrađeni detektor vodenog žiga, uređaji bi mogli biti napravljeni da zabranjuju snimanje kad god se na njegovom ulazu otkrije nikada kopirani vodeni žig. Ova funkcionalnost se naziva kontrolom zapisa. Takav je sustav je predviđen za upotrebu na DVD-ima od strane Copy Protection Technical Working Group (CPTWG) i za uporabu zvuka od strane SDMI.

Postoji jedan značajni ne-tehnički problem u postavljanju kontrole kopiranja sustava zasnovan na vodenim žigovima: Kako se može osigurati da svaki snimač sadrži detektor vodenog žiga? Ne postoji prirodni poticaj za proizvođače snimača kako bi nastali troškovi ugradnje detektora u njihove proizvode. Zapravo, postoji veliki motiv kojim detektor vodenih žigova zapravo smanjuje vrijednost snimača s gledišta kupca. Kupac

bi radije imao uređaj koji može izrađivati ilegalne kopije.

Izravno rješenje ovog problema bilo bi zahtijevanje detektora vodenog žiga u rekorderima po zakonu. Također, ova pravna bitka bi morala se voditi u svim zemljama svijeta prije nego što vodeni žigovi mogu pružiti svjetsku zaštitu.

Ideja poznata pod nazivom kontrola reprodukcije suprotstavlja se upravno tome. Kad na pirat koristi nesukladni snimač za izradu ilegalne kopije djela s vodenim žigom, ta će kopija sadržavati vodeni žig. Sukladni uređaji mogu biti dužni, patentnom licencom, provjeriti ima li vodenih žigova u sadržaju koji je reproducirao. Kad uređaj vidi vodeni žig koji nike bio kopiran, provjerava kako bi utvrdio bez obzira radi li se o kopiji ili originalu. To se može učiniti na razne načine, poput provjere je li Djelo ispravno šifrirano ili tražeći poseban potpis na medijima. Ako reproducira kopiju, uređaj se ugasi.

DVD video standard na kraju je odlučio da ne uvodi tehnologiju vodenih žigova u DVD uređaje za reprodukciju ili snimače [10]. Međutim, sljedeća generacija DVD uređaja i snimača visoke razlučivosti (HD) uključuju audio i video tehnologije vodenog žiga [11]. Zvučni vodeni je žig od tvrtke Verance, dok je vodeni žig od kompanije VEIL, Veil Interaktivne tehnologije.

VEIL video vodeni žig jednostavna je metoda koja modulira intenzitet video skeniranja. Ovaj video Vodeni žig namijenjen je kodiranju oznake za utvrđivanje prava (RAM) koja se koristi za podršku CGMS-A signalizacije. CGMS-A (Sustav upravljanja generiranjem kopija Analog) sastoji se od dva bita podataka koji predstavljaju četiri stanja: slobodno kopirajte, kopirajte više, kopirajte jednom i nikad [12]. CGMS-A je video standard koji prenosi dva bita u intervalu vertikalne praznine video signala. Kao takav se vrlo lako izgubi ili ukloni. RAM je namijenjen za ugradnju u video sadržaj koji sadrži CGMS-A signalizacije. Ako se izgubi signal CGMS-A, ali RAM je prisutan, uređaji za snimanje dizajnirani su da ne kopiraju videozapis signala.

3.1.7. Upravljanje uređajem

Kontrola kopiranja spada u širu kategoriju aplikacija na koje se nazivaju upravljanje uređajem. Postoji nekoliko drugih aplikacija u kojima uređaji reagiraju na vodene žigove koje se otkrivaju u sadržaju. S gledišta korisnika, mnogi od njih se razlikuju od kontrole kopiranja po tome što dodaju vrijednost sadržaju, umjesto da ograniči njegovu upotrebu.

Tradicionalno, glazba se distribuirala putem fiksnim linijama (tj. namjenskih telefonskih linija), koje su skupili distributeri. MusicScan, ovlaštenik patenta, namjeravao je smanjiti ovaj trošak zamjenom namjenskog distribucijskog sustava bežičnim sustavom emitiranja. Prostorije MusicScana primale bi glazbu s komercijalne radio stanice koja emitira reklame i razgovore, kao i glazbu. Tomberlin i ostali izumi su ugradili signal vodenog žiga u radio prijenos koji je naznačio kada se radijski prijenos treba zanemariti (npr. kad se emitirala reklama). To je postignuto sa dva upravljačka signala (ugrađena ili kao nadzvučna ili podzvučna audio frekvencija) koji su ukazivali na početak i kraj emitiranih segmenata koji su trebali biti blokirani.

O drugoj ranoj primjeni vodenog žiga za kontrolu govori se 1981. godine patent Ray Dolby-a [13] . U to su vrijeme bile brojne FM radio stanice emitiranje glazbe korištenjem tehnike smanjenja šuma koja se naziva Dolby DM. Da bi se u potpunosti iskoristio Dolby FM, radio je trebao odgovarajući dekoder. Slušatelji su se morali oslanjati na popis postaja koje emitiraju Dolby FM signale kako bi mogli ručno uključiti ili isključiti dekoder svog radija. Dolby je predložio da se izradi radio koji može u svoj dekoder automatski uključiti u svoj dekoder odgovor na nečujni ton emitiranja unutar spektra zvučne frekvencije. Takav ton predstavlja jednostavan vodeni žig.

1989. Broughton i Laumeister dobili su nagradu za patent tehnike koja akcijskim igračkama omogućuje interakciju s televizijskim programima [12]. U ovoj tehnici, jednostavni vodeni žig modulira intenzitet vodoravnih linija skeniranja unutar svakog polja ili kadra videozapisa. Ovaj signal modulacije je detektiran od uređaja osjetljivog na svjetlost postavljen u blizini televizora. Ovaj detektor prenosi visokofrekventni infracrveni

signal na interaktivne uređaje. U ovome djelu na koji se playeri mogu sinkronizirati s videozapisom koji se gledaju na televiziji. Broughton i Laumeister također spominju da modulacija intenziteta skeniranja dovodi do otkrivanja radio- frekvencijskog (RF) signala i da to može biti osnova alternativnog detektora signala. Prednost RF detektora je što nije osjetljiv na uvjete osvjetljenja okoline i ne treba neograničen pogled na televizijski prikaz.

U novijoj primjeni vodenog žiga za kontrolu uređaja, Digimarc-ov Mobilni sustav ugrađuje jedinstveni identifikator u ispisane i distribuirane slike kao što su oglasi u časopisima, pakiranja, ulaznice itd. Nakon slike ponovno snima kamera mobitela, softver na telefonu čita vodeni žig / QR kod i identifikator se koristi za usmjeravanje web preglednika na povezano web mjesto [14].

3.1.8. Poboljšanje nasljeđa

Ponekad se pojavi situacija u kojoj je implementirani sustav vrlo velik kojeg se treba nadograditi kako bi pružio poboljšanu funkcionalnost. Ova nadogradnja može biti nekompatibilna sa postojećim sustavom. Primjerice, velik dio svijeta je prelazilo s analogne na digitalnu televiziju u 2015. godini [15]. Ovo je skup i dugotrajan proces. Tijekom ove tranzicije mora se uvesti potpuno nova oprema za digitalno emitiranje, a potrošači moraju kupiti digitalni televizijski prijemnik. U međuvremenu, naslijeđeni analogni sustav mora nastaviti funkcioniraju sve dok velika većina potrošača ne prijeđe na digitalnu tehnologiju. U Sjedinjenim Državama očekuje se analogni granični datum 2009. godine, u Japanu je zakazan za 2011. godinu, dok je u Ujedinjenom Kraljevstvu okvirni cilj 2012. godine. [16]

U idealnom slučaju željeno je nadograditi sustav tako da novi sustav bude unatrag kompatibilan (tj. Nastavlja raditi s postojećim naslijeđenim sustavom). Digitalni vodeni žig jedan je od načina na koji se to može postići. Ukratko opisujemo dva predložena sustava koja ilustriraju ovu točku. [17]

Drugi primjer je Tektronixov digitalni koder vodenog žiga za sinkronizaciju audio i video signala. Problem se javlja kada se video i audio kanali televizijskog signala odrađuju odvojeno. Digitalna obrada signala uvodi različita kašnjenja u audio i video kanale i može dovesti do vrlo uznemirujućeg fenomena poznatog kao usna sinkronizacija, u je jasno vidljivo da je pokret usana ispred ili iza govora. Tektronix proizvod ugrađuje visoko komprimiranu verziju audio signala unutar video signala, prije bilo kakve digitalne obrade signala. Uostalom signal obrada je dovršena, audio signal u stvarnom vremenu uspoređuje se s ugrađenim audio signalom kako bi se utvrdilo je li uvedeno neko kašnjenje. Ako je tako da se ovo kašnjenje može ukloniti prije emitiranja.

Sličan problem može se dogoditi kada MP3 uređaji pokušavaju prikazati tekst pjesama sinkronizirano s glazbom. Jedno rješenje, čiji je pionir Mark Any iz Koreje, ugrađuje tekst izravno u audio signal pomoću tehnologije vodenog žiga. Tehnologija, poznata kao Media Sync, vrlo je popularna u Koreji.

3.2. Obilježja sustava vodenih žigova

Sustavi vodenih žigova mogu se okarakterizirati brojnim svojstvima. Relativna važnost svakog svojstva ovisi o zahtjevima prijave i ulogu koju će imati vodeni žig. Štoviše, tumačenje vodenog žiga je svojstvo koje se može razlikovati ovisno o primjeni. Najvažnija svojstva s kojima se obično povezuje postupak ugrađivanja vodenog žiga su: učinkovitost, vjernost i nosivost. Sekundarna svojstva koja su obično povezana s otkrivanjem: slijepo i informirano otkrivanje, lažno pozitivno ponašanje i robusnost. Sljedeća dva svojstva, sigurnost i uporaba ključeva je sastavni dio bilo koje sigurnosne značajke svojstvene shemi vodenog žiga. Mi zatim razgovaramo o mogućnosti promjene poruke kodirane vodenim žigom izmjenom samog vodenog žiga ili predstavljanjem poruke s više vodenih žigova.

3.2.1. Efektivnost embediranja

Rad s vodenim žigom definira se kao djelo koje kad se unese u detektor rezultira pozitivnim ishodom tj. prepoznatim vodenim žigom unutar tog specifičnog djela. S ovom definicijom djela s vodenim žigom, učinkovitost sustava vodenog žiga je vjerojatnost da na izlazu iz embedera je rezultat slike s vodenim žigom. Drugim riječima, učinkovitost je vjerojatnost otkrivanja odmah nakon ugradnje što znači da ova tehnika podrazumijeva da se sustav vodenog žiga može imati učinkovitost manju od 100%.

Iako je uvijek poželjna stopostotna učinkovitost, ovaj cilj često dolazi do vrlo visokih cijena u odnosu na druga svojstva. Ovisno o aplikaciji vodenog žiga, svojstvo učinkovitosti može se zamijeniti za bolje performanse s obzirom na ostale karakteristike vodenog žiga. Najpoznatiji primjer je stock photo house koji treba ugraditi dokaz o vlasništvu vodenih žigova tisuća slika svaki dan. Takav sustav mogao bi imati vrlo visoke zahtjeve za vjernošću, i to može se dogoditi da određene slike unutar njih ne mogu biti uspješno vodene te ograničavaju vjernost. Foto kuća će tada možda morati odlučiti hoće li dopustiti da slike ostanu neoznačene, a samim time i nezaštićene, ili dopustite uvođenje većih izobličenja kako bismo od održali stopostotnu učinkovitost.

U nekim slučajevima, učinkovitost sustava vodenog žiga može se odrediti analitički. Učinkovitost se može empirijski procijeniti jednostavnim ugrađivanjem vodenog žiga u veliki testni skup slike. Postotak izlaznih slika koje rezultiraju pozitivnim otkrivanjima hoće biti približni vjerojatnosti efektivnosti vodenog žiga, pod uvjetom da je broj slika u skupu dovoljno velik i izvučen iz iste distribucije kao i očekivane slike aplikacije.

3.2.2. Vjernost / Fidelity

Općenito, vjernost sustava vodenog žiga odnosi se na percepciju sličnosti izvorne verzije djela i djela s vodenim žigom. Međutim, kada će se djelo s vodenim žigovima degradirati u procesu prijenosa prije nego što ga osoba zaprimi, drugačija definicija vjernosti može biti prikladnija. Možemo definirati vjernost sustava vodenog žiga kao perceptivna slič-

Slika 7. Primjer vodenog žiga na slici

nost između Radova bez vodenog žiga i Djela sa vodenim žigovima na mjestu na kojem su predstavljena potrošačima.

U nekim aplikacijama možemo prihvatiti slabo uočljive vodene žigove u zamjenu za veću robusnost ili niže troškove. Na primjer, hollywoodski dnevni listovi nisu gotovi proizvodi. Obično su rezultat loših prijenosa s filma na video. Njihova jedina svrha je pokazati onima koju su uključeni u filmsku produkciju dosad snimljeni materijal. Malo vidljivo izobličenje uzrokovano vodenim žigom ne umanjuje njihovu vrijednost.

3.2.3. Opterećenje podataka ili Data payload

Nosivost podataka odnosi se na broj bitova koje vodeni žig kodira unutar jedinice vremena ili unutar Djela [17] . Za fotografiju bi se nosivost podatak odnosila na broj bitova kodiranih unutar slike. Za audio, nosivost podataka odnosi se na broj ugrađenih bitova u sekundi koji se prenose. Za video podatke nosivost se može odnositi ili na broj bitova po polju ili na broj bitova u sekundi. Vodeni žig koji kodira N bitova naziva se N-bitni vodeni žig.

Mnogi sustavi u kojima postoji samo jedan mogući vodeni žig, a detektor određuje je li taj vodeni žig prisutan ili ne. To se naziva i jednobitnim vodenim žigovima jer postoji 2^1 mogućih izlaza: vodeni žig prisutan i vodenog žiga nema. Međutim, to nije u skladu s prethodno opisanom konvencijom imenovanja.

3.2.4. Slijepo ili informirano otkrivanje / Blind or Informed Detection

U nekim je aplikacijama izvorni rad bez vodenih žigova dostupan tijekom detekcije. Na primjer, u aplikaciji za praćenje transakcija to je obično vlasnik originalnog djela koji upravlja detektorom, kako bi otkrio tko ilegalno distribuirao dani primjerak. Vlasnik bi, naravno, i dalje posjeduje verziju djela bez vodenog žiga i na taj ga način može dati detektoru zajedno s ilegalnom kopijom. To značajno poboljšava performanse detektora, tako da se original može oduzeti od kopije s vodenim žigom i dobiti uzorak samo vodenog žiga. Original se također koristiti za registraciju kod suzbijanja bilo kakvih vremenskih ili geometrijskih izobličenja koja su mogla biti primijenjena na kopiju s vodenim žigom.

U ostalim aplikacijama otkrivanje se mora izvoditi bez pristupa izvornom djelu. Kod aplikacija za kontrolu kopiranja detektor mora biti distribuiran u svakom uređaju za snimanje potrošača. Mora se distribuirati sadržaj bez vodenih žigova na svaki detektor koji izvršava detekciju vodenog žiga.

Detektor koji zahtijeva pristup izvorniku, djelo bez vodenih žigova nazivamo kao informirani detektor. Ovaj se izraz također može odnositi na detektore koji zahtijevaju samo neke informacije izvedene iz izvornog djela, a ne sve informacije iz djela. Suprotno tome, detektori koji ne zahtijevaju nikakve informacije povezane s izvornicima nazivaju se slijepim detektorima. [17]

3.2.5. Postotak krivih detekcija / False Positive Rate

Lažno pozitivna detekcija vodenog žiga u djelu se desi kada detektor "prepozna" vodeni žig na djelu koje zapravo ne sadrži nikakav vodeni žig. Kada se govori o lažno pozitivnoj stopi, misli se na broj lažno pozitivnih rezultata za koje se očekuje da će se pojaviti u zadanom broju pokretanja detektora.

Vjerojatnosti krivih detekcija je vjerojatnost koji daje određeni rad i slučajno odabrani vodeni žig, detektor izvješćuje da je u tom dijelu vodeni žig. Izvučeni su vodeni žigovi iz distribucije definirane dizajnom sustava za stvaranje vodenih žigova. Vodene žigove obično generira algoritam za kodiranje bitova ili pomoću Gaussove krivulje, neovisnim generatorom slučajnih brojeva (RNG - eng. "random number generation"). U puno slučajeva, vjerojatnost krive detekcije, prema ovoj prvoj definiciji je zapravo neovisno o djelu i ovisi samo o metodi generacije vodenog žiga.

Potrebna vjerojatnost krive detekcije ovisi o svrsi djela s vodenim žigom. U slučaju dokaza o vlasništvu, detektor se koristi tako rijetko da postoji vjerojatnost 10^{-6} bi trebalo biti dovoljno da se lažni pozitivi učine krivotvorenim. S druge strane, aplikacija za kontrolu kopiranja, milijuni detektora vodenih žigova neprestano se izvode na milijunima djela po cijelom svijetu. Ako neko djelo bez vodenog žiga dosljedno generira lažne pozitivne rezultate, to bi moglo dovesti do ozbiljnih problema, te zbog ovog razloga lažno pozitivna stopa trebala bi biti beskonačno mala.

3.2.6. Robusnost

Robusnost se odnosi na sposobnost otkrivanja vodenog žiga nakon standardnih operacija obrade signala. Primjeri uobičajenih operacija na slikama uključuju prostorno filtriranje, kompresiju s gubicima, ispis i skeniranje te geometrijska izobličenja (rotacija, prevođenje, skaliranje i tako dalje). Video vodeni žigovi moraju biti robusni za mnoge iste transformacije, kao i za snimanje na video kaseti i promjene brzine kadrova, među ostalim utjecajima. Audio vodeni žigovi možda će trebati biti robusni za takve procese

kao što su vremensko filtriranje i snimanje na audio kazeti i varijacije u brzini reprodukcije koje rezultiraju vauom i lepršanjem.

Ne zahtijevaju sve aplikacije s vodenim žigom robusnost na sve moguće signale operacija obrade. Vodeni žig treba preživjeti samo uobičajene postupke obrade signala koji će se vjerojatno dogoditi između vremena ugrađivanja i vremena otkrivanja. Na primjer, u praćenju televizijskih i radio emisija, vodeni žig treba preživjeti samo proces prijenosa. U slučaju emitiranog videa, to često uključuje gubitke kompresija, digitalno-analogna pretvorba, analogni prijenos što rezultira niskopropusnim filtriranjem, aditivnim šumom i nekom malom količinom vodoravne i okomite translacije. Općenito, vodeni žigovi za ovu aplikaciju ne moraju preživjeti rotaciju, skaliranje, visokopropusno filtriranje ili bilo koju od široke lepeze degradacija koje se javljaju prije ugradnje vodenog žiga ili nakon njegovog otkrivanja. Tako, na primjer, vodeni žig za praćenje emitiranja ne mora biti robustan na VHS snimke.

3.2.7. Sigurnost vodenog žiga

Sigurnost vodenog žiga odnosi se na njegovu sposobnost da se odupre napadima neprijatelja. Neprijateljski napad je svaki postupak koji je posebno namijenjen sprečavanju svrhe vodenog žiga. Vrste napada zbog kojih bismo mogli biti zabrinuti dijele se na tri vrste napada: neovlašteno uklanjanje, neovlašteno ugrađivanje te neovlašteno otkrivanje.

Neovlašteno uklanjanje i ugrađivanje nazivaju se aktivnim napadima jer ovi napadi mijenjaju naslovnicu djela. Neovlašteno otkrivanje ne mijenja se naslovnica rada i stoga se naziva pasivnim napadom.

Neovlašteno uklanjanje odnosi se na napade koji sprečavaju vodeni žig djela od otkrivanja. Uobičajeno je razlikovati dva oblika neovlaštenog uklanjanja: napadi eliminacije i napadi maskiranja. Intuitivno uklanjanje vodenog žiga znači da se ne može smatrati da napadnuto djelo ne sadrži a vodeni žig. Odnosno, ako se ukloni vodeni žig, to nije

moguće otkriti čak ni sofisticiranim detektorom. Cilj je protivnika napraviti novo djelo koje je perceptivno slično izvornom djelu, ali nikada neće biti otkriveno kao da sadrži vodeni žig. Izvornik bi sam po sebi ispunio ovaj cilj, ali samo je jedan od mnogih djela koja bi.

Maskiranje vodenog žiga znači da se napadnuto djelo i dalje može smatrati vodenim žigom, ali postojeći znak nije moguće otkriti detektorom. Sofisticiraniji detektori mogli bi ga moći otkriti. Na primjer, mnogi detektori vodenih žigova na slici ne mogu otkriti vodene žigove koji su bili lagano rotirani. Dakle, protivnik može primjeniti dovoljno malu rotaciju, biti neprimjetan, s time da iskrivljena slika ima prihvatljivu vjernost. Budući da je detektor vodenog žiga osjetljiv na rotacije vodeni žig neće moći ga otkriti. Ipak, vodeni žig još uvijek može otkriti više sofisticcirani detektor sposoban za korekciju rotacije. Stoga možemo misliti da je vodeni žig još uvijek prisutan.

Jedan zanimljiv oblik neovlaštenog uklanjanja poznat je kao tajno dogovoreni napad. Ovdje napadač dobiva nekoliko primjeraka danog djela, svaki sa drugačijim vodenim žigom i kombinira ih kako bi se stvorila kopija bez vodenog žiga. To je prvenstveno zabrinjavajuće u praćenju transakcija, što podrazumijeva postavljanje različite vodene žigove u svakoj kopiji. S postojećim sustavima vodenog žiga se općenito vjeruje da je dovoljan prilično mali broj primjeraka da bi napad bio uspješan. O tome koliko je ozbiljan ovaj problem ovisi kontekst u kojem se koristi praćenje transakcija. Iako možemo zamisliti da bi protivnik mogao dobiti desetak napadača i tako moći ukloniti vodeni žig. Međutim, u aplikaciji studijskih dnevnika vrlo je malo vjerojatno da će to moći raditi bilo koji zaposlenik i dobiti mnogo različitih kopija datog filmskog isječka; dakle, napadi tajnog dogovora su manja briga.

4. Klasifikacija metoda za označavanje slike digitalnim vodenim žigom

Mnoge aplikacije zahtijevaju otkrivanje vodenih žigova u radovima koji su možda bili izmjenjeni nakon ugradnje vodenog žiga. Vodeni žigovi koji su osmišljeni da prežive legitimne i procese svakodnevne uporabe nazivaju se robusnim vodenim žigovima. Algoritam igra vitalnu ulogu u označavanju slike, stoga pravilno uporabljena tehnika može biti veoma učinkovita i time činiti vodeni žig teškim za uočiti. Napadač može uništiti vodeni žig samo ako poznaje algoritam kojim je vodeni žig ugrađen u sliku. Postoje više algoritama koji se koriste za skrivanje informacija, a dolaze u dvije domene. To su prostorna domena i frekvencijska domena.

4.1. Prostorna domena

Prostorna domena jest domena gdje alogritam digitalnog vodenog žiga izravno učitava neobrađene podatke u izvornoj slici. Prostorni vodeni žig se također može primjeniti razdvajanjem boja te se na taj način vodeni žig pojavljuje samo u frekveniciji jedne boje. To čini vodeni žig vidljivo suptilnijim pa ga je teže otkriti promatrajući ga. Prostorna domena manipulira ili mijenja sliku koja predstavlja objekt u prostoru i time poboljšava sliku u zadanoj aplikaciju ili upotrebi. Tehnike prostorne domene se temelje na izravnoj manipulaciji piksela na slici i njihova podjela sljedi.
Aditivni vodeni žig je najjednostavnija metoda za ugradnju vodenog žiga u prostornu domenu i postiže se dodavanjme pseudo slučajnog uzorka šuma intezitetu piksela slike. Signal šuma je cijeli broj poput (-1, 0, 1) ili ponekad brojevi sa decimalnom točkom. Kako bi se osiguralo da se vodeni žig može otkriti, šum se generira ključem tako da korelacija između različitih ključeva bude minimalna.

Druga tehnika prostorne domene je Najmanje značajni bit. Ova metoda je laka za implementaciju i ne stvara ozbliljna izobličenja slike; međutim to čini vodeni žig ne robustnim i lakom metom za napade. Ugrađivanje vodenog žiga se vrši odabirom podskupa

slikovnih piksela i zamjenom najmanje bitnog bita svakog od odabranih piksela s bitovima vodenig žiga. Vodeni žig se može biti proširen kroz cijelu sliku ili se može nalaziti na odabranim mjestima slike. Ova tehnika je zato jako ranjiva na napade te se vodeni žig može jako lagano uništiti jer je ova tehnika jako osjetljiva na šum i uobičajenu obradu signala što ju čini ne praktičnom u svakodnevnim primjenama.

Tehnika temeljena na modulaciji proširenog spektra ili SSM (eng. "Spread Spectrum Modulation") je metoda u kojoj se energija generira na jednoj ili više diskretnih frekvencija te ih se širi i ditribuira kroz određeno vrijeme. Algoritmi vodenih žigova ugrađuju informacije linearnom kombinacijom izvorne slike s malim signalom pseudo šuma koji se modulira ugrađivanjem vodenog žiga.
Patchwork algoritam je tehnika skrivanja podataka koju su razvili Bender i dr. te objavili u IBM Systems Journal-u, 1996 [18]. Temelji se na pseudo slučajnom, statističkom modelu. Patchwork unosi vodeni žig s određenom statistikom pomoću Gaussove distribucije. Izvodi pseudo slučajni odabir dvije zakrpe "A" i "B". Zakrpa A su posvijetljeni podaci o slici a zakrpa B su zatamnjeni. Zatim se generira pseudo slučajni tok bitova za odabir parova piksela iz podatak naslovnice. Gleda se razlika između dva zadana bita se kodira poruka u sliku po parovima bitova.

4.2. Frekvencijska domena

Frekvencijska domena u usporedbi s metodama prostorne domene su primjenjenije u svakodnevnoj uporabi. Cilj je ugraditi vodene žigove u spektralne koeficijente slika. Najčešće korištene transformacije su diskretna kosinusna transformacija (DCT), diskretna Fourierova transformacija (DFT) i diskretna valovita transformacija (DWT). Razlog zašto se implementacija vodenog žiga u frekvnencijskoj domeni više koristi je jer karakteristike ljudskog vidnog sustava bolje uočavaju spektralne koeficijente.
Diskretne kosinusne transformacije (DCT): DCT predstavlja podatke u smislu frekvencijskog prostora a ne amplitudnog prostora. Taj aspekt je koristan jer je više prilagođen načinu na koji ljudi percipiraju svjetolst, tako da dio koji nebi mogli percipirati se idenrificira i odbaci. Tehnike vodenih žigova temeljene na DCT su robusne u usporedbi s teh-

nikama prostorne domene. Takvi algoritmi su robusni na jednostavne operacije obrade slike poput nisko frekventnog filtriranja, podešavanja svjetiline i kontrasta, te zamućivanje. Mana im je što su skuplji i što su teže za implementirati. Ujedno su slabi protiv geometrijskih napada poput rotacije, skaliranja, obrezivanja itd [19].

Diskretne valovite transformacije (DWT) je moderna tehnika koje se često koristi u digitalnoj obradi slika, kompresiji, označavanju vodenim žigom itd. Transformacije se temelje na malim valovima, zvanim wavelet, različitih frekvencija i ograničenog trajanja. Wavelet transformacija razlaže sliku u tri prostorna smjera, tj. vodoravni, okomiri i dijagonalni. Koeficijent DWT je veći u najnižim frekvencijama (LL) te manji u ostalim podjelama (HH, HL i LH). Diskretna valovita transformacija ima najčešću uporabu u raznim procesim obrade signala aplikacije kao što su kompresija zvuka i videa, uklanjanje šuma u zvuku i simulacija bežične antene. Valovi imaju svoju energiju koncentriranu u vremenu i vrlo su prikladni za analizu prolaznih, vremenski promjenjivih signala. Budući da je većina signala u svakidašnjem životu promjenjiva, DWT je prikladan odabir za mnoge aplikacije [20]. Primarni cilj kod poboljšanja efektivnosti vodenih žigova je potići bolji kompromis između robusnosti i percepcije. Robusnost se može postići povećanjem čvrstoće ugrađenog vodenog žiga te ali i time se povećava vidljivo izobličenje [izvor neki]. Prednost DWT-a je što pruža istodobno prostornu lokaciju i frekvencijsko širenje vodenog žiga unutar slike. Osnovna ideja diskretne valne transformacije u procesu slike je višestruko razlaganje slike na podslike različitih prostornih domena neovisnih o frekvencijama [20].

Diskretna Fourierova transformacija (DFT) pretvara kontinuiranu funkciju u svoje frekvencijske komponente. Posjeduje svojstvo robusnosti protiv geometrijskih napada poput rotacije, skaliranja, obrezivanja, translacije itd. DFT pokazuje translacijsku nepromjenjivost, prostorni pomaci na slici utječu na fazni prikaz slike a prikaz veličine i kružni pomaci u prostornoj domeni ne utječu na veličinu Fourierove transformacije.

5. Zaključak

Slike i digitalni mediji su važan dio multimedijskih podataka. Autentifikacija slike je izazovan zadatak zbog internetskog prometa te su u svijetu predstavljeni brojni izazovi za uspješnu uporabu vodenih žigova radi kontrole autorskih prava. Jedan od ključnih istraživačkih problema s kojima se danas suočava tiskarska industrija jest razvoj uspješnog, robusnog, transparentnog i sigurnog vodenog žiga za različite digitalne medije. Još jedan od postojećih problema je razvoj tehnike za poluautomatsku provjeru autentičnosti. Kako bi došlo do poboljšanja robusnosti i visoke sigurnosti slikovnih podataka uz zadržavanja neprimjetnosti i kapaciteta ugrađivanja, budući vodeni žigovi morat će kombinirati algoritme strojnog učenja i te zadržavanje vodenog žiga na digitalnim medijima.

S obzirom na postojeće tehnike apliciranja digitalnih vodenih žigova, možemo ih kategorizirati u dvije domene: Prostorna i Frekvencijska domena. Nadalje u Prostornoj domeni mogu se razlikovati sljedeći vodeni žigovi s obzirom na način apliciranja: Aditivni vodeni žig, Najmanje značajni bit, Modulacija proširenog spektra, te Patchwork algoritam. U kategoriji Frekvencijske domene najčešće korištene transformacije su diskretna kosinusna transformacija (DCT), diskretna Fourierova transformacija (DFT), te diskretna valovita transformacija (DWT). Iako postoji još mnogo različitih metoda označavanja slika digitalnim vodenim žigovima, te se nove tehnike razvijaju svakodnevno, ova kategorizacija može predstavlja temelj za buduća istraživanja i pokušaja sortiranja metoda vodenih žigova. sigurnosnih kompromisa.

6. Literatura

[1] Philip B. Meggs and Alston W. Purvis. *Meggs' History of Graphic Design*. John Wiley Sons, 2016.

[2] Chiaroscuro watermarks, 1958.

[3] J. Abbate. Inventing the web. *Proc. of the IEEE*, 1999.

[4] Andrej Dujella and Marcel Maretić. *Kriptografija*. Element, 2007.

[5] David Kilburn. Dirty linen, dark secrets, 1997. URL https://www.adweek.com/brand-marketing/media-agencies-dirty-linen-dark-secrets-21712/.

[6] URL http://www.computableminds.com/post/lena-soderberg-common-image-processing-test html.

[7] Monica Borda. *Fundamentals in Information Theory and Coding*. Springer, 2011.

[8] URL https://www.hollywoodreporter.com/news/general-news/an-actors-personal-tale-i-was-thrown-academy-sharing-screeners-976778/.

[9] S. P. Mohanty, O. B. Adamo, E. Kougianos, M. Varanasi, and W. Cai. *VLSI architecture and FPGA prototyping of a digital camera for image security and authentication*. IEEE, 2006.

[10] M. K. Arnold, M. Schmucker, and S. D. Wolthusen. *Techniques and Applications of Digital Watermarking and Content Protection*. Artech House, 2003.

[11] Verance technology, 2010. URL https://web.archive.org/web/20100612221956/http://www.verance.com/technology/index.php.

[12] R. S. Broughton and W. Laumeister. Interactive video method and apparatus, 1988. URL https://patentscope.wipo.int/search/en/detail.jsf?docId=WO1989004100.

[13] Ray dolby. apparatus and method for the identification of specially encoded fm stereophonic broadcasts. united states patent, 4,281,217, 1981. URL https://uspto.report/patent/grant/4281217.

[14] URL http://www.narodni-list.hr/posts/115675001.

[15] URL https://en.wikipedia.org/wiki/Digital_terrestrial_television#Analogue_to_digital_transition_by_countries.

[16] M. Hagmüller and G. Kubin. Speech watermarking for air traffic control, 2005. URL https://www.eurocontrol.int/sites/default/files/library/005_Speech_Watermarking_for_ATC.pdf.

[17] A. Hanjalic, G.C. Langelaar, P.M.D. van Roosmalen, J. Biemond, and R.L. Lagendijk. Image and video databases: Restoration, watermarking and retrieval, 2000.

[18] URL http://ippr-practical.blogspot.com/.

[19] V. M. Potdar, S. Han, and E. Chang. A survey of digital image watermarking techniques, 2005.

[20] E. Brannock, M. Weeks, and R. Harrison. Watermarking with wavelets: Simplicity leads to robustness, 2008.

[Slika 1.] URL:"http://baph.org.uk/watermarks.html"

[Slika 2.] URL:"https://fitsmallbusiness.com/wp-content/uploads/2021/04/Screenshot_of_Closeup_Po

[Slika 3.] URL:"https://www.zdnet.com/a/hub/i/r/2016/08/09/5d4189d0-2005-49cd-ba12-da50f46a0d73/thumbnail/770x578/b906417276f88d7e5666019ba5915284/mosaic.jpg"

[Slika 4.] URL:"https://mk0divxpbmdevm0tpf50.kinstacdn.com/wp-content/uploads/2019/03/conver

[Slika 5.] URL:"https://boingboing.net/images/corpse_screener_pirate.jpg"

[Slika 6.] URL:"https://enviragallery.com/wp-content/uploads/2016/02/remove-a-person-from-the-image.jpg"

[Slika 7.] URL:"https://www.shutterstock.com/image-photo/vintage-stylized-wall-street-sunset-lens-389584069?irclickid=XylywRxUPxyIToh2vQx9iVURUkBQ1n25HSfuVY0irgwc=1utm_m
77643"