Др Видоје Спасић, доцент
Универзитет у Нишу, Правни факултет

UDK: 004.738:347.772

ДИГИТАЛНИ ВОДЕНИ ЖИГ (WATERMARK) У ФУНКЦИЈИ ЗАШТИТЕ ДИГИТАЛНОГ САДРЖАЈА

Апстракт:
Дигитална револуција довела је до значајних промена у области интелектуалног стваралаштва. Осим несумњивих погодности, пред интелектуалне ствараоце и носиоце права појавио се крупан проблем који треба решавати без одлагања. Реч је о томе да носиоци права интелектуалне својине имају огромне потешкоће у контроли коришћења ауторскоправно заштићеног садржаја.
Постоје различити криптографски системи који омогућавају носиоцима права контролу коришћења заштићеног садржаја од стране уживалаца. Један од значајнијих инструмената контроле представља дигитални водени жиг. У суштини, дигитални водени жиг је неупадљиви елемент који је уграђен у електронски садржај током његове производње или дистрибуције у циљу праћења и контроле његове употребе. Постоје различите врсте водених жигова које имају различите функције, при чему је најважнија заштита дигиталног садржаја.
Међутим, упркос бројним позитивним карактеристикама и функцијама, стоји чињеница да за сада не постоји систем дигиталног воденог жига који је довољно робустан и ефикасан да апсолутно задовољи све захтеве у погледу заштите од неовлашћеног искоришћавања дигиталног садржаја. У сваком случају, дигитални водени жиг представља значајан систем заштите, који у садејству са другим технолошким средствима омогућује носиоцима права контролу употребе дигиталног садржаја.

Кључне речи:
водени жиг,искоришћавање дела, контрола употребе

1. ОСТВАРИВАЊЕ ПРАВА НАД ЗАШТИЋЕНИМ ДЕЛИМА

Дигитална револуција довела је до значајних промена у области интелектуалног стваралаштва. Осим несумњивих погодности, пред ауторе и остале интелектуалне ствараоце и носиоце права појавио се крупан проблем који треба решавати без одлагања. Реч је о томе да носиоци права интелектуалне својине имају огромне потешкоће у контроли коришћења ауторскоправно заштићеног садржаја. Са тог разлога, а имајући у виду динамичан развој ауторског права у информатичком друштву, системи за остваривање права над заштићеним делима изазивају све већу пажњу свих релевантних субјеката у ауторскоправном односу. Ови системи врше функције праћења и снимања употребе дела заштићених ауторским правом, као и давање лиценци за права и означавање и приписивање стваралачких права и власничких интереса. Власници (носиоци) ауторских права имају могућност комбинованог коришћења контроле приступа на бази фајла, технологије енкрипције, дигиталног потписа и стеганографије, у циљу решавања проблема остваривања и заштите ауторског права. Овакве сигурносне мере морају се пажљиво разрадити и спровести, како би обезбедиле не само ефикасну заштиту власничких интереса аутора, већ, и да не би прекомерно отежале употребу дела од легалних уживалаца, или нарушиле њихову тајност. Такође, ове мере треба да осигурају да системи, установљени с циљем остваривања ове функције, не буду лако откривени.

Да би се спровеле наведене функције за остваривање права, релевантна информација биће обухваћена дигиталном верзијом дела (тј. информација о остваривању ауторског права), да би се уживалац ауторског дела обавестио о ауторству и власништву над делом (тј. информација о пореклу дела), као и да би се означиле дозвољене употребе дела (тј. информација о дозвољеној употреби). Практично, информација може бити у „електронској коверти (омоту)", која садржи дело и даје информације о ауторству, власништву, датуму настанка (или последње модификације) и условима за овлашћене употреба. Како се мере неопходне за ову намену уводе на нижим нивоима, оваква информација може постати интегрална компонента фајла или објекта информације. Када се оваква информација једном пове-

же са информационим објектом (тј. подацима који конституишу дело) и лако јој се приступи, уживаоци ће моћи лако да реше питања у вези с давањем дозвола и употребом дела.У складу с тим, могу се развити системи за електронско давање дозвола базирани на информацијама о пореклу и дозвољеним употребама, заједно са информационим објектом.

За остваривање права над заштићеним делима могу се користити и електронски уговори. Даваоци права могу информисати претплатнике (уживаоце дела) да ће се одређена активност (нпр. коришћење лозинке да би се добила услуга или право на коришћење дела), сматрати прихватањем одређених услова за електронско давање дозволе. Библиотека Конгресног система за електронско остваривање ауторског права, у САД-у, предложила је систем, који се састоји из трију различитих компоненти: (1) систем за регистровање и евидентирање, (2) систем дигиталне библиотеке са повезаним складиштима дела заштићених ауторским правом и (3) систем за остваривање права. Систем ће послужити као тест за стицање искуства у вези с технологијом, као и за идентификовање проблема и усвајање прототипа стандарда за каснију употребу.

2. УЛОГА ТЕХНОЛОШКИХ СРЕДСТАВА У КОНТРОЛИ ПРИСТУПА, ТРАНСФЕРА И УМНОЖАВАЊА АУТОРСКИХ ДЕЛА

С обзиром на чињеницу да нове информационе технологије врше страховит притисак, па чак и озбиљан атак на субјективна ауторска права, постало је неопходно развијање нових метода за контролу искоришћавања ауторских дела, посебно њиховог умножавања. У том смислу, непроцењиву вредност и улогу има криптографија ― стара вештина која је у новим околностима само добила нове димензије и садржаје.

2.1. Појам и улога криптографије у информатичком друштву

Етимолошки, криптографија је грчка кованица и значи писање тајним знацима ― симболима.[1] Генерално посматрано, крипто-

[1] Криптографија се спомиње још у античко доба, код Херодота и Плутарха.

графија је уметност, или наука држања података тајним. Криптограм је текст, писмо, спис сачињен тајним знацима, тј. шифрама. Криптографија је грана математике која изучава математичку заснованост криптографских метода.

Криптографија или шифровање, јесте поступак транскрипције (превођења) јасне и разумљиве информације у неразумљив облик, применом тајног договора, при чему је такво дејство реверзибилно. Француско законодавство[2] под делатношћу криптологије подразумева све радње усмерене на трансформисање јасних информација или знакова у информације, или знакове нејасне за трећа лица помоћу тајних споразума, или на реализовање обратних операција, захваљујући опреми, материјалу или компјутерском програму замишљеним са тим циљем. Реч је о једној општој дефиницији која, такође, обухвата и стеганографију ― вештину тајног писања ― која се састоји у скривању једне поруке у другој поруци, у блажој форми.

Разлози за установљавање и постојање криптографије базирани су на исконским потребама људи да шаљу одређене поруке жељеним примаоцима, а да нико други не сазна њихов садржај. Криптографија је стара вештина која је првобитно практикована у илегалним, дипломатским и војним службама. У данашњим околностима - у дигиталном окружењу, поље њене примене знатно се проширило.

Данас технике криптографије имају велики економски, стратешки и правни значај. У друштву у коме се врши перманентна размена информација, неопходно је користити сигурносне системе за заштиту података личног или поверљивог карактера. Потребно је, дакле, имати техничка средства која омогућавају ефикасну заштиту поузданости података и комуникација против неовлашћеног коришћења. Криптографске технике имају водећу и растућу улогу у заштити од информатичких превара, повреда сигурности података, заштити поузданости кореспонденције, професионалне тајне и електронске трговине. Криптографија је повезана са свим аспектима сигурног, безбедног информисања и преношења порука, аутентификације (оверавања), дигиталног потписа и електронског плаћања.

[2] Члан 28, Закона 90/ 1170, са изменама од 29. 12. 1990. године.

2.2. Типови криптографије

Генерално, постоје два велика, основна типа криптографије:

• симетрична криптографија – код које се исти кључ користи за шифровање и дешифровање информација. Проблем ове методе је како наћи средство преноса кључа на кореспонденту, на безбедан начин;

• асиметрична криптографија – код које се једним кључем скрива а другим открива порука. Корисник поседује један приватни и један јавни кључ. Он дистрибуира свој јавни кључ, а чува скривеним тајни, односно приватни кључ. Криптографија овде обезбеђује веродостојност података који се преносе путем мреже. Подаци су пренети једино уз знање овлашћених лица.

Други, или исти пар кључева користи се да би се обезбедио идентитет емитера поруке (пошиљаоца). То је поступак аутентификације (оверавања). Корисник криптује (шифрује) поруку својим приватним кључем. Сви корисници ће моћи да дешифрују поруку јавним кључем, који се подудара са пошиљаочевим. Да би се проверио интегритет послате поруке користи се математичка функција, која се везује за израчунату вредност поруке. Када прималац прими поруку, он рачуна њену вредност и упоређује је са оном вредношћу која је била послата: ако су две вредности идентичне, сигурно је да порука није била модификована у току преноса. Спој поступака аутентификације пошиљаоца и провере интегритета његове поруке омогућава стварање правих електронских потписа, које је у пракси веома тешко фалсификовати, као и поступак парафирања и потписивања руком.

Да би систем био поуздан, неопходно је да кључеви за коришћено шифровање буду довољно сигурни.[3] При коришћењу метода актуелних кодирања, сигурност кључа произилази из његове дужине. Али, што је кључ дужи, то ће трансакција или комуникација бити спорија, у смислу времена потребног да се изврши прорачун. Тако, оно што је добијено на сигурности, губи се у погледу брзине и ефикасности.

[3] Најпознатији поступак криптовања и један од најсигурнијих, који поставља стандард поступања на интернету, где га је лако прибавити, јесте програм PGP, базиран на систему RSA, који је пронашао Американац Phil Zimmerman.

Да би се дешифровао један документ, без поседовања кључа, потребно је располагати моћним компјутером, способним да изврши велики број операција у секунди. Поузданост система зависи од способности рачунара потребног за предузимање радњи за "разбијање" шифре. Да би операција имала смисла, нужно је да трошак, потребан за „разбијање" шифре, буде пропорционалан вредности заштићене информације. Да би се данас „разбио" један кључ реда величине 1024 бита, потребно је више милијарди година рачунања компјутером. Међутим, овај систем зависи и од стања технике које еволуира веома брзо. Алгоритам, који је данас замишљен као неразрешив, не значи да ће такав остати за неколико година. Чак и ако је код (шифра) неразрешив, концепција компјутерског програма може понудити фајлове, који могу бити употребљени за проналажење шифрованих порука, без гломазних рачунања.

2.3. Стеганографија

Као што је раније истакнуто, појам криптографије, у ширем смислу обухвата и стеганографију. Стално се развијају нове технике које треба да реше проблем безбедности и управљања, у вези са ширењем и употребом дигитално-кодираних информација. Тако, на пример, развијене су методе које могу кодирати информацију, са атрибутима који се не могу одвојити од фајла који садржи ту информацију. Ова област технологије названа је Встеганографијом" и концептуално се односи на „дигитално узимање отисака прстију", или дигитално узимање водених жигова.

У суштини, коришћењем стеганографских техника, лице може уградити сакривену поруку у дигитализоване визуелне или аудио податке. Уграђена информација не деградира, нити на било који други начин утиче на аудио или визуелни квалитет дела. Уместо тога, уграђена информација једино се може детектовати уколико се тражи на специфичан начин. Развијеније стеганографске технике, базиране на статистичком или ентропијски руковођеном кодирању, показале су се тешким за откривање. Тако, на пример, један систем модулира познати звучни сигнал са информацијом коју треба уградити и додаје „измерени" сигнал оригиналним подацима. На овај начин, једном кодирани стеганографски идентификациони подаци дистрибуирају се читавим делом, као веома слаба бука, која се не може

у потпуности елиминисати из дела. Стога, може се осигурати детекција уграђене поруке чак и након значајнијег нарушавања или прекидања података, што се може десити у току компресије – декомпресије – кодирања, мењања или „вађења" оригиналних података. Проналажење начина да се дело неизбрисиво повеже са одређеном информацијом, омогућава да стеганографија игра комплементарну улогу у техникама скривања значења и давања аутентичности, базираним на дигиталним потписима.

2.4. Управљање дигиталним правима (*Digital Rights Management – DRM)*

Управљање дигиталним правима (DRM) је заједнички назив за скуп технологија које власницима, односно носиоцима ауторских права омогућују контролу употребе неког дигиталног записа. Овај појам има додирних тачака са заштитом од копирања (енг. copy protection), али DRM системи се пре свега користе за заштиту креативних садржаја, као што су музика и филм, док се заштита од копирања најчешће односи на програмску подршку (енг. software). Појам e-DRM (енг. Enterprise DRM) представља заједнички назив за све технологије управљања дигиталним правима коришћеним за заштиту пословних докумената у различитим форматима, као што су Microsoft Word, PDF (енг. Portable Document Format), AutoCAD и електронска писма и web странице унутар интерне рачунарске мреже (интранет-а), неке организације.[4]

3. ДИГИТАЛНИ ВОДЕНИ ЖИГ

Дигитални водени жиг (енг. watermark) је неупадљиви елемент који је уграђен у електронски садржај током његове производње или дистрибуције у циљу праћења и контроле његове употребе. Другим речима, дигитални водени жиг представља малу, скоро неприметну промену дигиталног дела, као нпр. Слика, фотографија

[4] Сопствене DRM технологије за заштиту докумената поседују фирме: Microsoft, Adobe Systems, Liquid Machines, Oracle, EMC Corporation и друге.

или низ звукова.[5] Ова технологија користи се у различите сврхе, а најважније су:

- Означавање власника ауторских права;
- Означавање дистрибутера;
- Означавање дистрибутивног ланца и
- Идентификовање купаца.

Важно је истаћи да дигитални жигови нису потпуни DRM системи. Они не штите садржаје непосредно, већ се користе као елемент таквих система приликом прикупљања доказа у судским поступцима везаним уз управљање дигиталним правима.[6]

3.1. Примена дигиталног жига

Дигитални водени жиг има широко поље примене, али најважнија примена ове технологије је код заштите ауторских права и предмета сродних права.

Начелно, примене дигиталних водених жигова могу се класификовати на више различитих начина (зависно од медија, врсте поруке итд.). Једна од најзначајнијих класификација темељи се на отпорности воденог жига на нападе.

3.1.1. Доказивање аутентичности садржаја

Постоје различити програмски системи за уређивање дигиталног садржаја. С обзиром на то да постоје могућности за једноставно мењање дигиталног садржаја битно је наћи начин за доказивање интегритета и аутентичности садржаја. Решење овог проблема може се потражити у криптографији, где се дигитални потпис користи за доказивање аутентичности. У случају означавања дигиталним воденим жигом, дигитални потпис може бити водени жиг који ће се уградити у садржај. За доказивање аутентичности препоручује се коришћење ломљивог воденог жига. Ово из следећих разлога: ломљиви водени жиг мора постати неважећи у случају измена, а коришћењем ломљивог воденог жига може се сазнати како је дигитални садржај измењен или који је део измењен.

[5] Уколико би текстуални документ заштитили воденим жигом то би проузроковало промену битова, што би даље довело до промене слова или интерпункције, и компјутерски програм би га пријавио као грешку.

[6] Тако, на пример, дигиталним воденим жиговима означене су iTunes песме чије копирање није онемогућено.

3.1.2. Праћење емитовања

Мноштво различитог садржаја (заштићеног путем интелектуалне својине) свакодневно се емитује преко многобројних телевизијских канала: вести, филмови, спортски догађаји, рекламе, итд. Емитовање је врло скупо и оглашивачи морају издвајати значајна финансијска средства за свако емитовање кратких реклама које се емитују за време пауза популарних филмова, серија или спортских догађаја. Могућност прецизне наплате емитованог садржаја, такође, је врло битна. Оглашивачи желе бити сигурни да плаћају само за рекламе које су се емитовале, па зато желе контролу емитованог садржаја.

Праћење емитовања (*Broadcast Monitoring*) обично се користи за прикупљање информације о садржају који се емитује. Прикупљене информације користе се за наплаћивање, али и за друге потребе. Најједноставнији начин праћења је коришћење људских посматрача који врше мониторинг емитованог садржаја. Ова врста праћења је скупа и склона грешкама. Аутоматизовано праћење је очито бољи избор. Постоје две врсте система за аутоматизовано праћење: пасивни и активни. Пасивни систем "прати" садржај који се емитује и покушава га повезати с познатим садржајем чуваним у бази. Имплементација пасивних система није једноставна из неколико разлога. Упоређивање одасланих сигнала са садржајем базе није једноставно. Одржавање велике базе садржаја за упоређивање је скупо. Активни системи за праћење ослањају се на додатну информацију која идентификује садржај. Додатна информација емитује се заједно са садржајем. Једно од решења за активно праћење је и означавање дигиталним воденим жигом. Водени жиг који садржи информацију за идентификацију емитовања уграђује се у сам садржај. За ову примену водени жигови морају бити отпорнији на нападе од ломљивих жигова и морају бити лако читљиви.

3.1.3. Остављање отисака

Постоје одређене примене воденог жига у којима додатна информација о дигиталном садржају треба да садржи информације о уживаоцу дела а не о власнику садржаја. Таква ситуација је, нпр. у окружењу у којме се стварају филмска дела. За време продукције филма, мањи делови рада на филму обично се сваки дан дистрибуи-

рају одређеном броју људи укљученом у стварање филма. Ти дневни делови филмова су поверљиви, па ако одређена верзија „процури", филмски студио жели имати могућност идентификовања узрочника цурења информација. Проблем идентификовања извора „цурења" информација може се решити дистрибуирањем незнатно различитих копија сваком примаоцу. Свака копија јединствено је везана уз лице коме је као примаоцу намењена.

Други пример примене је дистрибуција филмова у дигиталном формату биоскопима, уместо коришћења поштанских услуга и целулоидних трака. Иако је оваква дистрибуција флексибилнија, ефикаснија и јефтинија, продуценти и дистрибутери је слабо прихватају, јер се боје потенцијалног новчаног губитка узрокованог илегалним копирањем и редистрибуцијом филмова. Решење овог проблема је да сваки биоскоп прими копију која се јединствено веже уз биоскоп. У случају појаве илегалних копија, може се сазнати који је биоскоп одговоран и предузети потребне правне мере против истог.

Повезивање јединствене информације о свакој дистрибуираној копији дигиталног садржаја зове се остављање отисака (енг. *Fingerprinting*). Означавање воденим жиговима је адекватно решење за ову примену јер је невидљиво и недељиво од садржаја. Овај тип примене познат је и под именом "праћење издајица" (енг. *traitor tracing*). Користан је код праћења илегално произведених копија дигиталног садржаја. Ова примена захтева висок ниво отпорности воденог жига од различитих врста обраде података и неовлашћених и злонамерних напада.

3.1.4. Заштита ауторских права

Заштита ауторских права представља једно од примарних подручја за која је означавање дигиталним воденим жигом намењено. Водени жиг, у овом случају, садржи информацију о власнику ауторског права и неприметно се уграђује у за то намењени садржај. Ако уживаоци дигиталног садржаја имају лак приступ детекторима воденог жига, могу препознати и интерпретирати уграђени водени жиг и идентификовати власника ауторског права.

Било би корисно када би се уграђени водени жиг могао користити и као доказ власништва. Може се замислити следећа ситуаци-

ја: Власник ауторског права дистрибуира свој дигитални садржај с уграђеним сопственим невидљивим воденим жигом. У случају спора око власништва ауторског права, легални власник требало би да има могућност да докаже своје власништво. То се остварује на тај начин што стварни власник предочи оригинални документ и детектор воденог жига. Спорни садржај је оригинални документ у који је уграђен водени жиг. Детекцијом воденог жига власника у спорном документу доказује се власништво над документом. Нажалост, горњи сценарио уз одређене претпоставке може бити побијен, а и означавање воденим жигом још није довољно поуздано за доказивање власништва. Уз то, један потенцијални проблем повезан је с доступношћу детектора воденог жига. Ако је детектор доступан већем броју људи не може се очувати сигурност воденог жига. У том случају, увек је могуће детектовати и уклонити водени жиг. То се може остварити већим бројем неприметних измена на означеном садржају све док детектор више не може детектовати водени жиг. Уколико је водени жиг једном уклоњен, оригинални власник не може више доказати своје својство. Чак и ако се водени жиг не уклони, у неким условима могуће је додати нови водени жиг преко постојећег и то за све копије документа, укључујући оригинални документ. Због тога је потребно да се може идентификовати први водени жиг који је стварни власник уградио. Зато је за ову примену потребан највиши ниво отпорности воденог жига.

Све веће коришћење дигиталних медија за слике и видео секвенце има озбиљне реперкусије на заштиту ауторских права. Раније је било тешко неовлашћено копирати слике без приступа негативима, док су скенери били скупи и недовољно присутни. Када је слика већ у дигиталном окружењу, релативно јефтин и високо квалитетан софтвер може се користити при манипулацији сликама на начине који су били незамисливи пре само пар година. Видео је нешто теже копирати, због великог простора који заузима на диску.

Цена која се плаћа присуству глобалном аудиторијуму преко интернета огледа се у недостатку контроле над садржајем. Тако, на пример, ако веб сајт садржи неку фотографију, свако ко приступи сајту може помоћу свог браузера да сачува ту фотографију на диску, а исто то важи и за видео клипове. Слике и видео могу се затим користити без дозволе аутора. Треба подвући, да и прелазак са аналог-

ног на дигитални аудио сигнал такође има импликацију на неауторизовану дистрибуцију преко интернета.

Кључна идеја заштите је да се отисне информација у слику или видео која омогућује власнику ауторских права или кориснику који има то право, да буде идентификован. Та информација назива се вотермаркинг или водени жиг. Један од најстаријих вотермаркинга била је IBM шема за ватиканску библиотеку. Присуство вотермаркинга било је видљиво, али га је било немогуће уклонити без деградације слике. Међутим, сада се примењује невидљиви водени жиг, при чему слика не сме да буде деградирана његовим присуством. Знак треба да буде читљив кроз неку форму поређења са оригиналном сликом. Водени жиг треба да буде отпоран на детекцију и декодирање без приступа оригиналу, као и да при покушају његовог уништења проузрокује знатан губитак квалитета слике. Уз то, потребна је и толеранција релативно разумног губитка квалитета при компресији.

Механизам који се користи код обраде слике и видеа не сме да уништи водени жиг, што у себи укључује компресију са губицима, грешку при преносу, скалирање, ротацију, штампање, скенирање, аналогно-дигиталну и дигитално-аналогну конверзију. Осим тога, пожељно је да знак буде невидљив. Пример коришћења дигиталног жига срећемо код видео дистрибуције. Видео из извора сигнала најпре добија водени жиг, пре него што се меморише у видео бази података. Сврха воденог жига је да се на јединствен начин идентификује власник садржаја-материјала. Када корисник буде захтевао копију видео секвенце, додаје се други водени жиг који идентификује тог корисника. Систем треба тако да се пројектује да други водени жиг не оштети први. У случају да се појави илегална копија, техничка структура омогућава да и власник ауторских права и корисник могу идентификовати исту.

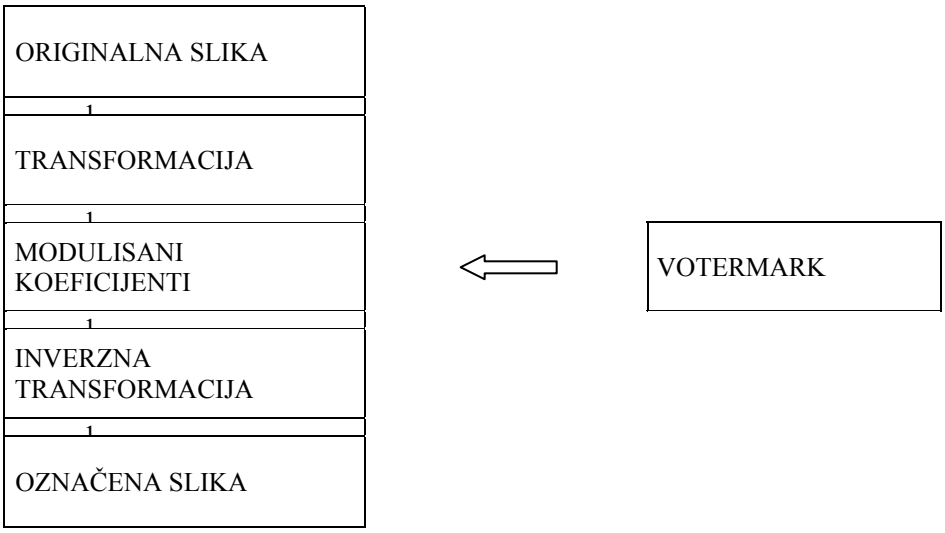
У последње време доста пажње посвећује се преласку из аналогне у дигиталну видео технологију, из разлога сигурности података.

Систем воденог жига може бити фрагилан и робустан, комплетан и некомплетан, видљив и невидљив. Већина система има додатну информацију помоћу које знак може да се реконструише, и та информација се зове тајни кључ. Кључ може бити псеудослучајна

секвенца шума, криптографски кључ, компоненте различитих просторних фреквенција и томе слично.

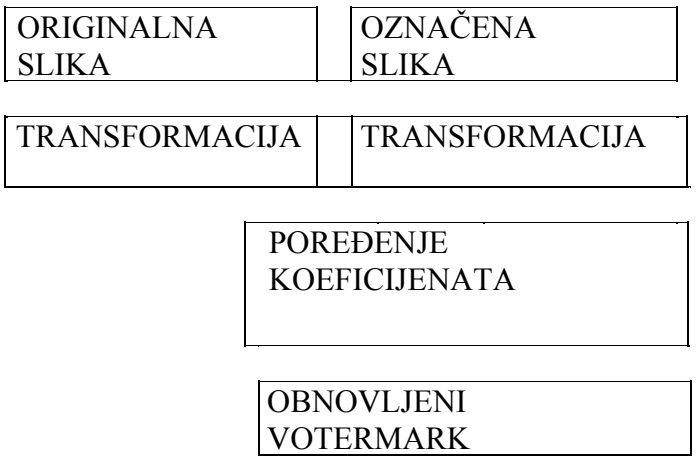
3.2. Техника дигиталног воденог жига

Технички посматрано дигитални водени жиг се креира на следећи начин. Оригинална слика се обично подвргава некој врсти трансформације, као што су дискретна косинусна (DCT), дискретна Фуријеова (DFT), или вејвлет трансформација. Затим се коефицијенти у трансформационом домену да би прихватили вотермаркинг информацију. Инверзна трансформација се онда примени да би се генерисала означена верзија оригинала која садржи водени жиг, и тиме је спремна за даљу дистрибуцију, што је показано на слици 1.



Слика 1. *Утискивање воденог жига*

Да би се водени жиг обновио, и оригинална и означена слика се трансформишу, што омогућава поређење модулисаних коефицијената, а то је приказано на слици 2.



Слика 2. *Обнављање воденог жига*

Постоје и системи за водени жиг који директно обрађују оригиналну слику, а да је претходно не трансформишу. Они обично користе секвенцу псеудослучајног шума, која може да се модификује преко вотермарк информације, на сличан начин као код технике проширеног спектра. Било који такав систем мора пажљиво да контролише спектар утиснуте вотермаркинг информације.

Повећано интересовање за технике засноване на објекту довело је до нових шема које користе особине воденог жига у односу на објекте, као и на водене жигове који сами представљају објекте. Један од таквих примера је утискивање воденог жига у параметре анимације MPEG-а представљања лица.

Неке шеме користе принцип поделе оригиналне слике на блокове, модификујући при томе коефицијенте трансформационе домене и формирајући означену слику. Разлог за то делом лежи у директној компатибилности са техникама компресије са губицима, као што је то MPEG стандард. Ово нам сугерише да је могућа уградња у кодере са компресијом са губицима без превише прекорачења.

Код дигиталног воденог жига постоји неколико тајних кључева који се користе у овом процесу. Један је прецизан низ коефицијената који се користе за утискивање жига. Други начин је релација која постоји између коефицијената, а трећи може бити релација између блокова у слици. Дигитални водени жиг је веома повезан са

криптографијом, при чему се криптографске технике конфузије и дифузије користе у овом случају.

Осим наведеног, код воденог жига користи се и техника проширеног спектра. Основна идеја је да се целокупна слика трансформише као један блок, нпр. користећи DCT над блоком коефицијената величине 512 x 512. Код процеса утискивања воденог жига, неки случајни број се придружује сваком коефицијенту у трансформационом домену резултујући низ коефицијената у трансформационом домену се затим инверзно трансформише да би се добила означена слика. Модификација коефицијената резултира тиме што се информација о воденом жигу шири кроз целу слику, чинећи тиме систем релативно отпорним на нападе. Издвајање воденог жига чини се упоређењем вредности добијеним из низа случајних бројева из означене слике са оним које су оригинално утиснуте.

Будући да телевизијска техника све више постаје дигитална, компримован дигитални видео све више постаје реалност. Пошто се видео декомпримује само онда када је неопходно да га уживалац види, то постоји потреба за дигиталним воденим жигомом. Рецимо, видео који се продаје кориснику може да има водени жиг са бројем који идентификује само тај уживалац. Уколико се пронађу пиратске копије, водени жиг се користи да би се идентификовао оригинални извор пиратског материјала. При томе, питање како најбоље придружити вотермарк компримованом видео сигналу, остаје отворено.

Исто тако, могуће је декомпримовати видео, придружити водени жиг и поново га рекомпримовати. Међутим, у вези с имплементациом овог процеса постоји неколико проблема које треба разрешити.[7]

[7] Један проблем је екстра кашњење које уноси процес, које може бити неприхватљиво. Други проблем је што укупни битски проток може бити повећан, јер вотермарк обично резултира лошијом компресијом. Додатни проблем је повећана цена и сложеност. Могуће разрешење проблема јесте да се процес изводи директно на MPEG битском протоку, што смањује могућност смештања вотермарка, јер није могуће користити више бита него што их је присутно.

3.3. Врсте дигиталних водених жигова

Постоје различите врсте водених жигова. Са аспекта теме овога рада најзначајнија је подела на ломљиве и отпорне водене жигове.

3.3.1. Ломљиви водени жигови

Ови жигови зову се ломљиви јер је пожељно да се приликом примене већине техника обраде докумената измене или униште. Ломљиви жигови имају следећа својства:

- Водени жиг је невидљив посматрачу;
- Водени жиг се мења приликом примене већина техника за обраду докумената;
- Неовлашћена лица не би смела моћи убацити лажни водени жиг;
- Овлашћена лица могу брзо извадити водени жиг;
- Очитани водени жиг показује где је дошло до промена.

3.3.2. Отпорни водени жигови

Ови жигови зову се отпорни јер се очекује да буду постојани независно од напада. Њихова главна својства су следећа:

- Водени жиг је невидљив посматрачу;
- Водени жиг остаје у документу чак и након обраде документа;
- Неовлашћена лица тешко могу детектовати водени жиг;
- Овлашћена лица могу брзо извадити водени жиг;
- Након што је документ исписан и скениран и даље је могуће учитати водени жиг.

3.4. Алгоритми за означавање текста

Велики број субјеката често има потребу за заштитом осетљивих докумената. Коришћењем дигиталног воденог жига могуће је уградити отисак у жељени документ. Отисак може бити јединствени идентификацијски број власника или примаоца документа. Уграђени идентификацијски број треба да буде такав да се може детектовати и декодирати у било којем тренутку, чак и након исписа и скенирања.

Технике за означавање слика могу се лако применити на текстуални документ, али оне у текстуални документ уносе били шум који се јако примећује. Тај шум настаје због бинарне (црно-беле) природе текстуалног документа и велике беле позадине. Како би се избегао претходно споменути проблем, развијено је неколико техника означавања воденог жига, посебно за текстуалне документе.

Постоје четири врсте техника за означавање текста: помицање линија текста (енг. *line-shift coding*), помицање речи унутар исте линије (енг. w*ord-shift coding*), означавање карактеристика текста (енг. *feature coding*) и језично означавање (енг. *natural language NL*).

Код помицања линија текста свака парна линија незнатно се помиче горе или доле, зависно од вредности информације која се уграђује. Ако је бит један одговарајућа линија помиче се горе, иначе се линија помиче доле. Непарне линије су контролне линије и оне се не мењају. Користе се као референце за мерења и упоређивање размака између линија за време декодирања. Декодирање се остварује упоређивањем размака између база линија или размака између центроида линија. Базе линија у оригиналном документу су обично униформно распоређене, дакле оригиналан документ није потребан ако се базне линије користе. Али, центроиди нису нужно униформно распоређени па је потребан оригинални документ код метода које користе центроиде.

Код друге методе помицања речи, прво се свака линија дели у групе речи. Свака група има довољан број знакова. Затим се свака парна група помиче у лево или десно, зависно од вредности специфичног бита информације који се уграђује. Непарне групе користе се као референце за мерење и упоређивање размака између речи за време декодирања. Метода корелације и метода центроида користе се за детекцију воденог жига и обе методе захтевају оригинални текст.

Трећи метод односи се на мењање одређених карактеристика текста (боје, фонта, величине, итд.).

Код четвртог метода, језичко означавање, уграђивање изводи се мењањем синтаксе или семантике одабраних реченица.

3.5. Метод уградње робусног дигиталног воденог жига у слику

Метод уградње дигиталног воденог жига (DWM = *digital watermark*) је, уз стеганографију једна од најпознатијих примена скривања информација (*information hiding*). Убацивање жига је поступак уметања одређене тајне информације (жига) у оригинални документ. Тајна информација може бити нека мања слика, текстуална порука, потпис, или пак низ псеудослучајних бројева. Тајна порука се може заштити кључем тако да јој само познаваоци кључа могу приступити. Оваква комбинација двеју информација у слици могућа је јер људски визуелни сиситем приликом обраде слике одбацује одређене делове информације. У основи, водени жигови искоришћавају редундантне податаке у документу сакривајући тајне информације унутар њих.

Познавање својстава људског визуелног система кључно је за дизајнирање робусног воденог жига. Познато је да су ниске просторне фреквенције слике боље видљиве него више фреквенције, па се додатне информације покушавају ставити у подручје виших фреквенција. Зависно од примене, DWM мора задовољити следеће особине:

- Да је неуништив од стране хакера;
- Да је перцептуално невидљив;
- Да се статистички не може детектовати;
- Да је отпоран на компресију слике;
- Да је отпоран на различите манипулације над сигналом.

У зависности од особина, DWM-ови се деле на видљиве и невидљиве, робусне и ломљиве, јавне и приватне итд. Примену DWM-а можемо посматрати кроз четири процеса: убацивање жига, дистрибуција означеног документа, екстрактовање жига из означеног документа, одлука о ваљаности жига.

Алгоритам уградње DWM-а у слику представљен овим радом дизајниран је да задовољи следеће критеријуме:

- Отпорност на кроповање;
- Отпорност на модификацију контраста и осветљености;
- Отпорност на филтрирање;
- Отпорност на JPEG компресију са губицима.

Све наведене карактеристике су значајна, али посебна пажња посвећена је последњем захтеву. Људско око је осетљивије на шум и друге артефакте у ниским него у високим фреквенцијама. Како год, енергија већине природних слика је концентрисана у областима ниских фреквенција. Информације скривене у високим фреквенцијама могу бити лако изгубљене након квантизационих операција као што су оне при JPEG компресији са губицима. Како уградња DWM -а не би направила уочљиве промене на слици и како би информације о DWM-у у оригиналној слици „преживеле“ компресију, логично решење је да се DWM уграђује у средње фреквенције оригиналне слике.

Основна идеја приликом израде овог алгоритма била је у томе да се искористе оригиналне слике у нивоу сивог (*grayscale images*) димензија 256×256 пиксела, у које се уграђује DWM у бинарном патерну (црно-бели) димензија 128×128 пиксела. Принцип алгоритма је такав да је потребно увек имати слику која је по димензијама дупло већа од DWM -а који се уграђује. Дакле, у алгоритам је могуће уградити watermарк произвољних димензија, али то имплицира да димензије слике буду дупло веће од димензија DWM -а.

4. ИЗАЗОВИ И ДИЛЕМЕ

У ери дигиталне технологије сва средства или механизми су добро дошли у функкцији заштите интелектуалног садржаја. Упркос постојању бројних технолошких могућности, треба истаћи да не постоји универзалан и савршен механизам или систем који би пружао ефикасну заштиту од неовлашћеног или злонамернорног коришћења заштићеног садржаја. Стога, нужна је комбинована, односно кумулативна примена различитих система и механизама, како би се постигли задовољавајући ефекти и остварили жељени циљеви заштите.

Дигитални водени жиг представља значајан инструмент контроле коришћења и заштите различитог садржаја у сајберспејсу. Међутим, упркос бројним позитивним карактеристикама и функцијама, стоји чињеница да за сада не постоји систем дигиталног воденог жига који је довољно робустан и ефикасан да апсолутно задовољи захтеве за заштиту од неовлашћеног искоришћавања дигиталног садржаја. Ово, пре свега, зато што не постоји ни довољно сигурна криптографска техника. Чини се да је кључни проблем код воденог жига

што у већини случајева нападач није заинтересован за садржину информације коју жиг штити: он једноставно жели да га уништи, што је знатно једноставније.

Сваки систем воденог жига има низ података који треба да буду прикривени и негде меморисани (као што су нпр. тајни кључеви, генератор псеудослучајних секвенци, итд.), што у случају видео сигнала може захтевати велики меморијски простор.

Задатак потенцијалних нападача воденог жига утолико је тежи ако он нема приступ софтверу за издвајање воденог жига, да би проверио ефикасност атака. Са друге стране, корисно је да се омогући корисницима да верификују информацију о воденом жигу. Релативну потешкоћу представља и потреба доказивања власништва на адекватан начин, ако је присутно више водених жигова. Један од начина је да се то реши је да се укључи печат у водени жиг. Међутим, при нападу је релативно лако наћи печат и касније га користити при другом атаку. Другим речима, неопходно је остварити везу између означеног печата и слике којој је он придружен.

Централно питање које се поставља код воденог жига, јесте да ли је он довољно безбедан за примену у реалном свету. Одговор зависи од апликације. Комбинација криптографије са техником дигиталног воденог жига обично се користи за аутентичност и интегритет безбедног видео преноса. Дигитални водени жиг који се употребљава при заштити од неовлашћеног копирања треба да буде неоштећен приликом обнављања, како слика или видео који га садрже, да би након тога био употребљив. Имплементирање система са саморегистрацијом представља још једну мету за малициозне атаке. Ефикасни системи морају да имају добар менаџмент воденог жига. Добро је познато да се успешни напади на криптографске системе не заснивају на криптоанализи, већ, управо, на лошем менаџменту заштите. У случају заштите ауторских права, сваки објекат треба да има низ кључева за јединствен водени жиг, што може имати компликован менаџмент за ову веома важну примену. У сваком случају, дигитални водени жиг у комбинацији са другим технолошким средствима представља значајан инструмент контроле коришћења заштићеног садржаја.

Doc. Vidoje Spasic LL.D.
Assistant Professor
Law Faculty, University of Niš

DIGITAL WATERMARKING IN A FUNCTION OF DIGITAL CONTENT'S PROTECTION

Summary

Digital revolution has lead to the significant changes in the area of intellectual creativity. Except some undoubtable advantages, intellectual creators and holders of right have to face to enormous problems that should be resolved without delaying. In addition, the holders of the intellectuall property have huge difficulties in controlling of using the copyrighted content.

There have been different systems of cryptography which enable the holders of the right to control the using of protected content by the simple users. One of the relevant parts of control is actually digital watermark. In essence, digital watermark is unnoticeable element that is constructed into electronic device during its production or distribution in a purpose of following and controlling its use. There have been various species of watermarks that have multiple functions, but the most relevant one is the protection of digital content.

However, despite numerous positive features and functions, there is a fact that the system of diigital watermark, which is effective and robust enough to accomplish all demands in sense of protection of unauthorized usage of digital content, hasn't been discovered yet. To sum up, digital watrmark is a significant system of protection, which enables the holders of the right to control the usage of the digital content togehter with other technological means.

Keywords: *watermark, usage of work, control of the usage*