

# DIGITALNI VODNI TISK

**Dr. Jasna Maver**

Filozofska fakulteta, Oddelek za bibliotekarstvo, Ljubljana  
(*jasna.maver@ff.uni-lj.si*)

---

Oddano: 17.02.2000 – Sprejeto: 22.03.2000

Pregledni znanstveni članek

UDK 777.6:347.78:007

## Izvleček

Velika količina multimedijskih vsebin, ki so na voljo na svetovnem spletu, poraja vprašanja njihove zaščite. Digitalni vodni tisk je tehnika, ki služi pri zaščiti intelektualne lastnine, preverjanju verodostojnosti in celovitosti multimedijskih vsebin ali ima vlogo dodatnega skritega ali vidnega označevanja vsebine. Posledica raznolikosti uporabe so številne tehnike digitalnega vodnega tiska, ki jih razvrščamo na osnovi različnih lastnosti. Najpogostejša je delitev na viden ali neviden vodni tisk in robusten ali krhek vodni tisk. Za razliko od vidnega vodnega tiska, kjer vstavimo vidni vzorec ali sliko v original, nevidni vodni tisk ne spremeni vizualnega izgleda slike. Nevidni vodni tisk v sliki lahko potrdimo le z določenim algoritmom. Robusten vodni tisk je namenjen zaščiti avtorskih pravic, medtem ko se krhek vodni tisk uporablja za preverjanje verodostojnosti in celovitosti multimedijskih vsebin. Digitalni vodni tisk ima smisel le, če ga lahko v primeru zlorabe multimedijske vsebine izločimo. V nekaterih primerih izločimo vodni tisk v njegovi originalni obliki, v drugih primerih izvedemo le potrditev prisotnosti določenega vodnega tiska. Digitalne knjižnice, preko katerih bodo kulturne institucije ponujale multimedijske vsebine, bodo morale vključevati širok spekter storitev, ki bodo zagotavljale zaščito intelektualne lastnine. Digitalni vodni tisk bo tu lahko odigral pomembno vlogo.

**Ključne besede:** digitalni vodni tisk, avtorsko pravo, multimedijski sistemi, digitalni nosilci informacij

## Abstract

The huge amount of multimedia contents available on the World-Wide-Web is beginning to raise the question of their protection. Digital watermarking is a technique which can serve various purposes, including intellectual property protection, authentication and integrity verification, as well as visible or invisible content labelling of multimedia content. Due to the diversity of digital watermarking applicability, there are many different techniques, which can be categorised according to different criteria. A digital watermark can be categorised as visible or invisible and as robust or fragile. In contrast to the visible watermark where a visible pattern or image is embedded into the original image, the invisible watermark does not change the visual appearance of the image. The existence of such a watermark can be determined only through a watermark extraction or detection algorithm. The robust watermark is used for copyright protection, while the fragile watermark is designed for authentication and integrity verification of multimedia content. A watermark must be detectable or extractable to be useful. In some watermarking schemes, a watermark can be extracted in its exact form, in other cases, we can detect only whether a specific given watermarking signal is present in an image. Digital libraries, through which cultural institutions will make multimedia contents available, should support a wide range of service models for intellectual property protection, where digital watermarking may play an important role.

**Key words:** digital watermark, copyright, multimedia systems

## 1 Uvod

Svetovni splet omogoča dostop do ogromne količine multimedijских vsebin: tekstov, grafik, slik, video posnetkov in zvočnih zapisov. Vse te vsebine so na voljo za pregledovanje in prenos na milijone uporabnikom na mreži, kar poraja problem zaščite avtorskih pravic. Digitalni vodni tisk je tehnika, ki jo je možno uporabiti za tovrstno zaščito. V nasprotju s kriptografijo-šifriranjem podatkov, ki je namenjena zaščiti zaupnih podatkov pri njihovem prenosu preko računalniških omrežij, je namen digitalnega vodnega tiska v zaščiti multimedijских vsebin, ko so na voljo v nešifrirani obliki. Digitalni vodni tisk ne preprečuje protizakonitih dejanj, kot je na primer kraja, pač pa se uporablja v procesu dokazovanja, ko je do protizakonitega dejanja že prišlo.

Digitalni vodni tisk (angl. watermarking) lahko smatramo kot del znanosti, ki jo imenujemo steganografija (angl. steganography). Beseda steganografija je grškega izvora in pomeni prikrito pisanje (Hawkins, 1998). V literaturi srečamo še izraza, vstavljanje informacije (angl. information embedding) in skrivanje

informacije (angl. information hiding). Navedeni izrazi so zamenljivi in se nanašajo na proces vstavljanja sekundarnega digitalnega signala v primarni digitalni signal, ki ga je možno v primeru zlorabe v procesu dokazovanja zaznati ali izločiti. V delu dajemo poudarek slikam. V primeru slik je sekundarni digitalni signal slika vodnega znaka. Vodni znak je lahko znak organizacije, lahko je sporočilo, lahko naključno proizveden vzorec ali slika, odvisno od namena in vloge, ki jo ima vodni tisk.

V delu najprej opisujemo vlogo, ki jo ima digitalni vodni tisk pri zaščiti intelektualne lastnine multimedijske vsebine, pri dokazovanju verodostojnosti multimedijske vsebine in vloge, ki jo ima pri vidnem ali skritem dodatnem označevanju vsebine. Nato predstavimo osnovne skupine tehnik digitalnega vodnega tiska, opišemo nekaj primerov vstavljanja digitalnega vodnega tiska v sliko in pojasnimo vlogo, ki jo ima varnostni ključ pri izločanju vodnega tiska oziroma potrjevanju prisotnosti določenega vodnega tiska v multimedijski vsebini. V poglavju, ki sledi, navajamo nekaj primerov kulturnih institucij, ki so s pomočjo tehnike digitalnega vodnega tiska omogočile dostop do izjemnih starih rokopisov v digitalni obliki.

## 2 Različna vloga vodnega tiska

Uporaba vodnega tiska v multimediji je raznolika (Memon in Wong, 1998). Razvoj digitalnega vodnega tiska je spodbudila uporaba varstvenih znamk, katerih namen je bila zaščita avtorskih pravic. Varstvene znamke so vključevale informacijo o lastniku in dobavitelju multimedijskih vsebin ter informacijo o licenčnih pogojih. Številna programska orodja na računalnikih omogočajo manipulacijo z informacijami v digitalni obliki. Digitalne podatke je možno na različne načine spreminjati, enostavno jih je razmnoževati, tiskati in razširjati. Kršenje avtorskih pravic je v primeru multimedijskih vsebin enostavno (Žnideršič, 1997). Digitalni vodni tisk lahko uporabimo za zaščito avtorskih pravic, za preverjanje verodostojnosti in celovitosti multimedijskih vsebin, za dodatno skrito ali vidno označevanje vsebine, ki omogoča npr. kontrolo uporabe multimedijskih produktov ter reklamiranje multimedijskih vsebin.

### 2.1 Potrjevanje lastništva, preprečevanje nepooblaščenega razmnoževanja in razširjanja

Digitalni vodni tisk omogoča preverjanje lastništva multimedijskih vsebin. Potrjevanje lastništva je zanimivo za organizacije, ki so lastniki avtorskih pravic

multimedijskih produktov in imajo pravico izdajanja licenc. Te organizacije so časopisne agencije, banke fotografij, muzeji in knjižnice. Lastnik multimedijske vsebine, na primer slike, zahteva pri objavi slike od uporabnika avtorski honorar. Z vgradnjo vodnega tiska v sliko želi lastnik slike odvrniti uporabnika od neplačila avtorskega honorarja. Vgrajeni vodni tisk vsebuje ali informacijo o lastniku ali uporabniku. V primeru informacije o lastniku mora lastnik občasno pregledati objavljene vsebine, kjer ga zanima potrjevanje svojega vodnega tiska. V primeru informacije o uporabniku odkriva lastnik piratske kopije. V tem primeru lahko uporabimo posebno shemo vgrajevanja vodnih znakov, ki jim pravimo prstni odtisi. Shema prstnih odtisov omogoča enostavno vgradnjo večkratnih vodnih znakov tako, da novi vgrajeni znak nima vpliva na že vgrajene znake in vizualni izgled slike. Prstni odtisi oblikujejo hierarhično shemo distribucije oziroma shemo sledenja, ki omogoča v primeru odkritja piratske kopije določitev izvorne kopije oziroma identifikacijo posameznikov, ki so odgovorni za nezakonite kopije.

Digitalni vodni tisk, ki služi za potrjevanje lastništva, se mora ohraniti pri namernih poskusih njenega odstranjevanja in ponarejanja oziroma najpogostejših operacijah, ki jih izvajamo nad slikami.

## 2.2 Preverjanje verodostojnosti in celovitosti

V primerih legalne uporabe multimedijskih vsebin v medicinskih aplikacijah, novinarstvu ali pri komercialnih transakcijah, potrebuje avtor multimedijske vsebine način, s katerim lahko potrdi, da je prišlo do spreminjanja, manipulacije in ponarejanja vsebine. Verodostojnost vsebine se v tem primeru preverja z neokrnjenostjo vodnega tiska.

## 2.3 Skrito in vidno označevanje vsebine

V tem primeru beleži vodni tisk, ki ga vgradimo, dodatno informacijo o vsebini.

- Dodatna informacija k sliki je lahko oznaka DOI (angl. Digital Object Identifier), ki označuje avtorsko pravno zaščiteno delo v digitalni obliki (Žnideršič, 1997)<sup>1</sup>.

1 DOI je razvila Mednarodna DOI fundacija na zahtevo založniške industrije. DOI določa ogrođe za upravljanje z intelektualno vsebino, omogoča povezovanje kupca z založnikom, olajša elektronsko trgovanje in omogoča avtomatsko upravljanje z avtorsko pravico.

- V multimedijskih aplikacijah lahko uporabljamo dodatno informacijo za video in avdio indeksiranje in iskanje na osnovi vsebine.
- Dodatno informacijo lahko uporabimo za kontrolo uporabe multimedijske vsebine. V zaprtih sistemih, kjer potrebujejo multimedijski produkti posebno strojno opremo za kopiranje in prikazovanje, lahko uporabimo vodni tisk za določitev števila kopij. Pri kreiranju kopije spremeni strojna oprema tudi vodni tisk. Po določenem številu kopij se vodni tisk tako spremeni, da strojni opremi ne dovoli izdelave nove kopije. Na primer: v vsak digitalni film bi lahko vgradili vodni tisk »never copy«, »copy once«, »no more copy«. Vsaka naprava za presnemavanje bi jih morala zaznati in zavrniti prepisovanje, ko to ne bi bilo dovoljeno.
- Dodatna vidna informacija je lahko v pomoč pri oglaševanju multimedijskih vsebin: lastnik multimedijskega produkta želi javno predstaviti vsebino produkta, ki ga namerava prodajati. Komerzialno neuporabnost predvajane vsebine lahko doseže tako, da jo potiska z vidnim vodnim tiskom, ki ga je zelo težko odstraniti na avtomatiziran način.

Univerzalna tehnika, ki bi zadovoljila vse našete primere uporabe vodnega tiska, ne obstaja. Vsako tehniko digitalnega vodnega tiska moramo načrtovati znotraj konteksta celotnega sistema, kjer jo bomo uporabili.

### 3 Tehnike vodnega tiska

Raznolikost uporabe vodnega tiska je vodila do številnih shem oziroma tehnik vodnega tiska, ki jih lahko razvrščamo na različni osnovi:

1. Vodni tisk je lahko *viden* ali *neviden*.
  - Vidni vodni tisk (slika 1) vsebuje vidni vzorec, sporočilo ali znak delovne organizacije v primeru identifikacije lastništva slike. Kvaliteto vidnega vodnega tiska določata v tehničnem smislu dva kriterija: kako težko je vgrajeni vidni vodni tisk odstraniti v primeru nepooblaščenega odstranjevanja in ali vgrajeni vodni tisk zagotavlja, da ga je v resnici vstavila oseba, na katero se sklicuje.
  - Slika, ki vsebuje nevidni vodni tisk je vizualno enaka sliki, ki ne vsebuje vodnega tiska, ni pa identična. Prisotnost vodnega tiska lahko v tem primeru določimo le z ustreznim algoritmom.
2. Vodni tisk je lahko *krhek* ali *robusten*.
  - Krhek vodni tisk pokvarimo s katerokoli tehniko obdelave slike. Takšnega tipa mora biti npr. vodni tisk za ugotavljanje verodostojnosti in celovitosti dokumenta.

- Robustni vodni tisk je odporen proti različnim poskusom njegovega ponarejanja ali odstranjevanja in proti najpogostejšim operacijam, ki jih izvajamo pri obdelavi slike, kot so JPEG zgoščevanje, rezanje, povečevanje, filtriranje, ostrenje slike, barvno popravljanje in spreminjanje kontrasta. Primeren je za potrjevanje lastništva.



Slika 1: Vidni vodni tisk: a) originalna slika, b) vodni znak, c) slika z vgrajenim vidnim vodnim znakom.

## 4 Vstavljanje vodnega tiska v dokument

Vodni tisk je lahko v splošnem funkcija večjega števila faktorjev, na primer, uporabnikove identitete (ID), ključa, slike in njenih parametrov, kot so npr. dimenzije slike. Za ilustracijo bomo opisali nekaj tehnik za primer robustnega in krhkega vodnega tiska.

### 4.1 Robustni vodni tisk

Prvotne robustne tehnike digitalnega vodnega tiska so vključevale vodni tisk neposredno v samo sliko oziroma v dvodimenzionalni prostor slike. Tehnika, ki jo bomo opisali (Nikolaidis in Pitas, 1996), je dokaj robustna za operacije zgoščevanja, filtriranja in povečevanja. Slikovne elemente v sliki razdeli v dve približno enako veliki množici  $A$  in  $B$ . Razporeditev slikovnega elementa v eno izmed množic je določena naključno.  $K$  vrednosti vsakega slikovnega elementa, ki je uvrščen v množico  $A$ , prištejemo majhno število  $k$ , od vrednosti vsakega slikovnega elementa, ki je uvrščen v množico  $B$ , število  $k$  odštejemo. Vrednost števila  $k$  je dovolj majhna, da vizualno ne spremeni slike. Za vsako množico  $A$  in  $B$  izračuna algoritem povprečno vrednost slikovnih elementov, ki jih vključuje. Razlika med povprečnima vrednostima je v sliki z vodnim

tiskom za  $2k$  večja kot v originalni sliki. Poznavanje razdelitve slikovnih elementov v množici  $A$  in  $B$ , razlike med povprečnima vrednostima slikovnih elementov v množici  $A$  in  $B$  in vrednosti števila  $k$  omogočajo potrditev prisotnosti vodnega tiska.

V nasprotju s tehnikami, ki vstavljajo vodni tisk v dvodimenzionalni prostor slike in pri tem spremenijo le majhno količino bitov, lahko z uporabo tehnik, ki prevedejo sliko v drugo domeno, vključimo večje število bitov. Te tehnike vgradijo vodni tisk v procesu transformacije, kot je na primer diskretna kosinusna transformacija, valčkova transformacija (angl. wavlet transform) ali Fourierova transformacija. Pomembna prednost tehnik, osnovanih na diskretni kosinusni transformaciji, je v vstavljanju vodnega znaka in njegovem potrjevanju na zgoščeni predstavitvi slike. To omogoča, da vključimo vodni tisk direktno v JPEG sliko ali MPEG in MJPEG video. Te tehnike so primerne za digitalno radiodifuzijo in video na zahtevo. Slabost teh tehnik je, da se pri prevedbi slike v nezgoščeno obliko spremembe ojačajo in lahko popačijo izgled slike. Obstaja vrsta tehnik, ki poskušajo minimalizirati tovrstne napake.

## 4.2 Krhki vodni tisk

Tehnike, ki jih uporabljamo za dokazovanje verodostojnosti in celovitosti morajo zaznati vsako spremembo v sliki. Željeno je, da spremembo v sliki tudi lokalizirajo. Shema, ki jo lahko uporabimo, je shema digitalnega podpisa (Friedman, 1993). Podpis izračunamo za sliko na enak način kot za splošne digitalne podatke. Digitalni podpis se nato shrani skupaj s sliko. Uporabnik preveri verodostojnost slike na način, kot ga zahteva običajen digitalni podpis.

Yeung in Mintzer (1997) sta predlagala vgradnjo binarne slike vodnega znaka. Njun algoritem vgradi sliko vodnega znaka s pomočjo naključnega binarnega zaporedja  $R$  in binarne funkcije zgoščevanja  $f$ . Vrednost slikovnega elementa v originalni sliki na lokaciji  $(i,j)$  je indeks na element v zaporedju  $R$ , ki predstavlja vhod v funkcijo  $f$ . Algoritem primerja binarni izhod iz funkcije  $f$  z binarno vrednostjo slikovnega elementa v sliki vodnega znaka na mestu  $(i,j)$ . V primeru, da sta vrednosti različni, spremeni algoritem vrednost slikovnega elementa v originalni sliki na mestu  $(i,j)$  za majhno vrednost tako, da kaže na element v zaporedju  $R$ , ki da skladen rezultat. Slika spremenjenih vrednosti slikovnih elementov je slika z vgrajenim vodnim znakom. Izhodi iz funkcije  $f$ , ki jih določata slika z vgrajenim vodnim znakom in binarno zaporedje  $R$ , tvorijo sedaj binarno sliko vodnega znaka. V primeru barvne slike je binarni izhod enak vsoti po modulu dva, rezultatov iz treh barvnih ravnin.

## 5 Izločanje ali potrjevanje prisotnosti vodnega tiska

Pri nekaterih shemah izločimo vodni tisk v originalni obliki, pri drugih shemah lahko izvedemo le potrditev prisotnosti določenega vodnega tiska. Izločanje oziroma potrjevanje prisotnosti vodnega tiska običajno zahteva varnostni ključ. Varnostni ključ je najpogosteje geslo, ki ima obliko fraze, ali seme pseudo naključnega generatorja števil. V opisanem primeru robustnega vodnega tiska je varnostni ključ seme pseudo naključnega generatorja števil, ki generira naključno razporeditev slikovnih elementov v množici  $A$  in  $B$ . V procesu dokazovanja lahko izvedemo le potrditev prisotnosti vodnega tiska. V opisanem primeru krhkega vodnega tiska je varnostni ključ seme pseudo naključnega generatorja števil, ki generira naključno binarno zaporedje  $R$ . Sliko vodnega znaka lahko izločimo le s poznavanjem zaporedja  $R$ .

Sheme vodnega tiska, ki uporabljajo ključ, lahko klasificiramo ali kot *sheme tajnega ključa* ali kot *sheme javnega ključa*. Sheme tajnega ključa uporabljajo isti ključ v proceduri za vstavljanje in proceduri za izločanje ali potrjevanje prisotnosti vodnega tiska. Sheme tajnega ključa zato zahtevajo zaščiteno komunikacijo pri prenosu informacije o ključu med lastnikom in uporabnikom slike. Sheme javnega ključa uporabljajo za vnos vodnega tiska drugačen ključ kot ga uporabljajo za izločanje ali potrjevanje prisotnosti. Privatni ključ se uporablja za vnos vodnega tiska, javni ključ pa za potrjevanje prisotnosti ali izločanje. Iz navedenega izhaja, da lahko z uporabo javnega ključa vsak preveri, ali vsebuje slika vodni tisk.

Nekatere sheme zahtevajo za izločanje oziroma potrjevanje prisotnosti vodnega tiska originalno sliko. Taka shema se imenuje *privatna shema*. Shema, ki originalne slike ne zahteva, se imenuje *shema s pozabo*. Sheme s pozabo z javnim ključem so atraktivne za številne aplikacije, npr. za preverjanje kršitev avtorskih pravic v arhivih slik, ali v primeru, ko so slike objavljene na internetu. V slednjem primeru bi lahko uporabili programske agente, kot je npr. Webcrawler, ki bi preveril identiteto za vse slike, ki jih najde na internetu. Sheme, ki zahtevajo originalne slike, niso primerne za tovrstno kontrolo.

## 6 Starodavne umetnine v digitalni obliki

Digitalni vodni tisk je pritegnil pozornost nekaterih pomembnih korporacij, kot je na primer IBM. Od leta 1985 IBM skupaj s sodelavci deluje na številnih projektih digitalizacije zbirk umetniških in zgodovinskih materialov. Pomembnejši projekti vključujejo institucije Biblioteca Vaticana Apostolica



(Vatikan), Archivo General de Indias (Sevilla, Španija), Klau Library of Hebrew Union College (Cincinnati, Ohio, ZDA), Yale Beinecke Library (New Haven, Connecticut, ZDA) in delo Andrewa Wyetha (Chadds Ford, Pennsylvania, ZDA). V naštetih projektih gradnje digitalnih knjižnic je bila posebna pozornost namenjena kvalitetni predstavitvi vsebin in zaščiti intelektualne lastnine. V delu bomo na kratko opisali le primer Vatikanske knjižnice, ostale lahko bralec poišče v dostopni literaturi (npr. Gladney et al., 1998).

Vatikanska knjižnica hrani izredno zbirko redkih knjig in rokopisov. Med 150.000 rokopisi so tudi prve kopije del Aristotela, Danteja, Evklida, Homerja in Vergila. Profesorji in študentje z univerz Pontifical Catholic iz Ria de Janeira, Case Western Reserve iz Clevelanda, osebje iz Vatikanske knjižnice in raziskovalci iz IBM-a so sodelovali pri gradnji digitalne knjižnice, ki študentom in raziskovalcem preko interneta omogoča dostop do pomembnega števila starih rokopisov v digitalni obliki. Zaradi strahu pred nezadostno varnostjo na internetu je Vatikanska knjižnica vztrajala pri dodatni zaščiti (poleg omejenega dostopa), ki bi odvrčala od nezakonitega prisvajanja in spreminjanja vsebin iz digitalne knjižnice. Komercialna uporaba slik, kot so na primer CD-ROM igre ali tiskanje slik na srajčke in druge spominke, bi knjižnico prikazala v slabi luči in jo oropala za dohodek. Prvotni poskus zaščite, da bi bile slike, ki so dostopne preko interneta, na voljo le v obliki z nizko ločljivostjo in kot take nezanimive za popularno umetnost, je bil neustrezen. Nizka ločljivost je ovirala delo raziskovalcev umetnostne zgodovine. Potrebno je bilo uporabiti drugo vrsto zaščite. Slike so zaščitili z vidnim vodnim znakom, ki je jasno viden, hkrati pa odraža skrb po kvaliteti. Vodni znak je nevsiljiv, ohranja podrobnosti, ki so zanimive za študente in raziskovalce in ga je težko odstraniti.

Navedeni primeri kažejo, da je mogoče institucijam in skupinam olajšati dostop do posebno vrednega in občutljivega materiala s prevedbo le tega v digitalno obliko in organizacijo v digitalno knjižnico. Infrastruktura digitalne knjižnice mora nuditi podporo pripravi, diseminaciji in uporabi različnih multimedijskih vsebin od tekstov, slik, zvočnih zapisov, video posnetkov do 3-D modelov. Za vse navedene oblike multimedijskih vsebin bo morala digitalna knjižnica zagotoviti širok spekter storitev, ki bodo med drugim zagotavljale preverjanje verodostojnosti in zaščito avtorskih pravic (Chowdhury, 1999). Digitalni vodni tisk bo tu lahko odigral pomembno vlogo.

## 7 Zakonit status vodnega tiska

Vodni tisk bo tudi v praksi deloval le, če bomo določili pravno veljavne protokole in standarde, ki bodo reševali dejanske probleme piratstva in zlorabe.

Dobrodošel bi bil standardiziran vmesnik za vstavljanje in izločanje vodnega tiska, ki bi nudil okolje (»plug and play«), kjer bi na enostaven način zamenjali eno tehniko vodnega tiska z drugo (Mintzer et al., 1998). Takšno okolje zahteva standardne formate varnostnih ključev in standardne oblike podatkov, ki jih vstavljamo v sliko, npr. slike vodnega znaka, podatkov za skrito dodatno označevanje.

Oblikovati je potrebno enotne kriterije, ki bi jih uporabili za primerjalno presojo (benchmarking) pri testiranju odpornosti robustnega digitalnega vodnega tiska. Ti kriteriji vključujejo določitev množice operacij, ki jih običajno izvajamo nad multimedijskimi vsebinami, in množice zlonamernih operacij oziroma poskusov odstranjevanja in ponarejanja digitalnega vodnega tiska. Poleg množice operacij je potrebno določiti stopnjo degradacije multimedijske vsebine, ki naj jo pri testiranju digitalni vodni tisk preživi, in testno množico multimedijskih vsebin.

Čeprav so bili za nekatere aplikacije že predlagani protokoli, npr. za radiodifuzijo, DVD in elektronsko dostavljanje, še vedno ni zanesljivih splošno sprejetih protokolov. Poleg odgovorov na vprašanja o registraciji in potrjevanju tehnik digitalnega vodnega tiska bi morali tovrstni protokoli dati tudi odgovore na vprašanja, kot na primer, kdo skrbi za storitve v zvezi z digitalnim vodnim tiskom in kdo za uveljavljanje digitalnega vodnega tiska. Primeren kandidat so organizacije za registracijo avtorskih pravic, kot je na primer Urad za intelektualno lastnino, za standardizacijo in meroslovje.

## 8 Zaključek

V delu smo predstavili različne oblike in različne vloge, ki jih ima digitalni vodni tisk. Od vseh naštetih vlog je najzahtevnejše potrjevanje lastništva multimedijske vsebine. Potrjevanje lastništva zahteva robusten vodni tisk, ki se mora ohraniti pri namernih poskusih njenega odstranjevanja in ponarejanja in pri številnih operacijah, ki jih običajno izvajamo nad multimedijskimi vsebinami. Kljub mnogim predlaganim tehnikam robustnega vodnega tiska še ni povsem zadovoljive tehnike, ki bi preživela različne poskuse odstranjevanja in ponarejanja spretnih in iznajdljivih uporabnikov.

Kljub temu, da je digitalni vodni tisk sorazmeroma novo raziskovalno področje, pa je že pritegnilo v raziskave prvovrstne raziskovalce s področij računalniških znanosti, kriptografije, komunikacij in procesiranja signalov. V delu navajamo primere, kjer je bil vodni tisk že uspešno uporabljen za zaščito intelektualne lastnine. Digitalni vodni tisk je obetajoča tehnologija, ki bo odigrala pomembno

vlogo v boju proti piratstvu in zlorabi multimedijskih vsebin v informacijski dobi.

## Citirani viri

1. **Chowdhury, G.G. & Chowdhury, S.** (1999). Digital Library Research: Major Issues and Trends. *Journal of Documentation* 55(4), 409-448.
2. **Friedman, G.** (1993). The trustworthy digital camera: Restoring credibility to the photographic image. *IEEE Trans. Consum. Electron.* 39(4), 905-910.
3. **Gladney, H.M., Mintzer, F., Schiattarella, F., Bescós, J. & Treu, M.** (1998). Digital Access to Antiquities. *Communication of the ACM* 41(4), 49-57.
4. **Hawkins, D.T.** (1998). 'Digital Watermarking - Intellectual Property Protection for the Internet. *Online* 22(4), 91-93.
5. **Memon, N. & Wong, P.W.** (1998). Protecting Digital Media Content. *Communication of the ACM* 42(7), 35-43.
6. **Mintzer, F., Braudaway, G.W. & Bell, A.E.** (1998). Opportunities for Watermark Standards. *Communication of the ACM* 42(7), 57-64.
7. **Nikolaidis, N. & Pitas, I.** (1996). Copyright protection of images using robust digital signature. V *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing* (str. 2168-2171). Piscataway, N.J.: IEEE Press.
8. **Yeung, M. & Mintzer, F.** (1997). An invisible watermarking technique for image verification. V *Proceedings of IEEE ICIP'97* (str. 680-683). Piscataway, N.J.: IEEE Press.
9. **Žnidaršič, M.** (1997). DOI-DIGITAL OBJECT IDENTIFIER. Revolucija v upravljanju in trgovanju z avtorsko pravno zaščitenimi informacijami na internetu v tretjem tisočletju. *Knjižnica* 41(4), 33-39.