

**ТЕХНОЛОГИЈЕ ВОДЕНОГ ЖИГА
WATERMARK TECHNOLOGIES**

Жељко Гаврић, Вања Мишковић, Душан Старчевић

РЕЗИМЕ: Обзиром на развој и количину мултимедијалних датотека на Интернету јавила се потреба да се ови подаци на неки начин заштите. Једна од метода заштите је управо додавање воденог жига на мултимедијалне податке. Овај рад описује врсте водених жигова, начин њихове имплементације као и потенцијалне пријетње које могу оштетити водени жиг. У раду је приказано неколико практичних пријемјера уметања воденог жига у фреквенцијском домену. Примјери су рађени у програмском пакету Матлаб.

КЉУЧНЕ РЕЧИ: Мултимедији, мултимедијалнекомуникације, водени жиг.

ABSTRACT: Considering a fast development and a huge amount of multimedia contents on the Internet, there is a need to improve security of these data. One of the most important security methods is the digital watermarking technology that allows embedding of a watermark in the multimedia files and extraction of it without affecting the perceptual quality of the multimedia files. This paper describes types of watermarking techniques, the way of their implementation as well as their robustness to different type of attacks. In this paper, we present practical examples of the image watermarking in a frequency domain. Our examples are written and illustrated in the software package Matlab.

KEY WORDS: Multimedia, multimedia communications, watermark.

1. УВОД

Нови облик пословања заснован на дигиталним производима, као што су дигиталне фотографије, видео записи, аудио записи – музика, књиге или други облици дигиталних докумената, омогућен је развојем Интернета. Овакав облик пословања представља, без преседана, велике могућности за промовисање и зараду креатора садржаја и велике користи за крајње кориснике садржаја. Digital Watermarking Allinase наводи да је највећи проблем нових модела е-пословања то што је садржај постављен на Интернет без поузданих механизма који омогућују утврђивање власништва над садржајем, контролу коришћења садржаја и поштовање лиценци. Због тога садржај губи на својој вриједности и корисности, а власници ауторских права губе зараду [1]. Поред наведени сигурносних проблема потребно је обезбиједити заштиту од неауторизованог читања садржаја. Једна од метода оваквог типа заштите приказана је у [2].

Дигитални водени жиг може бити уграђен и прочитан из различитих мултимедијалних садржаја како би омогућио идентификовање поријекла и власништва над садржајем или како би се спријечиле или омогућиле одговарајуће активности корисника над садржајем, нпр. копирање. Дигитални водени жигови су елементи дигиталних података тако што су уграђени у стварни садржај дигиталних података, а не уметнути у њихова заглавља, тако да могу преживјети аналогне конверзије и промјене типова датотека / медијских формата [3]. Термин Дигитални Водени Жиг (*енг. Digital Watermark*) први пут је кориштен 1992. године, а 1993. први алгоритам дигиталног воденог жига у свом раду објавио је аутор кованице А. Z. Tirkel et al. [4]. Сваки алгоритам за имплементацију треба имати сљедећа својства:

1. Транспарентност

Обично дигитални водени жиг не би требао бити видљив људском оку, али треба бити читљив од стране рачунара. Постоје и видљиви дигитални водени жигови и користе се код фотографија/мирних слика или видео записа. Видљиви дигитални водени жигови деградирају квалитет слике и нису погодни за детекције помоћу рачунара.

2. Отпорност

Робусним дигиталним воденим жигом сматра се дигитални водени жиг непримјетно уграђен у дигиталне податке – домаћина, а није га могуће елиминисати без примјетног деградирања садржаја домаћина. Водени жиг мора бити довољно отпоран да се одупре било каквим операцијама обраде сигнала, нападима и неауторизованом приступу.

3. Капацитет

Описује количину података која треба бити уметнута у неки садржај као водени жиг за успјешну детекцију приликом извлачења воденог жига.

4. Сигурност

Само овлаштене особе имају могућност промјене садржаја означеног воденим жигом. За спречавање неовлаштеног приступа садржају уобичајена је примјена неког облика шифровања воденог жига.

5. Једноставност уметања и извлачења жига

Вријеме потребно за извођење одређених рачунских операција мора бити минимално, како би се жиг могао користити и у случају апликација са радом у реалном времену.

6. Утицај на пропусни опсег

У случају да водени жиг постане терет за доступну пропусност мреже, метода имплементације се одбацује.

7. Интероперабилност

Садржај означен дигиталним воденим жигом мора бити интероперабилан, на начин да се може приказати или извести на различитим уређајима и мрежним окружењима.

Алгоритам за уметање дигиталног воденог жига се састоји из три дијела: водени жиг, кодер, декодер и компаратор – алгоритам за екстракцију воденог жига и компарацију. На Сл. 1. се може видјети поједностављена шема описаног алгоритма. Убацавање воденог жига је поступак уметања одређене тајне поруке у оригинални документ. Тајна информација може бити нека мања слика, текстуална порука или пак низ псеудо-случајних бројева. Тајна информација се може заштити кључем тако да јој само познаваоци кључа могу приступити. Након означавања документа слиједи његов транспорт - најчешће преко Интернета. При транспорту означени документ проживљава низ промјена. У случају слике промјене могу бити компресија слике, промјена величине слике, промјена контраста или освјетљења. Свака од ових манипулација документом може се сматрати као напад на водени жиг. Такође, могуће су и геометријске манипулације сликом попут промјене величине, ротације или одсијецања дијелова слике.

У процесу екстракције жига потребно је моћи издвојити водени жиг из документа који је дожио низ трансформација. Ако је приликом екстракције жига познат оригинални документ или ако је познат кључ, тада је поступак екстракције једноставан. Постоје и системи водених жигова у којима за екстракцију жига није потребан оригиналан документ. У таквим системима се подаци о уметнутом жигу добијају на основу података и својстава самог

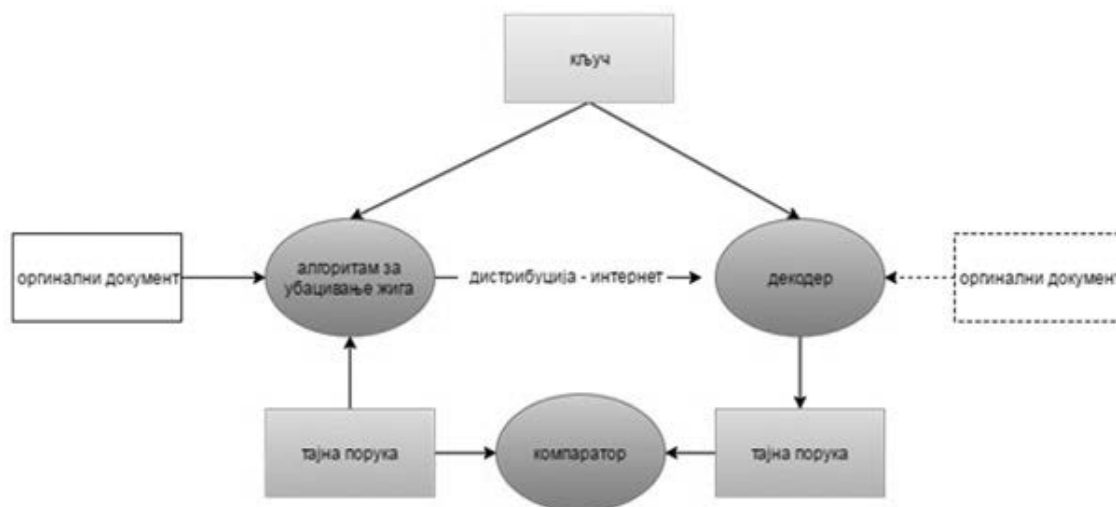
документа. Након екстракције жига из означене слике потребно је извршити анализу тих података и потврдити да ли је жиг пронађен у документу или не. Добијене податке из означене слике потребно је упоредити с оригиналним жигом. Резултат поређења је мјера сличности са оригиналним воденим жигом. Ако мјера покаже да је одступање између екстракцијом добијеног жига и оригиналног жига мање од задатог прага, тада се тврди да је документ заштићен воденим жигом.

2. ПОДЈЕЛА ВОДЕНИХ ЖИГОВА

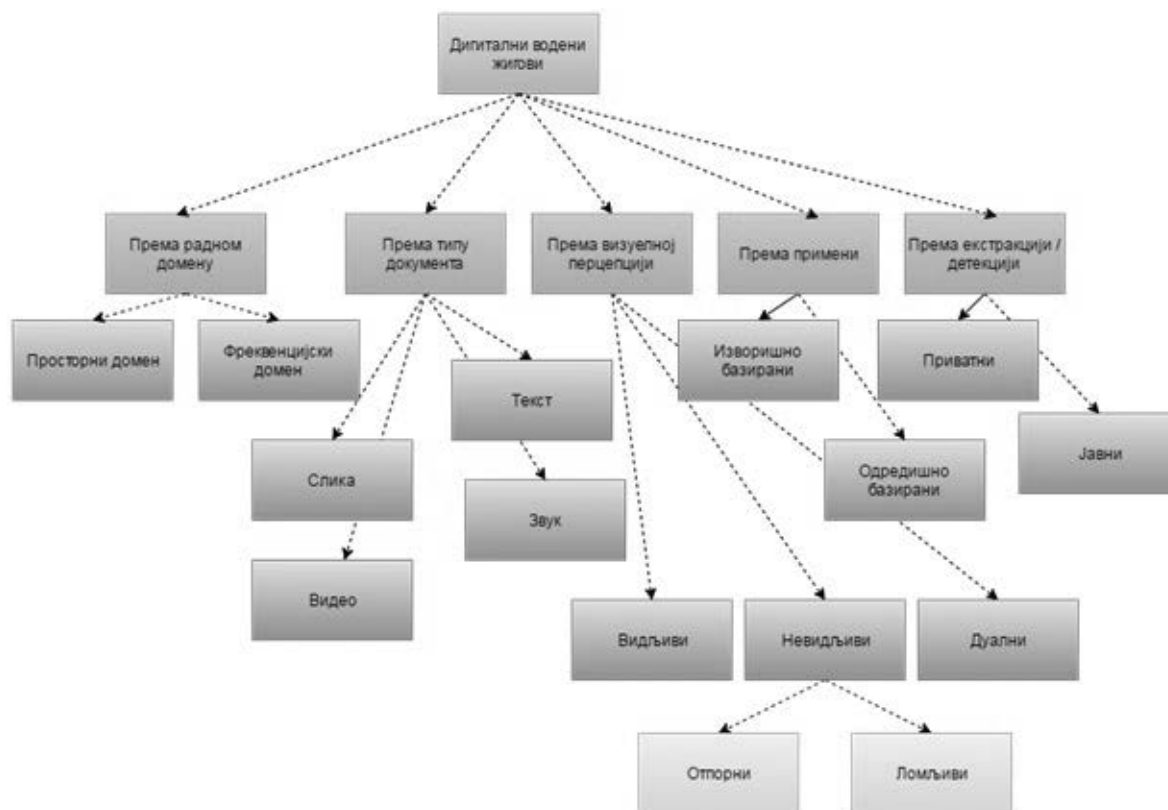
Поред класификације водених жигова према визуелној перцепцији, постоје и следеће подјеле: према отпорности (робусности), према радној домени (просторна и фреквенцијска), према примјени, према типу документа и према начину екстракције / детекције воденог жига [5].

Технике водених жигова могу се подијелити према типовима докумената у четири групе: означавање слике, означавање видеа, означавање звука и означавање текста. Из саме подјеле може се закључити намјена поједине врсте водених жигова.

Жигови се могу уносити у просторном домену (енг. Spatial Domain) или у фреквенцијском домену (енг. Frequency Domain). Фреквенцијски домен уметања жига има предности над просторним доменом јер је робуснији, тј. отпорнији на нападе. Промјеном једног параметра у фреквенцијском домену, мијења се садржај цијелог документа. Код просторног домена промјена се очитује у само једном сегменту. Ако се тај сегмент „изреже“, код просторног домена жиг је уништен, а код фреквенцијског жиг је постојан и детектује се из преосталог дијела документа. На Сл. 2 приказана је детаљна подјела дигиталних водених жигова у хијерахији стабла.



Слика 1 – Алгоритам за имплементацију воденог жига



Слика 2 – Подјела дигиталних водених жигова у хијерархији стабла

3. ВРСТЕ НАПАДА НА ДИГИТАЛНЕ ВОДЕНЕ ЖИГОВЕ

Прије свега треба разликовати двије врсте или сврхе напада на водени жиг: непријатељски или злонамјерни, којима је циљ ослабити, избрисати, уништити или промијенити водени жиг; и случајни до којих може доћи приликом стандардне обраде слике. Случајни немају за циљ промијенити водени жиг.

Компресија с губицима се сматра једним од најчешћих напада којем се водени жиг мора одупријети. Термин напад (говорећи о компресији) може се оправдати чињеницом да је циљ компресије пригушивање или одбацивање перцепцијски небитне информације унутар слике (између осталог и воденог жига).

Могући напади на водени жиг могу се подијелити у следеће 4 категорије [6]:

- Напади уклањања и ометања (интерференције) воденог жига,
- Геометријски напади,
- Криптографски напади,
- Протоколарни напади.

Напади уклањања покушавају одвојити и уклонити водени жиг из заштићеног садржаја. Најчешћи начин уклањања је употреба модела филтрирања. Уклањање шума помоћу високопропусних или медијан филтара, нелинеарна скраћивања и просторна предвиђања дигиталног воде-

ног жига сматрају се прилично успјешним методама уклањања жига. Код ометања је циљ додати дисторзију на слику, на начин да водени жиг постане немогуће прочитати. Напад се сматра успјешним ако се водени жиг више не може детектовати, а слика је и даље искористива за жељену намјену.

Геометријски напади нису усмјерени на уклањање воденог жига, већ на његово уништавање или онемогућавање његове детекције. Покушавају уништити детекцију корелације оригиналног и извученог воденог жига помоћу транслације, ротације, те скалирањем означене слике. То је могуће постићи мијешањем пиксела у слици. Њихове вриједности остају исте, међутим мијења се њихова позиција унутар саме слике. Ови напади се могу додатно подијелити на оне које користе афине трансформације и оне које користе пројекцијске трансформације [7].

Криптографски напади циљају на пробијање сигурносних метода кориштених у имплементацији дигиталног воденог жига чиме траже начин уклањања воденог жига или уметања лажног на његово мјесто. Једна таква техника је brute-force претраживање за уметнутом тајном информацијом. У пракси, коришћење оваквих напада је врло ограничено због високе комплексности њиховог извођења. Покривају директне нападе на тражење тајног кључа. Криптографски напади на дигитални водени жиг врло су слични онима који се користе у подручју криптографије. То су, на примјер, претходно споменути brute-force напади с циљем проналаaska тајног кључа. Како

многе имплементације дигиталног воденог жига користе тајни кључ, пожељно је да он буде задовољавајуће дужине за довољну сигурност. Још један од напада у овој категорији је тзв. Ogaclе напад који се може искористити за стварање неозначене слике када нападач има приступ уређају за детекцију дигиталног воденог жига [8].

Протоколарним нападима циљ није уклањање утиснуте информације, као ни њено уништавање, нити онемогућавање детекције. Напротив, ови напади искориштавају семантичке недостатке у имплементацији дигиталног воденог жига. Циљају на схватање концепта имплементације дигиталног воденог жига. Први протоколарни напад имао је задатак приказати да за коришћење дигиталног воденог жига за заштиту ауторских права он мора бити неинверзибилан. За ту намјену се уз водени жиг користе неинверзибилне хеш функције и технологија дигиталног потписа. Идеја инверзије воденог жига састоји се од чињенице да нападач посједује заштићени материјал и може тврдити да тај материјал садржи и његов дигитални водени жиг. Један примјер таквог напада је ИВМ напад [9]. Овај напад уграђује један или неколико додатних водених жигова, таквих да није јасно који водени жиг припада првобитном власнику. Водени жиг неког већ означеног документа се зове поновно утискивање воденог жига. Међутим дигитални потпис гарантује једнозначно идентификовање оригиналног власника и његовог воденог жига.

4. ТЕХНИКЕ ИМПЛЕМЕНТАЦИЈЕ ДИГИТАЛНОГ ВОДЕНОГ ЖИГА

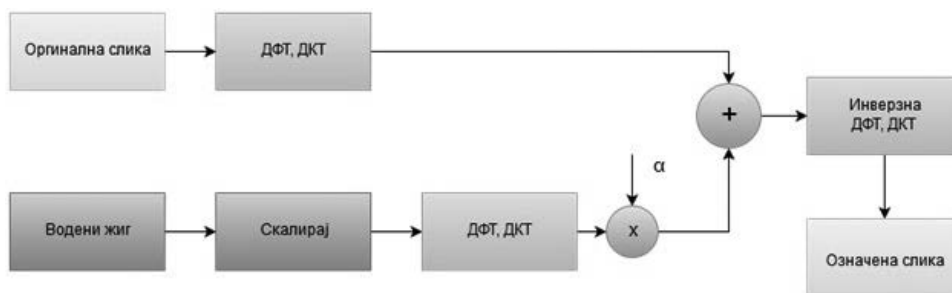
По домену рада дигитални водени жигови се дијеле на двије групе: просторни и фреквенцијски домен рада.

Уметање воденог жига у просторном домену може се извести кориштењем раздвајања хроминантних компоненти слике. На тај начин, дигитални водени жиг појављује се само у једном хроминантном појасу слике. Дигитални водени жиг је тешко видљив под нормалним условима посматрања коришћењем ових техника. Међутим, водени жиг постаје видљив код сепарације боја за вријеме исписивања слике. Тиме документ постаје бескористан након штампања, док се водени жиг не уклони из појаса у којем се налази. Метода налази комерцијалну употребу у новинарству, гдје новинари могу прегледати означене дигиталне слике прије куповине њихових неозначених верзија.

У поређењу с техникама које дјелују у просторном домену, чешће су кориштене технике које дјелују у фреквенцијском домену. Циљ је уметање воденог жига унутар спектралних компоненти слике. Најчешће кориштене трансформације су дискретна косинусна (ДКТ), дискретна Фуријеова (ДФТ) и дискретна wavelet трансформација (ДВТ). Разлог за коришћење фреквенцијског домена при имплементацији дигиталног воденог жига је боља прилагодљивост спектралних коефицијената карактеристикама људског визуелног система. Људско око је осјетљивије на промјене у нижим фреквенцијама, него на промјене виших фреквенција. Другим ријечима, информације садржане у нижим фреквенцијама су перцепцијски битније, па самим тим промјене на коефицијентима нижих фреквенција узрокују више видљиве дисторзије на самој слици. С друге стране високофреквенцијске компоненте сматрају се небитнима, тако да се све технике обраде слике, као што је компресија базирају на уклањању тих компоненти.

Дискретна Фуријеова трансформација (ДФТ) омогућује дигиталном воденом жигу да буде отпоран на геометријске промјене на слици, попут ротације, трансляције, скалирања итд. Као и код осталих фреквенцијских техника уметање дигиталног воденог жига обавља се у појасу средњих фреквенција, док својства Фуријеове трансформације омогућавају релативно једноставну детекцију дигиталног воденог жига унутар слике, чак и након подвргавања слике дисторзијама попут компресије, ротације, замућивања и сл. Из тог разлога дискретна Фуријеова трансформација је врло погодна за уметање дигиталног воденог жига унутар слике.

Дискретна косинусна трансформација (ДКТ), као и Фуријеова, користи фреквенцијски, а не амплитудни простор за приказ података. То је корисно јер више одговара начину на који људско око перципира свјетлост, тако да се дијелови који су мање примјетни или непримјетни могу одбацили. Методе базиране на ДКТ су отпорније од метода које користе просторни домен рада. Алгоритми који користе ДКТ отпорни су на једноставне манипулације слике попут филтрирања нископропусним филтром, промјена свјетлине и контраста, замућивања и сл. Са друге стране, теже их је имплементирати и рачунски су доста комплекснији, односно скупији за изведбу. Изведба ДКТ може бити над цијелом сликом или блоковска [10]. На Сл. 3 приказана је шема за уметање и извлачење дигиталног воденог жига код ДФТ и ДКТ.



Слика 3 – Основна шема система за уметање и извлачење дигиталног воденог жига код ДФТ, ДКТ

5. ПРИМЈЕРИ ЗА УТИСКИВАЊЕ ВОДЕНОГ ЖИГА У ФРЕКВЕНЦИЈСКОМ ДОМЕНУ

За потребе објективне процјене квалитета слике након утискивања воденог жига обично се користи SNR мјера (енг. Signal to Noise Ratio) однос сигнал - шум и формула за рачунање ове мјере је сљедећа:

$$SNR = 10 \log_{10} \frac{\sum_{i=1}^M \sum_{j=1}^N [z(i,j)]^2}{\sum_{i=1}^M \sum_{j=1}^N [o(i,j) - z(i,j)]^2} \quad (1)$$

гдје је z означена слика, o оригинална слика, а M и N су димензије слике.

Такође као мјера сличности оригиналног и екстрахованог жига користи се SF мјера (енг. Similarity Factor) фактор сличности, који може да има вриједности од 0 до 1. Што SF има већу вриједност значи да су екстраховани и оригинални жиг сличнији. Прихватљиво је да SF има вриједност већу од 0,75 [12]. Формула за рачунање SF је сљедећа:

$$SF = \frac{\sum_{i=1}^M \sum_{j=1}^N [Z(i,j) * Z^*(i,j)]}{\sqrt{\sum_{i=1}^M \sum_{j=1}^N [Z(i,j)^2 * Z^*(i,j)^2]}} \quad (2)$$

гдје је Z оргинални жиг и Z* екстраховани жиг, а M и N су димензије жига.

ДФТ омогућује да се слика из просторног домена, гдје се за памћење информација о бмп слици 512x512 пиксела мора меморисати информација о сваком пикселу, пребаци у фреквенцијски домен као сума синусних и косинусних компоненти, гдје су информације битне визуелном људском систему сконцентрисане у нпр. 10-так ДФТ коефицијената. То значи да је највећи дио енергије 2Д сигнала слике детектован у одабраним коефицијентима. Детаљи слике се налазе на већим фреквенцијама и они се у одговарајућој мјери жртвују како би се добила боља компресија слике. Мале енергије на већим фреквенцијама су подложније и утицајима шума. При томе треба водити рачуна о балансу квалитета слике и степена сажимања. Због наведених карактеристика ДФТ има јако широку примјену у обради слике, њеном филтрирању, компресији, па и у подручју дигиталних водених жигова.

Алгоритам за дискретну Фуријеову трансформацију ДФТ за утискивање жига:

1. Потребно је прво учитати оргиналну слику (o) и слику воденог жига (z).
2. Уколико су различитих величина слику воденог жига треба скалирати на величину оригиналне слике.
3. Затим се рачунају ФФТ (ДФТ) коефицијенти обе слике.
4. Дефинише се фактор уметања α који одређује степен видљивости воденог жига у оригиналној слици.
5. ФФТ (ДФТ) коефицијенти оргиналне слике се мијењају на основу коефицијената воденог жига. При томе се користи сљедећа формула:

$$R = \sum_{i=1}^M \sum_{j=1}^N [FO(i,j) + \alpha * FZ^*(i,j)] \quad (3)$$

гдје је FO Фуријеова трансформација оригиналне слике, а FZ Фуријеова трансформација воденог жига. M и N су димензије жига и оргиналне слике, а R је резултат.

6. Затим се над резултатом изврши инверзна Фуријеова трансформација и добије означена слика.

Извлачење воденог жига се врши помоћу означене слике (гдје се за потребе тестирања отпорности воденог жига могу додати одређене дисторзије) и оригиналне слике и то према сљедећој формули:

$$z^* = \sum_{i=1}^M \sum_{j=1}^N \frac{[z(i,j) * o(i,j)]}{\alpha} \quad (4)$$

гдје је z означена слика и o оригинална слика, а α дефинисани степен видљивости.

Одабрана слика за тестирање је слика Бабоон.бмп. За жиг је генерисана нова слика и обе се могу видјети на Сл. 4.



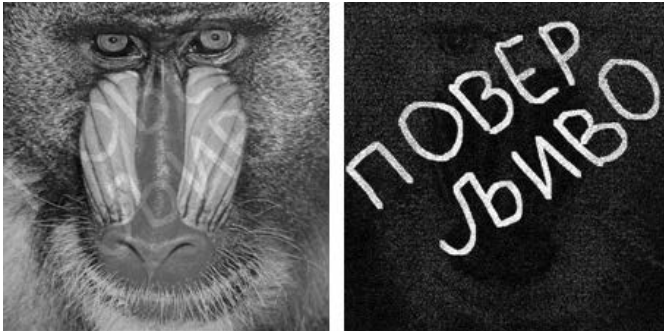
Слика 4 – Слика Бабоон.бмп [11] и слика одабрана за водени жиг зиг.бмп

Уколико се жели постићи видљив водени жиг, коефицијент треба имати вриједност ближу 1. Слика је након уметања воденог жига подвргнута ЈПГ компресији са коефицијентом $q=75$. Након тога је извучен водени жиг и упоређен са оригиналом. Добијена вредност за SNR је 11.602, а за SF 0.9204. Ово значи да је водени жиг отпоран на извршену компресију и да је веома сличан оригиналном воденом жигу. Примјер је илустрован на Сл. 5.



Слика 5 – Слика лијево је добијена након уметања воденог жига у оргиналну слику ($\alpha = 1$) и примјене ЈПГ компресије са $q=75$. Слика десно је примјер извученог воденог жига из десне слике.

Коефицијент α је затим постављен на вриједност 0.1. Слика је након уметања воденог жига подвргнута ЈПГ компресији са коефицијентом $q=50$. Након тога је извучен водени жиг и упоређен са оригиналом. Добијена вриједност за SNR је 20.7663, а за SF 0.6191. На основу добијених података се види да је и водени жиг изгубио на квалитету и његов коефицијент сличности је испод прага 0.75. Водени жиг је и даље примјетан на слици. Примјер је илустрован на Сл. 6.



Слика 6 – Слика лијево је добијена након уметања воденог жига у оригиналну слику ($\alpha=0.1$) и примјене ЈПГ компресије са $q=50$. Слика десно је примјер извученог воденог жига из десне слике.

Са $\alpha=0.01$ и $q=80$ водени жиг је потпуно непримјетан за људско око, али је коефицијент сличности доста мањи 0.1547, а SNR већи 27.0413. Примјер је илустрован на Сл. 7.



Слика 7 – Слика лијево је добијена након уметања воденог жига у оригиналну слику ($\alpha=0.01$) и примјене ЈПГ компресије са $q=80$. Слика десно је примјер извученог воденог жига из десне слике.

Матлаб код за посљедњи примјер дат је у наставку:

```
close all; clc;

%Učitavanje slike
I = im2double(imread('Baboon.bmp'));
figure;
imshow(I);
title('Originalna slika');
FO=fft(I);
alpha=0.01;

% Učitavanje vodenog žiga
```

```
close all; clc;

%Učitavanje slike
I = im2double(imread('Baboon.bmp'));
figure;
imshow(I);
title('Originalna slika');
FO=fft(I);
alpha=0.01;

% Učitavanje vodenog žiga
o=im2double(imread('zig.bmp'));
figure;
imshow(o);
title('Vodeni žig');

% Umetanje vodenog žiga
FZ=fft(o);
K=FZ.*alpha;
FO=FO+K;
T=ifft(FO);

% JPEG kompresija označene slike kao vid nenamjernog napada
q=80;
imwrite(T, 'vidljivzig.jpg','jpg',quality,q);
a=imread('vidljivzig.jpg');
a=im2double(a);
figure;
imshow((a));
title('Označena slika');

% Izvlačenje žiga
z = (a-I)./alpha;
figure;
imshow((z));
title('Ekstrahovani vodeni žig');
imwrite(z, 'izvucen_vidljivzig.bmp')

% Računanje SNR
z1=double(a);
snr_num=0;
snr_den=0;
for i=1:512
for j=1:512
snr_num=snr_num+(z1(i,j)*z1(i,j));
snr_den=snr_den+(|(i,j)-z1(i,j)|*(|(i,j)-z1(i,j)|));
end
end
snr=10*log10(snr_num/snr_den)

% Računanje faktora sličnosti (SF)
sf_num=0;
sf_den=0;
a=0;
b=0;
for i=1:512
for j=1:512
sf_num=sf_num+(z(i,j)*o(i,j));
a=a+(o(i,j)*o(i,j));
b=b+(z(i,j)*z(i,j));
sf_den=sqrt(sf_den+a*b);
end
end
sf=(sf_num/sf_den)
```

JPG standard za kompresiju slike koristi Diskretnu Kosinusnu Transformaciju (DKT). Ona ima jako dobro svojstvo sažimanja energije pa slika ostaje vizuelno „nepromiješana“, čak i onda kada je stepen kompresije jako veliki, jer su bitni dijelovi slike koncentrisani u jako malom broju DKT koeficijentata. Problem kod primjene DKT kompresije u oblasti vodenih žigova je taj što se slika i vodeni žig dijele u blokove (obično 8x8 piksela) i nad svakim blokom se vrši diskretna kosinusna transformacija unaprijed, pa je moguće da dođe do diskontinuiteta u slici. Osnovni algoritam za umetanje i izvlačenje vodenog žiga je jako sličan diskretnoj Furijeovoj transformaciji, samo se sada koristi drugi oblik transformacije i to posebno za svaki blok 8x8 bita. U Matlab kodu $\text{fft}(o)$ funkcije i $\text{dct2}(o)$ odnosno $\text{ifft}(x)$ funkcija i $\text{idct2}(x)$ daju iste rezultate. ФФТ је само рачунски бржа од ДЦТ2.

Matlab kod za umetanje vodenog žiga korištenjem DKT transformacije dat je u nastavku:

```
clear all; close all; clc;
% Umetanje žiga korišćenjem DCT transformacije
% Faktor vidljivosti vodenog žiga (snage)
alpha=1;

% Originalna slika
originalImage=imread('Baboon.bmp');
watermarkedImage = zeros(512,512);

% Po potrebi promijeni veličinu slike na 512x512
inputImage= im2double(imresize(originalImage,[512 512],'bilinear'));
figure,imshow(inputImage),title('Originalna slika');

% Slika vodenog žiga
% Promijeni joj veličinu na 64x64
xx=imread('zig.bmp');
watermarkImage = im2double(imresize(xx,[64 64],'bilinear'));
figure,imshow(watermarkImage),title('Vodeni žig');

% Iz 2d matrice kreiraj 1d niz 64x64 elemenata
w = watermarkImage(:);

r1=1;r2=8; % Inicijalizacija redova pod-blokova slike vodenog žiga
c1=1;c2=8; % Inicijalizacija kolona pod-blokova slike vodenog žiga

count = 0;
for i = 1: 64
for j = 1: 64
count = count +1;

% Preuzmi 8x8 pod-blok originalne slike
block = inputImage(r1:r2,c1:c2);

% Primijeni DCT na pod-blok
f = dct2(block);

% Utisni žig sa formulom f(m,n)=w(x)*alpha
```

```
f(8,8) = w(count) * alpha;

% Primeni inverznu DCT na žig
out = idct2(f);

% Sačuvaj rezultat kao odgovarajući blok označene slike
watermarkedImage(r1:r2,c1:c2) = out;
c1=c1+8;
c2=c2+8;

% Pomjeri se na sledeću kolonu - blok slike, piksel vodenog žiga
end
r1=r1+8;
r2=r2+8;
c1=1;c2=8;
% Pomjeri se na sledeći red
end
res = im2uint8(watermarkedImage);
imwrite(res,'Oznacenaslika.bmp','bmp');
figure,imshow(res),title('Slika nakon oznacavanja');

%distorzije... primjer jpg
%q=50;
res=im2double(watermarkedImage);
%imwrite(res, 'vidljivzig.jpg','jpg','quality',q);
%res=imread('vidljivzig.jpg');
%res=im2double(res);
%figure;
%imshow((res));
%title ('Označena slika JPG');
%res=imnoise(res,'gaussian',0,0.02)
res = imrotate(res, 45);

%Ekstrakcija vodenog žiga
alpha=1;
w1 = zeros(64,64);

r1=1;r2=8; % Inicijalizacija redova pod-blokova slike vodenog žiga
c1=1;c2=8; % Inicijalizacija kolona pod-blokova slike vodenog žiga

count = 0;
for i = 1: 64
for j = 1: 64
count = count +1;

% Preuzmi 8x8 pod-blok originalne slike
block = res(r1:r2,c1:c2);

% Primijeni DCT na pod-blok
f = dct2(block);

% Ukloni faktor vidljivosti
w1(count) = f(8,8) / alpha;
c1=c1+8;
c2=c2+8;
end
r1=r1+8;
```

```

r2=r2+8;
c1=1;c2=8;
end
op = vec2mat(w1,64);
imshow(op,[],),title('Ekstrahovan vodeni žig');
imwrite(op,'EktrahovanVZ.bmp','bmp');

% Računanje SNR
z1=double(res);
snr_num=0;
snr_den=0;
for i=1:512
for j=1:512
snr_num=snr_num+(z1(i,j)*z1(i,j));
snr_den=snr_den+((inputImage(i,j)-z1(i,j))*(inputImage(i,j)-z1(i,j)));
end
end
snr=10*log10(snr_num/snr_den)

% Računanje faktora sličnosti (SF)
sf_num=0;
sf_den=0;
a=0;
b=0;
for i=1:64
for j=1:64
sf_num=sf_num+(op(i,j)* watermarkImage(i,j));
a=a+( watermarkImage(i,j)* watermarkImage(i,j));
b=b+(op(i,j)*op(i,j));
sf_den=sqrt(sf_den+a*b);
end
end
sf=(sf_num/sf_den)

```

Дискретна wavelet трансформација користи комбинацију нископропусних и високопропусних филтара и подзорковања (децимацију) броја узорака 2Д сигнала слике. Уколико се сигнал пропусти кроз два филтра, нископропусни и високопропусни, његов фреквенцијски садржај ће бити раздвојен на два опсега једнаких ширина. Излаз из ових филтара садржи половину фреквенцијског садржаја оригиналног сигнала, а исти број одбирака као оригинални сигнал. Зато се врши децимација ових сигнала. Децимација преполови број одбирака, тако да се временска резолуција такође преполови, док се фреквенцијска резолуција повећа. Високопропусни филтар је пропустио високофреквентни садржај тј. детаље сигнала. Нископропусни сигнал је пропустио нискофреквентни садржај тј. апроксимацију сигнала. Управо овај сигнал апроксимације може даље бити пропуштен кроз два филтра, и поступак се може понављати док се не достигне жељени ниво декомпозиције. Цјелокупна информација о оригиналном сигналу садржана је у последњем сигналу апроксимације и свим сигнаlima детаља. Приликом извршења сваког нивоа декомпозиције, добијају се коефицијенти груписани у четири групе: ЛЛ, ХЛ, ЛХ, ХХ, где Х представља високофреквенцијски садржај, а Л

нискофреквенцијски садржај. ЛЛ су заправо тзв. коефицијенти апроксимације, а ХЛ, ЛХ и ХХ су коефицијенти детаља, и то хоризонтални, вертикални и дијагонални, респективно.

ЛПЕГ 2000 користи управо wavelet трансформацију за декомпозицију слике на коефицијенте. DWT трансформирани сигнали имају јако добро временску диференцираност у подручју високих фреквенција, односно јако добру фреквенцијску диференцираност у подручју нижих фреквенција.

6. ЗАКЉУЧАК

Подручје истраживања дигиталних водених жигова је јако актуелно и непрестано се развијају нове технологије у спрези са облашћу криптографије. Овај рад је описао основне ове области и практичном реализацијом у Матлабу тестирао по један примјер описаних технологија, чиме се добија добар увид у њихове слабости и могућности, те и полазна тачка за даља истраживања.

Од наведених метода утискивања воденог жига на одабраној оригиналној слици и генерисаном воденом жигу најбоље резултате је имала DWT технологија. Она се добро супроставила како компресији, шуму, тако и геометријским промјенама слике. Затим ДКТ трансформација је имала најгори резултат код геометријских ротација, а ДФТ је била лошија код мањег квалитета односно веће ЛПГ компресије. Просторне технологије, које нису детаљније описане у раду, су неупоредиво мање отпорне на све сигурносне нападе од технологија у фреквенцијском домену. Резултати односно квалитет екстрахованог жига јако зависи од његове видљивости (снаге утискивања) и степена дисторзије слике. Резултати компресије зависе и од карактеристика саме слике, нпр. количине детаља, јер се код компресије слике обично одбацују високофреквентне компоненте које у себи носе информацију о детаљима слике.

7. ЛИТЕРАТУРА

- [1] Digital Watermarking Alliance, „The case for content identification - Supporting new business models and effectively managing key business assets“, Доступно на: http://www.digitalwatermarkingalliance.org/docs/papers/DWA_WhitePaper_Case4ContentID.pdf [Приступљено: 10. Април 2016.]
- [2] Чисар, П., „Општи аспекти квантне криптографије“, ИнфоМ, Вол. 14, Бр. 54, Факултет организационих наука, Београд, 2015.
- [3] P2P Digital Watermark Working Group, Digital Watermarking Alliance, DIGITAL WATERMARK TECHNOLOGIES-Applications in P2P Networks, Доступно на: http://www.digitalwatermarkingalliance.org/docs/papers/dcia_whitepaper_p2p.pdf [Приступљено: 10. Април 2016.]
- [4] A.Z.Tirkel, G.A. Rankin, R.M. Van Schyndel, W.J.Ho, N.R.A.Mee, C.F.Osborne. “Electronic Water Mark”. DICTA 93, Macquarie University. str. 666-673., 1993.
- [5] N. Singh, M. Jain, S. Sharma, „A Survey of Digital Watermarking Techniques“, International Journal of Modern Communication Technologies & Research (IJMCTR), str. 6-11., Vol. 1, br. 6, August 2013., ISSN: 2321-0850

- [6] M. Kaur, S. Jindal, S. Behal, "A Study of Digital Image Watermarking", International Journal of Research in Engineering & Applied Sciences, str. 126-136., Vol. 2, br. 2, ISSN: 2249-3905, February 2012.
- [7] X. Шалковић, „Примјена дигиталног воденог жига у заштити власништва слика у дигиталном запису“, СВЕУЧИЛИШТЕ У ЗАГРЕБУ, ФАКУЛТЕТ ЕЛЕКТРОТЕХНИКЕ И РАЧУНАРСТВА, 2013. Доступно: https://bib.irb.hr/datoteka/658620.Hrvoje_alkovi_-_Diplomski_rad.pdf [Пристапљено: 15. Април 2016.]
- [8] G. Coatrieux, L. Lecornu, Members, IEEE, Ch. Roux, Fellow, IEEE, B. Sankur, Member, IEEE'a review of digital image watermarking in health care'.
- [9] G. L. Friedman, "The Trustworthy Digital Camera: Restoring Credibility to the Photographic Image," IEEE Transaction on Consumer Electronics, Vol. 39, No. 4, November 1993, стр. 905-910.
- [10] C. Way Hun Fung, A. Gortan, W. G. Junior, "A Review Study on Image Digital Watermarking", In: The Tenth International Conference on Networks (ICN 2011), pp. 24-28., 2011.
- [11] Извор слика за тестирање: <http://www.eecs.qmul.ac.uk/~phao/CIP/Images/>
- [12] R. Chaturvedi, A. Sharma, N. Hemrajani, D. Goyal, „Analysis of Robust Watermarking Technique Using Mid Band DCT Domain for Different Image Formats“, International Journal of Scientific and Research Publications, Vol. 2, Issue 3, March 2012, ISSN 2250-3153.



Mr Željko Gavrić, viši asistent, Slobomir P Univerzitet, Doboj-Bijeljina, RS-BIH
Kontakt: zeljko.gavric@spu.ba
Oblasti interesovanja: Multimedije, Multimedijske komunikacije, Senzorske mreže



Dr Vanja Mišković, docent, Slobomir P Univerzitet, Doboj-Bijeljina, RS-BIH
Kontakt: vanja.elcic@gmail.com
Oblasti interesovanja: Mobilno računarstvo, Senzorske mreže, Multimedije



Dr Dušan Starčević, redovni profesor, Fakultet Organizacionih Nauka, Beograd
Kontakt: starcev@fon.rs
Oblasti interesovanja: Računarske mreže, Multimedijske komunikacije, Multimedije



UPUTSTVO ZA PRIPREMU RADA

1. Tekst pripremiti kao Word dokument, A4, u kodnom rasporedu 1250 latinica ili 1251 ćirilica, na srpskom jeziku, bez slika. Preporučeni obim – oko 10 strana, single prored, font 11.
2. Naslov, abstrakt (100-250 reči) i ključne reči (3-10) dati na srpskom i engleskom jeziku.
3. Jedino formatiranje teksta je normal, bold, italic i bolditalic, VELIKA i mala slova (tekst se naknadno prelama).
4. Mesta gde treba ubaciti slike, naglasiti u tekstu (Slika1...)
5. Slike pripremiti odvojeno, VAN teksta, imenovati ih kao u tekstu, radi identifikacije, u sledećim formatima: rasterske slike: jpg, tif, psd, u rezoluciji 300 dpi 1:1 (fotografije, ekranski prikazi i sl.), vektorske slike – cdr, ai, fh, eps (šeme i grafikoni).
6. Autor(i) treba da obavezno priloži svoju fotografiju (jpg oko 50 Kb), navede instituciju u kojoj radi, kontakt i 2-4 oblasti kojima se bavi.
7. Maksimalni broj autora po jednom radu je 5.

Redakcija časopisa Info M