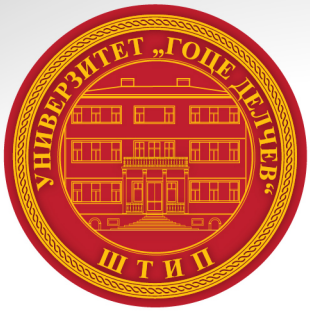


УНИВЕРЗИТЕТ „ГОЦЕ ДЕЛЧЕВ” - ШТИП
ФАКУЛТЕТ ЗА ИНФОРМАТИКА

ISSN:1857-8691

ГОДИШЕН ЗБОРНИК
2014
YEARBOOK
2014

ГОДИНА 3 VOLUME III

GOCE DELCEV UNIVERSITY - STIP
FACULTY OF COMPUTER SCIENCE

УНИВЕРЗИТЕТ „ГОЦЕ ДЕЛЧЕВ“ – ШТИП
ФАКУЛТЕТ ЗА ИНФОРМАТИКА

ГОДИШЕН ЗБОРНИК
2014
YEARBOOK
2014

ГОДИНА 3 ЈУНИ, 2015 VOLUME III

GOCE DELCEV UNIVERSITY – STIP
FACULTY OF COMPUTER SCIENCE

ГОДИШЕН ЗБОРНИК
ФАКУЛТЕТ ЗА ИНФОРМАТИКА
YEARBOOK
FACULTY OF COMPUTER SCIENCE

За издавачот:
Проф д-р Владо Гичев

Редакција и администрација
Универзитет „Гоце Делчев“-Штип
Факултет за информатика
ул. „Крсте Мисирков“ 10-А
п. фах 201, 2000 Штип
Р. Македонија

Address of the editorial office
Goce Delcev University – Stip
Faculty of Computer Science
Krste Misirkov 10-A
PO box 201, 2000 Štip,
R. of Macedonia

СОДРЖИНА
CONTENT

ДИГИТАЛЕН ВОДЕН ЖИГ ВО СЛИКА ВО ФРЕКВЕНТЕН ДОМЕН СО ДИСКРЕТНА КОСИНУСНА ТРАНСФОРМАЦИЈА

Ана Љуботенска[1*], Александра Милева[1]

[1]Факултет за информатика, Универзитет „Гоце Делчев“ - Штип
ana.ljubotenska@ugd.edu.mk
aleksandra.mileva@ugd.edu.mk

Апстракт. Во денешното современо општество дигиталните медиуми ги заменија традиционалните аналогни медиуми, што е разбирливо живеејќи во ера на информации, каде билиони битови податоци се создаваат во секој дел од секундата. Под поимот дигитален медиум се подразбира дигитално претставување на текст, слики, аудио, видео и сл. Ваквиот начин на претставување има голем број на предности споредено со традиционалниот, како на пример лесна манипулација и модификација, едноставно зачувување, правење копии и дистрибуција, без загуби и нарушувања на квалитетот. Но јасно е дека предностите со себе повлекуваат и голем број проблеми. Суштината на проблемите е неовластениот пристап до дигиталните податоци. Нивното надминување се врши со шифрирање или заштита од копирање, односно заштита на авторските права. Како крајна линија на оваа одбрана е вметнување на податоци, односно дигитални водени жигови (анг. Watermark) директно во документите. Во овој труд е објаснет поимот дигитален воден жиг, направен е преглед на начините на нивно криење, ставајќи акцент на криењето на дигитален воден жиг во слика со користење на дводимензионална дискретна косинусна трансформација, скратено DCT. Овој метод работи во фреквентен домен со внесување на псевдослучаен редослед на реални броеви во одбран сет на DCT коефициенти. Изборот на дигитален воден жиг се врши со маскирање на карактеристиките на човечкиот визуелен систем, за да се направи печатот невидлив. Техниката за криење на информација во рамките на дигитална слика со DCT е имплементирана со користење на MATLAB програмскиот јазик. Ваквиот начин овозможува одржување на доверливоста и приватноста на критичните информации и заштита на истите од потенцијална кражба или неовластен пристап. Освен техниката за криење и извлекување на дигитален воден жиг од слика со DCT, во трудот се тестирани и повеќе напади кои се вршат врз дигиталниот воден жиг.

Клучни зборови: *дигитален воден жиг, слика, фреквентен домен, авторски права, напад на слика, DCT*

1. Вовед

Ако земеме банкнота од 100 денари и ја доближиме до светло јасно ќе ја забележиме сликата од резбан таван од македонска куќа од левата страна. Ова на некој начин претставува лого на оваа банкнота и во нормални услови не се забележува добро. Благодарение на логото може да се потврди дека банкнотата не е фалсификат. Ова е пример за воден жиг кој се користи за да се докаже автентичноста, односно да се идентификува оригиналноста и вредноста на парчето хартија. Водениот жиг на банкнотата од 100 денари, даден на слика бр.1, исто како и повеќето водени жигови на хартија (анг. paperwatermarks), има две својства. Прво, водениот жиг е скриен од поглед при нормална употреба и станува видлив само како резултат на посебен процес на гледање, во овој случај, изложување на светлина. Второ, тој носи информации за објектот во кој е скриен, во овој случај, водениот жиг укажува на автентичноста на банкнотата. Ваквиот пример од секојдневието укажува на важноста на оваа проблематика и потребата истата да се разбере и применува.

Слика 1. Воден жиг кај банкнота од 100 денари

Кај дигиталните податоци, пак, основата на проблемите предизвикани од лесната манипулација е неовластениот пристап. Надминувањето на проблемите се врши со шифрирање или заштита од копирање. Меѓутоа, ако податокот еднаш биде дешифриран, тој лесно може да се копира и дистрибуира и на тој начин механизмите за заштита од копирање можат да се заобиколат. Како заштита од неуспешното шифрирање и заштита од копирање е предложено вметнувањето, односно извлекувањето на дигитален воден жиг. Оваа техника првично била позната како „последна линија на одбраната“ против неовластениот пристап [1]. Вметнувањето на дигитален воден жиг е различно од шифрирање, во

насока на тоа што овозможува корисникот да пристапи, да го види и интерпретира сигналот, но го заштитува сопственикот на содржината. Системот на дигитални водени жигови ги вметнува информациите директно во документот, како што се име на сопственик, заштита од копирање, име на легитимен корисник итн. Сепак, фалсификаторите се обидуваат да го деградираат квалитетот на водените жигови во слика со нејзино напаѓање. Обично нападите се со скалирање, препокривање, компресија и ротација на воденият жиг на сликата. Со напаѓање на воденият жиг станува тешко истиот да се поправа и да се извлече од сликата, па дури и ако е извлечен веќе не може да се користи за да се докажат сопственоста и авторските права.

Од аспект на дигиталната обработка на слики, вметнувањето и извлекувањето на дигитален воден жиг во слика претставува псевдослучајна секвенца на битови, додадена во сликата. Оваа секвенца треба да биде позната само за сопственикот на сликата, со што други корисници не можат да ја отстранат или направат нејзини дупликати. На овој начин се докажува веродостојноста на сопственикот.

2. Дигитален воден жиг

Постојат различни видови на дигитални водени жигови. Нивната класификација може да се направи според повеќе критериуми. Еден од нив е видот на оригиналниот документ. Според ова, разликуваме четири видови на техники за криење на дигитални водени жигови:

- TextWatermarking – криење на дигиталниот воден жиг во текст;
- ImageWatermarking – криење на дигиталниот воден жиг во слика;
- AudioWatermarking – криење на дигиталниот воден жиг во аудио;
- VideoWatermarking – криење на дигиталниот воден жиг во видео.

Друг критериум за класифицирање е според природата на дигиталните водени жигови, според што тие можат да се поделат во три различни групи:

- Видлив дигитален воден жиг;
- Невидлив – робустен дигитален воден жиг (невидлив дигитален воден жиг, отпорен на напади);
- Невидлив – нежен дигитален воден жиг (невидлив дигитален воден жиг, кој не е отпорен на напади) [2].

Може да се користи комбинација од повеќе од споменатите видови на жигови. На пример, често е комбинирањето на невидливи робустни со видливи дигитални водени жигови. Причината за нивно комбинирање е остварување на поголема безбедност. Поделбата може да се направи уште според методот за модификација на сликата домаќин или според перцептивната стратегија на моделирање.

Според првиот критериум се разликуваат:

- Спојување на слики (кога се вметнува лого);
- Метод на нелинеарна кванитизација и замена;
- Линеарно собирање на проширен спектар на сигнал.

Според вториот критериум разликуваме:

- Без моделирање;
- Имплицитно моделирање, со помош на карактеристиките на доменот на трансформација;
- Експлицитно моделирање, со користење на модели на човечкиот визуелен систем.

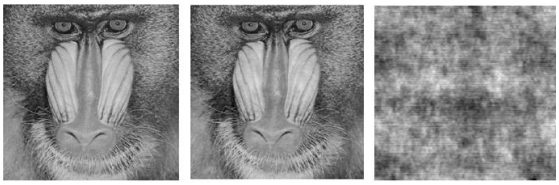
За имплементирање на дигиталните водени жигови постојат повеќе методи кои се делат според доменот во кој се работи. Доменот може да биде просторен (анг. Spatial domain), фреквентен (анг. Frequency domain) и wavelet т.е. брановиден домен (анг. Wavelet domain) [3]. Во овој труд е опфатено само криењето на податоци во фреквентен домен, поради фактот што ваквиот начин на криење на податоци има предност пред криењето во просторен домен, поради поголемата робустност, односно отпорност од напади. Со промена на еден параметар во фреквентен домен се менува содржината на целиот документ, додека кај просторниот домен промената е во само еден сегмент. Во просторен домен ако таквиот сегмент се отстрани тогаш воденият жиг ќе биде уништен, додека во фреквентен домен жигот е постојан и се детектира од останатата содржина на документот.

3. Преглед на техники за вметнување на дигитален воден жиг во слика

Истражувањето на дигиталните водени жигови е доста интензивно во последните неколку години. Преглед на методите за означување на слики отпорни на ротација, транслација и скалирање, имаат направено Zheng и неговите соработници [4]. Тие имаат развиено метода што се базира на Фуриевата трансформација, отпорна на JPEG компресија, ротација и транслација, но слабо отпорна на скалирање. Алгоритамот користи логаритамско-поларно мапирање, па затоа има големи побарувања. Базирана на Фуриевата трансформација е и методата на Cai и Du [5], која има еден голем недостаток, а тоа е што не е отпорна на транслација. Нивното истражување е насочено кон постигнување на отпорност на

геометриски напади, што е постигнато со одредување на фиксни координати на оригиналната слика. Meerwald и Uhl [6], пак, имаат направено преглед на алгоритамите кои се користат во wavelet домен. Al – Haj [7] ја комбинира wavelet и косинусната трансформација за развивање на метод кој е отпорен на JPEG компресија. Оваа метода постигнува доста добри резултати, благодарение на својствата на wavelet трансформацијата, но сепак не е отпорна на отсекување и ротација.

Во областа на примена на дискретната косинусна трансформација за вметнување на водени жигови во слика, значајни се резултатите на Cox [8] и Koch [9]. Во Cox алгоритамот како дигитален воден жиг се зема Гаусова низа од 1.000 псевдослучајни броеви, кои се собираат со 1.000 најголеми DCT коефициенти. Коефициентите на трансформација се делат на значајни (најмногу 1.000) и отфрлени. Автори на овој алгоритам се Ingemar J.Cox, Joe Kilian, Tom Leighton и Talal G.Shamoon од NEC Research Institute, Princenton, Америка. Cox методата започнува со вметнување на оригинална слика во која ќе се крие податок. Методот работи со црно-бели слики. Големината на сликата треба да се намали, па се вметнува дигиталниот воден жиг. Cox тестирањата ги правел со параметри N=1000 и $\alpha = 0.3$, при што α е коефициент на вметнување на воден жиг, објаснет подолу во трудот, а N претставува должина. Големината на оригиналната слика изнесува 512x512 пиксели. На сликата во продолжение се прикажани а) намалената црно-бела слика со име 4.2.03.tiff пред вметнување на дигитален воден жиг и б) по вметнувањето на параметрите N=1000 и $\alpha = 0.3$.



Слика 2. Cox алгоритам, а) слика без дигитален жиг б) слика по вметнување на дигитален жиг со $\boldsymbol{\alpha = 0.3}$ в) разлика меѓу оригиналната слика и означената со Cox алгоритамот

За вредност $\alpha = 0.3$ се добива невидлив жиг, што е потврдено и на слика 2 погоре. Коефициентите кај овој алгоритам се модифицираат во согласност со стримингот на битови од пораката во согласност со равенката:

$$C_{AW} = C_A \cdot (1 + \alpha \cdot W_i)$$

каде што C_{AW} е коефициент на водениот жиг, C_A на оригиналната слика, а W_i одговара на битовите на податокот кој се обработува. Хеминговото растојание, добиено од споредбата меѓу извлечениот дигитален воден жиг од означената слика и вметнатиот жиг, изнесува $\delta = 0.9998$. Разликата меѓу нив е прикажана на делот под в) на претходната слика. Земајќи го предвид тоа што вметнувањето кај овој алгоритам се одвива во DCT домен, истиот е користен за текстурирани слики со што помал број делови со еднаква осветленост. Ако оригиналната слика при тестирањето на овој алгоритам е сликата Lena, од стандардните тест слики за обработка на слики, а останатите параметри останат исти, тогаш резултатите ќе бидат од облик:

Слика 3. Примена на Cox алгоритам а) слика пред вметнување на жиг б) слика по вметнување на жиг

Истражување во оваа насока направиле и Eckhard Koch и Jian Zhao од Институтот за компјутерска графика - Fraunhofer во Германија. Алгоритамот што тие го добиеле е познат како алгоритам Koch [9]. Овој алгоритам спаѓа во групата на отпорни алгоритами, базирани на квантизација. Квантизација претставува пресликување на големи, бесконечни групи на вредности во многу помала група на вредности, со што се намалува количината на елементи. Други алгоритами во оваа група се: Chae, Ejima, Jayawardena, Lin, Ohnishi, Tzovaras и Xie. Дел од нив се во брановиден домен, како на пример Xie и Ohnishi, а дел во фреквентен домен. Алгоритамот Koch случајно избира блок од DCT коефициенти, со големина 8x8. Во внатрешноста на секој блок b_i, случајно се избираат два коефициенти со средна фреквенција. За да се постигне максимална отпорност и невидливост на водениот жиг, според посебни

критериуми се отфрла еден блок или неколку коефициенти. Вметнувањето на жигот, односно низа од бинарни вредности – $w_i \in \{0,1\}$ во оригиналната слика, се врши така што прво секој блок се квантизира според JPEG матрицата на квантизација и квантизацискиот фактор Q. Апсолутната разлика помеѓу избраните коефициенти е од облик:

$$\Delta_b = |f_b(m_1, n_1) - f_b(m_2, n_2)|$$

каде што f_bе DCT 8x8 блок, а $f_b(m_1, n_1)$ и $f_b(m_2, n_2)$ се одбрани коефициенти во одреден блок. Кога би се вметнал жиг од еден бит (w_i), потребно е да се променат неколку коефициенти $f_b(m_1, n_1)$ и $f_b(m_2, n_2)$ за оддалеченоста Δ_b да го добие обликот:

$$\Delta_b = \begin{cases} \geq q, & \text{за } w_i = 1 \\ \leq q, & \text{за } w_i = 0 \end{cases}$$

каде што q е параметар што ја контролира јачината на вметнување на жигот. Земајќи го предвид тоа што овој алгоритам жигот го вметнува во DCT 8x8 блокови, веројатни се видливи промени на означената слика, особено во нејзините еднолични делови. Како подобрување на овој алгоритам, Benham и Zhao наместо пар од два коефициенти вовеле множество од три коефициенти, што придонело за зголемување на отпорноста и намалување на видливите нарушувања на означената слика.

Освен методи базирани на некоја математичка трансформација, постојат и други пристапи на проблемот за заштита на авторските права на слика со дигитални водени жигови. Bulan и неговите соработници [10] ја испитуваат можноста за заштита на слика со модулација на ориентацијата на растерските елементи. Нивниот метод е многу добро решение за означување на слики, кои користат амплитудна модулација. Недостаток е што методата се користи за означување за време на растеризација и не може да се користи за заштита на дигиталните слики. Постојат пристапи при кои сликата се означува со користење на математички дефинирани моменти на сликите, кои имаат неколку привлечни својства, како инференција на шум, ротација итн. Ismail со соработниците [11] користи момент добиен со мапирање на вредностите на елементите на слика во множество комплексни полиноми. Предности на овој метод се малата побарувачка, отпорност од ротација, транслација, компресија и шум. Недостаток е големата осетливост на отсекување. Како главна пречка при користењето на овие методи во процесот на вметнување на дигитални жигови во слика, авторите ја наведуваат промената на медиумите што ги носат визуелните информации и деградацијата за време на прикажување и дополнителна дигитализација. Најголемиот број истражувања направени во информатичката технологија за заштита на слики се однесуваат на нивната дигитална форма, а многу поретко на нивното прикажување и дополнителна дигитализација. Затоа, најчесто користени методи за заштита на дигиталните водени жигови се математичките трансформации и тоа: *дискретната косинусна трансформација (DCT), дискретната wavelet трансформација (DWT)* и *дискретната Фуриева трансформација (DFT)*.

4. Користена методологија

Методологија за криење на податоци во слика која е користена во овој труд е дискретната косинусна трансформација. DCT работи во фреквентен домен и сликата ја претставува како сума од синусоиди со променливи магнитуди и фреквенции. Битно својство е што повеќето значајни визуелни информации на сликата се концентрирани само во неколку DCT коефициенти, познати како „енергетска согласност на сопственост“ [12]. Вметнувањето на воден жиг базирано на DCT се заснова на два факти: поголемата енергија на сигналот лежи во нискофреквентните опсези што ги содржат повеќе значајните визуелни податоци за сликата и вториот факт е дека компонентите со високи фреквенции од сликата обично и најчесто се отстрануваат за време на компресијата и нападите на шум. Математички пресметката на 2-D DCT, за слика со димензија NxN, се врши со:

$$F(u,v) = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} C(u)C(v)f(i,j) \cos\left[\frac{\pi(2\mathrm{i}+1)\mathrm{u}}{2\mathrm{N}}\right] * \cos\left[\frac{\pi(2\mathrm{j}+1)\mathrm{u}}{2\mathrm{N}}\right]$$

каде што $f(i,j)$ се елементи на сликата во просторен домен, $F(u,v)$ се елементи на сликата во фреквентен домен, а коефициентите $C(u)$ и $C(v)$ имаат вредности:

$$C(u) = \begin{cases} \frac{1}{\sqrt{2}}, & \text{за } u = 0 \\ 1, & \text{за } u \neq 0 \end{cases}, \quad C(v) = \begin{cases} \frac{1}{\sqrt{2}}, & \text{за } v = 0 \\ 1, & \text{за } v \neq 0 \end{cases}.$$

Пресметката на дводимензионална инверзна дискретна косинусна трансформација е:

$$f(i,j) = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} C(u)C(v)F(u,v) \cos\left[\frac{\pi(2\mathrm{i}+1)\mathrm{u}}{2\mathrm{N}}\right] * \cos\left[\frac{\pi(2\mathrm{j}+1)\mathrm{u}}{2\mathrm{N}}\right]$$

Сликата број 4 графички го прикажува процесот на криење податок во слика со оваа техника. На неа е прикажан коефициент α, што се нарекува фактор на вградување, односно watermarking коефициент. За видливи дигитални водени жигови добра вредност на α е $\alpha = 10$ или поголеми вредности [12]. За

невидливи дигитални водени жигови вредноста на α треба да биде помала, на пример $\alpha = 0{,}09$ или $\alpha = 0{,}3$, како кај Cox алгоритамот. Чекорите кои се применуваат во процесот на криење податок во слика со DCT техниката се следниве:

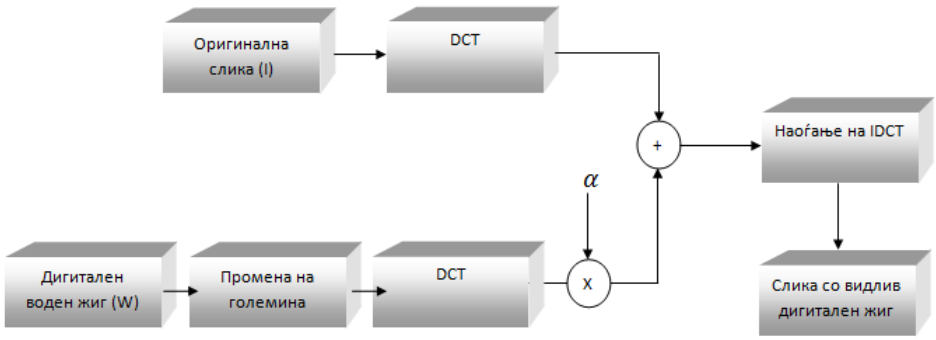
- Се вчитува оригиналната слика I, во која треба да се крие податок. Се вчитува и водениот жиг W. Двете слики не мора да се со иста големина.
- Се менува големината на сликата W, за да биде иста како големината на оригиналната слика.
- Се наоѓаат DCT коефициентите на двете слики паралелно.
- Вредноста на факторот на вметнување α се дефинира за да биде погоден за видливо или невидливо криење на податок во слика.
- DCT коефициентите од двете слики се модифицираат со користење на равенството дадено во продолжение. IDCT од модифицираните коефициенти ја дава сликата со скриен податок.

$$I_{w\,i,j} = I_{i,j} + \alpha \;\; w_{ij}\,, \qquad i,j = 1,\ldots,n$$

Извлекувањето на дигиталниот воден жиг од слика, со техниката на дискретна косинусна трансформација, се врши со примена на следнава равенка:

$$w_{ij} = (I_{w,ij} - I_{ij})/\alpha$$

каде што сите коефициенти претходно беа споменати во текстот.



Слика 4. Чекори на алгоритамот за криење податок во слика со DCT техника

5. Тестирања и резултати

Апликацијата за вметнување и извлекување на дигитален воден жиг во слика направена во MATLAB има три функционалности: *вметнува дигитален воден жиг во оригинална слика, тестира четири видови на напади врз жигот и извлекува дигитален воден жиг од слика.* За тестирања се вклучени две слики: една оригинална слика и една слика како дигитален воден жиг. На почетокот корисникот треба да внесе вредност на коефициентот на вметнување на жиг α, во зависност од тоа дали сака жигот да биде видлив или невидлив. Како оригинална слика при тестирањето е земена сликата Lena која е со големина 512x512 и е од Bitmap формат. Од истиот формат е земена и сликата за дигитален воден жиг. Почетните симулирани резултати се прикажани во продолжение, на слика 5. На истиот прозорец при извршувањето се прикажува оригиналната слика, водениот жиг и сликата со вметнат дигитален воден жиг, за да се направи подобар преглед и да се воочат разликите меѓу нив. Тестирањата потврдија дека колку жигот ќе биде видлив во сликата, зависи од вредноста на коефициентот α. За поголеми вредности жигот е позабележлив, а за доста мали вредности жигот станува невидлив.

Слика 5. Симулирани резултати

За да се укаже на значењето на коефициентот на вметнување α се направени три различни тестирања. Во првото е земено дека коефициентот има вредност $\alpha = 100$. Со оваа вредност добиената слика е со вметнат видлив дигитален воден жиг. Резултатот е прикажан на слика 6, под а.

Слика 6. Резултат од вметнувањето на дигитален воден жиг со а) α=100 и б) α=10

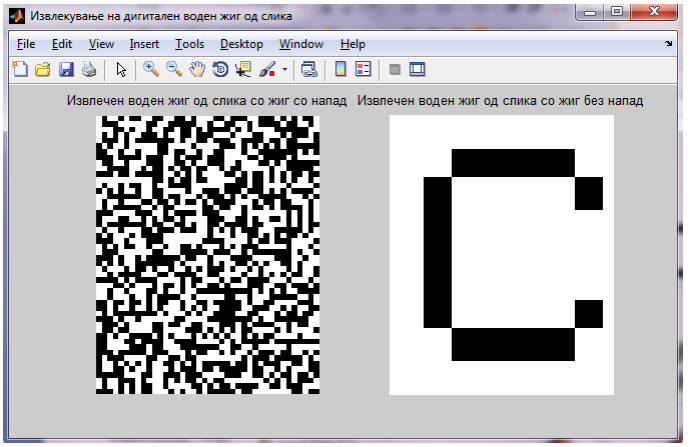
Поради големата вредност на α водениот жиг е доста забележлив. Со помала вредност на коефициентот $\alpha = 10$, водениот жиг е повторно видлив, но помалку за разлика од претходниот случај. Ова е дадено на сликата број 6, под б. Доколку го промениме коефициентот на $\alpha = 0.3$, водениот жиг ќе стане невидлив, како што е прикажано на слика 7.

Слика 7. Невидлив дигитален воден жиг

Втората функционалност се однесува на нападите врз дигиталните водени жигови. Разгледани се четири вида на напади: додавање на шум сол и пипер (анг. Salt&Pepper) со параметар 0.05, додавање на Гаусов шум (анг. Gaussian) со параметар 1.2, отсекување на дел од слика и ротирање на сликата под агол од 45°. Тестирањето на овие напади е извршено за $\alpha = 10$. Добиените резултати се прикажани на слика 8.

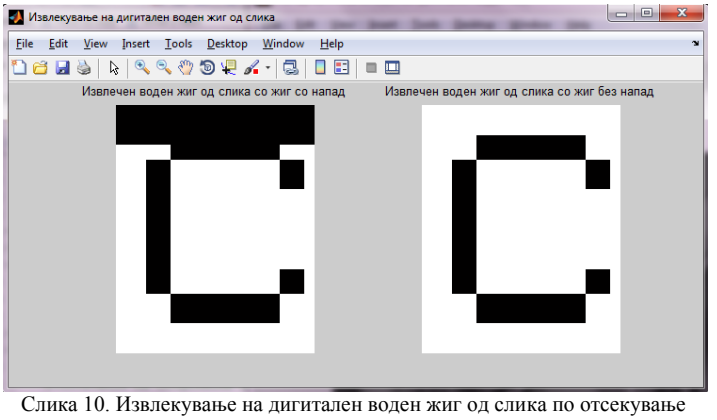
Слика 8. Напади врз дигитален воден жиг

Се забележува дека нападите можат значително да влијаат врз квалитетот на сликата со вметнат дигитален воден жиг. Влијанието најдобро се забележува при извлекувањето на дигиталниот воден жиг. За да се укаже на ова влијание, жигот се извлекува прво од сликата врз која е применет некој од нападите, а потоа се извлекува и од сликата со вграден жиг која не е нападната. На пример, на слика 9 е прикажан изгледот на извлеченият дигитален воден жиг од слика кај која прво е вметнат дигитален воден жиг со $\alpha = 10$, па на сликата е додаден шум сол и пипер, како што беше покажано на претходната слика. Може да се забележи големо нарушување на воденият жиг по нападот.



Слика 9. Извлекување на дигитален воден жиг од замаглена слика

Доколку се отсече дел од слика, во која е додаден дигитален воден жиг со $\alpha = 32$, тогаш извлеченият дигитален воден жиг ќе биде од облик:



Слика 10. Извлекување на дигитален воден жиг од слика по отсекување

Слични резултати се добиваат и со останатите напади. Во зависност од условите нарушувањата можат да бидат поголеми или помали. За да нема нарушувања најдобро би било да се избегне каков било напад врз слика во која се крие некој податок, доколку е можно.

6. Заклучок

На домашниот пазар сè уште во одредена мера е присутна софтверската и музичка пиратерија. Интернетот нуди неисцрпна база на нелегален дигитален материјал во форма на слики, текст, аудио и видео. Воведувањето на дигитални водени жигови во изворните носачи на информација сигурно значително ќе го намали бројот на пиратски материјал кој може да се најде на црниот пазар. За да се крие податок во слика за спомената цел, потребно е да најде техника за криење, која ќе биде ефикасна. Во оваа насока беше спроведено целото истражување, спакувано во овој труд, каде што е претставен и имплементиран начинот за криење на дигитален воден жиг во слика со примена на дискретна косинусна трансформација. Имплементацијата имаше за цел да задоволи три функционалности: вметнување на дигитален воден жиг во слика во фреквентен домен со користење на DCT методот, тестирање на четири различни видови на напади врз сликата во која се крие податок и извлекување на дигиталниот воден жиг од сликата.

Тестирањата покажаа дека дискретната косинусна трансформација нуди доста добри резултати за криење на податоци во слика. Времето потребно за вметнување, како и извлекување на дигитален воден жиг, е релативно кратко, а сликите се со добар квалитет. Единствен проблем со кој не може да се справи DCT техниката се нападите врз дигиталниот воден жиг. Иако, за разлика од техниките кои работат во

просторен домен, оваа техника е посигурна и поробустна, сепак и таа не е имуна на напади. Тестирањата презентирани во последниот дел покажаа дека каков било напад врз слика со скриен жиг влијае за уништување на дигиталниот воден жиг. Поради актуелноста и применливоста што оваа област ја има, планирано е да се подобри ефикасноста на системот за криење на податоци во слика со DCT, со тоа што ќе се направат тестирања на робустноста и безбедноста и на некои други видови на напади. Во насока на добивање на подобри резултати, ќе се имплементира и тестира и wavelet техниката, за која теоретските факти говорат дека нуди најдобри перформанси во секој поглед.

Користена литература

[1] Jonathan K. Su, FrankHartung, BerndGirod, “DigitalWatermarkingofText, Image, andVideoDocuments”, Telecommunications Laboratory University of Erlangen-Nuremberg Erlangen, Germany, 1998.

[2] Robert L., and T. Shanmugapriya, “A Study on Digital Watermarking Techniques”, International Journal of Recent Trends in Engineering, vol. 1, no. 2, pp. 223-225, 2009.

[3] DarshanaMistry “Comparison of Digital Water Marking methods” (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 09, 2010.

[4] Zheng, D., Liu, Y., Zhao, J., andElSaddik, “A surveyof RST invariantimagewatermarkingalgorithms”. ACMComput. Surv. 39, 2, Article 5 (June 2007).

[5] Cai, L., Du, S.”Rotation, Scale and Translation Invariant Image Watermarking Using Radon Transformand Fourier Transform IEEE 6th CAS Symp. On Emerging Technologies: Mobile and Wireless Communications. Shanghai, China. May 31 - June 2, 2004.

[6] Peter Meerwald and Andreas Uhl, “Survey of wavelet-domain watermarking algorithms”, Proc. SPIE 4314, 505 (2001); doi: 10.1117/12.435434.

[7] PETER MEERWALD, Digital Image Watermarking in the Wavelet Transform Domain, Master'sThesis, Department of Scientific Computing, University of Salzburg, Austria, January 2001.

[8] INGEMAR J. COX, JOE KILIAN, TOM LEIGHTON, TALAL SHAMOON, Secure Spread Spectrum Watermarking for Multimedia, IEEE Transactionson Image Processing, 1995.

[9] J. ZHAO, E. KOCH, Embedding robustlabels into images for copyright protection, Fraunhofer Institute for Computer Graphics, Darmstadt, Germany, 1995.

[10] Bulan, O., Sharma, G., Monga, V., &Oztan, B., “Data Embedding In Hardcopy Images Via Halftone-Dot Orient ation Modulation”, Proc. of SPIE-IS&T ElectronicImaging, SPIE Vol. 6819, 68190C, 2008.

[11] Ismail, I. A. , Shouman, M. A., Hosny, K. M., &AbdelSalam H.M. Invariant Image Watermarking Using Accurate Zernike Moments, Journal of Computer Science 6 (1): 52-59, 2010.

[12] Pravin M. Pithiya and H.L.Desai “DCT Based Digital Image Watermarking, De-watermarking & Authentication”, International Journal of Latest Trends in Engineering and Technology (IJLTET), Vol. 2 Issue 3 May 2013.