Metoda ugradnje robusnog digitalnog vodenog žiga u sliku

Luka Perazić i Đorđe Smiljanić
Mentor: prof. dr Branimir Reljin

***Sadržaj* — U ovom radu predstavljena je metoda ugradnje digitalnog vodenog žiga u sliku (u daljem tekstu *digitalni watermark*, DWM) bazirana na diskretnoj kosinusnoj transformaciji (DCT). Watermarking je tehnika označavanja digitalnih slika, skrivanjem informacija u sliku. Predloženi metod DWM-A bazira na modifikovanju srednjih frekvencija u slici. Eksperimentalni rezultati pokazuju da je metoda otporna na obradu slike kao što su: kropovanje, modifikaciju kontrasta i osvetljaja, JPEG (*Joint Photographic Experts Group*) kompresiju sa gubicima.**

***Ključne reči* — Digitalna obrada slike, diskretna kosinusna transformacija, watermarking.**

I. UVOD

METODA ugradnje digitalnog vodenog žiga (DWM = *digital watermark*) je uz steganografiju jedna od najpoznatijih primena skrivanja informacija (*information hiding*) [1] [2]. Dok se stenografija bavi načinom kako sakriti informaciju, tj. Komunikaciju, u naizgled nebitan sadržaj, metode watermarking-a su se razvile zahvaljujući potrebi za zaštitom autorskih prava [3]. Ubacivanje žiga je postupak umetanja određene tajne informacije (žiga) u originalni dokument. Tajna informacija može biti neka manja slika, tekstualna poruka, potpies, ili pak niz pseudo-slučajnih brojeva. Tajna poruka se može zaštiti ključem tako da samo poznavaoci ključa mogu do nje pristupiti.

Ovakva kombinacija dvaju informacija u slici je moguća jer ljudski vizuelni sisitem prilikom obrade slike odbacuje određene delove informacije. U osnovi, vodeni žigovi iskorišćavaju redundantne podatake u dokumentu sakrivajući tajne informacije unutar njih. Poznavanje svojstava ljudskog vizuelnog sistema je ključno za dizajniranje robusnog vodenog žiga. Poznato je da su niske prostorne frekvencije slike bolje vidljive nego više frekvencije, pa se dodatne informacije pokušavaju staviti u područje viših frekvencija. Zavisno od primene, DWM mora zadovoljiti sledeće osobine [3] [4]:

- da je neuništiv od strane hakera
- da je perceprtualno nevidljiv
- da se statistički ne može detektovati
- da je otporan na kompresiju slike
- da je otporan na različite manipulacije nad signalom

U zavisnosti od osobina, DWM-ovi se dele na vidljive i nevidljive, robusne i lomljive, javne i privatne itd. Primenu DWM-a možemo posmatrati kroz četiri procesa: ubacivanje žiga, distribucija označenog dokumenta, ekstraktovanje žiga iz označenog dokumenta, odluka o valjanosti žiga.

Algoritam ugradnje DWM-a u sliku predstavljen ovim radom dizajniran je da zadovolji sledeće kriterijume:

- otpornost na kropovanje
- otpornost na modifikaciju kontrasta i osvetljaja
- otpornost na filtriranje
- otpornost na JPEG kompresiju sa gubicima

Posebna pažnja posvečena je poslednjem zahtevu. Ljudsko oko je osetljivije na šum i druge artefakte u niskim nego u visokim frekvencijama. Kako god, energija većine prirodnih slika je koncentrisana u oblastima niskih frekvencija. Informacije skrivene u visokim frekvencijama mogu biti lako izgubljene nakon kvantizacionih operacija kao što su one pri JPEG kompresiji sa gubicima. Kako ugradnja DWM-a ne bi napravila uočljive promene na slici i kako bi informacije o DWM-u u originalnoj slici „preživele“ kompresiju, logično rešenje je da se DWM ugrađuje u srednje frekvencije originalne slike.

Osnovna ideja prilikom izrade ovog algoritma bila je u tome da se iskoriste originalne slike u nivou sivog (*grayscale images*) dimenzija 256×256 piksela, u koje se ugrađuje DWM u binarnom paternu (crno-beli) dimenzija 128×128 piksela. Princip algoritma je takav da je potrebno uvek imati sliku koja je po dimenzijama duplo veća od DWM-a koji se ugrađuje. Dakle, u algoritam je moguće ugraditi watermark proizvoljnih dimenzija ali to povlači da dimenzije slike budu duplo veće od dimenzija DWM-a.

U sledećim poglavljima opisane su metode ugradnje i ekstraktovanja („izvlačenja“) DWM-a i prikazani su eksperimentalni rezultati.

II. METODA UGRADNJE

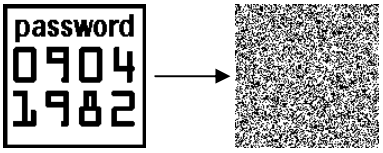
Neka je X originalna slika u skali sivog dimenzija 256×256. DWM, W, je binarna slika (0=crno,1=belo) dimenzija 128×128. Metoda ugradnje se zasniva na manipulaciji koeficijentima srednjih frekvencija dobijenih DCT transformacijom 8×8 blokova originalne slike [4] [5] [6]. Za svaki 8×8 blok originalne slike samo 16

Luka Perazić, Elektrotehnički fakultet u Beogradu, Srbija (telefon: 381-64-1818548; e-mail: lukaperazic@yahoo.com).
Đorđe Smiljanić, Elektrotehnički fakultet u Beogradu, Srbija (telefon: 381-64-4090174; e-mail: djordje.smiljanic@gmail.com).

koeficijenata će biti iskorišćeno za ugradnju DWM-a.

A. Pseudoslučajna i blok permutacija DWM-a

Na samom početku ideja je da se pikseli DWM-a permutuju slučajnim rasporedom čiji ključ samo pošiljalac i primalac znaju. To se radi iz razloga otpornosti na napad kropovanjem kao i radi zaštite (kriptovanja) DWM-a [4]. Dakle, posle ove operacije dobija se matrica DWM-a, W_p, gde crni pikseli ne obrazuju više pravilan natpis već su relativno ravnomerno razbacani po celom prostornom domenu DWM-a (Sl. 1).



Sl. 1. Pseudoslučajna permutacija DWM-a

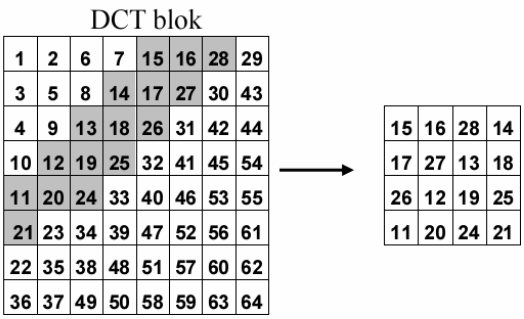
Sledeći korak je blok permutacija pseudoslučajno permutovanog DWM-a u cilju obezbeđivanja perceptualne nevidljivosti nakon ugradnje. Blokove (4×4) pseudoslučajno permutovanog DWM-a permutujemo na osnovu varijansi blokova (8×8) originalne slike, tako da se blok DWM-a koji nose najviše informacija (broj jedinica) postavlja na poziciju (u matrici W_p) koja odgovara poziciji bloka originalne slike sa najvecom varijansom. Označimo sa W_b matricu DWM-a nakon blok permutacije.

B. Generisanje binarne slučajne matrice

Uz pomoć generatora binarnih brojeva, na slučajan način se generiše matrica, S, 128×128 [7]. Nakon toga se vrši operacija EKSKLUZIVNO ILI (XOR) nad matricama S i W_b i dobijamo matricu P. Ovo se praktično radi u svrhu skrivanja matrice watermarka kao dodatni način borbe protiv otkrivanja digitalnog sadržaja istog.

C. DCT transformacija i odabir srednjih frekvencija

Diskretna kosinusna transformacija (DCT) je primenjena na blokove 8×8 piksela [5] [6]. U našem slučaju iz svakog 8×8 bloka DCT koeficijenata izvlači se 16 koeficijenata iz oblasti srednjih frekvencija. Zatim te koeficijente razmeštamo u blokove dimenzija 4×4 tj. blokove dimenzija bloka DWM-a. Znači, odabirom koeficijenata srenjih frekvencija iz slike veličine 256×256 dobijamo redukovanu sliku, Y_r, veličine 128×128 što odgovara veličini DWM-a W. Odabir koeficijenata je prikazan na Sl. 2.



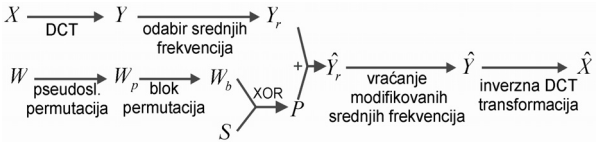
Sl. 2. Odabir srednjih frekvencija

D. Ugradnja DWM-a i inverzna DCT transformacija

Sada je potrebno izvršiti modifikaciju DCT koeficijenata srednjih frekvencija (matrica Y_r) i na taj način 'utisnuti' DWM u srednje frekvencije originalne slike. U tu svrhu izvršićemo prosto sabiranje matrica P i Y_r. Ovim postupkom dobili smo matricu $\hat{Y}_r$ koja predstavlja modifikovanu matricu srednjih frekvencija originalne slike.

Konačno, modifikovane koeficijente matrice $\hat{Y}_r$, vraćamo u originalnu matricu, na mesta srednjih frekvencija, i dobijamo matricu $\hat{Y}$. Matrica $\hat{Y}$ predstavlja DCT transformaciju originalne slike sa ugrađenim DWM-om. Još preostaje da iz matrice $\hat{Y}$ korišćenjem inverzne DCT transformacije rekonstruišemo sliku sa ugrađenim DWM-om. Označimo je sa $\hat{X}$.

Treba prodiskutovati još i to, da u algoritmu u sklopu ovog dela postoji deo koji prepravlja matricu P. Kao što smo rekli matrica P je binarna, dakle sastavljena iz niza nula i jedinica. Deo za ispravku obavlja sledeći proces: tamo gde su jedinice dodaje se PRAG (threshold), T, koji specificira korisnik, a tamo gde su nule oduzima istu vrednost praga. Ova ideja je sprovedena u cilju 'ojačanja' bitova matrice P, jer kada se sada ovako uvećane vrednosti utisnu u srednje frekvencije postaje jasno da će ti delovi slike lakše podneti razne napade. Da ne postoji ovaj deo za ispravku i da se čisto binarna matrica sabira sa matricom Y_r onda bi matrica $\hat{Y}_r$ bila manje imuna na napade jer je razlika među bitovima matrice najviše 1. Na primer sa tresholdom čija je vrednost 10, stvar je nešto drugačija; najveća razlika među bitovoma je 20 (-10, 10), tako da tolika razlika napadom može da bude promenjena, a da se to praktično ne odrazi na promenu u ekstraktovanju DWM-a.



Sl. 3. Metoda ugradnje

III. METODA EKSTRAKTOVANJA

Za ekstraktovanje DWM-a potrebna je originalna slika, ključ koji sadrži informacije o tome kako su raspoređeni pikseli DWM-a pri pseudoslučajnoj i blok permutaciji, i generator slučajnih binarnih brojeva. Metoda ekstraktovanja DWM-a se vrši na način koji je prikazan u narednom izlaganju.

A. DCT transformacija i odabir srednjih frekvencija

Najpre se izvršava DCT transformacija originalne matrice slike i matrice slike sa ugrađenim DWM-om. Nakon izvršenih DCT transformacija potrebno je izdvojiti koeficijente srednjih frekvencija da bi se dobile matrice Y_r i $\hat{Y}_r$. Od matrice $\hat{Y}_r$ se oduzme matrica Y_r, u cilju dobijanja matrice P koja predstavlja binarnu matricu u kojoj se nalazi utisnut DWM. U ovom delu algoritma uveden je i jedan korektivni deo. Naime, prilikom

oduzimanja matrica Y_r i $\hat{Y}_r$ neće se uvek dobiti binarna matrica kao što se očekuje (zbog dodavanja thresholda). To se dešava takođe, zbog toga što je prethodno možda izvršen napad na sliku pa se samim tim menjaju i DCT koeficijenti u matrici $\hat{Y}$. Zato taj korektivni deo omogućava da se matrica P prebaci u binarnu sa što je moguće manjom greškom.

B. Izračunavanje blok permutovane matrice DWM-a

U postupku ugradnje matricu P smo dobili primenom XOR operacije nad matricama W_b i S. Ključ za izračunavanje matrice S poznajemo iz metoda ugradnje. U postupku ekstraktovanja, na osnovu osobine operacije XOR, blok permutovanu matricu W_b izračunavamo primenom operacije XOR nad matricama P i S.

C. Inverzna blok i pseudoslučajna permutacija

Blok permutacija se satojala u tome da su blokovi matrice W_b raspoređeni tako da je blok koji sadrži najveći broj informacija (broj pojavljivanja 1 u bloku) smešten na mesto bloka originalne slike sa najvećom varijansom. Sada se prema ključu koji je sačuvan tokom ugradnje DWM-a blokovi matrice W_b vraćaju na tačno određena mesta i dobija se matrica W_p. Matrica W_p predstavlja permutovane piksele watermarka. Dakle, ostao je samo još jedan korak da se konačno ekstraktuje DWM. Inverznom pseudorandom permutacijom matrice W_p dobijamo DWM W. Ključ za inverznu pseudorandom permutaciju poznat je iz metode ugradnje.

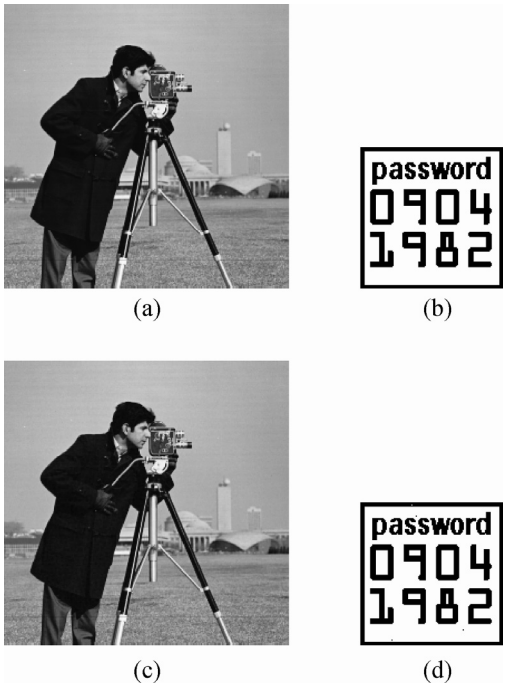
IV. Eksperimentalni rezultati

Naredni primeri pokazuju eksperimentalne rezultate ugradnje i ekstraktovanja DWM-a. Najpre će biti prikazan kvalitet ekstraktovanog DWM-a. Nakon toga posmatraćemo kvalitet ekstraktovanog DWM-a nakon raznih napada na sliku u koju je ugrađen. U tu svrhu posmatraćemo sledeće vrste napada: napad modifikacijom osvetljaja slike, napad modifikacijom kontrasta u slici, redukovanje sadržaja slike (kropovanje), napad JPEG kompresijom sa gubicima (lossy), filtriranje niskih frekvencija (Average, Median filtar, Gauss) i filtriranje visokih frekvencija (izoštravanje slike).

Nakon ekstraktovanja podataka o žigu iz označene slike potrebno je izvršiti analizu tih podataka i potvrditi da li je žig pronađen u dokumentu ili ne. Dobijene podatke iz označene slike potrebno je prema nekoj meri sličnosti uporediti s originalnim žigom. Ako mera pokaže da odstupanje između ekstrakcijom dobijenog žiga i originalnog žiga manja od zadatog praga tada se tvrdi da je dokument zaštićen vodenim žigom. Često korišćena mera sličnosti između originalnog žiga (W) i ekstraktovanog žiga ($\hat{W}$) je [4]:

$$Normalized\ Corelation\ (NC) = \frac{\sum_i \sum_j W(i,j)\hat{W}(i,j)}{\sum_i \sum_j [W(i,j)]^2}$$

A. Prikaz kvaliteta ekstraktovanog DWM-a



(a) (b)

(c) (d)

Sl. 4. (a) originalna slika (b) DWM
(c) slika sa ugrađenim DWM-om sa $T = 2$
(d) ektraktovani DWM sa $NC = 0{,}9997$

B. Napad modifikacijom osvetljaja i kontrasta u slici

(a) (b) (c)

Sl. 5. Ekstraktovani DWM iz slike sa modifikovanim osvetljajem od (a) $k = -30\%$ $NC = 0{,}8658$
(b) $k = +10\%$ $NC = 0{,}9971$
(c) $k = +30\%$ $NC = 0{,}8852$

Tabela 1. Zavisnost kvaliteta ekstraktovanog DWM-a od modifikacije osvetljaja u slici

k[%]	-50	-40	-30	-20	-10	0
NC	0,6931	0,7704	0,8658	0,9593	0,9945	0,9977
k[%]	10	20	30	40	50	60
NC	0,9971	0,9973	0,8815	0,7241	0,5643	0,3204

(a) (b) (c)

Sl. 6. Ekstraktovani DWM iz slike sa modifikovanim kontrastom (a) od $k = +90\%$ $NC = 0{,}8702$
(b) od $k = +130\%$ $NC = 0{,}9379$
(c) od $k = +150\%$ $NC = 0{,}8319$

TABELA 2. ZAVISNOST KVALITETA EKSTRAKTOVANOG DWM-A OD MODIFIKACIJE KONTRASTA U SLICI

k[%]	60	70	80	90	100	110
NC	0,7773	0,8525	0,8711	0,8702	0,9997	0,9977
k[%]	120	130	140	150	160	170
NC	0,9717	0,9379	0,891	0,8319	0,7642	0,7404

C. Redukovanje sadržaja slike (kropovanje)

(a) (b) (c)

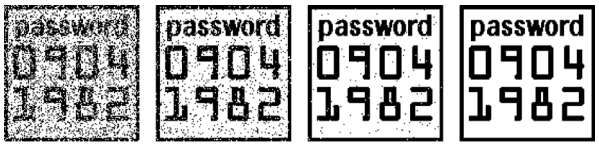
Sl. 7. Ekstraktovani DWM iz kropovane slike
(a) kropovano 25% slike u koju je ugrađen DWM bez pseudoslučajne permutacije
(b) kropovano 25% slike *NC* = 0,8825
(c) kropovano 50% slike *NC* = 0,7554

D. Napad JPEG kompresijom sa gubicima (lossy)

Kompresija generalno redukuje informaciju u slici, što praktično znači da i DWM koji je prethodno ugrađen u sliku takođe trpi promene. Ako je cilj da DWM bude izdržljiv na napade (robusan) onda je od izuzetnog značaja da preživi što veći stepen kompresije. Korišćen je faktor kompresije *FK* (compression ratio) kao mera odnosa nekomprimovane i komprimovane slike :

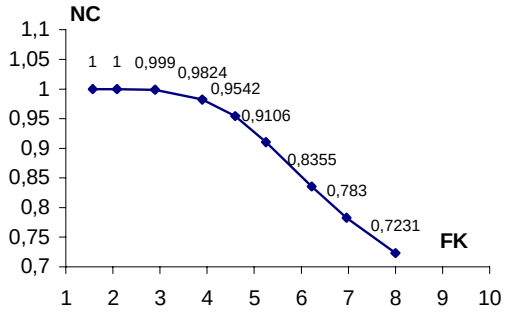
$$FK = \frac{nekomprimovana\ slika\,[KB]}{komprimovana\ slika\,[KB]}$$

Na Sl. 8. je prikazana otpornost DWM-a na JPEG kompresiju sa gubicima. DWM je prethodno ugrađen u sliku sa pragom 10.



(a) (b) (c) (d)

Sl. 8. Otpornost DWM-a na JPEG kompresiju sa gubicima
(a) *FK* = 7 *NC* = 0,7830 (b) *FK* = 4,9 *NC* = 0,9356
(c) *FK* = 3,6 *NC* = 0,9907 (d) *FK* = 2 *NC* = 1

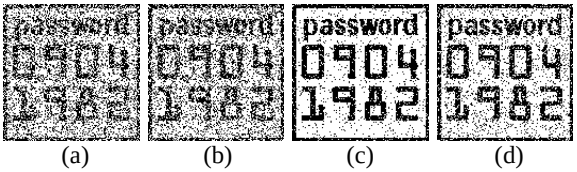


Sl. 9. Zavisnost faktora *NC* od *FK*

Na Sl. 9. je prikazan grafik zavisnosti kvaliteta ekstraktovanog DWM-a (izraženog preko veličine *NC*) od faktora kompresije (*FK*).

E. Otpornost na filtriranje

Na Sl. 10. je prikazana otpornost DWM-a na dejstvo različitih filtara. DWM je ugrađen u sliku sa pragom 10.



(a) (b) (c) (d)

Sl. 10. Otpornost DWM-a na filtriranje slike
(a) Average filtrom *NC* = 0,7409
(b) Medijan filtrom *NC* = 0,7612
(c) Gausovim filtrom *NC* = 0,9433
(d) Unsharp filtrom *NC* = 0,8866

LITERATURA

[1] Niels Provos And Peter Honeyman, *Hide and Seek: An Introduction to Steganography*, University of Michigan. Published by IEEE computer society,2003.

[2] Jonathan Cummins, Patrick Diskin, Samuel Lau and Robert Parlett, "*Steganography and Digital Watermarking*", Copyright © 2004, School of Computer Science, The University of Birmingham.

[3] Digitalna obradba slika: "*Usporedba algoritama označavanja slika digitalnim vodenim žigom*" , Drobac Senka,Keserica Hrvoje,Poljak Tihana,Turudić Tijana, Zavod za elektroničke sustave i obdradbu informacija,Fakultet elektrotehnike i računarstva,Sveučilište u Zagrebu. 2005.

[4] Chiou-Ting Hsu and Ja-Ling Wu, *"Hidden Digital Watermarks In Images*", IEEE Trans. Image Processing, Vol 8, No. 1. Jan. 1999, pp. 58-68.

[5] Rafael C. Gonzalez and Richard E. Woods, *Digital Image Processing*, Prentice-Hall Inc, 2002.

[6] Rafael C. Gonzalez, Richard E. Woods. and Steven L. Eddins, *Digital Immage Processing Using MATLAB®*, Prentice-Hall Inc, 2002.

[7] Navneet Mandhani and Subhash Kak, *Watermarking using decimal sequences*, Department of Electrical and Computer Engineering, Louisiana State University, Baton Rouge, LA 70803, USA. 2005

ABSTRACT

This paper deals with method of embedding robust invisible digital watermarks into images using mid-frequency DCT range. Watermarking is technique for labeling digital pictures by hiding secret information into the images. Our point was to embed a watermark that can survive image processing operations, image cropping and the Joint Photographic Experts Group (JPEG) lossy compression. The experimental results show that proposed algorythm successfully survives all of those operations.

HIDDEN ROBUST DIGITAL WATERMARK IMAGE EMBEDDING METHOD

Luka Perazić i Đorđe Smiljanić