

UNIVERZITET SINGIDUNUM
FAKULTET ZA INFORMATIKU I RAČUNARSTVO

**Primena digitalnih vodenih pečata za
zaštitu dokumenata i skrivanja
informacija**

- Diplomski rad -

Mentor:

Doc. dr Saša Adamović

Student:

Jelena Tašić

Br. indeksa: 2011/202304

Beograd, 2014.



FAKULTET ZA INFORMATIKU I RAČUNARSTVO

UNIVERZITET SINGIDUNUM

FAKULTET ZA INFORMATIKU I RAČUNARSTVO

Beograd, Danijelova 32

Kandidat: Jelena Tašić

Broj indeksa: 2011/202304

Smer: Informatika i računarstvo

Tema: Primena digitalnih vodenih pečata za zaštitu dokumenata i skrivanja informacija

Datum odobrenja rada:
Beograd, __. __. ____.

MENTOR

Doc. dr Saša Adamović

DEKAN

Prof. dr Dragan Cvetković

Primena digitalnih vodenih pečata za zaštitu dokumenata i skrivanja informacija

Sažetak: U radu ćemo se baviti digitalnim vodenim pečatima i algoritmima koji implementiraju različite metode za sakrivanje određenih informacija u originalnom signalu. Paralelno sa razvojem Interneta uvećava se medijski prostor koji podrazumeva stalno uvećanje multimedijalnih sadržaja i novih medija za prenos informacija.

Postojanje i razvoj ove tehnologije u računarskoj nauci i digitalnoj obradi signala, obezbeđuje zaštitu multimedijjskih dokumenata u smislu autorskog prava i zaštite kopiranja, provere autentičnosti signala ili dodavanje određenih informacija vezanih za autora.

Naš cilj je da napravimo aktuelan pregled ove tehnologije koja se bavi vodenim pečatima i da se usmerimo na metode i tehnike u cilju zaštite autorskih prava nad digitalnim fotografijama. Pored teorijskih osnova istraživanja, drugi deo rada predstavlja posebno modelovano simulaciono okruženje na osnovu koga će ovaj rad sadržati i eksperimentalne rezultate.

Ključne reči: Digitalni vodeni pečat, LSB supstitucija, JPEG kompresija, Diskretna kosinusna transformacija (DCT), Diskretna talasna transformacija (DWT), Zaštita autorskih prava, Zaštita od kopiranja, Geometrijska transformacija, Napadi na digitalne vodene pečate

Usage of digital watermarks to protect documents and hiding information

Abstract: In this report, we review digital watermarking and algorithms that deal with various methods for concealing certain information in the original signal. Along with the development of the Internet, also grows the media space that constantly increases multimedia content and introduces new broadcast media.

Existence and development of this technology in computer science and digital signal processing provide protection of multimedia documents in terms of copyrights, justification of a signal, or adding certain information regarding the author.

Our aim is to provide a review of the technology that deals with digital watermarking and to focus on methods and techniques for protection of the copyrights of digital images. In addition to theoretical aspects, the second part of the report includes simulations of the reviewed models and experimental results.

Keywords: Digital watermarking, LSB substitution, JPEG compression, Discrete cosine transform (DCT), Discrete wavelet transform (DWT), Copyright protection, Copy protection, Geometric transformations, Watermarking attacks

SADRŽAJ

1	Uvod	1
1.1	Predmet istraživanja.....	1
1.2	Doprinosi rada	2
1.3	Struktura rada	2
2	Pregled u oblasti istraživanja.....	3
2.1	Istorija digitalnih vodenih pečata	3
2.2	Primena metode srednje vrednosti piksela protiv geometrijskog napada.....	3
2.3	Upotreba robusnih reverzibilnih vodenih pečata protiv geometrijskog napada korišćenjem GTC tehnike primenjene na metode prostornog domena.....	4
2.4	Digitalni vodeni pečat zasnovan na talasnoj transformaciji za kolor slike.....	5
2.4.1	Poređenje sa drugim najnaprednijim algoritmima.....	7
3	Teorijske osnove istraživanja.....	8
3.1	Vrste kompresije slike.....	8
3.2	JPEG kompresija	8
3.3	Transformacije slike	10
3.3.1	Diskretna Furijeova transformacija	11
3.3.2	Diskretna kosinusna transformacija.....	11
3.3.3	Diskretna talasna transformacija.....	12
3.4	Klasifikacija digitalnih vodenih pečata.....	13
3.5	Primena digitalnih vodenih pečata.....	15
4	Algoritmi za označavanje i detekciju digitalnih vodenih pečata	17
4.1	Savremena steganografija	17
4.2	Algoritmi za označavanje i detekciju digitalnih vodenih pečata.....	18
4.3	Izmena najmanje značajnih bitova (LSB supstitucija)	19
4.3.1	Slika u slici	20 -
4.4	Tehnika kodovanja proširenim spektrom.....	21
4.5	Ostali poznati algoritmi.....	22
4.5.1	Cox-ov algoritam.....	23
4.5.2	Algoritam Corvi.....	23 -
4.5.3	Algoritam Xia.....	24
4.6	Tehnike za korekciju slike	24
4.7	Kvantizacija.....	25
5	Napadi na digitalne vodene pečate i njihova sigurnost	26
5.1	Vrste napada.....	27
5.2	Geometrijske transformacije	28
5.3	Operacije za poboljšanje kvaliteta slike.....	30
5.4	Otpornost digitalnih vodenih pečata na napade.....	33
6	Eksperimentalno okruženje - CrypTool.....	35
6.1	Skrivanje tajnih podataka primenom LSB supstitucije.....	35
7	Zaključak.....	37
	Literatura	38

1 Uvod

Zaštita podataka danas je veliki problem, s obzirom da svako sa malo znanja i iskustva, može doći do privatnih podataka. To znači da se podaci mogu veoma lako menjati, falsifikovati ili zloupotrebiti. Sa razvojem tehnologije raste i problem zaštite podataka, jer su na Internetu privatni podaci svima dostupni. Ovo predstavlja ozbiljan problem i postavlja se pitanje njegovog rešavanja.

Relativno jednostavno i efikasno rešenje ovog problema je primena digitalnog vodenog pečata. Utiskivanjem digitalnog vodenog pečata u audio i video zapis, ili digitalnu sliku, sačuvaće se autentičnost podataka i omogućiti vlasniku praćenje bilo kakvih promena.

Digitalni vodeni pečat se koristi za zaštitu autorskih prava, za zaštitu od kopiranja, za autentifikaciju, proveru integriteta, upravljanje digitalnim pravima, protiv falsifikovanja, kao i u medicini.

U ovom radu biće dat pregled vrsta digitalnih vodenih pečata, njihova primena, algoritmi za utiskivanje, vrste napada, kao i zaštita od napada na digitalne vodene pečate. Takođe, u drugom delu rada biće dato praktično rešenje i prikaz tehnike za utiskivanje digitalnog vodenog pečata u sliku primenom CrypTool-a.

1.1 Predmet istraživanja

Prilikom prelaska iz analognog u digitalni domen, pojavio se problem nemogućnosti razlikovanja originalnog dokumenta od kopije, što je otežalo zaštitu autorskih prava i vlasništva. Tako je nastala tehnika za digitalno označavanje podataka koja se bavi ubacivanjem digitalnog vodenog pečata (engl. *Digital watermarking*) u digitalni dokument sa mogućnošću kasnijeg detektovanja ili ponovnog uzimanja pečata.

Tehnika digitalnog vodenog pečata potiče od imena vodenih pečata papira kao mere bezbednosti, u koji bi vlasnik dokumenta zapečatio svoj logo u dokument. Digitalni vodeni pečat se primenjuje na digitalni audio i video zapis, slike, dokumenta, mape i računarske programe, a naročito se koristi za zaštitu autorskih prava, u medicini i vojsci.

Digitalni vodeni pečat štiti digitalna dokumenta od neovlašćenog korišćenja i distribucije. Ova metoda ipak ne sprečava kopiranje, već ugrađuje skrivene informacije u vidu pečata, koje postaju nerazdvojne sa zaštićenim dokumentom, čak i nakon njegovog kopiranja i ponovne distribucije.

Skrivene informacije se ugrađuju u dokument da bi se osigurala bezbednost, autentifikacija podataka, indentifikacija vlasnika i zaštita od nezakonitog kopiranja. Kod slika, skrivena informacija može biti takođe u vidu slike (npr. logo vlasnika ili kompanije, noseće informacije o autorskim pravima), ili u vidu grupe bitova koji se šire oko slike prema određenom algoritmu.

Da bi vodeni pečat bio jak, mora se primeniti dobra tehnika utiskivanja vodenog pečata. Postoje mnogi algoritmi digitalnog vodenog pečata koji služe za zaštitu autorskih prava digitalnih slika i proveru integriteta podataka. Kod većine algoritama obavlja se transformacija slike originala u domenu koji omogućuje utiskivanje otpornih i nevidljivih digitalnih vodenih pečata.

1.2 Doprinosi rada

U radu je obrađen istraživački deo, kao i eksperimentalni rezultati u posebno modelovanom simulacionom okruženju. Takođe, dat je detaljan pregled algoritama koji se koriste za utiskivanje digitalnih vodenih pečata, kao i vrste napada na digitalne vodene pečate.

Osim navedenih vrsta napada, u radu su teorijski obrađene performanse digitalnog vodenog pečata otpornog na napade.

1.3 Struktura rada

Struktura ovog rada biće ukratko objašnjena u sledećem tekstu.

U drugom poglavlju, biće data istorija digitalnih vodenih pečata i teorijska osnova istraživanja. U sklopu teorijske osnove istraživanja biće prikazana primena metode srednje vrednosti piksela i upotreba robusnih reverzibilnih vodenih pečata protiv geometrijskih napada. Takođe, biće prikazani i digitalni vodeni pečati zasnovani na talasnoj transformaciji za kolor slike, kao i poređenje sa drugim najnaprednijim algoritmima.

U trećem poglavlju biće data podela i detaljno objašnjenje kompresije i transformacije slike. Nakon toga biće prikazana podela digitalnih vodenih pečata, kao i detaljno objašnjenje gde se koji pečat primenjuje.

U četvrtom poglavlju pričaćemo o algoritmima za označavanje i detekciju digitalnih vodenih pečata. Pomenućemo LSB supstituciju, tehnike na bazi korelacije, kodovanje proširenim spektrom, aditivne vodene pečate, kao i mnoge druge poznate tehnike koje se koriste za utiskivanje digitalnog vodenog pečata.

U petom poglavlju imaćemo detaljnu podelu napada na digitalne vodene pečate. Pomenućemo i geometrijsku transformaciju, modifikaciju histograma, gama korekciju i više vrsta filtriranja, tehnike koje, osim što se koriste za poboljšanje kvaliteta slike, veoma često se primenjuju i kao tehnike za napade. Osim vrsta napada, spomenućemo i kakav pečat mora da bude da bi preživeo napad.

U šestom poglavlju, biće prikazana detaljna analiza utiskivanja digitalnog vodenog pečata. Kao pečat ćemo koristiti tekst (tajnu poruku) koju ćemo utisnuti u sliku (nosilac poruke), a nakon toga ćemo iz stego podatka izdvojiti tu istu tajnu poruku.

U sedmom poglavlju biće prikazana konačna analiza našeg rada i zaključak, kao i predlog na čemu bi moglo da se poradi u daljoj budućnosti.

2 Pregled u oblasti istraživanja

2.1 Istorija digitalnih vodenih pečata

Istorija digitalnih vodenih pečata datira od 1954 godine. Digitalni vodeni pečati su patentirani u Americi, od strane Emil Hembrooke (Muzac Corporation), pod nazivom „Identifikacija zvuka i sličnih signala“, u kojem je opisan metod za neprimetno ugrađivanje identifikacionog koda u muziku, radi dokazivanja vlasništva (Kundur i Hatzinakos, 1997; Xia et al., 1997; i Bartolini et al., 1998). Istraživanje na vodenim pečatima bilo je zanemareno sve do 1990 godine. U periodu od 1990. do 2000. godine pojavljuje se prilično veliko interesovanje za digitalne vodene pečate, koje je dalo značajan doprinos u različitim tehnikama. Značajan napredak donelo je istaživanje o digitalnim vodenim pečatima (Schyndel et al., 1994; Pitas, 1996; Cox et al., 1997; Kundur i Hatzinakos, 1997; Xia et al., 1997; Bartolini et al., 1998; Bas et al., 1998; Craver et al., 1998; Delaigle et al., 1998; i Hernandez et al., 2000). Ovo istraživanje objašnjava postupak zaštite slike pomoću vodenog pečata, sa ciljem zaštite autorskog prava. Različite tehnike, kao što su umetanje Diskretne kosinusne transformacije (**DCT**), Diskretne talasne transformacije (**DWT**), Diskretne Furijeove transformacije (**DFT**), LSB supstitucije (engl. *Least Significant Bit*) i **CDMA** (engl. *Code Division Multiple Access*), razvijale su se od 2000. do 2010. godine. Do tada najviše se radilo na maksimalnom odnosu signal/šum (engl. *Peak Signal to Noise Ratio*, **PSNR**). Tokom ovog vremena postignut je razvoj reverzibilnih vodenih pečata. Za primenu u medicini postignuta je maksimalna sličnost između originalne i obnovljene slike (slika iz koje je izvučen vodeni pečat). Robusni reverzibilni vodeni pečati sa geometrijskim napadom će se usavršiti u daljoj budućnosti.

2.2 Primena metode srednje vrednosti piksela protiv geometrijskog napada

U radu „Primena metode srednje vrednosti piksela protiv geometrijskog napada za robusne semi-reverzibilne vodene pečate“ (R. Kanphade i N. Narawade, 2013) je izložena nova metoda digitalnih vodenih pečata koja primenjuje tehniku srednje vrednosti piksela, a koristi se u vojsci i za zaštitu autorskih prava. Potpuni oporavak vodenog pečata nije moguć, ali ova metoda omogućuje njegov oporavak sa kompromisom u kvalitetu. Izložena metoda srednje vrednosti je robusna i polu-reverzibilna. Izabran je najniži nivo piksela da bi se dobila glatkoća originalnog izgleda i bolja vizualna percepcija. Kombinacija sa unapređenom geometrijskom transformacijom i predznanje geometrijskih transformacija rezultira u robusnosti protiv geometrijskih napada. Rezultati simulacije pokazuju da je predloženi metod vodenih pečata, osim što je polu-reverzibilan, veoma robusan protiv različitih vrsta napada kao što su rotacija, skaliranje i translacija. Takođe, ograničen je kvalitet slike sa vodenim pečatom, kapacitet utiskivanja je optimalan i složenost je manja [5].

LSB supstitucija daje bolji kvalitet slike sa vodenim pečatom, ali nije robusna na geometriske napade. DCT metoda omogućuje ograničen kvalitet i robustnost, dok CDMA metoda daje slab kvalitet i prihvatljivu robustnost na napad. DWT metoda, takođe, daje slab kvalitet slike sa vodenim pečatom i malu robustnost. Ove metode daju umeren kvalitet slike sa vodenim pečatom i izgladuju sliku. Bitovi su direktno ubačeni u LSB skrivene slike. LSB metoda supstitucije daje veći PSNR u poređenju sa drugim metodama. Kod drugih metoda slika je prvo transformisana u drugi domen.

Takođe, ponuđene metode vodenog pečata su pogodnije za primenu u medicini jer daju bolji kvalitet za snimke u medicini, ali daju lošiji kvalitet za crtane slike. Metoda je polu-reverzibilna, a postignuta je 100% sličnost obnovljenog vodenog pečata sa originalnim vodenim pečatom. Perceptualno, postignut je veoma dobar kvalitet. Praktični rezultati pokazuju da je predložena metoda vodenog pečata jednostavna. Slika ima kvalitetnu vizuelnu percepciju i tehnički je usavršena.

2.3 Upotreba robusnih reverzibilnih vodenih pečata protiv geometrijskog napada korišćenjem GTC tehnike primenjene na metode prostornog domena

Tian (2003) je predstavio reverzibilne vodene pečate kako bi dobio veoma dobar kapacitet utiskivanja. Koristio je dve tehnike: nejednaku ekspanziju i LSB utiskivanje. Alattar (Narawade i Kanphade, 2011b) je izveo nejednaku ekspanziju transformisanu za „tri“ i proširio Tian-ov algoritam kako bi utiskivao dva bita u svaka tri piksela. Coltuc i Chassery (2007) su razvili jednostavnu i efikasnu reverzibilnu skrivenu šemu zasnovanu na RCM algoritmu (engl. *Reverse Cuthill - McKee algorithm*), za koji ne treba mapa lokacija da bi se obnovila originalna slika. Međutim, njihova šema ne može potpuno da kontroliše poziciju gde je informacija utisnuta, pa je kvalitet stego slike loš. Kanphade i Narawade (2012) razvili su dupli RCM algoritam koji smanjuje celu funkciju u algoritmu Coltuc i Chassery (2007). Na račun kvaliteta, Tzu-Chuen i Li-Ling Hsu (2008) uklonili su ove nedostatke i predstavili novi oblik RCM algoritma. Metoda pomeranja histograma je jedna od najboljih metoda u oblasti reverzibilnih vodenih pečata.

Hong et al. (2010) je modifikovao ovu metodu i predstavio brži metod. Xiangli i Xuefang (2010) predstavili su „Reverzibilni nula-bit vodeni pečat zasnovan na haotičnom šifrovanju“ koji daje više sigurnosti za vodeni pečat. Yang et al. (2010) je predstavio „Reverzibilni vodeni pečat primenom metode podešavanja koeficijenata“. Ali et al. (2011) je predstavio „Višeslojno pečatiranje videa primenom standarda H.264/AVC, korišćenjem nejednake ekspanzije na IPCM (engl. *Intra Pulse Code Modulation*) blokove“. Oni su primenili nejednaku ekspanziju na video. Huang i Fang (2011) predstavili su „Histogram zasnovan na reverzibilnim skrivenim podacima za medicinske snimke“. Narawade i Kanphade (2011a) razvili su novu tehniku pomeranja histograma koja omogućuje kvalitet i kapacitet utiskivanja reverzibilnih vodenih pečata. Awrangzeb et al. (2006) je prezentovao „Metodu korekcije geometrijske distorzije“ koja nam pokazuje kako da prepoznamo geometrijski napad. U tehnici pomeranja histograma Hong et al. (2010) utiskuje podatke pomeranjem histogramskih binova. Ovaj metod konstruiše sliku histograma iz originalne slike kao bi dobio par vrhova i nultu tačku. Podaci su utisnuti pomeranjem histogramskih binova.

U radu, „Upotreba robusnih reverzibilnih vodenih pečata protiv geometrijskog napada korišćenjem GTC tehnike primenjene na metode prostornog domena“ (Rajendra D. Kanphade i N. S. Narawade, 2013), je izloženo poništavanje geometrijskog napada uz korišćenje GTC tehnike. Razvijanjem ove tehnike postignut je bolji PSNR i kapacitet utiskivanja u poređenju sa postojećim tehnikama. Takođe je dato poređenje metoda pomeranja histograma, reverzibilne metode kontrastnog mapiranja, metode nejednake ekspanzije primenjenih na robustne vodene pečate protiv geometrijskog napada.

Eksperimentalni rezultati pokazuju da metoda pomeranja histograma ima bolji PSNR, dok je metoda nejednake ekspanzije bolja u kapacitetu utiskivanja. Metode su primenjivane na slikama visokog i niskog kvaliteta, i pokazalo se da su sve metode pogodne za slike visokog kvaliteta. Samo je metoda pomeranja histograma pogodnija za medicinske snimke i dijagrame [7].

U radu je napravljeno poređenje metode pomeranja histograma, metode nejednake ekspanzije i reverzibilne metode kontrastnog mapiranja. Za vreme ekstrakcije, kombinacije svih ovih metoda sa GTC će stvoriti robustni reverzibilni vodeni pečat protiv geometrijskog napada.

Kada je slika napadnuta sa geometrijskim napadom kao što je rotacija, skaliranje i translacija, menjaju se vrednosti piksela. Kombinacijom metode (Rajendra D. Kanphade i N. S. Narawade, 2013) sa GTC metodom može se prepoznati geometrijski napad (Yang et al., 2010). Neutralizacija geometrijskog napada koriguje napadnutu sliku, a zatim koristi obrnuti proces za oporavak slike i vodenog pečata.

2.4 Digitalni vodeni pečat zasnovan na talasnoj transformaciji za kolor slike

Mnogi planovi vodenih pečata predstavljeni su za digitalne slike u prostornom domenu i domenu transformacione tehnike (Bender et al., 1996; Banf et al., 2002; Ganic i Eskicioglu, 2004; i Guangmin, 2007). Prostorne tehnike prilagođavaju manje značajne bitove piksela slike i tako garantuju neprimetnost. Spektralne ili transformacione tehnike pripajaju vodeni pečat i transformacione koeficijente jedne slike. Algoritmi zasnovani na transformacijama omogućuju da se vodeni pečat lako smesti u perceptualno značajan deo slike. Ovo stvara pečat koji je više robustan na napad, pošto se teško može ukloniti bez izobličenja slike (Hartung i Kutter, 1999; Kong et al., 2003; i Guangmin, 2007). Poznate transformacije uključuju DCT i DWT. Postoje različiti planovi za utiskivanje digitalnog vodenog pečata u crno-bele slike (Guangmin, 2007; i Vikas, 2007). Međutim, samo utiskivanje vodenog pečata u kolor sliku nije dovoljno.

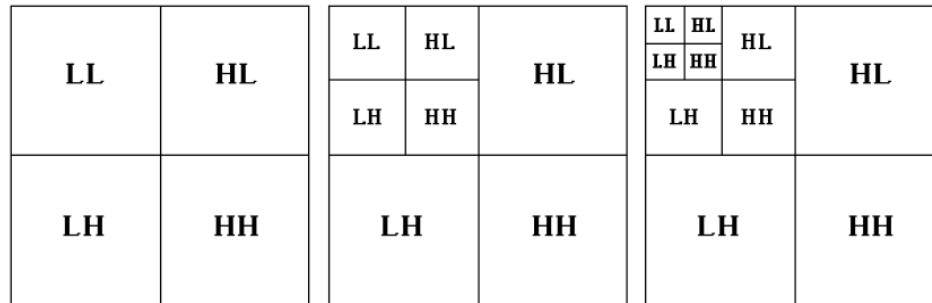
Od tri kanala (crveni, zeleni i plavi), crveni kanal je najrobustniji protiv JPEG kompresionog napada, dok je plavi najmanje. Međutim, skrivene informacije vodenog pečata su mnogo sigurnije u crvenom nego u plavom kanalu. Guangmin (2007) predlaže plan za digitalni vodeni pečat kolor slike baziran na DWT, koja transformiše kolor sliku u YIQ model, i utiskuje vodeni pečat u Y i Q komponente (Hartung i Kutter, 1999). Mei et al. (2001) predstavlja plan za skrivanje vodenog pečata u koeficijente niske frekvencije 8x8 DCT blokova crvenog, zelenog i plavog kanala (Kong et al., 2003). Banf et al., (2002) predlaže šemu u kojoj su crveni, zeleni i plavi kanali transformisani celim ramom DCT, i selektuje koeficijente niske frekvencije da sakrije vodeni pečat (Kundur i Hatzinakos, 1999).

I pored mnogo istraživanja urađenih u DCT, danas planovi bazirani na DWT imaju sve veću popularnost. DWT ima dosta prednosti nad DCT (Lee i Lee, 2005). Talasno kodovana slika je multi-rezolucioni opis slike. Dakle, jedna slika može biti prikazana sa različitim nivoima rezolucije i može biti sekvencijalno obrađena od niske do visoke rezolucije. Talasna transformacija je mnogo bliža HVS nego DCT. Vizuelni efekat talasno kodovane slike je manje jasan u poređenju sa DCT, jer talasna transformacija ne rastavlja sliku na blokove da bi je obradila.

U odnosima visoke kompresije, blokovni efekat je uočljiv u DCT, međutim u talasno kodovanim slikama je mnogo jasniji. DFT i DCT su transformacije punog rama i zato bilo kakva promena u koeficijentima transformacije utiče na celu sliku, izuzev ako je DCT upotrebljena korišćenjem blokovnog pristupa.

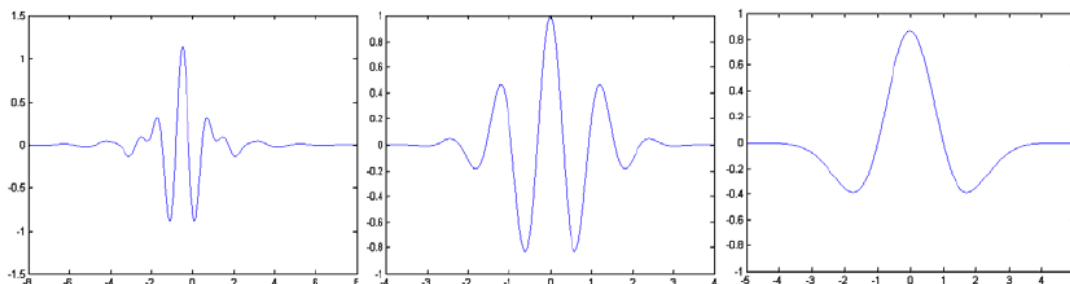
Utiskivanje signala sa DWT koja ima prostorno frekventnu poziciju, imaće lokalni uticaj na sliku (Mei et al., 2001; Meerwald i Uhl, 2001; i Liu et al. 2005). Talasna transformacija omogućuje frekventni i prostorni opis slike. Ponekad utiskivanje u HL i LH podopseg je otporno na izjednačavanje histograma i napad gama korekcijom (Polikar, 2001). Zato su algoritmi vodenog pečata zasnovani na DWT postali važna oblast istraživanja (Stollnitz, et al., 1995; Saraju, 1999; Reza et al., 2004; Raviraj i Sanavullah, 2007).

Kada primenimo DWT na 2D sliku, slika se deli na 4 jednaka kvadrata. LL opseg sadrži aproksimacije, a svi drugi opsezi sadrže detalje, horizontalna komponenta (HL), vertikalna komponenta (LH) i dijagonalna komponenta (HH). Možemo ponoviti proces da računa talasnu dekompoziciju u više nivoa, kao na slici 2.4.1, gde je prikazano piramidno razlaganje u 3 nivoa.



Slika 2.4.1: Piramidalno razlaganje talasa na jedan, dva i tri nivoa

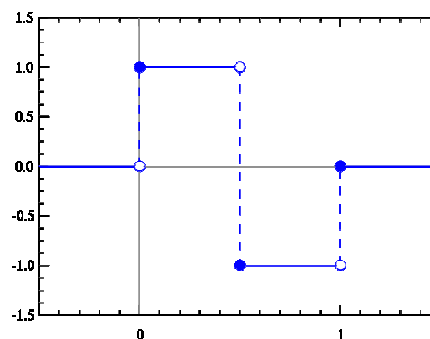
Postoje i druge talasne transformacije kao Meyer, Morlet i Mexican Hat talasi. Nedostatak ovih transformacija je mnogo veća cena proračuna od Harovih talasa.



Slika 2.4.2: Meyer, Morlet i Mexican hat talasi

Harov talas je najjednostavniji talas. Uveo ga je Alfred Haar (1909). Možemo ga opisati kao skok funkciju $f(x)$ sa:

$$f(x) = \begin{cases} 1 & 0 \leq x < 1/2, \\ -1 & 1/2 \leq x < 1, \\ 0 & \text{izvan ovih intervala} \end{cases}$$



Slika 2.4.3: Harov talas

Harova talasna transformacija ima brojne prednosti jer je jednostavna i brza (Vikas, 2007a), reverzibilna je bez efekta ivica, što je problem kod drugih talasnih transformacija. Osnovna mana Harovog talasa je da on nije neprekidan, pa zato ni diferencijabilan.

2.4.1 Poređenje sa drugim najnaprednijim algoritmima

Mnogi od planova vodenog pečata baziranih na DWT postižu robustnost na račun kvaliteta skrivene slike. Algoritam baziran na CDMA u velikoj meri pokriva sliku, ali obnavljanje slike je veoma robustno.

Sa druge strane, algoritam vodenog pečata baziran na filtriranju podopsega Shih-Chang et al. (2004), učinio je da vodeni pečat u slici bude neprimetan, ali istovremeno otkriva vodeni pečat za odnos kompresije 10-11.

U radu „Vodeni pečat zasnovan na talasnoj transformaciji za kolor slike“ (Mohit Gupta, Deep Tarun Gupta i Vikas Saxena, 2013) upoređeni su rezultati klasičnog algoritma baziranog na CDMA (Vikas, 2007b) i algoritma baziranog na filtriranju podopsega Shih-Chang et al. (2004). Vikas (2007b) otkriva uspešno vodeni pečat do JPEG kvaliteta faktora $Q=10$. Prednost ovog algoritma zasnovanog na CDMA šemi je što mu treba znatno manje vremena za utiskivanje i obnavljanje vodenog pečata. Predloženi algoritam ne utiče na kvalitet skrivene slike u poređenju sa algoritmom baziranim na CDMA. U poređenju sa algoritmom baziranim na filtriranju podopsega datog od Shih-Chang et al. (2004), predloženi algoritam obnavlja podatke vodenog pečata do nivoa kompresije 4 [6].

3 Teorijske osnove istraživanja

3.1 Vrste kompresije slike

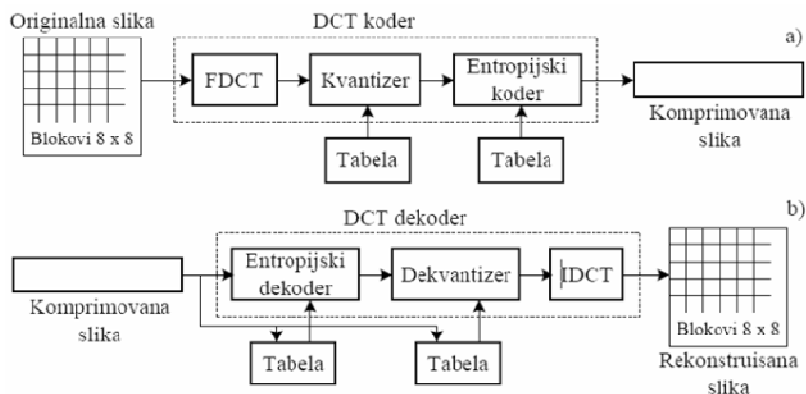
Postoje dve vrste kompresije:

1. **Kompresija bez gubitaka** (engl. *Lossless compression*) smanjuje originalnu veličinu slike upotrebom različitih algoritama. Nakon toga je moguće takvu sliku dekompresovati i vratiti u originalno stanje. Kod ove kompresije ne može se postići značajno smanjenje broja bitova. Takođe, kvalitet slike se neće bitno smanjiti. Kompresija bez gubitaka se zasniva na statistici podataka. Koristi se u medicini za kompresiju različitih snimaka kod kojih bi svaki gubitak mogao dovesti do neupotrebljivosti i netačnosti. Koristi se i za kompresiju multimedijalnih podataka za maksimalni kvalitet. Pravi predstavnik kompresije bez gubitaka su .zip i .rar kompresija. Kompresija bez gubitaka ima vrlo ograničene mogućnosti, pa se zbog toga češće koristi kompresija sa gubicima. Stepen kompresije je ograničen i iznosi od 1:2 do 1:8.
2. **Kompresija sa gubicima** (engl. *Lossy compression*) takođe smanjuje originalnu veličinu slike, ali to radi na račun kvaliteta slike. U poređenju sa kompresijom bez gubitaka, kompresijom sa gubicima postižu se znatno veće uštede u prostoru. Tu se pre svega koriste osobine ljudskog oka koje nekim informacijama pridaje veći značaj nego drugim. Odbacujući vizuelno manje važnu informaciju, podaci mogu biti komprimovani znatno intenzivnije. Stepen kompresije iznosi od 2 do 100. Slika rekonstruisana posle kompresije sa gubicima ima oštećenja u odnosu na original, ali pod normalnim uslovima gledanja ta oštećenja nisu primetna. Takvu sliku je nemoguće vratiti u originalno stanje jer su neki njeni delovi trajno uklonjeni. Koristi se kod audio i video zapisa, računarske grafike i skeniranih slika. Metode kompresije sa gubicima mogu se podeliti u nekoliko grupa: Redukovanje prostora boja, Chroma subsampling, Transform coding i Kompresija fraktalima. U praksi se često neke od ovih metoda kombinuju. Pravi predstavnik kompresije sa gubicima jeste JPEG kompresija. JPEG kompresija za sliku u boji obuhvata u sebi dve metode: chroma subsampling i transform coding. Za kompresiju podataka može se koristiti bilo koji algoritam.

3.2 JPEG kompresija

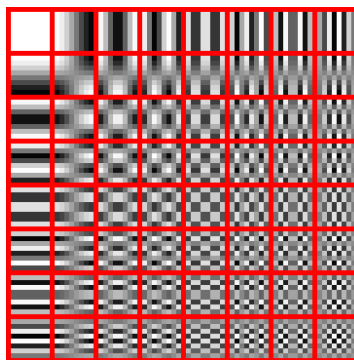
JPEG (engl. *Joint Photographic Experts Group*) kompresija je vrsta napada na digitalne vodene pečate i trenutno jedan od najraširenijih formata zapisa slika. JPEG je kompresovani format fajlova slika sa gubicima, izveden iz bitmape.

Ovaj format najbolje komprimuje fotografije u punoj boji, dok se slabije pokazuje kod slika u nijansama sive. JPEG format može da prikaže svih 16,7 miliona boja. Ovo je doprinelo tome da JPEG postane najpopularniji format za prikazivanje realističkih slika. Najslabiji je kod jednostavnih crteža sa ostrim ivicama, gde se i pri manjem intenzitetu kompresije pojavljuju vidljivi defekti. Što je viši nivo kompresije, fajlovi će biti manji, a oštećenja slike veća. Da bi stavili što veću količinu podataka u sliku, možemo pre ubacivanja podataka, da te iste podatke kompresujemo i tako smanjimo njihovu veličinu, a ujedno povećamo prostor za skladištenje podataka unutar slike.



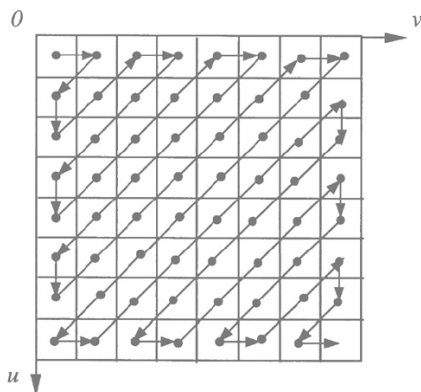
Slika 3.2.1: Blok šema JPEG sistema za kompresiju slike: (a) koder, (b) dekode

Svaka komponenta slike (Y, Cb, Cr) deli se u blokove od po 8×8 piksela. Zatim se svaki blok konvertuje u prostor frekvencije koristeći dvodimenzionu Diskretnu kosinusnu transformaciju (DCT). Cilj je pronaći blok gde bi promena vrednosti piksela bila najmanja. Ako je vrednost prevelika, blok se deli na 8×8 podblokova, sve dok vrednost ne bude dovoljno niska. Ako dimenzije slike nisu multipli broja 8, onda se nekompletni blokovi (u desnom, donjem delu slike) prethodno dopunjavaju „lažnim“ podacima (crnim pikselima ili ponavljanjem piksela sa ivice slike). Svaki 8×8 blok, ili podblok, je transformisan u 64 DCT koeficijenta koji su približni osvetljenju (svetlosti, tami i kontrastu) i signalu boje tog dela slike.



Slika 3.2.2: Osnovni talasni oblici 8×8 DCT transformacije

Kvantizovane komponente slike uređuju se u cik-cak redosled (slika 3.2.3), čime se dodatno grupišu slične frekvencije i povećavaju dužine sekvenci nula, a zatim se koristi Hafmenovo kodiranje tako uređenog niza. JPEG standard dozvoljava i korišćenje aritmetičkog kodiranja umesto Hafmenovog. Aritmetičko kodiranje je matematički superiornije od Hafmenovog, ali se retko koristi zato što je pokriveno patentima, kodiranje i dekodiranje je dosta sporije, a fajlovi su nešto manji (za oko 5%) [12].



Slika 3.2.3: Cik-cak očitavanje DCT koeficijenata

Rezultujuća mera kompresije može se menjati u skladu sa izborom delilaca korišćenih pri kvantizaciji. Kompresija 10:1 obično rezultuje u slici koju ljudsko oko ne može da razlikuje od originala, dok će kompresija od 100:1, imati uočljive blokovske artefakte. Ovi kompresioni artefakti pojavljuju se zbog koraka kvantizacije JPEG algoritma.

JPEG se generalno smatra lošim formatom za komprimovanje, jer je slika obnovljena iz kompresije blizu originalnoj slici, ali nije i identična. Oštećenja su trajna, a gubici se akumuliraju prilikom višestrukog uređivanja slike.

U 2000. godini donesen je novi standard JPEG 2000, koji se bazira na primeni Diskretne talasne transformacije (DWT). Slika se razlaže u tri slike u nijansama sive, koje se zatim zasebno komprimuju. Nakon komprimovanja, svaka slika se deli u pločice, koje se zatim transformišu i kodiraju zasebno. Sve pločice imaju istu veličinu. Takođe je moguće da se cela slika tretira kao jedinstvena pločica. Na pločice se zatim primenjuje DWT do proizvoljne dubine, i nakon toga kodiranje. JPEG 2000 koristi dve različite transformacije talasima, a to su: CDF 9/7 transformacija, koja uvodi kvantizacioni šum, i CDF 5/3 transformacija, koja koristi samo celobrojne koeficijente (korak kvantizacije je 1) [14].

JPEG 2000 omogućuje bolji kvalitet slike pri vrlo niskim brzinama prenosa i daje veću fleksibilnost u multimedijalnim prenosima. Primenjuje se u oblastima u kojima JPEG standard nije dao zadovoljavajuće rezultate. Područja primene su medicinske slike, satelitske slike, Internet, mobilna telefonija, e-poslovanje, digitalne arhive, pretraživanja slike, senzori, faks u boji itd.

3.3 Transformacije slike

Transformacija je najvažniji deo kompresije sa gubicima. Kod transformacije podaci slike preslikavaju se iz prostornog domena u domen transformacije i pritom se čuva energija slike. Uglavnom su unitarne i ortogonalne.

Raspodela energije je veoma važna kod kompresije slike. Poželjno je koristiti takvu transformaciju koja, za određenu klasu slika, raspodeli maksimalnu količinu energije u što manji broj koeficijenata. Kod ortogonalnih transformacija veliki deo srednje energije se raspodeljuje u svega nekoliko koeficijenata, dok ostali koeficijenti sadrže mali deo energije. U domenu transformacije energija je skoncentrisana na sasvim malom broju koeficijenata.

Postoje sledeće transformacije:

- Diskretna unitarna transformacija,
- Diskretna Furijeova transformacija (**DFT**),
- Diskretna kosinusna transformacija (**DCT**),
- Diskretna sinusna transformacija (**DST**),
- Diskretna talasna transformacija (**DWT**),
- Diskretna Hartlijeva transformacija (**DHT**),
- Diskretna Volš-Adamarova transformacija (**WHT**),
- Diskretna Harova transformacija,
- Diskretna slant transformacija i
- KL (optimalna) transformacija (**KLT**).

Najpoznatija transformacija je DFT. DCT, DFT i WHT, koriste matricu transformacije koja zavisi od dimenzija slike, ali ne i od same slike. Ipak, najbolje rezultate u kompresiji daje KLT, ali je ujedno i najkomplicovanija za korišćenje, jer zahteva da se matrica transformacije računa za svaku sliku posebno. Od svih navedenih transformacija, DCT je najbližnja KLT.

3.3.1 Diskretna Furijeova transformacija

Diskretna Furijeova transformacija je jedna od Furijeovih transformacija često korišćena u algoritmima za digitalnu obradu signala. Njene modifikacije su primenjene kod JPEG kompresije slike, kao i u drugim oblastima vezanim za analizu diskretnih signala (npr. digitalizovani analogni signal). DFT zahteva kao ulaz diskretnu funkciju. Takve funkcije se često dobijaju uzorkovanjem (semplovanjem) kontinualne funkcije. DFT pomaže u rešavanju diferencijalnih jednačina i operacija kao što je konvolucija.

Ova transformacija je robustna protiv geometrijskih napada, kao što su rotacija, skaliranje, odrezivanje, translacija itd. Može se koristiti za oporavak od geometrijske distorzije. Nedostaci su kompleksna implementacija i visoka cena. Postoji i multidimenzionalna DFT.

3.3.2 Diskretna kosinusna transformacija

Diskretna kosinusna transformacija je nastala iz Furijeove transformacije. Njen zadatak je da signal iz vremenskog domena prebaci u frekvencijski domen. Pomoću ove transformacije vrednosti elemenata slike se pretvaraju u koeficijente koji se dalje lakše mogu podvrgnuti postupku kompresije. DCT ne vrši kompresiju, već se samo pomoću nje izvorni elementi slike pretvaraju u oblik iz kojeg je moguće jasno odrediti redundansu. Dakle, DCT vrši razlaganje proizvoljnog diskretnog signala u sinusoidalne komponente različitih učestanosti, koje pokazuju koliko brzo se menja sjajnost ili boja.

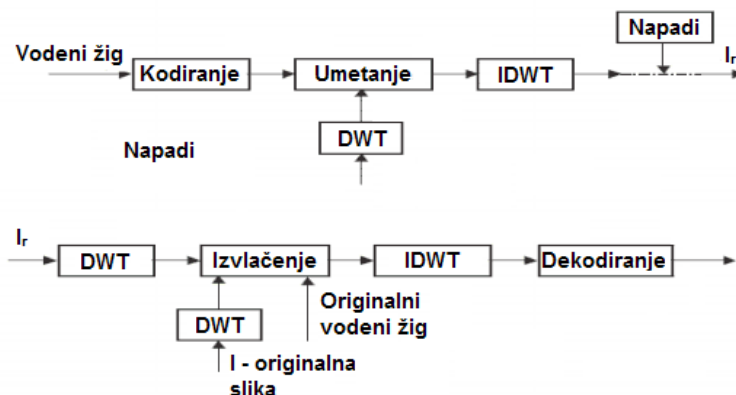
Tehnika vodenih pečata, zasnovana na DCT, je robustna u poređenju sa tehnikom prostornog domena. Ovi algoritmi su robustni protiv jednostavne obrade slike, kao što je niskofrekventno filtriranje, podešavanje osvetljenosti, kontrasta i zamućenosti. U isto vreme, oni su slabi na geometrijske napade, kao što su rotacija, skaliranje i odrezivanje. Utiskivanje u perceptualno značajan deo slike ima svoje prednosti, jer mnogi postupci kompresije uklanjaju perceptualno nebitan deo slike.

Vodeni pečat je utisnut u koeficijente srednje frekvencije, što neće uticati na vidljivost slike i vodeni pečat neće biti uklonjen bilo kakvim napadom. Neke više komponente frekvencija biće potisnute u koraku kvantizacije.

3.3.3 Diskretna talasna transformacija

Talasna transformacija je moderna tehnika koja se često koristi u obradi digitalne slike, kompresiji i u vodenom pečatiranju. Transformacija se zasniva na malim talasima (talasićima) promenljive frekvencije i ograničenog trajanja. Talasna transformacija razlaže sliku na tri prostorna pravca: horizontalni, vertikalni i dijagonalni. Primenom niskopropustnog i visokopropustnog filtra na svaki red podataka, dobijaju se takvi podaci da prva polovina reda sadrži niske, a druga polovina visoke frekvencije. Nakon toga se obavlja filtriranje za svaku kolonu međupodataka. Magnituda DWT koeficijenata veća je na nižim opsezima (LL), na svakom nivou razlaganja, a manja na drugim opsezima (HH, LH i HL).

DWT se trenutno koristi u širokom spektru aplikacija za obradu signala kao što je audio i video kompresija, uklanjanje šuma kod zvuka i simulaciji bežičnog prenosa. Talasići imaju energiju koncentrisanu u vremenu i pogodni su za analizu kratkotrajnih vremenski promeljivih signala. DWT je pogodna jer omogućuje istovremeno lociranje u prostoru, i frekventno raspršen vodeni pečat u originalnoj slici. Zbog očiglednih prednosti u odnosu na JPEG, noviji grafički formati uglavnom koriste DWT u kompresiji (PDF i DjVu). Ima viši odnos kompresije, što odgovara ljudskoj percepciji. Nedostatak ove tehnike je visoka cena, duže vreme kompresije, šum, zamućenost na ivicama slika ili video ramova. Zbog svojih naglih promena, DWT zahteva vrlo širok spektar frekvencija, što je slučaj i sa DCT.



Slika 3.3.3.1: Blok šema za utiskivanje i izvlačenje vodenog pečata pomoću DWT

3.4 Klasifikacija digitalnih vodenih pečata

Digitalni vodeni pečati mogu se, osim po domenu, podeliti u nekoliko kategorija i to: prema tipu, moći opažanja, karakteristikama (robustnosti), upotrebi ključeva, procesu detekcije i prema nameni [4].

Podela prema domenu:

- **Prostorni domen** (engl. *Spatial domain*) – Ovaj domen se fokusira na modifikovanje piksela jednog ili dva slučajno izabrana podskupa slika. Direktno smešta neobrađen podatak u piksele slike. Takođe, ovaj domen se može primeniti i odvajanjem boja. Neki od ovih algoritama su LSB, algoritam zasnovan na tehnici SSM modulacije, aditivni vodeni pečat, tehnika kodovanja teksturne mape, Pačvork algoritam i tehnika na bazi korelacije.
- **Frekventni domen** (engl. *Frequency domain*) – Ova tehnika se još naziva i transformacioni domen. U poređenju sa prostornim domenom, frekventni domen ima širu primenu. Cilj je utisnuti vodeni pečat u spektralne koeficijente slike. Primenom ove tehnike vrednosti određenih frekvencija su promenjene u odnosu na originalne. Razlog primene vodenih pečata u frekventnom domenu je da ljudski vizuelni sistem bolje uočava spektralne koeficijente. Najčešće korišćene transformacije su Diskretna Furijeova transformacija (DFT), Diskretna kosinusna transformacija (DCT) i Diskretna talasna transformacija (DWT).

Tabela 1: Poređenje prostornog i frekventnog domena

Faktori	Prostorni domen	Frekventni domen
Cena troškova	Niska	Visoka
Robustnost	Lomljiv	Više robustan
Kvalitet percepcije	Visoka kontrola	Niska kontrola
Kompleksnost	Mala	Velika
Vreme obračuna	Kraće	Duže
Kapacitet	Veliki	Mali
Primer primene	Uglavnom u autentifikaciji	Zaštita autorskih parava

Izvor: Prabhishak Singh, R. S. Chadha (2013), International Journal of Engineering and Innovative Technology (IJEIT), Volume 2, Issue 9, str. 166

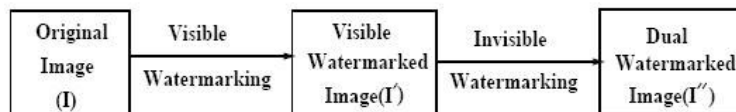
Podela prema tipu vodenih pečata:

- **Zavisno od vrste šuma za:** pseudo šum, Gausove slučajne i haotične sekvence.
- **Zavisno od vrste slike za:** binarne slike, žigove, logo i etikete.

Podela prema moći opažanja:

- **Vidljivi vodeni pečati** (engl. *Visible watermarking*) su dizajnirani tako da posmatrač može lako da ih primeti i jasno identifikuje vlasnika. Takođe, vodeni pečat ne sme uticati na sadržaj same slike. Koristi se za naprednu zaštitu od kopiranja i zaštitu autorskih prava.

- **Nevidljivi vodeni pečati** (engl. *Invisible watermarking*) su dizajnirani tako da posmatraču izgledaju nevidljivo pri normalim uslovima gledanja. Postoje pristupačne tehnologije koje mogu ubaciti u sliku informacije koje se ne mogu videti, ali se mogu ispitati odgovarajućim softverom. Na ovaj način se ne može zaštititi slika od krađe, ali se može dokazati da je slika ukradena, što je dobro.
- **Dvostruki vodeni pečati** (engl. *Dual watermarking*) predstavljaju kombinaciju vidljivog i nevidljivog vodenog pečata.



Slika 3.4.1: Šematski prikaz dvostrukog vodenog pečata

Podela prema karakteristikama (robustnosti):

- **Robusni nevidljivi vodeni pečati** (engl. *Robustness watermarking*) su vizuelno nevidljivi, ali ga dekodirer lako detektuje i uklanja. Otporan je na različite vrste napada, bilo da su u pitanju geometrijski ili ne geometrijski napadi. Koriste se za detekciju nelegalnih dokumenata i za evidentiranje autorskog prava.
- **Lomljivi nevidljivi vodeni pečati** (engl. *Fragile watermarking*) su vizuelno nevidljivi, ali se mogu detektovati i nisu otporni na napade. Prema stanju lomljivog vodenog pečata možemo odrediti da li se podacima neovlašćeno pristupilo. Uglavnom se koriste za zaštitu integriteta, koji može biti veoma osetljiv na promene signala, kao nevidljivi pečati za pouzdane (sigurne) kamere i za detekciju promene slike u digitalnoj biblioteci.
- **Polu lomljivi vodeni pečati** (engl. *Semi fragile watermarking*) su sposobni da, do izvesnog stepena, tolerišu promenu slike sa vodenim pečatom kao što je kvantizacioni šum koji se pojavljuje kod kompresije sa gubicima.

Podela prema upotrebi ključeva:

- **Asimetrični vodeni pečati** (engl. *Asymmetric watermarking*) – Ova tehnika koristi različite ključeve za utiskivanje i detekciju vodenih pečata.
- **Simetrični vodeni pečati** (engl. *Symmetric watermarking*) – Kod ove tehnike se koriste isti ključevi i za utiskivanje i za detekciju vodenog pečata.

Podela prema procesu detekcije:

- **Vizuelni vodeni pečati** (engl. *Visual watermarking*) – Zahtevaju originalni podatak pri testiranju i imaju veliku robusnost. Primena ove vrste pečata je ograničena.
- **Polu slepi vodeni pečati** (engl. *Semi blind watermarking*) – Ne zahtevaju originalni podatak za detekciju.
- **Slepi vodeni pečati** (engl. *Blind watermarking*) – Takođe ne zahtevaju originalni podatak, ali zahtevaju savremeniju tehnologiju vodenih pečata. Ova vrsta pečata ima široko aplikaciono polje.

Podela prema nameni:

- **Vodeni pečati za zaštitu autorskih prava** (engl. *Copyright protection watermarking*) – Ako vlasnik želi da vodeni pečat bude vidljiv, on to može učiniti dodavanjem vodenog pečata u sliku, tako da on i dalje postoji čak i ako postoji mogućnost da bude napadnut.
- **Vodeni pečat koji obaveštava o promeni** (engl. *Tampering tip watermarking*) – Štiti integritet sadržaja slike, označava promenjeni sadržaj i pruža otpornost kompresiji sa gubitkom.
- **Vodeni pečat protiv falsifikovanja** (engl. *Anti-counterfeiting watermarking*) – Dodaje se prilikom procesa izgradnje beleški, i može se detektovati nakon štampanja, skeniranja ili drugih procesa.
- **Anonimna oznaka vodenog pečata** (engl. *Anonymous mark watermarking*) – Može sakriti važne pribeleške poverljivih podataka i ograničiti nelegalne korisnike da dođu do poverljivih podataka.

3.5 Primena digitalnih vodenih pečata

Digitalni vodeni pečat se koristi za identifikaciju i zaštitu autorskog prava (engl. *Copyright protection*). Digitalni sadržaj koji je utisnut sa vodenim pečatom identifikovaće vlasnika autorskog prava.

Kod zaštite od kopiranja (engl. *Copy protection*), digitalni sadržaj sa vodenim pečatom treba da ukaže da digitalni sadržaj ne može biti ilegalno kopiran. Sredstva sposobna za kopiranje mogu tada detektovati vodeni pečat i sprečiti neautorizovano kopiranje sadržaja.

Digitalni vodeni pečati koji su po prirodi lomljivi, mogu se koristiti za proveru neovlašćenog pristupa (engl. *Tamper proofing*). Digitalni sadržaj može biti utisnut sa lomljivim vodenim pečatom koji će biti uništen uvek kada se napravi bilo kakva vrsta modifikacije sadržaja. Ovakvi vodeni pečati mogu se koristiti za potvrdu autentičnosti sadržaja.

Kod autentifikacije izgleda i sadržaja (engl. *Image and content authentication*) detektuju se promene na podacima. Karakteristike slike, kao što su npr. njene ivice, utisnute su u važeću sliku i poređenjem se lako može otkriti razlika. Rešenje ovog problema možemo pronaći u kriptografiji, gde je digitalni potpis jedan od metoda autentifikacije. Digitalni potpis, na primer, se koristi za autentifikaciju slike kod verodostojne digitalne kamere.

Upravljanje digitalnim pravima (engl. *Digital right management, DRM*) može biti definisano kao opis, identifikacija, trgovina, zaštita, monitoring i praćenje svih formi korišćenja materijalne i nematerijalne svojine. To se odnosi na upravljanje i primenu digitalnim pravima.

Različite vrste plaćanja daju različite privilegije korisnicima (play/copy kontrola). U nekim sistemima je poželjno da korisnici imaju kopiju i pristup kontrolnom mehanizmu za zaštitu od ilegalnog kopiranja sadržaja ili ograničenje broja kopiranja (engl. *Access control*). Robustni vodeni pečat može se koristiti u ove svrhe.

Otisak prsta (engl. *Fingerprinting*) je karakteristika jednog objekta koja je izdvojena od drugih malih objekata. Kao u aplikaciji za zaštitu autorskih prava, vodeni pečat za otisak prsta je korišćen da prati autorizovane korisnike koji krše licencne ugovore i nezakonito distribuiraju kopirani materijal. Dakle, korisnik ima korisnički identifikacioni broj koji je kao informacija utisnut u sadržaj.

Forenzička aplikacija (engl. *Media forensics*) vodenog pečata povećava sposobnost vlasnika sadržaja da detektuje i odgovori na zloupotrebu svoje imovine. Forenzički vodeni pečat se koristi da bi se sakupili dokazi za krivični postupak. Osim toga, kod ugovora između vlasnika sadržaja i kompanija ili ljudi koji dele taj sadržaj, forenzički vodeni pečat treba da natera korisnike ugovora da isti poštuju.

U medicini, izveštaji igraju veoma važnu ulogu u tretmanima namenjenim pacijentima (engl. *Medical application*). Imena pacijenata mogu biti odštampana na rendgenskim snimcima i snimcima magnetne rezonance koristeći tehnike vidljivog vodenog pečata. Bilo bi katastrofalno ukoliko bi se zamenili izveštaji dva pacijenta.

Vodeni pečat se može koristiti i za pribeležke na slici. Na primer, evidencija pacijenta i detalji vazani za snimak, mogu se pažljivo umetnuti u sliku. To će smanjiti prostor za smeštanje i omogućiti povezanost slike i pribeležke. Privatnost pacijenta može se sačuvati ako se osetljive informacije ne čuvaju kao jasan tekst u čitljivoj formi, a vodeni pečat se dodatno osigurava šifrovanjem (engl. *Annotation and privacy control*).

Poslednjih nekoliko godina broj televizijskih i radio kanala se znatno povećao. Količina protoka sadržaja kroz ove medije prenosa eksponencijalno raste. Nadgledanje ovog, veoma izdvojenog i brzo promenljivog tržišta, važno je za vlasnike svojine, imaoce vlasničkih prava, distributere i emitere (engl. *Broadcast monitoring*).

Moderni digitalni formati namenjeni za prodaju ili iznajmljivanje audio i video sadržaja potrošačima (DVD, Blu-Ray Disc i iTunes) objedinjuju tehnologije za zaštitu sadržaja (engl. *Content protection for audio and video content*). One kontrolišu pristup i upotrebu sadržaja i ograničavaju neautorizovano kopiranje i ponovnu distribuciju.

4 Algoritmi za označavanje i detekciju digitalnih vodenih pečata

4.1 Savremena steganografija

Steganografija je tehnika skrivanja tajnih poruka koja se temelji na sakrivanju poruke unutar teksta, slika i filmova. To se radi na takav način da niko osim predajne i prijemne strane nije toga svestan i ne privlači pažnju na sebe. Takođe, steganografija podrazumeva i sakrivanje poruka unutar računarskih fajlova i podataka.

Savremeni pojam steganografije, odnosno steganografskog sistema (stegosistema), podrazumeva skup sredstava i metoda koji se koriste za formiranje skrivenog kanala prenosa informacija [11].

Nosilac poruke ima zadatak da prenese skrivenu informaciju. Tajna poruka se ugrađuje u nosioca poruke pomoću stego ključa. Stegosistem može imati jedan ili više stego ključeva. Nosilac i skrivena poruka, koja se tajno prenosi, čine steganografski medijum. Komunikacioni kanal kojim se šalje stego nosilac poruke je steganografski kanal (stegokanal).

Steganografija se primenjuje na sledeći način: pošiljalac tajne poruke bira nasumično nosioca poruke; u izabrani nosilac poruke implementira se tajna poruka uz pomoć stego ključa; primaocu se šalje steganografski medijum, a primaoc na drugoj strani obrnutim postupkom dolazi do sadržaja tajne poruke. Da tajna poruka ne bi bila vidljiva, bitno je da nosilac poruke sadrži dovoljno redundantnih bitova, koji mogu biti zamenjeni tajnom porukom. Važno je napomenuti da nisu svi digitalni formati pogodni za prenošenje tajnih poruka, jer npr. promena bitova u nekom izvršnom fajlu dovodi do toga da program ne radi ili javlja greške pri radu.

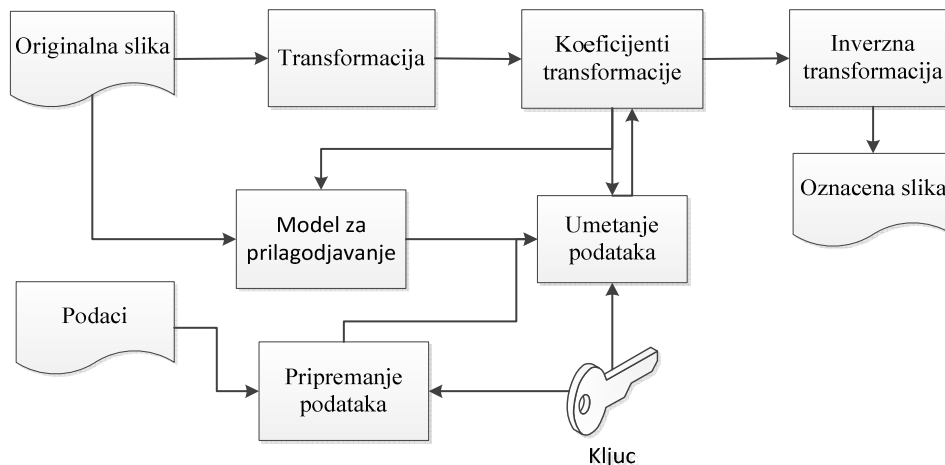
Kompjuterska steganografija je deo steganografije koja se bavi realizacijom stegosistema primenom kompjuterske tehnike. Postoje mnogi programi koji primenjuju različite steganografske tehnike za skrivanje informacija. Savremene metode kompjuterske steganografije koriste posebne kompjuterske formate i obilje informacija u vidu digitalnih audio i video signala.

Specijalna svojstva kompjuterskih formata, manje se koristi kao metod za realizaciju kompjuterske steganografije namenjene zaštiti informacija, a više kao metod napada, ubacivanjem malicioznih programa. Postoji mnogi programi za stegoanalizu čiji je zadatak da prepoznaju steganografiju u komunikaciji i da unište poruku.

Preobilje informacija u audio i video digitalnim signalima je osnovni pravac razvoja metoda kompjuterske steganografije. Digitalna fotografija, digitalna muzika i digitalni video predstavljaju matricu brojeva koji kodiraju intenzitet (jačine svetlosti kod fotografije, intenzitet jačine zvuka kod muzike) u diskretnom trenutku u vremenu i prostoru. Kako bitovi sa najmanjim značenjem sadrže malo korisnih informacija, njihova zamena sa tajnom porukom ne utiče značajno na kvalitet reprodukovano zvuka ili slike.

4.2 Algoritmi za označavanje i detekciju digitalnih vodenih pečata

Algoritam koji opisuje postupak označavanja dokumenata digitalnim pečatom sastoji se od vodenog pečata, koda, dekodera i komparatora. Svaki korisnik poseduje jedinstveni pečat za identifikaciju. Pečat se može dodati u bilo koji digitalni dokument pomoću algoritma za kodiranje, dok se sa algoritmom za dekodiranje on vadi iz označenog dokumenta i jednoznačno se određuje vlasnik i integritet dokumenta [10]. Vodeni pečat se može utisnuti u bilo koji domen (prostorni ili frekventni domen). Oba domena se koriste u različitim scenarijumima i imaju svoje prednosti i mane.



Slika 4.2.1: Algoritam utiskivanja vodenog pečata u sliku

Algoritmi koji služe za označavanje nekog digitalnog dokumenta, treba da zadovolje sledeće zahteve [13]:

- Digitalni vodeni pečat treba da bude jednoznačna veza između označenog dokumenta i njegovog autora;
- Mora biti otporan na različite napade, pa čak i one nepoznate (namerne ili ne namerne);
- Algoritam bi trebao da unese i podatke o korisniku označenog dokumenta, kako bi se u slučaju zloupotrebe mogao otkriti krivac;
- Bilo bi dobro da postoji algoritam koji će detektovati vodeni pečat, a da ga pritom ne ukloni.

Sposobnost algoritma da otkrije pečat je jako cenjena i komplikovana tehnika, pa se retko primenjuje u programima. Prisutnost vodenog pečata u slici otkriva se upoređivanjem originalne (neoznačene) i označene slike.

Algoritmi se mogu podeliti prema:

- Domenu u kojem se obavlja utiskivanje i detekcija pečata,
- Dotupnosti referentnih podataka za detekciju pečata,
- Metodi modifikacije slike,
- Strategiji perceptualnog modeliranja,
- Nameni.

4.3 Izmena najmanje značajnih bitova (LSB supstitucija)

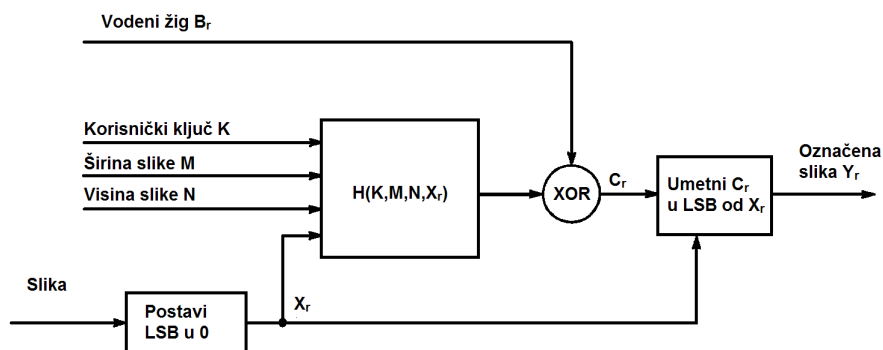
LSB supstitucija (engl. *Least Significant Bit*) je jedna od najčešće korišćenih steganografskih tehnika. Ima veoma dobre performanse kada se primenjuje na slikama. Sakrivanje velike količine informacija moguće je izvesti uz minimalni uticaj na datoteku nosioca skrivene informacije. LSB supstitucija uzima bitove sa najmanjim značenjem iz izabrane datoteke i zamenjuje ih sa bitovima tajne poruke. Ova supstitucija se lako primenjuje na slike velike rezolucije sa mnogo detalja. Odlikuje se velikim kapacitetom za skrivanje poruka ili ugrađivanje digitalnog vodenog pečata, ali ne pruža veliku sigurnost.

Mnogo je lakše sakriti informacije u slici visokog kvaliteta i rezolucije. Najbolji format slike za sakrivanje informacija je 24-bitna BMP slika, kao najveći tip fajla, a samim tim i najkvalitetniji, ali zbog njene veličine mnogi se opredeljuju za 8-bitni GIF ili BMP format slike. Jedan od razloga je taj što slanje slika velikih dimenzija preko Interneta može izazvati sumnju. Najveći broj aplikacija za digitalne slike danas podržava 24-bitne slike, gde je svaki piksel kodiran u 24 bita (3 Bajta). Tipična 8-bitna slika dimenzija 640x480 sa 256 nijansi boja omogućava skrivanje poruke od 300 KB, a 24-bitna slika dimenzije 1024x768 do 2.3 MB. GIF i BMP se generalno uzimaju u obzir da bi se obezbedila idealna kompresija, zato što je obnovljena slika posle kodiranja i kompresije identična u bit originalnoj slici.

LSB supstitucija je laka za razumevanje, malo kviri kvalitet slike i ima veliku transparentnost. Vodeni pečat može biti raspršen preko cele slike, ili lociran u određenom delu slike. Jednostavnost ove metode je ujedno pogodna i za dešifrovanje poruke koju slika nosi, jer svako može da pročita niz bitova i po potrebi ih izmeni. Postoje različite primene ove tehnike, a neke od njih su sledeće [8]:

- Može da postoji sopstvena tabela za konverziju, gde se svakom znaku dodeljuje određena kombinacija bitova;
- Pikseli u koje se skrivaju znakovi mogu da se selektuju po poznatom pravilu;
- Mogu da postoje pravila po kojima se selektuju pikseli, koji zavise od ključa korisnika.

Međutim, uprkos svojoj jednostavnosti LSB ima dosta nedostataka. Nedostaje mu osnovna robustnost. Podlozan je šumu, odrezivanju i skaliranju. Iako bi vodeni pečat mogao da preživi transformacije kao što su odrezivanje, dodavanje šuma ili kompresija sa gubitkom, najverovatnije će biti izgubljen.



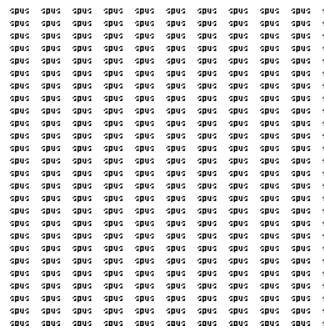
Slika 4.3.1: Blok šema utiskivanja vodenog pečata primenom LSB supstitucije

Digitalni vodeni pečat, koji je nastao LSB supstitucijom, nije otporan na većinu napada, što ga svrstava u kategoriju lomljivih pečata. Program koji menja samo dva informaciona bita dovoljan je da uništi pečat, a da pritom ne naruši kvalitet slike. Najbolji napad na vodeni pečat, a da pritom slika ostane nepromenjena, je da se svi LSB bitovi postave na jedinicu. Kada se otkrije metoda, odnosno algoritam, sakriveni pečat se lako može promeniti.

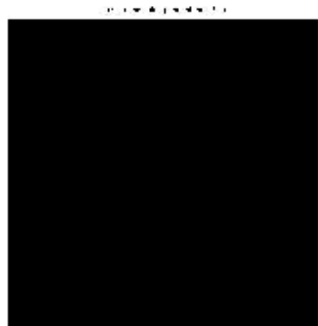
Ako vodeni pečat sakrijemo unutar slike (slika 4.3.2 i 4.3.3), dobićemo novu sliku koja u sebi sadrži vodeni pečat. Kao rezultat dobijamo sliku u kojoj nema vidljivih promena (slika 4.3.4). Iz tako nepromenjene slike može se lako izvući vodeni pečat (slika 4.3.5).



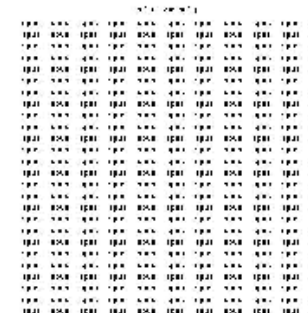
Slika 4.3.2: Originalna slika



Slika 4.3.3: Primer vodenog pečata



Slika 4.3.4: Razlika između originalnog i pročitano vodenog pečata



Slika 4.3.5: Pročitani vodeni pečat

4.3.1 Slika u slici

Slika u slici je zapravo jedna vrsta LSB supstitucije. Da bi se poslala gruba aproksimacija tajne slike, dovoljna su tri bita. Pošiljalac tajne poruke zamenjuje tri bita najmanje težine originalne slike sa tri bita najveće težine tajne slike. Primalac izvlači tri bita najmanje težine iz primljene slike, dobijajući tako pristup do tri najznačajnija bita tajne slike. Degradacija slike u koju je ugrađena druga slika uglavnom nije vizuelno uočljiva [12].



Slika 4.3.1.1: Originalna slika



Slika 4.3.1.2: Tajna slika



Slika 4.3.1.3: Slika – kombinacija



Slika 4.3.1.4: Slika dobijena od tri ravni najmanje težine slike 4.3.1.3

4.4 Tehnika kodovanja proširenim spektrom

Tehnika kodovanja proširenim spektrom (engl. *Spread Spectrum Modulation Based Technique*) je metoda u kojoj se energija generisana u jednu ili više diskretnih frekvencija namerno proširi ili rasporedi u vremenu. Vodeni pečati, bazirani na SSM algoritmu, utiskuju informaciju linearnim kombinovanjem originalne slike sa malim signalom pseudo šuma koji je modulisan sa utisnutim vodenim pečatom.

Da bi obrada bila što kvalitetnija, na sam spektar će se primeniti neka od transformacija: Diskretna kosinusna transformacija (**DCT**), brza Furijerova transformacija (**FFT**), Diskretna talasna transformacija (**DWT**) ili Diskretna Volš-Adamarova transformacija (**WHT**). Zatim se bira jedan skup spektralnih koeficijenata dobijen takvom transformacijom. Ukoliko neki od koeficijenata povećamo za neku vrednost, znači da u njega želimo sakriti vrednost „1“. Smanjenje znači vrednost „0“. Spektralni koeficijenti biraju se tako da pečat bude „raspršen“ po celom frekventnom spektru slike, a energija pečata neprimetna u svakoj odabranoj frekvenciji, bez vidljivih promena na slici. Pri obradi slike, filtriranje visokih frekvencija može ukloniti pečat zajedno sa ostalim sadržajem u tom području, ali ne i u području niskih frekvencija.

Zamislimo sliku kao neki komunikacioni kanal kojim prenosimo signal (u našem slučaju pečat). Razne smetnje i šumovi deluju, kao i na ostale komunikacione kanale, i na ovaj. Signal mora biti takav da ga eventualno sužavanje frekventnog opsega ne uništi, a koeficijenti tako modulisani da im eventualni šumovi ne izmene značenje.

Pošto su dobro poznata frekventna područja za dodavanje signala pečata, u cilju što teže detekcije, moguće je dodati skup slabijih signala tako da zajedno čine signal sa velikim odnosom signal/šum. Pečati su otporni na različite vrste filtriranja, kompresije ali i na štampanje i kopiranje, budući da se pri dodavanju pečata na sliku on postavlja tamo gde će njegovo uklanjanje značajno degradirati kvalitet slike. Gotovo svi programi koji generišu robustan digitalni vodeni pečat koriste tehnike transformacije.

4.5 Ostali poznati algoritmi

Aditivni vodeni pečat (engl. *Additive watermarking*) je najdirektnija metoda za utiskivanje vodenog pečata u prostornom domenu i sastoji se u dodavanju uzorka slučajnog pseudo šuma intenzitetu piksela slike. Signal šuma je obično intedžer $(-1,0,1)$ ili decimalni broj. Da bi obezbedili detekciju vodenog pečata, šum treba da se generiše po ključu, tako da korelacija između brojeva različitog ključa bude veoma mala [4].

Tehnika kodovanja teksturne mape (engl. *Texture Mapping Coding Technique*) je metoda koja je korisna samo u onim slikama koje imaju u sebi teksturni deo. Ova metoda krije vodeni pečat u teksturnom delu slike. Nedostatak ovog algoritma je što je pogodan samo za one oblasti sa velikim brojem slučajnih teksturnih slika i ne može biti urađen automatski. Ovaj metod krije podatke u kontinualnoj slučajnoj teksturnoj šari slike.

Pačvork algoritam (engl. *Patchwork Algorithm*) – Pačvork je tehnika skrivanja podataka koju je razvio Bender et alii (IBM Systems Journal, 1996). Bazira se na slučajnom pseudo statističkom modelu. Pačvork neprimetno ubacuje vodeni pečat koristeći posebnu statistiku Gausove raspodele. Pseudo slučajna selekcija se izvršava na dva parčeta, gde je prvo A i drugo B. Podatak u delu slike A je posvetljen, a u delu slike B je potamnjen. Prednost ove tehnike je visok nivo robustnosti protiv većine napada, a nedostatak što može da sakrije malu količinu informacija.

Tehnika na bazi korelacije (engl. *Correlation Based Technique*) – U ovoj tehnici uzorak slučajnog pseudo šuma $W(x,y)$ je dodat u skrivenu sliku $I(x,y)$.

$$Iw(x, y) = I(x, y) + k * W(x, y), \quad (4.5.1)$$

gde k predstavlja faktor pojačanja, Iw predstavlja sliku sa vodenim pečatom na poziciji x,y , a I predstavlja skrivenu sliku. Prednost ove tehnike je što porast faktora pojačanja rezultira porastom robustnosti. Sa velikim porastom faktora pojačanja opada kvalitet slike.

Maskiranje za vid nebitnih delova – Ova tehnika koristi nemogućnost ljudskog oka da razlikuje sitne detalje, naročito na onim delovima slike koji predstavljaju teksture. Na tim delovima slike, pošto je oko skoncentrisano na celinu, moguće je izmeniti intenzitet osvetljaja pojedinih piksela, a da oko ne primeti razliku. Algoritmu ide u prilog loš kvalitet računarskih monitora, pa je označena područja nemoguće razlikovati, bilo da je u pitanju označena ili neoznačena slika. Nedostatak ove tehnike je što ne mogu da se označavaju područja koja su ispunjena jednom bojom, jer bi se odmah primetila. Neki algoritmi kompresije slike sa gubicima upravo traže teksturirana područja, izbacuju delove koji su suvišni i na taj način uništavaju pečat.

4.5.1 Cox-ov algoritam

Cox-ov algoritam je najpoznatiji algoritam koji koristi DCT. Autori ovog algoritma su Ingemar J. Cox, Joe Kilian, Tom Leighton i Talal G. Shamoon (NEC Research Institute). Kao digitalni vodeni pečat uzima se Gausov niz od 1000 pseudo-slučajnih brojeva koji se zatim sabiraju sa 1000 najvećih koeficijenata DCT-a.

Na slici 4.5.1.1 prikazana je umanjena crno-bela slika (originalne dimenzije slike su 512x512 piksela) pre utiskivanja digitalnog vodenog pečata Cox-ovim algoritmom, a na slici 4.5.1.2 posle utiskivanja. Upoređivanjem digitalnog vodenog pečata izvučenog iz označene slike i utisnutog pečata dobija se Hamingovo rastojanje, tj. faktor sličnosti između početne slike i slike sa digitalnim pečatom $d=0.999999$ [10].



Slika 4.5.1.1: Slika pre utiskivanja digitalnog vodenog pečata Cox-ovim algoritmom



Slika 4.5.1.2: Slika posle utiskivanja digitalnog vodenog pečata Cox-ovim algoritmom

4.5.2 Algoritam Corvi

Algoritam Corvi su razvili Marco Corvi i Gianluca Nicchiotti (Elsag-Bailey Research Laboratory, Italy). Digitalni vodeni pečat je Gausov niz pseudo-slučajnih realnih brojeva dužine 32x32 (ukupno 1024 realna broja). Algoritam originalnu sliku prebacuje u DWT, i samo se niskofrekventni koeficijenti sabiraju sa pečatom. Na slici 4.5.2.1 prikazana je crno-bela slika pre utiskivanja digitalnog vodenog pečata algoritmom Corvi, a na slici 4.5.2.2 posle utiskivanja. Upoređivanjem digitalnog vodenog pečata izvučenog iz označene slike i utisnutog pečata dobija se Hamingovo rastojanje $d=0.950000$.



Slika 4.5.2.1: Slika pre utiskivanja digitalnog vodenog pečata algoritmom Corvi



Slika 4.5.2.2: Slika posle utiskivanja digitalnog vodenog pečata algoritmom Corvi

4.5.3 Algoritam Xia

Algoritam Xia je još jedan od algoritama koji koristi DWT transformaciju. Razvili su ga Xiang-Gen Xia, Charles G. Boncelet i Gonzalo R. Arce (Univerzitet u Delawareu, Newark, USA). Kao digitalni vodeni pečat koristi se Gausov niz pseudo-slučajnih realnih brojeva. Autori preporučuju prelaz u DWT razlaganjem na dva nivoa uz upotrebu Harovog filtra. Digitalni vodeni pečat se utiskuje u velike koeficijente visokih i srednjih frekventnih pojaseva (detaljnih podpojaseva) pa se, za razliku od algoritma Corvi, digitalni vodeni pečat uopšte ne nalazi u niskofrekventnom podpojasu.

S obzirom na to da veliki koeficijenti u detaljnim podpojasevima najčešće predstavljaju ivice, ovim algoritmom se najviše energije digitalnog vodenog pečata smešta u područja ivica i tekstura. Time se postiže dobra nevidljivost utisnutog pečata, jer je ljudsko oko manje podložno primećivanju promena kod ivica i tekstura, za razliku od promena uzrokovanim u području niskih frekvencija. Na slici 4.5.3.1 prikazana je slika pre utiskivanja digitalnog vodenog pečata, a na slici 4.5.3.2 posle utiskivanja. Upoređivanjem digitalnog vodenog pečata izvučenog iz označene slike i utisnutog pečata dobija se Hamingovo rastojanje $d=0.997599$.



Slika 4.5.3.1: Slika pre utiskivanja digitalnog vodenog pečata algoritmom Xia



Slika 4.5.3.2: Slika posle utiskivanja digitalnog vodenog pečata algoritmom Xia

Cox-ov algoritam je efikasan za teksturne slike koje imaju što manje jednako svetlih površina. Za razliku od njega, Corvi algoritam je efikasan za slike sa što manje tekstura. Digitalni vodeni pečat ubačen Xia algoritmom najmanje se primećuje na slikama koje sadrže deo tekstura.

4.6 Tehnike za korekciju slike

Nakon ubacivanja skrivenih podataka u sliku, može doći do zamućenosti u određenom delu slike. Ovaj problem možemo rešiti pomoću **maskiranja i filtriranja**, tako što ćemo originalne slike malo potamniti, a zatim ubaciti skrivene podatke u pomenutu sliku. Maskiranje i filtriranje je jedna od najzastupljenijih tehnika u steganografiji. Uspeh ove tehnike zasniva se na činjenici da ljudsko oko teško uočava razlike među bojama slabije sjajnosti.

Dodavanje šuma je veoma efikasna tehnika i zasniva se na dodavanju belih tačaka ili izbeljivanju tamnijih, pa se kod krajnjeg korisnika stvara utisak da je slika skenirana i da je slika slabijeg kvaliteta. Ovakvu sliku će retko ko detaljno analizirati. Pri dodavanju šuma važno je da se ne menjaju bitovi koji nose skriveni podatak.

Aditivni šum i nekorelisani multiplikativni šum se često pominju u telekomunikacijama i obradi signala. Autori pečata često tvrde da njihovi pečati preživljavaju ovakav šum, ali mnogi ne napomenu koliko amplitudu šuma njihov pečat može zaista da podnese.

Korekcija boje piksela je najsavršenija tehnika i funkcioniše tako što se skriveni podatak upisuje u svaki drugi piksel, a pikseli koji ostanu slobodni koriguju se prema bojama susednih piksela. Korekcija slobodnog piksela vrši se tako što se, pored njegove originalne boje, gledaju i one susedne (slika će bolje izgledati ako se gledaju i susedne boje), a potom se nalazi srednja vrednost boje. Na ovaj način slika će izgledati skoro isto kao original. Nedostatak ove tehnike je što se koristi svaki drugi piksel za skrivanje podataka, pa se ima duplo manje prostora za podatke. Velika prednost ove tehnike je to što se šanse za otkrivanje tajnog sadržaja svode na minimum. Slika će još bolje izgledati ako se podaci sakrivaju u svakom trećem pikselu, ali će biti srazmerno manje mesta. Korekcija boje piksela može se koristiti na slikama velikog formata za skrivanje male količine podataka [11].

4.7 Kvantizacija

Kvantizacija (engl. *quantization*) je proces preslikavanja velike grupe vrednosti u mnogo manju grupu vrednosti. Kvantizacija je osnova kod mnogih šema kompresije podataka sa gubicima, pošto ona smanjuje količinu različitih elemenata.

Postoje dve vrste kvantizacije:

- skalarna kvantizacija
- vektorska kvantizacija

Kod skalarne kvantizacije, ulazna i izlazna veličina kvantizatora su skalari, a kod vektorske kvantizacije su vektori. Kvantizator se sastoji od kodera i dekodera. Prvo koder podeli ulazni signal na manje intervale i svaki interval dobije svoju kodnu reč. Svim ulaznim elementima, koji sa svojim karakteristikama pripadaju jednom intervalu, koder dodeljuje istu kodnu reč. Postoji mnogo različitih elemenata sa istom kodnom reči, i zato je kodiranje ireverzibilan proces. Svaku kodnu reč koju je stvorio koder, dekodek rekonstruiše u novu vrednost.

Kada se izvrši dekompozicija slike, veliku količinu energije slike i većinu šuma slike (sopstveni šum) nose pojasevi niske frekvencije. Pre vađenja pečata, kod vizuelnih algoritama, od označene slike može se oduzeti originalna slika, pa sopstveni šum ne stvara problem.

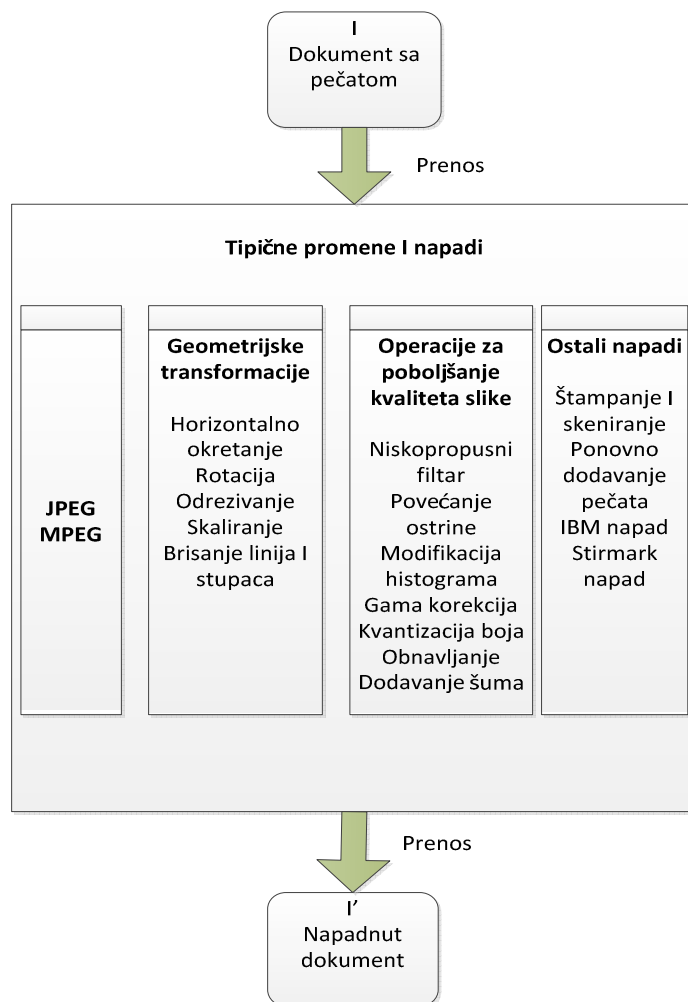
Međutim, kod slepih algoritama moguće je da se pečat ne prepozna ili zameni sa signalom same slike zbog smetnji prouzrokovanih sopstvenim šumom. Sopstveni šum ima i pozitivna svojstva kod označavanja slike. Operacije nad slikama uopšte ne utiču na pojaseve niske frekvencije, već se promene uglavnom odvijaju u području visokih frekvencija. Visoke frekvencije prouzrokuju zanemarljivo malo sopstvenog šuma.

Da bi rešili problem sopstvenog šuma i sačuvali otpornost algoritma, kod slepih algoritama teži se da se pečat utiskuje u srednje frekvencije. Kompromis između dobre otpornosti i niskog sopstvenog šuma, postižu metode utiskivanja pečata u sliku koje koriste kvantizatore [13].

5 Napadi na digitalne vodene pečate i njihova sigurnost

Svrha napada na digitalne vodene pečate je uništavanje vodenog pečata sa ciljem ukidanja zabrane kopiranja, brisanja vlasnika dokumenta i ostalih nelegalnih radnji. Osim toga neki pečati moraju biti otporni na osnovne operacije kao što su pojačavanje kontrasta, osvetljenosti, kompresija slike itd.

Postoje različiti mogući maliciozni namerni ili nenamerni napadi kojima objekat sa vodenim pečatom može biti izložen. Raspoloživost širokog spektra softvera za procesuiranje slike čini mogućim napad na robustnost sistema sa vodenim pečatom. Cilj ovih napada je da spreči vodeni pečat u njegovoj nameni.



Slika 5.1: Šema tipičnih napada na digitalne vodene pečate

5.1 Vrste napada

- **Napad uklanjanja:** Ovaj napad ima za nameru da ukloni podatak vodenog pečata iz objekta koji sadrži vodeni pečat. Napad uklanjanja koristi činjenicu da je vodeni pečat obično dodatni signal šuma prisutan u originalnom signalu.
- **Napad interference:** Ovaj napad pridodaje šum na objekat sa vodenim pečatom. Primeri ovog napada su kompresija sa gubitkom, kvantizacija, potiskivanje šuma, konverzija i beli šum.
- **Geometrijski napad:** Sve manipulacije koje utiču na geometriju slike kao odrezivanje, rotacija, horizontalno okretanje i skaliranje, mogu se detektovati. Odrezivanje sa desne strane donjeg dela slike su primeri za napad odrezivanja.
- **Napad niskopropusnog filtriranja:** Ako se uradi niskopropusno filtriranje na sliku sa vodenim pečatom to će rezultirati drugačijom mapom sastavljenom od šuma.
- **Lažni napad:** Lažni napad ima za posledicu umetanje i brisanje objekta, promenu pozadine slike, i kao krajnji cilj, zamenu slike.
- **Napad na sigurnost:** Ako je algoritam vodenog pečata poznat, napadač može pokušati da učini vodeni pečat ne važećim tako što će ga podesiti ili modifikovati. U tom slučaju mi govorimo o napadu na sigurnost. Algoritam vodenog pečata se smatra sigurnim ukoliko utisnuta informacija ne može biti uništena, detektovana ili zaboravljena.
- **Napad na protokol:** Napad na protokol nema za cilj da uništi utisnutu informaciju niti da onemogućiti detekciju utisnute informacije. Umesto toga, on daje prednost semantičkom nedostatku u implementaciji vodenog pečata.
- **Kriptografski napad:** Ovaj napad se bori sa razbijanjem sigurnosti. Na primer, kriptografski napad koristi iscrpnu nasilnu metodu u pronalaženju tajnog vodenog pečata. Drugi primer ovog tipa napada je oracle napad. Oracle napad koristi sopstveni detektor da vodi proces uklanjanja vodenog pečata. Najbolje je ako napadač ima sopstveni softver za detekciju vodenog pečata. Ovi napadi su slični napadima koji se koriste u kriptografiji.
- **Aktivni napadi:** Ovde haker namerno pokušava da ukloni vodeni pečat ili da ga jednostavno učini nemogućim za detekciju. Ovo je veliki problem u zaštiti autorskih prava, aplikaciji otiska prsta i u zaštiti od kopiranja.
- **Pasivni napad:** U ovom slučaju napadač ne pokušava da ukloni vodeni pečat, već jednostavno pokušava da odredi da li je oznaka vodenog pečata prisutna ili nije. Cox et al (2002) sugerise da je zaštita od pasivnog napada od najveće važnosti u skrivenoj komunikaciji gde je prepoznavanje prisutnosti vodenog pečata više nego dovoljno.
- **Koluzioni napad:** Cilj hakera je isti kao i kod aktivnog napada, ali je metoda malo drugačija. U nameri da ukloni vodeni pečat, haker koristi nekoliko kopija istog podatka, gde svaka kopija sadrži drugačiji vodeni pečat, kako bi napravio novu kopiju bez vodenog pečata. Ovo je problem u primeni aplikacija otiska prsta (npr. filmska industrija), ali nije široko rasprostranjen zato što napadač mora da ima pristup višestrukim kopijama istog podatka.

- **Degradacija slike:** Ovaj tip napada oštećuje robustnost vodenog pečata tako što uklanja delove slike. Delovi koji su zamenjeni mogu nositi informaciju vodenog pečata. Primer za ovu operaciju su parcijalno odrezivanje, uklanjanje redova i kolona. Umetanje Gausovog šuma takođe spada u ovu kategoriju, gde se slika degradira dodavanjem šuma.
- **Poboljšanje slike:** Ovaj napad je skup operacija koje desinhronizuju informaciju vodenog pečata u slici. Napad uključuje ujednačavanje histograma, izoštravanje, izgladivanje, median filter i poboljšanje kontrasta.
- **Kompresija slike:** Da bi se smanjio prostor za smeštanje podataka i cena širine opsega koji je potreban za emitovanje slike, kompresija slike se obično vrši sa tehnikama JPEG i JPEG2000. Ove metode kompresije sa gubicima su mnogo štetnije od metoda kompresije bez gubitaka. Metode kompresije bez gubitaka mogu sakriti informaciju vodenog pečata pomoću inverzne operacije. Međutim, tehnike kompresije sa gubicima stvaraju nepovratne promene na slikama. Verovatnoća otkrivanja informacije vodenog pečata je uvek veoma mala.
- **Transformacija slike:** Ovaj tip napada zove se još i sinhronizacioni ili geometrijski napad. Čuveni softver StirMark koristi male lokalne geometrijske distorzije da onespobli detekciju vodenog pečata. Geometrijski napad uključuje rotaciju, skaliranje i translaciju [4].

5.2 Geometrijske transformacije

Pečat, osim što mora da bude otporan na kompresiju sa gubicima, i na digitalno/analogne i analogno/digitalne konverzije, takođe mora da izdrži i geometrijske distorzije kao što su translacija, rotacija, skaliranje i smicanje.

Geometrijske transformacije su operacije koje se primenjuju na geometrijski opis objekta. Takođe, one menjaju sliku, pa se smatraju i vrstom napada na vodene pečate. Neke od geometrijskih transformacija su:

- **Translacija** (engl. *Translation*) – Translacija je transformacija Euklidovog prostora koja pomera svaku tačku slike ili prostora sa fiksnim rastojanjem za istu vrednost u datom pravcu. Refleksija preko jedne ose praćena je refleksijom preko druge ose koja je paralelna prvoj osi, i rezultira potpunim kretanjem što je translacija. Translacija takođe može biti interpretirana kao dodatak konstantnog vektora za svaku tačku, ili kao pomeranje koordinatnog početka sistema. Translacija se može opisati kao kruto kretanje, dok druga kruta kretanja uključuju rotaciju i refleksiju.
- **Rotacija** (engl. *Rotation*) – Rotacija je transformacija koja je izvedena „okretanjem“ objekta oko fiksne tačke poznate kao centar rotacije. Rotacija ravni oko tačke, praćena drugom rotacijom oko druge tačke, rezultuje ukupnom kretanju koje je ili rotacija ili translacija. Objekat se može rotirati za bilo koji ugao (najčešće za 90° i 180°). Rotacija za „mali“ ugao, posebno u kombinaciji sa odrezivanjem, obično ne menja komercijalnu vrednost slike, ali može učiniti pečat neprepoznatljivim. Rotacija je jako česta operacija u procesu skeniranja slika.
- **Skaliranje** (engl. *Scaling*) – Ovo je česta operacija koja se dešava uvek kad se otisnuta slika skenira. Isto tako obavezna je u pripremi slika za web izdavaštvo. Postoje dva vrste skaliranja: uniformno i neuniformno. Uniformno skaliranje je ono skaliranje kod kojeg se zadržava odnos veličina stranica slike, dok se kod neuniformnog skaliranja taj odnos ne čuva.

Uniformno skaliranje je linearna transformacija koja uvećava ili umanjuje objekte, dok neuniformno skaliranje menja oblik objekta. Kod uniformnog skaliranja, faktor skaliranja je isti u svim pravcima, pa je rezultat sličan originalu. Ukoliko se najmanje jedan od faktora skaliranja razlikuje od ostalih, tada dobijamo neuniformno skaliranje. Mnogi pečati otporni su samo na uniformno skaliranje.

- **Smicanje** (engl. *Shearing*) – Smicanje je transformacija koja efektivno rotira određenu osu, tako da ose ne budu više upravne. Smicanje se ne sme mešati sa rotacijom. U planarnoj geometriji, smicanje je linearna mapa koja premešta svaku tačku u fiksni pravac, za iznos proporcionalan njegovoj određenoj udaljenosti od linije koja je paralelna tom pravcu. Primenom smicanja na skup tačaka ravni, promeniće se svi uglovi između njih, i dužina bilo koje duži koja nije paralelna smeru premeštanja, dok će linije koje su paralelne sa osama ostati iste dužine. Dakle, smicanje će uglavnom iskriviti oblik geometrijske figure (npr. kvadrat će postati paralelogram, a krug elipsa), ali neće sačuvati površinu geometrijskih figura, uskađenost i relativno rastojanje kolinearnih tačaka.
- **Refleksija** (engl. *Reflection*) – Refleksija je mapiranje iz Euklidove ravni u istu ravan, što je izometrija sa hiperravni kao skup fiksnih tačaka. Ovaj skup se zove osa (u 2D) ili ravan (u 3D) refleksije. Izgled figure u refleksiji je njen odraz u ogledalu u osi ili ravni refleksije. Na primer, odraz u ogledalu malog slova *p* pri refleksiji, vodeći računa o vertikalnoj osi, izgledaće kao *q*. Njegov odraz refleksijom u horizontalnoj osi izgledaće kao malo *b*. Kada se refleksija uspešno primeni dva puta, svaka tačka se vraća u svoj prvobitni položaj i svaki geometrijski objekat se vraća u prvobitno stanje.
- **Odsecanje** (engl. *Cropping*) – Odsecanje je jedan od najosnovnijih procesa kod digitalne obrade slike i odnosi se na uklanjanje spoljnih delova slike da bi se poboljšala pozicija i naglasio dotični predmet, poboljšao kvalitet slike, otklonio neželjeni deo sa slike, ili promenila razmera slike. U nekim slučajevima napadači su zainteresirani samo za neki određeni deo slike. Mnoge web stranice koriste segmentaciju slike, a segmentacija slike je zapravo i osnova za „Mosaic“ napad. „Mosaic“ napad može se opisati kao ekstreman slučaj odsecanja slike.
- **Okretanje** (engl. *Flopped and Flipped image*) – Okrenuta ili obrnuta slika (engl. *Flipped image*) se generiše od strane odraza originala preko horizontalne ose, dok se kod okrenute slike (engl. *Flopped image*), slika reflektuje preko vertikalne ose. Slike okrenute oko vertikalne ose su češće, jer one mogu da se koriste za korekciju neprekidnih grešaka između slika i teško se vide bez obimnog ispitivanja, dok je kod slike okrenute oko horizontalne ose to veoma očigledno. Mnoge slike mogu se okrenuti oko horizontalne ose bez gubljenja informacije. Iako je otpornost na ovu operaciju lako izvesti, malo sistema vodenih pečata je preživljava.
- **Promena slike i brisanje linija** (engl. *Image Shifting and Line Deletion*) – Napadač može da pomera pečat horizontalno ili vertikalno, ili da obriše ceo niz piksela, kako bi uništio informaciju koju vodeni pečat nosi. Ovaj napad je vrlo efikasan protiv jednostavnih implementacija pečata koji rade na principu raspršenog spektra u prostornom domenu.

5.3 Operacije za poboljšanje kvaliteta slike

Za poboljšanje kvaliteta slike mogu se koristiti različiti, pažljivo odabrani filtri i efekti za obradu slike. Prema načinu obrade, metode za popravku kvaliteta slike se mogu podeliti na tri grupe:

1. Lokalne operacije nad pojedinačnim pikselima,
2. Prostorne operacije nad grupom piksela,
3. Transformacione tehnike.

Lokalne operacije nad pojedinačnim pikselima predstavljaju preslikavanje nivoa sivog piksela iz originalne slike u novi nivo sivog.

- **Modifikacija histograma** – Histogram je trakasti grafik koji služi za prikazivanje vrednosti osvetljenja pojedinačnog piksela. Na vertikalnoj osi histograma se nalazi broj piksela u slici, a na horizontalnoj osi se nalazi specifična vrednost osvetljenosti. Modifikacija histograma uključuje rastezanje i izravnavanje histograma, kako bi se kompenzovali loši uslovi osvetljenja. Na ovaj način se može poboljšati kvalitet slike, popraviti osvetljenost i kontrast slike.
- **Gama korekcija** – Gama korekcija je vrlo česta operacija koja služi za poboljšanje kvaliteta slike, korekciju osvetljenosti i boje komponenti digitalne slike. Gama korekcija je naročito korisna za isticanje detalja iz tamnih oblasti slike, koji se teško mogu videti na većini kompjuterskih monitora. Pa tako, prilikom osvetljivanja možemo dobiti nove detalje u tamnim oblastima koji prethodno nisu bili vidljivi.
- **Kvantizacija boja** – Kvantizacija boja je operacija koja se često koristi u konverziji slika u GIF format zapisa za prikazivanje na web stranicama.
- **Obnavljanje** – Ova tehnika se obično koristi da bi se smanjio efekat određene degradacije slike, ali može se upotrebiti i za uklanjanje degradacije koju je uneo vodeni pečat, čime bi se uklonio i sam vodeni pečat.

Kod **prostornih operacija** se u postupak izračunavanja jednog piksela uvodi i grupa piksela koja ga okružuje, a koja se naziva lokalno susedstvo. Vrlo često se prostorne operacije izvode konvolucijom slike i konačnog impulsnog odziva filtra koji se naziva prostorna maska. Zavisno od oblika i sadržaja prostorne maske, prostorne operacije mogu biti veoma raznovrsne i mogu imati različite namene.

Neke operacije obrade slike pogodnije se izvode u transformacionom domenu. To je naročito slučaj sa operacijama filtriranja, kod kojih se prelaskom u frekvencijski domen pomoću Furijeove transformacije preciznije može opisati postupak filtriranja. Kao transformacija slike se najčešće koristi dvodimenzionalna Diskretna Furijeova transformacija.

Promena frekvencijskog sadržaja slike može se izvršiti množenjem 2D transformacije slike sa funkcijom prenosa linearnog filtra. Inverznom transformacijom funkcije dobija se željena određena slika. Ako se kao transformacija koristi DFT, onda se funkcija prenosa najčešće tako definiše da ne utiče na faznu karakteristiku spektra slike, odnosno filtarska funkcija ima fazu jednaka nuli.

- **Niskofrekventno filtriranje (Prostorno usrednjavanje)** – Niskofrekventno filtriranje se obavlja zamenom vrednosti svakog piksela sa težinskom srednjom vrednošću lokalnog susedstva tog piksela. Slike koje su dobijene sa ovakvim filtrom imaju velika izobličenja. Prvi tip izobličenja je karakterističan za male vrednosti granične učestanosti i ogleda se u tome da slika postaje neoštra, nejasna ili razmazana. Gubitak oštine je posledica činjenice da su ukinute visoke učestanosti, koje su odgovorne za prikaz ivica i detalja u slici. Drugi tip izobličenja se pojavljuje nezavisno od vrednosti granične učestanosti i manifestuje se pojavom lažnih varijacija nivoa sivog u okolini stvarnih ivica. Ove varijacije su posledica oscilatornog karaktera impulsnog odziva idealnog filtra. Ovaj negativni efekat se može ublažiti modifikacijom postupka usrednjavanja. U modifikovanom postupku usrednjavanja zamenjuju se samo one vrednosti piksela koje su znatno promenjene uticajem šuma. Zbog toga je ovaj postupak pogodniji za redukciju šuma kada treba zadržati ivice u slici.

Niskofrekventno filtriranje je pogodno za uklanjanje Gausovog šuma iz slike, ako intenzitet šuma nije preterano veliki. U slučaju kada je intenzitet šuma veliki, usrednjavanjem se znatno menjaju i vrednosti piksela koje nisu promenjene šumom čime se kviri i subjektivni kvalitet slike. Na ovaj način se utiče i na digitalni vodeni pečat unutar slike. Najčešće se koristi Gausov filter.

- **Visokofrekventno filtriranje (Izoštavanje slike)** – Vizuelni utisak posmatrača poboljšaće se izoštravanjem slike tj. isticanjem ivice na slici. Izoštavanje se može postići isticanjem visokih učestanosti u spektru slike, ali i metodama u prostornom domenu koje imaju isti efekat. Jedna grupa metoda za izoštravanje slike zasnovana je na primeni aproksimacije gradijenta koja predstavlja izvod funkcije slike i nosi informacije o ivicama. Druga grupa metoda maskira neoštre delove tako što vrši oduzimanje slike dobijene niskofrekventnim filtriranjem od originalne slike. Visokofrekventno filtriranje se često kombinuje sa drugim metodama, na primer sa ekvalizacijom histograma, da bi se dobio još bolji subjektivni kvalitet slike.

Izoštavanjem se ponekad može pokvariti izgled slike. Takav slučaj se javlja kada originalna slika sadrži šum. Pošto šum ima širokopojasni, a često i visokofrekventni karakter, izoštravanjem se uticaj šuma još više pojačava i kviri izgled slike. Ovi filteri su jako dobri za napade na neke tipove pečata, jer vrlo uspešno pronalaze i uklanjaju visokofrekventni šum, koji takav tip pečata unosi u sliku. Veštiji napadi zasnovani su na Laplasovom operatoru.

Filtriranje slike niskofrekventnim ili visokofrekventnim filterskim funkcijama može se izvršiti i u prostornom domenu i u transformacionom domenu.

U prostornom domenu filtriranje se vrši konvolucijom slike sa maskom, koja u stvari predstavlja impulsni odziv filterske funkcije. Pošto se najčešće koriste maske malih dimenzija, amplitudska karakteristika takve filterske funkcije ne može biti mnogo selektivna, pa je filtriranje lošije. Međutim, male dimenzije maski utiču na to da je broj aritmetičkih operacija pri filtriranju u prostornom domenu mali.

U frekventnom domenu, filtriranje se vrši množenjem frekventnog spektra slike sa frekventnom karakteristikom filtra. Zbog toga je filtriranje znatno bolje, jer se preciznije mogu eliminisati neželjene komponente spektra slike. Na žalost, broj računarskih operacija je obično veći nego kod filtriranja u prostornom domenu, zbog toga što se mora izračunavati direktna i inverzna 2D DFT slike velikih dimenzija.

- **Uvećanje (Prostorna interpolacija) slike** – Najjednostavniji metod prostorne interpolacije predstavlja replikacija (ponavljanje) piksela. Kod ovog načina interpolacije svaki piksel duž linije se ponavlja još jednom, a svaka tako dobijena linija se takođe ponavlja. Tako se dobije stepen povećanja od dva puta duž svake koordinatne ose, odnosno, broj piksela u slici se povećava četiri puta. Mnogo bolji rezultati se dobijaju primenom linearne (ili bilinearne) interpolacije, kod koje se pretpostavlja linearna zavisnost intenziteta između dva susedna piksela u istoj vrsti ili koloni. U velikom broju primena linearne interpolacije daje zadovoljavajuće rezultate, znatno bolje od postupka uvećanja replikacijom piksela.
- **Smanjivanje (decimacija) slike** – Pre izvođenja postupka decimacije potrebno je izvršiti niskofrekventno filtriranje, filtrom čije su granične učestanosti manje od originalnih oćestanosti odabiranja po obe ose za najmanje $2n$ puta. Najjednostavniji niskofrekventni filter, koji se ujedno i najčešće koristi predstavlja jednostavan postupak usrednjavanja kojim se grupa od 2×2 piksela zamenjuje jednim pikselom čiji je intenzitet jednak srednjoj vrednosti intenziteta grupe piksela. Kod slika sa izraženijim visokofrekventnim sadržajem često je potrebno koristiti 2D filter bolje selektivnosti. U praksi se češće koristi 2D FIR filteri, zbog toga što se filtriranje obavlja konvolucijom filtra i slike u prostornom domenu.

U slučajevima kada transformacije kontrasta ili linerano filtriranje ne daju dobre rezultate, može se primeniti neka od metoda nelinearnog filtriranja. Najčešće korišćene metode nelinearnog filtriranja su razne vrste medijan filtriranja, filtriranje korenovanjem i homomorfno filtriranje.

- **Medijan filtriranje** – Medijan filtriranje se obavlja zamenom vrednosti piksela ulazne slike sa medijanom lokalnog susedstva tog piksela. Lokalno susedstvo, ili prozor nad kojim se obavlja medijan operacija, ima najčešće neparan broj elemenata i dimenzije 3×3 , 5×5 ili 7×7 elemenata. Važna osobina medijan filtriranja je da uspešno uklanja impulsni šum iz slike, koji se manifestuje u vidu izolovanih piksela ili linija u slici. Pri tome je očuvana prostorna rezolucija slike.
- **Filtriranje korenovanjem** – Kod filtriranja korenovanjem vrši se nelinearna transformacija modula transformacionih koeficijenata, dok se fazni spektar ne menja. Filtriranje korenovanjem ističe male amplitude u spektru, a potiskuje velike. S obzirom na sadržaj spektra tipičnih slika, korenovanje ističe visoke učestanosti.
- **Homomorfno filtriranje** – Predstavlja nelinearnu filtarsku operaciju kod koje se prvo vrši logaritmovanje ulaznog signala, a zatim se na tako dobijeni signal primenjuju konvencionalni algoritmi linearnog filtriranja u prostornom ili transformacionom domenu. Na kraju se na dobijeni signal primeni eksponencijalna transformacija, čime se dobija obrađeni signal slike.

Metod homomorfnog filtriranja je pogodan za uklanjanje degradacija slike (šuma ili neuniformne osvetljenosti) koje su multiplikativnog karaktera. U tom slučaju, posle logaritmovanja, degradacije dobijaju aditivni karakter, pa ih je lakše eliminisati iz slike.

5.4 Otpornost digitalnih vodenih pečata na napade

Efikasnost tehnike označavanja otpornim vodenim pečatom može se ocenjivati prema: veličini i kompleksnosti vodenog pečata, statističkoj nevidljivosti, neprimetnosti, sigurnoj detekciji, kao i prema otpornosti na uklanjanje, otpornosti na distorziju, mogućnosti izmene i višestrukosti označavanja vodenog pečata. Svaki od ovih parametara je važan za postizanje funkcionalnosti pečata [8].

Otpornost se može postići ako je pečat postavljen u perceptualno bitno područje slike. To je zato što je kvalitet slike očuvan samo ako su perceptualno bitna područja slike zadržana. Dakle, perceptualno nebitna područja slike mogu biti uklonjena, a da se pri tome ne naruši kvalitet slike. Posledica toga je da pečati koji se nalaze u perceptualno nebitnim područjima neće biti otporni i mogu se lako ukloniti.

Otpornost pečata se može proveriti pomoću dva pitanja: da li je pečat prisutan u podacima nakon što signal pretrpi promene, i može li ga detektor pečata detektovati. Pečati koje mnogi algoritmi ubacuju, ostaju u podacima nakon geometrijskih promena (npr. skaliranje). Algoritmi detekcije mogu detektovati pečat samo ako se geometrijska promena prethodno ukloni. Ukoliko se promena ne ukloniti, detektor neće moći da detektuje pečat.

Kao što pečat mora biti otporan na uobičajene transformacije kroz koje dotični signal prolazi, pečat može biti podvrgnut i procesiranju signala koje je isključivo namenjeno uklanjanju pečata. Osim toga, kada postoji više kopija sadržaja označenih različitim pečatima, kao što je na primer slučaj sa označavanjem koje služi za identifikaciju kupca, mogući su dodatni napadi koji se baziraju na kombinaciji sadržaja nekoliko kupaca. Izuzetno je važno da pečat bude otporan na zloupotrebe. To se može postići na nekoliko načina: pomoću privatnog pečata, asimetričnog koda i dekodera, kao i pomoću neinvertibilnih pečata.

- **Privatni pečati** – Privatni pečat je sistem gde je potrebno poznavanje neoznačenog sadržaja za dekodovanje ili pseudo-slučajnog ključa koji generiše pečat, poznat samo pošiljaocu i primaocu. Privatni pečat je otporniji na napade od javnih pečata gde svako može da dekoduje pečat. Ukoliko je dostupna samo jedna označena kopija sadržaja, da bi se uništio pečat, jedini mogući napad je dodavanje šuma u sliku. Pokazalo se da je red veličine dodatog šuma, koji je potreban da bi se pečat sigurno uništio, toliko velik da značajno narušava kvalitet slike. Kada imamo više kopija istog sadržaja označenog različitim pečatima raspoloživi su drugi napadi, od kojih bi najjednostavniji bio računanje srednje vrednosti svih kopija. U slučaju da su raspoložive sve informacije potrebne za dekodovanje pečata, najjednostavniji napad je jednostavno invertovanje postupka označavanja.

- **Asimetrični koder/dekoder** – Ako uklanjanje javnog pečata zahteva invertovanje procesa kodovanja, poželjno je da proces kodovanja bude što je moguće više kompleksan, posebno ako se pečat unosi samo jednom. Ipak, ako dekoder mora da funkcioniše u realnom vremenu, onda je neophodno da proces dekodovanja bude znatno jednostavniji od kodovanja.
- **Neinvertibilni pečati** – Ako je proces unošenja pečata neinvertibilan, tj. ako je sam pečat generisan pomoću sadržaja koji se označava, onda reverzni proces brisanja pečata nije moguć bez posedovanja originalnog, neoznačenog sadržaja. Tako se sprečava da potencijalni napadač u označenom sadržaju potraži neki set vrednosti i onda njih proglasi za svoj pečat, stvarajući konfuziju oko toga ko zapravo ima originalni, neoznačeni sadržaj i ko je prvi ubacio pečat u sadržaj.

Ako korisnik poseduje veći broj digitalnih dokumenata, koji su označeni istim ključem, pečat ne sme biti otkriven primenom statističkih metoda, pa se koriste pečati koji su zavisni od sadržaja. Pečat se maskira pomoću pseudo-slučajnih sekvenci kako bi se postigla što veća sličnost pečata i slučajnog šuma. Što je pečat sličniji slučajnom šumu, to ga je teže otkriti, a samim tim i ukloniti.

Veličina pečata označava količinu informacija koja se može ubaciti u zadati signal. Ovaj parametar je posebno važan za javne pečate. Veličina pečata i njegova otpornost na manipulacije je obično obrnuto proporcionalna. Ukoliko želimo da u zadati signal ubacimo veću količinu podataka, neki od bitova će biti manje zaštićeni, jer će imati manje originalnih bitova koji bi ih maskirali. Zato je potrebno napraviti kompromis između otpornosti i veličine pečata.

Poželjno je da pečat bude takav da omogućuje veliki broj valjanih pečata. Što je broj mogućih pečata veći, veće su i mogućnosti primene sistema. Što su pečati međusobno više različiti, to će biti bolja verovatnoća tačne detekcije pečata u označenom materijalu.

U nekim okolnostima, poželjno je izmeniti pečat nakon unošenja. Na primer, u slučaju digitalnih video diskova, diskovi mogu biti označeni tako da omogućuju jednu kopiju sadržaja. Nakon što je kopija napravljena, potrebno je izmeniti pečat na originalu tako da se onemogući dalje kopiranje. Promena pečata se može postići tako da se prvobitni pečat ukloni i ubaci novi, ili da se ubaci novi pečat koji bi zabranio kopiranje. U prvom slučaju pečat je moguće ukloniti, što znači da takav sistem ne bi bio otporan na napade. U svakoj tački distributivnog lanca može se ubaciti novi jedinstveni pečat u sadržaj, pa je poželjno postojanje višestrukih pečata koji omogućuju praćenje sadržaja od mesta proizvodnje preko distribucije do eventualne prodaje.

6 Eksperimentalno okruženje - CrypTool

CrypTool je interaktivna kriptografska laboratorija razvijena kao „open-source“ projekat. Predstavljen je kao moćan alat za kombinovanje teorije i prakse u kriptologiji. Nudi vizuelizaciju pojmova, podataka i fundamentalnih kriptografskih objekata i metoda. Uključuje popularne algoritme i protokole za šifrovanje kao i više metoda za kriptanalizu. Moguće je modelovati metode za kriptanalizu. Kriptanaliza klasičnih i modernih šifara, na teoriskoj i praktičnoj osnovi, moguća je modelovanjem eksperimentalnog okruženja sa simulacijom u realnom vremenu. Sa nekim od kriptanalitičkih metoda moguće je razbiti klasične i moderne šifre. Na raspolaganju je mnogo funkcija za kriptanalizu, kao što su testovi frekvencija za analizu strukture prirodnih jezika [1].

CrypTool pruža grafički korisnički interfejs za vizuelno programiranje. Sa okruženjem je lako upravljati, a podaci mogu lako da se kontrolišu i vizuelizuju. Na taj način je ostvarena jednostavna interakcija sa kriptografskim funkcijama. Vektorski orijentisano grafičko okruženje daje korisnicima mogućnost dobrog trenutnog pregleda.

Mnoge komponente mogu da se koriste za vizuelizaciju toka programa (algoritma) i tako demonstriraju svoj unutrašnji rad. To omogućava korisniku da shvati sve detalje kriptografskog algoritma u realnom vremenu.

CrypTool je licenciran od strane Apache Open Source Licence 2.0. Laboratorija koristi originalne algoritme izrađene po NIST-ovom (engl. *National Institute of Standards and Technology*) standardu. Autori CrypTool-a nisu implementirali funkcionalnosti tamo gde su bili dostupni dobri besplatni programi na internetu. Tako, npr. rečnički napadi na datoteke sa lozinkama još uvek nisu deo CrypTool-a.

6.1 Skrivanje tajnih podataka primenom LSB supstitucije

U sledećem primeru korišćićemo LSB steganografsku tehniku u CrypTool projektu. Prvo ćemo da utisnemo tajnu poruku u nosilac poruke pomoću ključa. Za podatak nosilac izabrali smo sliku:



Slika 6.1.1: Podatak nosilac

U objekat podatka nosioca (slika 6.1.1) ugrađićemo sledeću tajnu poruku:

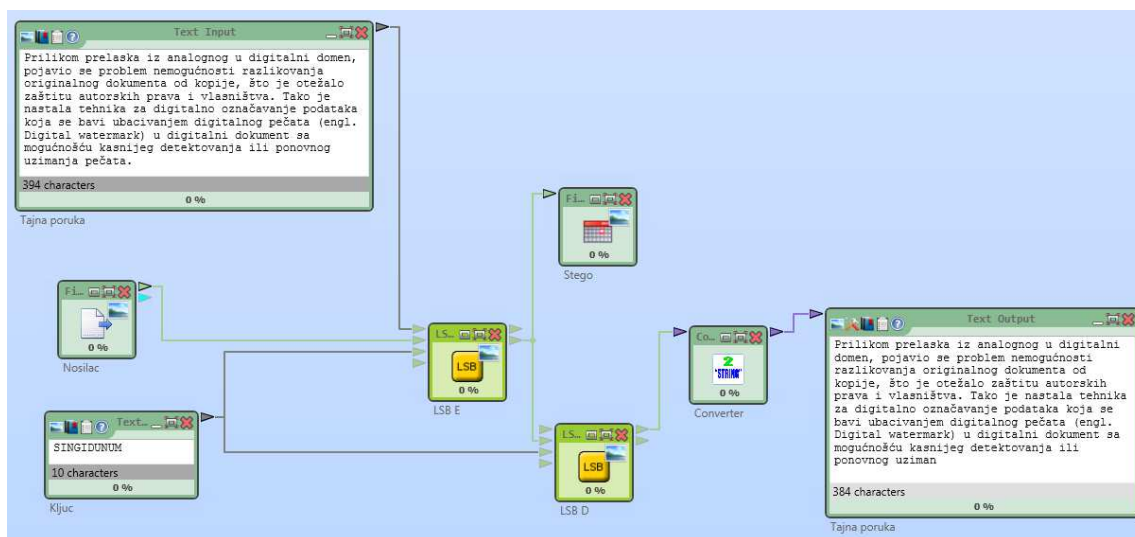
„Prilikom prelaska iz analognog u digitalni domen, pojavio se problem nemogućnosti razlikovanja originalnog dokumenta od kopije, što je otežalo zaštitu autorskih prava i vlasništva. Tako je nastala tehnika za digitalno označavanje podataka koja se bavi ubacivanjem digitalnog pečata (engl. Digital watermark) u digitalni dokument sa mogućnošću kasnijeg detektovanja ili ponovnog uzimanja pečata.“

Kao rezultat smo dobili steganografski objekat koji sadrži tajnu poruku (slika 6.1.2).



Slika 6.1.2: Stego podatak koji sadrži tajnu poruku

Nakon toga smo dekodovali steganografski podatak i uspeali da izdvojimo tajnu poruku.



Slika 6.1.3: LSB supstitucija - kreiranje stego objekta i izdvajanje tajne poruke iz stego objekta

Na osnovu dobijenih rezultata možemo da zaključimo da nema vidljivih promena na slici, tj. da nema razlike između podatka nosioca i stego podatka. Napadač može teško da posumnja da postoji tajna poruka unutar slike. Međutim, sa modifikacijom stego medijuma menjaju se njegova statistička svojstva, pa postoji mogućnost da napadač može da otkrije postojanje tajne poruke u stego medijumu, ali ne može da je pročita. Do tajne poruke se može doći jedino ako je ključ poznat. U ovom slučaju ključ je „SINGIDUNUM“. Ključ je tajni i poznat je samo pošiljaocu i primaocu tajne poruke.

Najjednostavniji i najpoznatiji slučaj šifrovanja je simetrično šifrovanje, kod kojeg i pošiljalac i primalac imaju zajednički ključ. Kod simetričnog šifrovanja napadač, i ako poznaje šifrat, teško može da dođe do otvorenog teksta. Napadač bi mogao da dođe do otvorenog teksta u 2^n pokušaja, pod uslovom da je n neki mali broj. Takođe, napadač može da poznaje model šifarskog sistema, algoritam po kojem je vršeno šifrovanje ili da ima na raspolaganju šifrat, ali ako napadač ne zna ključ, nije u stanju da otkrije tajnu poruku koja se prenosi.

7 Zaključak

Digitalni vodeni pečati se primenjuju u legalne svrhe, pa su veoma značajni za utvrđivanje vlasništva i autorskih prava nad dokumentima, ali se takođe koriste i kao sigurnije metode za čuvanje važnih i poverljivih informacija ili podataka.

Kao što smo mogli da vidimo, digitalni vodeni pečati raspolažu sa efikasnim i snažnim tehnikama koje omogućavaju bezbednu i sigurnu komunikaciju i razmenu podataka u savremenom životu. Digitalni vodeni pečati su vrlo jednostavni za upotrebu i veoma su pouzdani. Ukoliko vodeni pečat predstavlja skriveni tekst unutar slike, veoma teško se otkriva. U kombinaciji sa kriptografijom digitalni vodeni pečati predstavljaju dodatni stepen sigurnosti u zaštiti informacija.

U ovom radu razmatrali smo algoritme za ugrađivanje digitalnog vodenog pečata u sliku. Takođe, dat je pregled skorijih istraživanja u ovoj oblasti, kao i detaljan pregled teorijske osnove istraživanja. Osim toga, govorili smo o napadima na digitalne vodene pečate i njihovoj robustnosti.

Poslednji deo rada je fokusiran na analizi algoritma i na generalnu upotrebu skrivanja i zaštite informacija, kao i pregled algoritma detekcije. Data je verovatnoća mogućnosti napada na taj sistem i kako napadač može da dođe do tajnog podatka.

Sa razvojem tehnologije razvila se i zloupotreba digitalnih multimedijalnih sadržaja na Internetu. U poslednjih nekoliko godina, radilo se intenzivno na unapređenju i razvoju digitalnih vodenih pečata, ali sa razvojem algoritama za utiskivanje digitalnih vodenih pečata razvili su se i napadi na iste, kojih ima sve više. Naš cilj, za neki budući rad, je da napravimo neki snažniji algoritam koji će, u kombinaciji sa nekom kriptografskom tehnikom, biti delimično ili možda čak potpuno otporan na napade.

Literatura

- [1] M. Veinović, S. Adamović, **Kriptologija 1**, Univerzitet Sigidunum, Beograd, 2013.
- [2] M. Popović, **Digitalna obrada slike**, Akademska misao, Beograd, 2006.
- [3] M. Petrović, **Osnovi televizije - Priručnik za laboratorijske vežbe**, Visoka škola elektrotehnike i računarstva, Beograd, 2010.
- [4] Prabhishek Singh, R S Chadha, „A Survey of Digital Watermarking Techniques, Applications and Attacks“, International Journal of Engineering and Innovative Technology (IJEIT), Volume 2, Issue 9, pp.165-175, March 2013.
- [5] Rajendra D Kanphade, Navnath S Narawade, „Robust Semi-Reversible Watermarking Using Pixel Averaging Method Against Geometric Attack“, The IUP Journal of Telecommunications, Vol. V, No. 1, pp.46-55, 2013.
- [6] Mohit Gupta, Deep Tarun Gupta, Vikas Saxena, „A Wavelet-Based Watermarking Scheme for Color Images“, The IUP Journal of Telecommunications, Vol. V, No. 2, pp.56-66, 2013.
- [7] Rajendra D Kanphade, Navnath S Narawade, „Robust Reversible Watermarking Against Geometric Attack Using Geometric Transformation Correction Applied on Spatial Domain Methods“, The IUP Journal of Telecommunications, Vol. V, No. 3, pp.47-56, 2013.
- [8] Samčović, G. Murić, „Primena tehnike digitalnog vodenog žiga u zaštiti vlasništva nad slikama“, Konferencija o bezbednosti informacija BISEC 2013, str.64-69, Beograd, 2013.
Preuzeto sa: <http://bisec.rs/wp-content/uploads/Zbornik-Finis-2013.pdf>
- [9] D. Uljarević, M. Veinović, „Digitalna steganografija JPEG slika primenom DCT transformacije“, INFOTECH 2013 ICT Conference & Exhibition, Arandelovac, 2013.
Preuzeto sa: <http://www.infotech.org.rs/blog/autorski-radovi-infotech-2013/>
- [10] Nacionalni CERT, LSS, NCERT-PUBDOC-2010-08-310, „Digitalni vodeni žigovi“, Hrvatska Akademska Istraživačka Mreža, Zagreb, 2010.
Preuzeto sa: <http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-08-310.pdf>
- [11] M. Đuričkov, Master rad, „Antiforenzicke tehnike i alati“, Fakultet za informatiku i menadžment, Beograd, 2009.
Preuzeto sa: www.singipedia.sigidunum.ac.rs/
- [12] V. Vučković, Doktorska disertacija, „Optimalna snaga žiga belog Gausovog šuma“, Matematički fakultet, Beograd, 2010.
Preuzeto sa: <http://elibrary.matf.bg.ac.rs/>
- [13] M. Topalović, Diplomski rad, „Digitalni vodeni žig“, Univerzitet Vitez, Travnik, 2012.
- [14] H. Šalković, Diplomski rad br. 618, „Primjena digitalnog vodenog žiga u zaštiti vlasništva slika u digitalnom zapisu“, Fakultet elektrotehnike i računarstva, Zagreb, 2013.