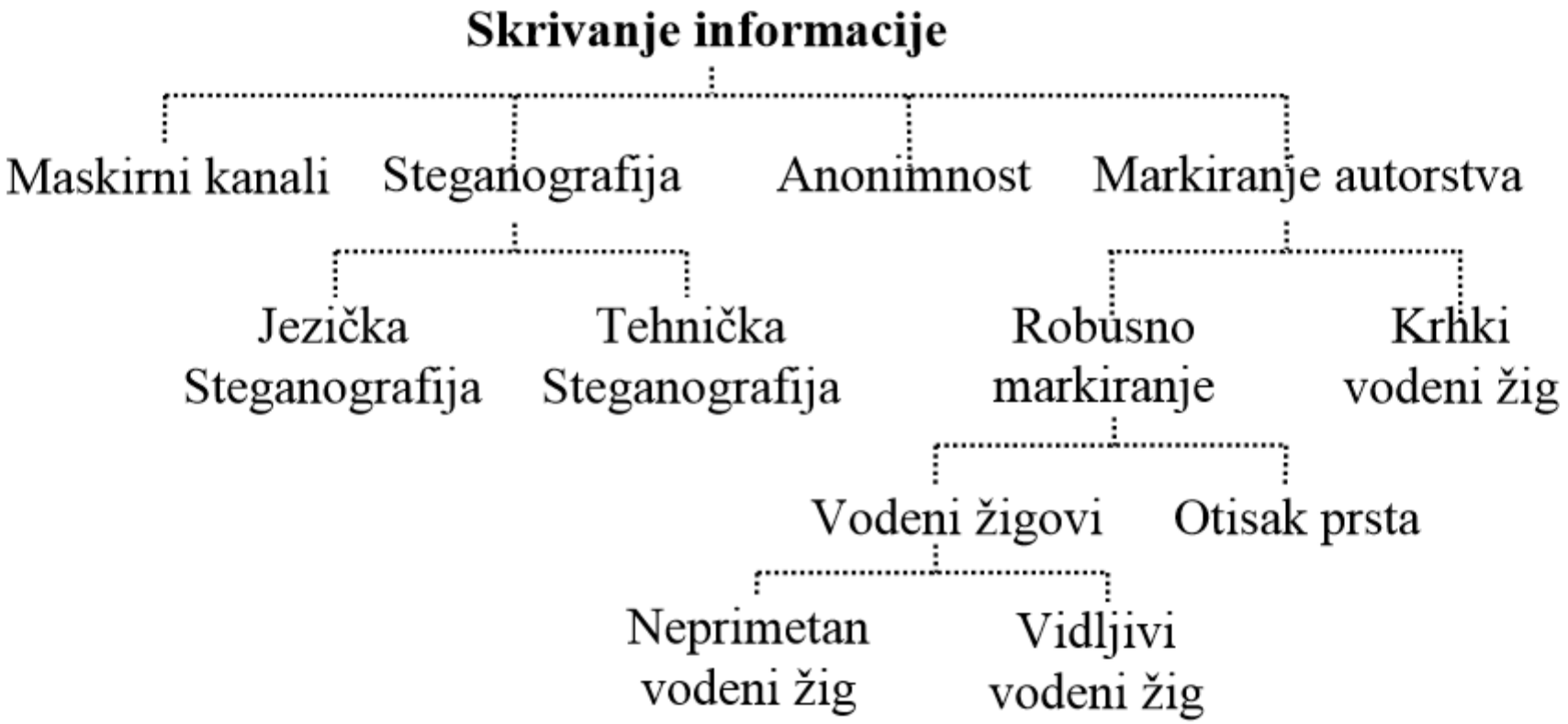
Zaštita digitalnog sadržaja
Digitalni Watermark

Sadržaj

- Istorija skrivanja informacija
- Steganografija
- Digitalni Watermarking
  - Osnovni principi
  - Zahtevi
  - Tehnike i Algoritmi
  - Image watermarking
  - Osobine
  - Robusnost
  - Primene

Uvod

- *Watermarking* je, uz *steganografiju*, jedna od najpoznatijih primena skrivanja informacija.
- Dok se steganografija bavi proučavanjem načina kako sakriti informaciju tj. komunikaciju u naizgled nebitni sadržaj, metode watermarkinga razvile su se zahvaljujući potrebi za autorskom zaštitom digitalnog sadržaja.
- Razvoj metoda watermarkinga je pojačan u poslednje vreme, što govori i podatak o porastu broja objavljenih radova na ovu temu. Značajan uticaj na razvoj ima sve veći broj digitalnih sadržaja na mreži i uopšte čije se autorstvo štiti.



Slika 3. *Klasifikacija tehnika skrivanja informacije bazirano na [08].*

Discipline i istorija skrivanja informacija

Anonimnost

Steganografija (razlike u odnosu na kriptografiju)

Watermarking (razlike u odnosu na steganografiju)

Istorija skrivanja informacija

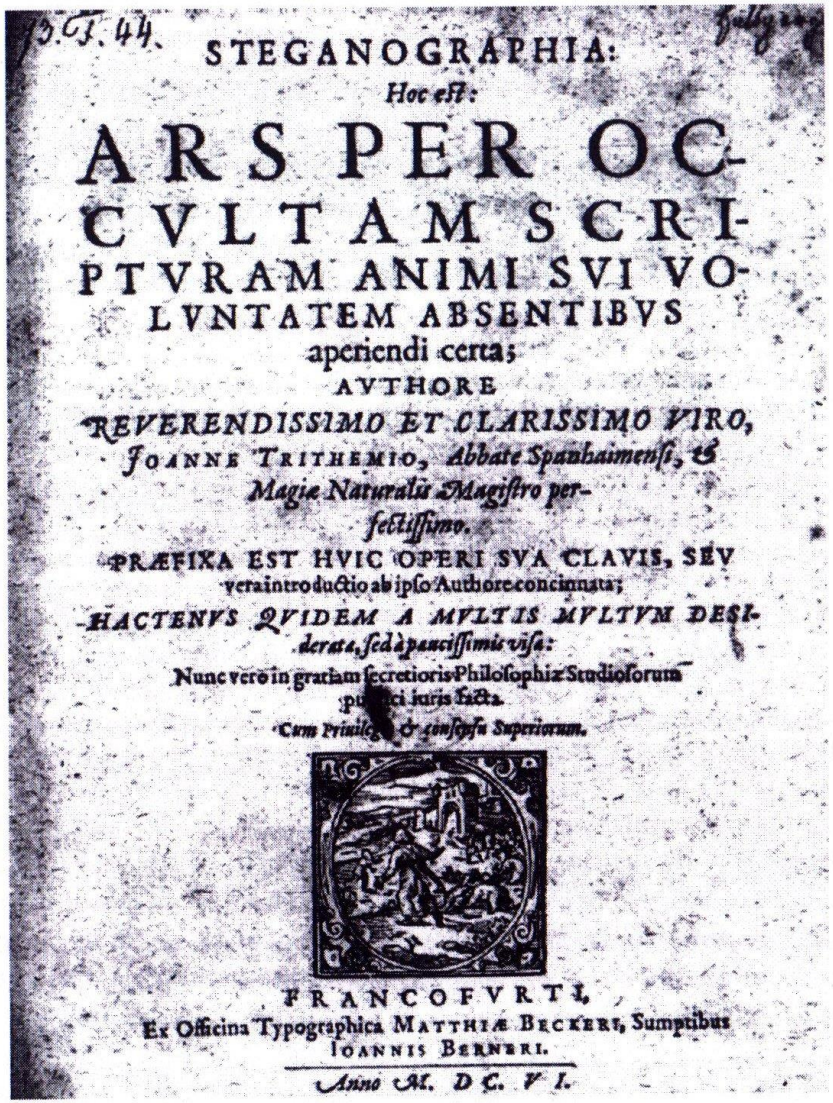
Anonimnost

- *Anonimnost* je disciplina skrivanja informacija u kojima se menja ili skriva meta-sadržaj poruke, npr. pošiljalac ili primalac.
- Primene ovakvih metoda skrivanja informacija su vrlo česte toliko da ih ponekad ni ne primećujemo: npr. skrivanje popisa primaoca poruke (popularni "undisclosed-recipients") u e-mail komunikaciji, zatim skrivanje pošiljaoca poruke kod slanja spam poruka itd..

Steganografija

- *Steganografija* je veština skrivanja samog postojanja informacija, dok se kriptografija, sa kojom se često meša bavi zaštitom sadržaja informacije (informacija je vidljiva ali je kriptovana na način koji je nepoznat onom kome poruka nije namenjena).
- Sama reč je grčkog porekla i doslovno znači "**skriveno pisanje**", a primeri steganografije su prisutni u skoro svim špijunskim filmovima – pisanje nevidljivim mastilom, snimanje jedva čujnih poruka u neki audio sadržaj i slično.

Jedna od prvih knjiga o steganografiji



STEGANOGRAPHIA:

Hoc eſt:

ARS PER OCCVLTAM SCRIPTVRAM ANIMI SVI VOLVNTATEM ABSENTIBVS aperiendi certa;

AVTHORE

REVERENDISSIMO ET CLARISSIMO VIRO,

IOANNE TRITHEMIO, Abbate Spanhaimenſi, & Magiæ Naturalis Magiſtro perfectiſſimo.

PRÆFIXA EST HVIC OPERI SVA CLAVIS, SEV veraintroductio ab ipſo Authore concinnata;

HACTENVS QVIDEM A MVLTIS MVLTVM DESIderata, ſed à paucissimis viſa:

Nunc vero in gratiam ſecretioris Philoſophiæ Studioſorum publici iuris facta.

Cum Priuilegio & conſenſu Superiorum.

FRANCOFVRTI,

Ex Officina Typographica MATTHIÆ BECKERI, Sumptibus IOANNIS BERNERI.

Anno M. DC. VI.

Watermarking

- *Watermarking* je ubacivanje informacija u neki sadržaj, sa osnovnim zadatkom da mora biti otporan, tj. da se iz sadržaja ne može lako ukloniti. Šta je "lako", i kako ga ukloniti, zavisi i od funkcije watermarka i od samog sadržaja.
- Glavna razlika između steganografije i watermarkinga jeste da watermark ne mora nužno biti nevidljiv.
- Takođe, razlika je i u primeni – u steganografiji je primena isključivo skrivanje informacija, a u watermarking-u je zaštita autorskih prava ili dodavanje informacija vezanih uz sadržaj.
- Takođe, komunikacija je u steganografiji obično prirode jedan na jedan (tj. od pošiljaoca primaocu), a u watermarkingu jedan na više.

Istorija skrivanja informacija

- Sami začeci skrivanja informacija sežu još u antička vremena - Herodot npr. opisuje kako su Rimske vojskovođe oko 440 pre nove ere brijali glave svojih najvernijih sluga, tetovirali im poruke na glavu, puštali da im kosa ponovno izraste, i onda ih slali na destinaciju. Istu metodu koristili su i nemački špijuni na početku 20. veka.
- Grci su takođe skrivali poruke u ženske minđuše, a i bili su prvi koji su koristili golubove pismonoše, što se u to vreme moglo smatrati korišćenjem tajnih kanala, jer se na golubove nije sumnjalo da nose bilo kakve poruke.
- u 17. veku počela su da se koriste nevidljiva mastila koja su ostala u upotrebi sve do kraja II svetskog rata (a primer su i čekovi u Americi koji su koristili specijalna mastila koja su vidljiva samo u ultraljubičastom spektru koji je izrazito prisutan u lampama fotokopirnih uređaja – čime se sprečava fotokopiranje), zaštita novčanica
- Zanimljiv rad na temu lingvističke steganografije je Hypnerotomachia Poliphili od nepoznatog autora davne 1499.godine. U tom delu govori se o zabranjenoj ljubavi između sveštenika i jedne žene: Kad se spoje prva slova naslova iz 38 poglavlja tog dela i prevedu sa latinskog bukvalno znače "Brat Francesco Colonna strastveno voli Poliu“

O watermarkingu

Terminologija

Osnovni principi watermarkinga

Primene

Zahtevi watermarking sistema

Terminologija

- Termin "watermark" u prevodu znači "vodeni žig", koji možemo videti na gotovo svim novčanicama. Prvi vodeni žigovi pojavili su se već davne 1292. godine u Italiji kako bi označili poreklo papira tj. označili iz koje od tadašnjih 40 štamparija, je stigao.
- Primena klasičnih, papirnatih vodenih žigova uticala je da se i u kontekstu digitalnih podataka koristi ovaj termin za označavanje zaštite autorskih prava.
- Uz watermarking se pojavljuju razni pojmovi koji označavaju specijalne primene ili tehnike. Neki od njih su: **Vidljivi watermark, fingerprinting, Labeling, Embedded signatures, Fragile watermarks**

Primer

Novčanica od 100 USD i watermark koji se na njoj nalazi

USD, Euro - žigovi

Watermark

RSD žigovi

Watermark

Sistemi zaštite novčanica

- **Rastuća veličina serijskog broja –** Serijski broj se neznatno povećava u visinu i širinu, sa svakom novom cifrom u serijskom broju.
- **Bar kodovi i numeracije –** Koristi se uglavnom za čekove banaka. Samo mali broj zemalja se odlučio na ovaj sistem zaštite.
- **Obojena vlakna –** Vlakna su najčešće crvene, plave ili zelene boje. Dodaju se u mešavinu celuloze od koje se pravi papir za novčanice ili se dodaju u procesu sušenja papira, nasumično, po celoj površini papira. Ova vlakna su vidljiva golim okom posmatrača.
- **Sigurnosna nit –** Sigurnosne niti su niti velike čvrstoće, ponekad su i namagnetisane. Ugrađuju se u papir za izradu novčanica na početku faze sušenja papira. Vide se golim okom kao tanka, tamna nit u samom papiru.
- **Izdignute oznake –** Vrsta Brajevog crteža na novčanicama, omogućuje slepim ljudima da prepoznaju vrednost novčanice koju drže u rukama.

Sistemi zaštite novčanica

- **Transparentni dizajn –** tehnika gde se jedna polovina određene slike štampa na aversu, a druga polovina iste slike na reversu novčanice, ali tako da se tačno poklapaju. Kada se ovakva novčanicu pogleda prema svetlu, ove dve polovine daju jednu celu sliku.
- **Folija –** Neke novčanice kao zaštitu imaju tanku metalnu foliju koja se nalazi u tragovima.
- **Hologram –** Svetlucava aplikacija koja sadrži sliku koja menja boju i dizajn, u zavisnosti od ugla pod kojim se gleda.
- **Nevidljiva štampa –** Novčanica je štampana bojom koja je vidljiva samo na jakoj sunčevoj svetlosti ili pod ultraljubičastom svetlošću. Ponekad se koristi za novčanice male nominalne vrednosti, kao zamena za skuplji vodeni žig.
- **Skrivene impresije –**Delovi novčanice sadrže gravure, koje prikazuju određeni crtež ili legende, a vidljive su samo kada ih posmatrate na jakom svetlu ili pod određenim uglom.

Sistemi zaštite novčanica

- **Kinegram –** Slično kao i "Folija", crteži i boje se menjaju kada ih posmatrate pod različitim uglovima.
- **Metalik boja –** Boja koja sadrži veoma sitne granule metala, koje daju tzv "metalik sjaj".
- **Mikro štampa –** Veoma mala slova se dodaju na štampanu ploču u procesu izrade novčanica. Ponekad se dodaju samo pojedinačne linije, a ponekad linije u više redova, koje zajedno formiraju jedan veći blok linija. Duboka štampa prikazuje ctrež oštro i jasno, ali ako je reč o falsifikatu oblast koja je bila izložena mikro štampi je mutna i nejasna.
- **Promenljivi optički element –** Folija koja prikazuje trodimenzionalnu sliku kada se gleda pod određenim uslovima osvetljenja.
- **Optički promenjiva boja –** Boja koja se štampa na specijalnim kalupima i koja menja svoje nijanse u zavisnosti pod koji uglom se posmatra.
- **Planšete –** Mali, raznobojni diskovi papira ugrađeni u mix celuloze, ili nasumično posuti po papiru za izradu novčanica, u procesu sušenja.

Sistemi zaštite novčanica

- **Segmentirana (podeljena) sigurnosna nit -** Zaštitna nit iz jednog dela, obično malo širih dimenzija i sa slovima, koja se dodaje na papir u toku procesa sušenja. Kada se doda na papir, koristi se specijalan alat da se, još uvek mokar papir provuče iznad niti, u određenom obrascu. Na ovaj način se pojedini delovi niti jasno vide.
- **Ultraviolet (flourescentno) osvetljenje -** Kada se novčanica posmatra u zamračenom prostoru i izloži UV svetlosti, njeni pojedini delovi i segmenti (nominalna vrednost, vlakna,…) će svetleti.
- **Vodeni žig -** Intenzivno se koristi kao sistem zaštite. Vodeni žig nastaje izradom crteža (mustre) u cilindru za sušenje, pri kraju procesa za proizvodnju papira za izradu novčanica. Izrada crteža stvara tanak prostor u papiru, koji kada se gleda prema svetlosti prikazuje portret, reči ili sliku. Ova tehnologija je u zadnje vreme napredovala i postignut je još bolji postepeni prelazak od svetle do tamne nijanse vodenog žiga.

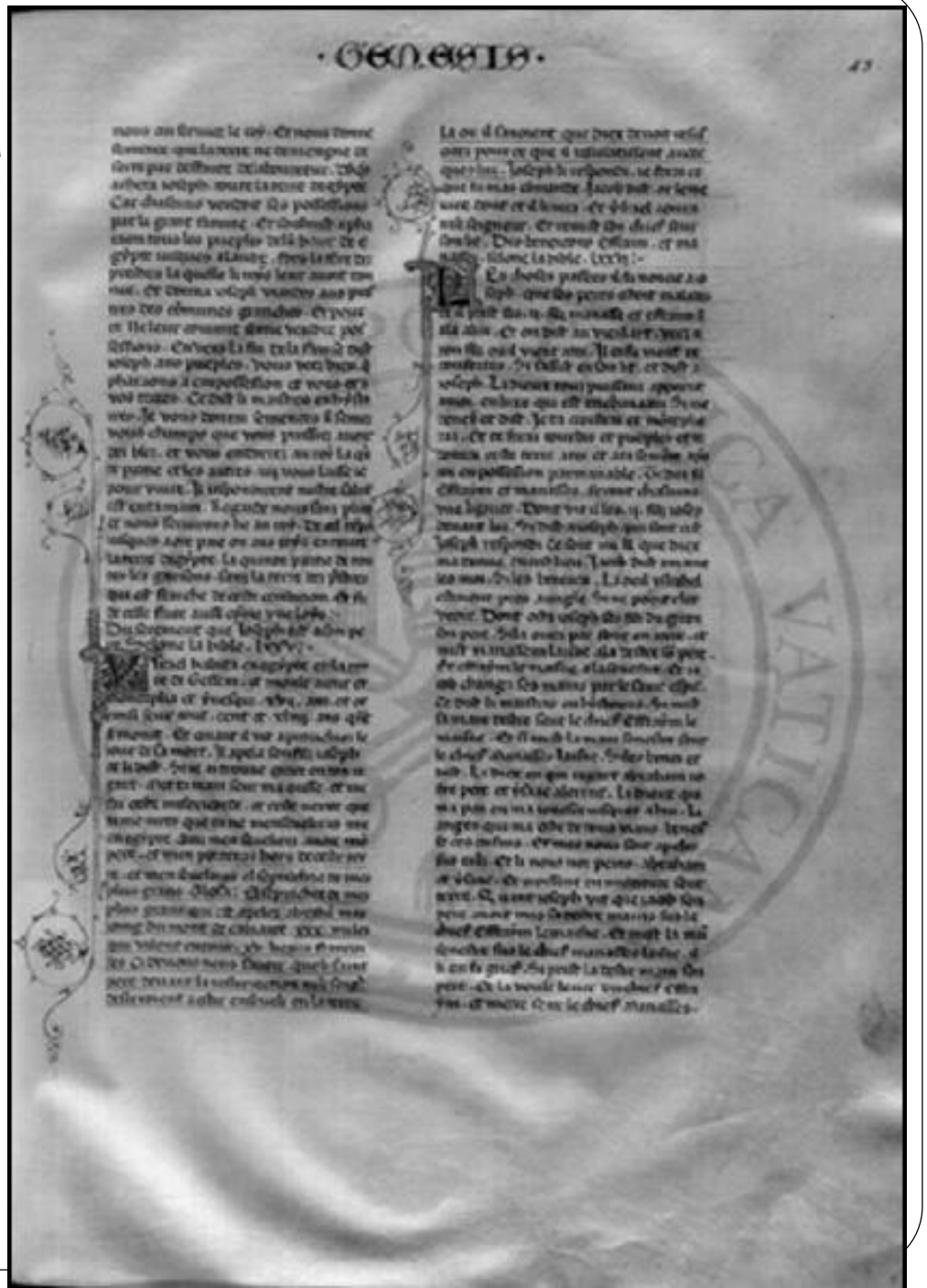
Vrste i primene watermarka (1)

- Vidljivi watermark - vizuelni uzorak (npr. logo) koji se ubacuje na sliku ili video, vrlo sličan vidljivom papirnatom vodenom žigu. Najčešće se upotrebljava na slikama prisutnim na internetu, kako bi se original zaštitio od kopiranja ili upotrebe u komercijalne svrhe.
- Jedan od primera široke primene vidljivih watermarka je dodavanje zaštitnog logoa u IBM projektu „Vatikanske knjižnice". Primeri: logo na TV kanalima, free sample copy, …
- Fingerprinting - posebna primena watermarkinga kod koje se informacije (npr. o autoru ili primaocu digitalnog sadržaja) ugrađuju u sam sadržaj u obliku watermarka.

Vatikanska knjižica

- Primer jedne stranice

„Vatikanske knjižice“ na internetu

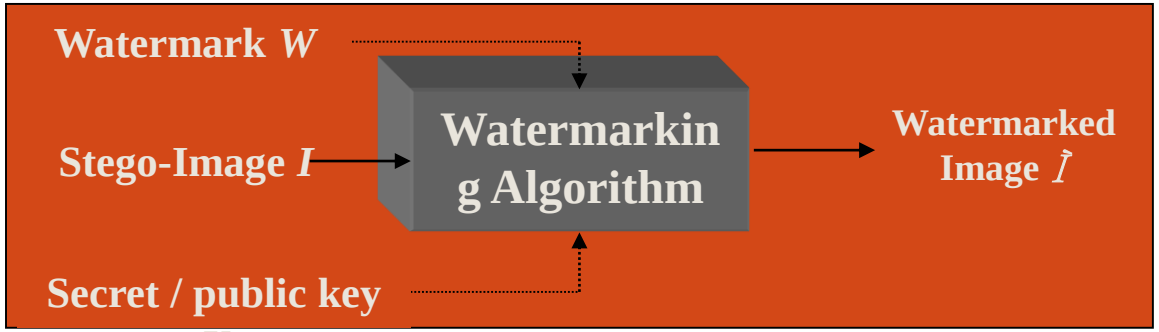


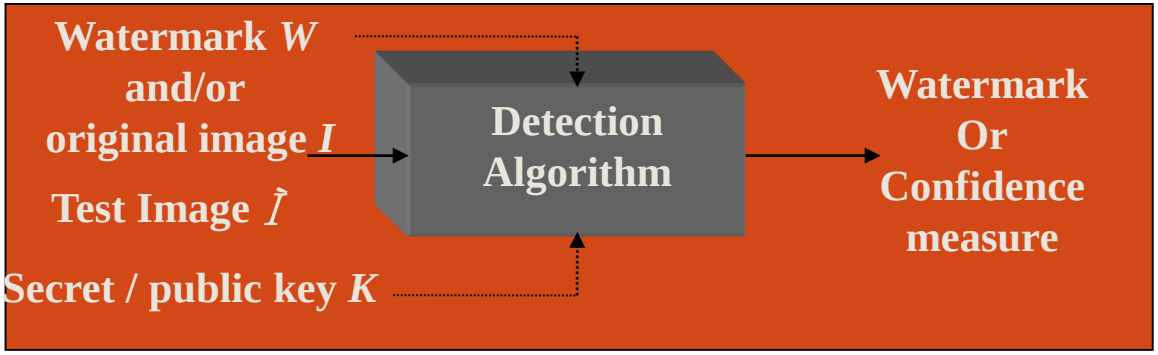
Vrste i primene watermarka (2)

- Labeling - posebna primena watermarkinga kod koje ubačena informacija u obliku watermarka ima svrhu dodatnog obeležavanja sadržaja (npr. u slučaju neke slike dodatne informacije o slici "ulje na platnu, 2017. godina")
- Embedded signatures - (ugrađeni potpisi) je pojam koji se u ranim radovima koristio umesto pojma watermark, ali je napušten jer se vrlo često pogrešno povezuje sa pojmom digitalnog potpisa. Koja je bitna razlika između ova dva pojma može ilustrovati činjenica da je digitalni potpis dizajniran kako bi detektovao svaku i najmanju promenu u dokumentu (tako se čuva autentičnost), dok je watermark (tj. ugrađeni potpis) dizajniran upravo tako da bude neosetljiv na promene u dokumentu.
- Fragile watermarks - su dizajnirani upravo sa vrlo malom robustnošću tj. otporom na izmene, sa svrhom detekcije menjanja sadržaja

Osnovni principi watermarkinga

- Sve metode watermarkinga imaju dva osnovna dela: deo za ubacivanje watermarka i deo za izdvajanje watermarka





- Sve watermark sisteme u praksi karakterišu osobine kao što su: neprimetnost, redundantnost, ključevi, …

Primene watermarkinga

- Zaštita autorskih prava

  -Najviše se ulaže; zaštita autorskih prava; ubacuje se informacija o autoru; nagli razvoj razvojem interneta; mora biti robustan; mora biti otporan na dodavanje novog sadržaja.

- Fingerprinting

  -U sadržaj se ubacuju informacije o primaocu podataka, i na ovaj način se može relativno jednostavno pratiti i odrediti izvor ilegalno napravljenih kopija; obično se u svaku kopiju ubacuje jedinstveni watermark (kao serijski broj); mora biti robustan i lak za ekstrahovanje radi brze provere legalnosti kopije.

- Copy protection

  -Onemogućavanje kopiranja digitalnog sadržaja u distribuciji multimedijalnog sadržaja sve je interesantnije. Npr.DVD koji prati standard sa statusom „omogući reprodukciju" ili pak status „ne kopiraj".

- Identifikovanje slike

  -fragile watermarks, najmanje robustan, gde je bitno odrediti da li je neka slika autentična ili ne, odnosno da li se sadržaj promenio i za koliko.

Zahtevi watermarking sistema 1

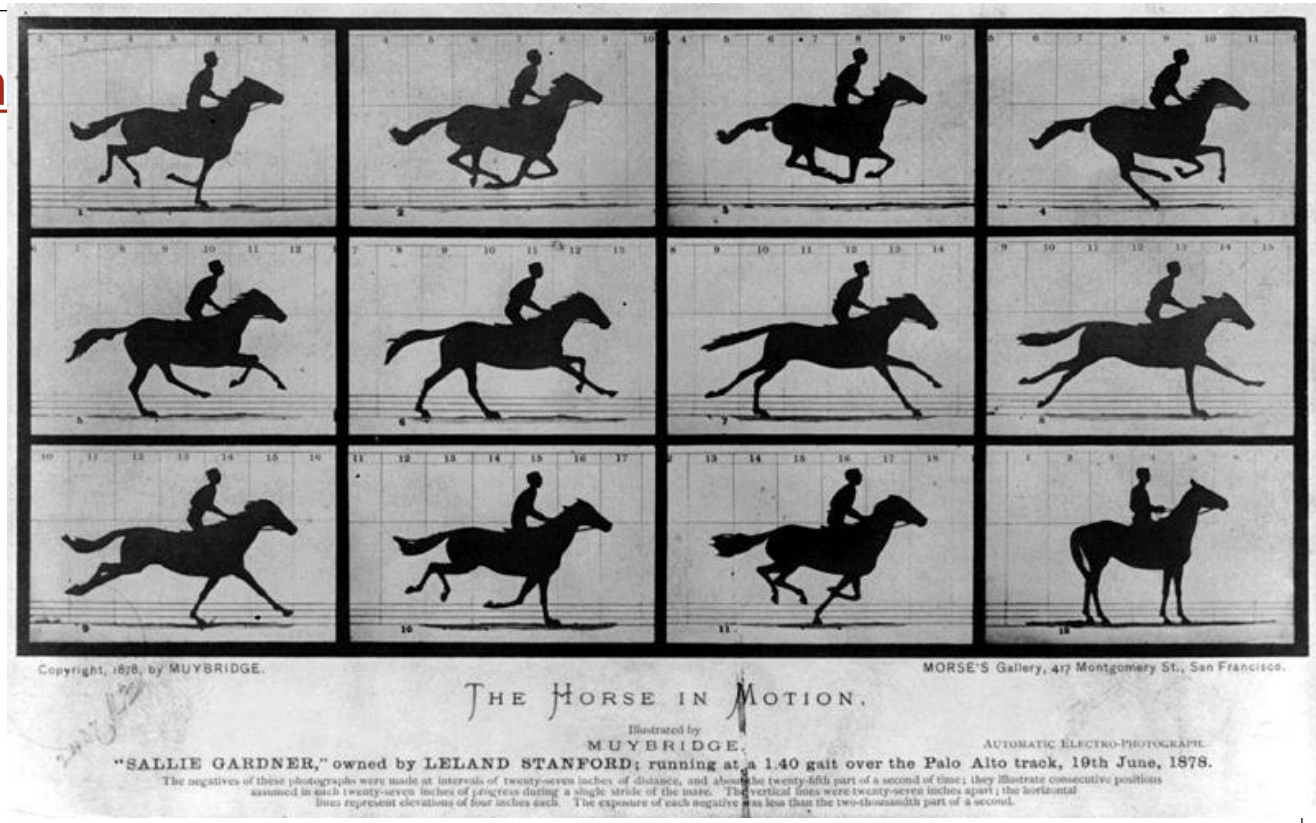
- **Neprimetnost**

  Jedan od najbitnijih zahteva (karakteristika) na watermark sisteme je **neprimetnost**, nezavisno od primene sistema. Ukoliko je ubačena informacija primetna tj. vidljiva, ona je u boljem slučaju neželjena tj. smeta, dok u lošijem čak čini sadržaj neupotrebljivim. Vrlo je važno dizajnirati watermark sistem koji iskorišćava nesavršenost ljudskih čula kako bi se ubacilo što više informacija a da se pritom ne pređe prag vidljivosti. Vrlo je bitno prilikom projektovanja sistema dobro odrediti koliko zapravo distorzije watermark u sistem unosi, ili kako će se razna procesiranja koja se očekuju na sadržaju (npr. povećanje slike, rotacija) odraziti na prag vidljivosti.

- **Autorska prava**

  Kako bi se osiguralo ispravno utvrđivanje autorskih prava, prilikom projektovanja watermarka potrebno je osigurati mogućnost detekcije redosleda ubacivanja watermarka (u svaki sadržaj moguće je dodati više watermarka). Ovakve zahteve moguće je ostvariti npr. posebnim timestamp-ingom i neinverznošću ubačenih watermarka.

Nesavršenost ljudskih čula - Video



Kao ilustracija može da posluži niz od 12 fotografija konja u pokretu. The Horse in Motion by Eadweard Muybridge. Noted photographer, Eadweard Muybridge was hired, in 1872, by Leland Stanford a railroad baron and future university founder, to find out if there was moment mid-stride where horses had all hooves off the ground.[1] It took several years but Muybridge delivered having captured a horse, named "Sallie Gardner," owned by Stanford; running at a 1:40 gait over the Palo Alto track, on 19th June 1878.[1] Muybridge used a dozen cameras all triggered one after another with a set of strings. [1]

Zahtevi watermarking sistema 2

- **Robusnost**

  Savršeni watermark sistem morao bi podneti svako modifikovanje, menjanje i distorziju primenjeno na sadržaj u standardnim (npr. izoštravanje slike) ili zlonamernim (uništavanje watermarka) procesima. Savršene metode (za sada) nema i nije sigurno da li uopšte postoji.

- Neki od napada na koje watermark mora biti otporan su npr:

  - Poboljšanje signala (npr. izoštravanje, pojačanje kontrasta, korekcija boje ili gama kanala),
  - Aditivni ili multiplikativni šum (Gaussov šum, uniformni šum),
  - Linearno filtriranje (niskopropusni ili visokopropusni filter),
  - Nelinearno filtriranje (median filter),
  - Kompresije s gubitkom (JPEG),
  - Geometrijske transformacije (rotacija, skaliranje),
  - Redukcija podataka (cropping, clipping, modifikacija histograma),
  - Kompozicija podataka (dodavanje logoa, kompozicija scene),
  - Transkodiranje (JPEG->GIF),
  - D/A i A/D konverzija,
  - Višestruki watermark, Mozaični napad

Zahtevi watermarking sistema 3

- **Sigurnost watermarka i ključevi**

  U nekim primenama watermarkinga potrebno je ubačenu informaciju u sistem zaštititi od neovlašćenog korišćenja ili detektovanja. Ukoliko je sigurnost tj. privatnost nužna, moguće ju je implementirati uvođenjem tajnog ključa prilikom ubacivanja watermarka, čime se mogu dobiti dva osnovna nivoa sigurnosti:

1.) **Visok nivo:** izabrani mehanizam mora osiguravati da neovlašćeni korisnik ne samo da ne može pročitati informaciju koja je ubačena watermarkom, već ne može ni detektovati da je u originalni sadržaj watermark ubačen

2.) **Nizak nivo:** izabrani mehanizam mora osiguravati da neovlašćeni korisnik ne može pročitati informaciju koja je ubačena u watermark bez posedovanja tajnog ključa, ali spomenuti watermark može detektovati

Tehnike watermarkinga

- **Odabir pixela ili blokova u koje će watermark biti uključen**
  - Patchwork algoritam
  - Public key kriptografija i watermarking
  - Prediktivno kodovanje i vizuelni izbor pixela
- **Odabir domena**
  - Diskretna Fourierova transformacija
  - Diskretna kosinusna transformacija
  - Mellin-Fourierova transformacija
- **Formatiranje poruke**
  - Raspršeni spektar (spread spectrum)
  - Korišćenje niskih frekvencija
  - Error-correcting codes
- **Spajanje watermarka i pokrivača, Optimizacija watermark receivera**

Patchwork algoritam

- Patchwork algoritam-ubacivanje poruke u sadržaj (može i sa tajnim ključem)

Pomoću tajnog ključa **K** koji korisnik koristi kao seme za generator slučajnih brojeva, odabira se ***n*** parova (**a**i, **b**i) kojima se menja luminiscencija na sledeći način:

$$\bar{a}_i = a_i + 1$$

$$\bar{b}_i = b_i + 1$$

Prilikom detekcije jednostavno se na izabranim pixelima primeni sledeći operator sume

$$S = \sum_{i=1}^{n} \bar{a}_i - \bar{b}_i$$

Ukoliko korisnik zna ključ, njegova bi suma trebala biti približno **2n**, dok bi u suprotnom slučaju suma trebala biti 0, jer

$$E[S] = \sum_{i=1}^{n} (E[a_i] - E[b_i]) = 0$$

Public key kriptografija i watermarking

- Ubacivanje tajnog ključa predstavlja velik problem – naime, bez posedovanja tajnog ključa nije moguće pročitati watermark.
- Ubacivanjem elemenata public key kriptografije moguće je koristiti tajni ključ za ubacivanje watermarka, a javni ključ za detektovanje ili verifikaciju watermarkinga.
- Jedan od mogućih načina implementacije jeste ubacivanje redundantnosti u watermark, čime je moguće da javni ključ na slučajni način izabira **n** potrebnih bitova watermarka, uvek na različiti način, dok tajni ključ pokazuje na sve pozicije bitova.

Prediktivno kodovanje i vizuelni izbor pixela

- Prediktivno kodovanje je vrlo popularno u kodovanju signala, naročito slika. Temelji se na predviđanju vrednosti sledećeg bita u zavisnosti od prethodnog bita, što je često vrlo efikasno kada postoji korelacija između bitova kao što je to npr. na slikama neke prirode.
- Grubo rečeno, ovom metodom kodira se tzv. greška, tj. razlika između stvarne i predviđene vrednosti pixela.
- U kontekstu watermarka, prediktivno kodovanje je korisno jer je ljudsko oko manje precizno u delovima slika gde su aplicirane razne teksture ili ima puno ivica, dok je vrlo osetljivo u delovima gde je površina ravna te uniformna. Kod prediktivnog kodovanja ta se područja lako detektuju jer se distribucija greške poklapa sa tim područjima, pa se signal greške može koristiti kao nosioc modulacije za signal watermarka.

Diskretna Fourierova transformacija

- Jedna od najpopularnijih transformacija u disciplini obrade signala,
- DFT u sferi watermarkinga nudi mogućnost kontrolisanja frekvencija signala originalnog sadržaja, tj. prilikom odabira adekvatnog mesta za ubacivanje watermarka.
- Nije često korišćena u svom izvornom obliku, nego se češće koriste njeni derivati: diskretna kosinusna transformacija i Mellin-Fourierova transformacija.

$$X_k = \sum_{n=0}^{N-1} x_n \cdot e^{-i 2\pi k n / N}$$

$$= \sum_{n=0}^{N-1} x_n \cdot [\cos(2\pi k n / N) - i \cdot \sin(2\pi k n / N)],$$

$$x_n = \frac{1}{N} \sum_{k=0}^{N-1} X_k \cdot e^{i 2\pi k n / N}, \quad n \in \mathbb{Z},$$

Diskretna kosinusna transformacija

$$X_k = \sum_{n=0}^{N-1} x_n \cos\left[\frac{\pi}{N}\left(n+\frac{1}{2}\right)k\right] \qquad k = 0, \ldots, N-1.$$

- Kako je ova transformacija vrlo popularna u svetu digitalne fotografije i videa (JPEG i MPEG kompresija), ova transformacija nametnula se kao rešenje za watermarking iz sledećih razloga:
  - veća otpornost na napade JPEG i MPEG kompresijom,
  - vrlo mala uneta distorzija jer se područja odabiraju prediktivnim kodovanjem,
  - mogućnost detektovanja watermarka direktno u transformacionom domenu, što utiče na brzinu detekcije tj. performanse.
- Najjednostavniji način apliciranja watermarka u DCT domenu je dodavanje DCT koeficijenata watermarka DCT koeficijentima originalnog sadržaja. Postoje i bolji algoritmi koji vezu između DCT koeficijenta sadržaja i watermarka temelje na bit-vrednostima watermarka.

Mellin-Fourierova transformacija (MFT)

- Osnova MFT - pretvaranje Dekartovog prostora u log-polarni prema sledećim formulama:

$$(x, y) \rightarrow \begin{cases} x = e^{\rho \cos\theta} \\ y = e^{\rho \sin\theta} \end{cases}$$

- Većina watermark algoritama ima problema sa izdvajanjem watermarka nakon što je na sliku primenjena neka geometrijska modifikacija. MFT rešava te probleme jer deluje u prostoru koji je neosetljiv na: translaciju, rotaciju i povećanje/smanjivanje. To je ostvareno na sledeći način:
  - 1. Translacija: translacija se manifestuje samo pomakom faze u transformisanom klasičnom Fourierovom domenu. U apliciranju watermarka, koristi se samo amplituda
  - 2. Rotacija: rotacija bilo kojeg elementa u Dekartovom prostoru rezultuje translacijom u logaritamskom koordinatnom sistemu
  - 3. Povećanje/smanjenje: bilo kakva zoom operacija u Dekartovom prostoru rezultuje translacijom u polarnom koordinatnom sistemu.

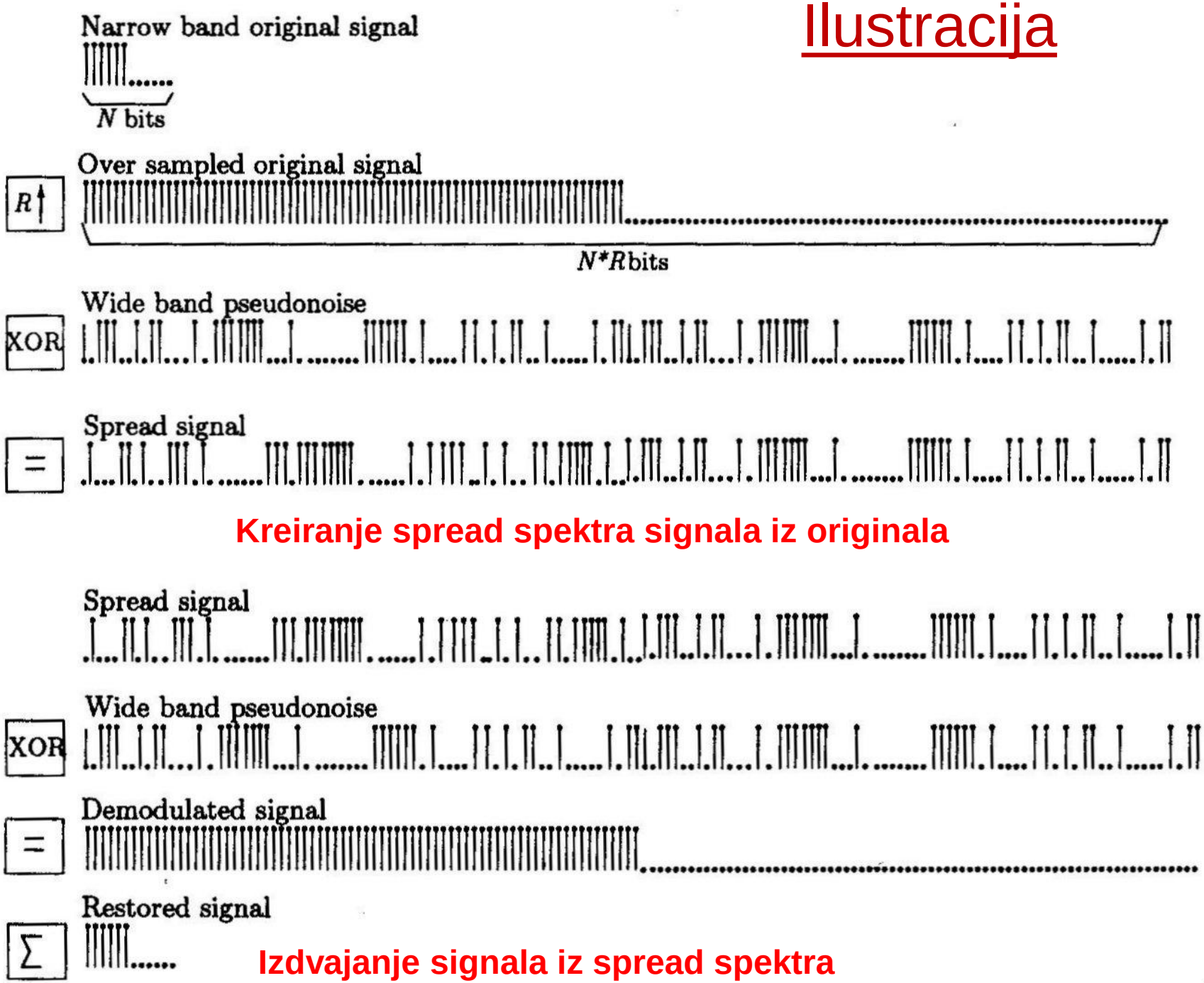
Raspršeni spektar (1)

- Tehnika pripreme bitova koji reprezentuju watermark za ubacivanje u sadržaj može se generalno podeliti na dve grupe:
  - tehnike koje omogućavaju direktno ubacivanje bitova
  - tehnike koje zahtevaju transformaciju pre umetanja.
- Poruka koja je watermark je po pravilu signal uskog opsega (narrow band) u poređenju sa širinom opsega signala sadržaja. Upravo ovom tehnikom omogućava se da se frekvencije signala watermarka i sadržaja ujednače pre samog kodiranja.
- Visoke frekvencije su važne za **nevidljivost** watermarka, a niske frekvencije za **robusnost**, a ovom tehnologijom je moguće ubaciti signal male snage u bilo koji frekvencijski opseg.

Raspršeni spektar (2)

- Direct-sequence spreading - sastoji se od vremenske modulacije originalnog signala koristeći širokopojasni signal pseudo-šuma. Rezultat je signal koji takođe izgleda kao šum. Spektar signala rezultata i signala pseudo-šuma su slični čak i u slučaju da je originalni signal bio uskopojasni. Kod primaoca, originalni signal se rekonstruiše demodulirajući primljeni signal koristeći isti signal pseudo-šuma, te ga je moguće rekonstruirati bez greške čak i ako su se neke frekvencije izgubile u toku prenosa jer je informacija ubačena u nekoliko frekvencijskih opsega.
- Frequency-hoping spreading - koristi se metoda u kojoj se frekvencija nosioca menja koristeći neki pseudoslučajni algoritam. Kao rezultat dobija se širokopojasni signal.
- Kod oba pristupa najveći problem je resinhronizacija između primljenog signala i slučajnog signala prilikom rekonstrukcije sadržaja. Da bi to bilo uspešno, generator slučajnog signala mora biti poznat.

Ilustracija



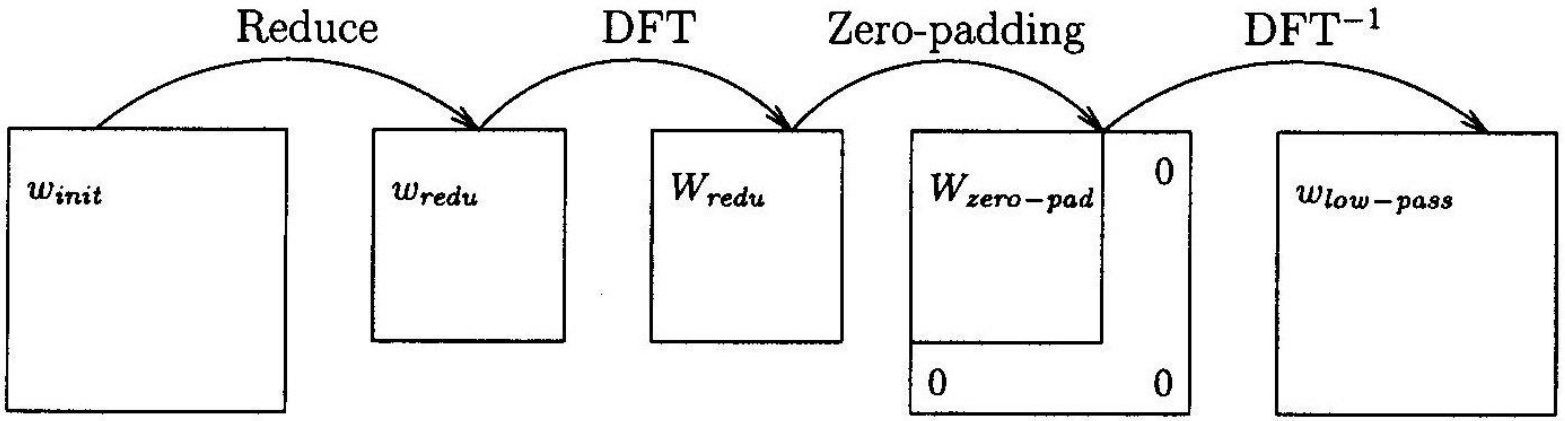
Kreiranje spread spektra signala iz originala

Izdvajanje signala iz spread spektra

Korišćenje niskih frekvencija

- Kako je robustnost vrlo važna karakteristika watermarka, a mnogi napadi se temelje na niskopropusnom filtriranju (npr. JPG), preporučuje se korišćenje niskih frekvencija za formatiranje watermark bitova iako je distorzija koju takav watermark unosi u sadržaj značajna.
- Jedna od tehnika koja koristi niske frekvencije (Fourierova transformacija) jest Braudaway-ova metoda: Originalni watermark $W_{init}(i, j)$ koji je istih dimenzija kao i originalni sadržaj (te sadrži veliku količinu redundanse) se redukuje u watermark $W_{redu}(i', j')$ te se izračunaju njegovi koeficijenti Fourierovom transformacijom čime se dobija $W_{redu}(u, v)$. Taj watermark se dopunjuje nulama sve dok se ne postigne veličina originalnog watermarka. Nakon inverzne transformacije Watermarka $W_{zero\text{-}pad}(u', v')$ dobija se watermark $W_{low\text{-}pass}(i', j')$ koji u sebi sadrži samo niske frekvencije.

Braudaway-ova metoda



Error-correcting kodovi

- Kako bi se poboljšalo izdvajanje watermarka, moguće je koristiti error-correcting kodove.
- Ukoliko se watermarking uporedi sa prenosom signala preko kanala sa šumom, kao rešenje se nameće nekoliko popularnih metoda koje u tom području pokazuju vrlo dobre rezultate.
- Nažalost, te se metode u velikom broju slučajeva ne mogu koristiti jer je u opštem slučaju smetnja u kanalu sa šumom (tj. šum) slučajna (Gaussov šum), dok se u watermark dizajnu mora obratiti pažnja ne samo na slučajan šum već i na namerne napade.
- Stoga se sve više i više napušta korišćenje standardnih error correcting kodiranja već se projektuju nova koja su otpornija na određene vrste napada.

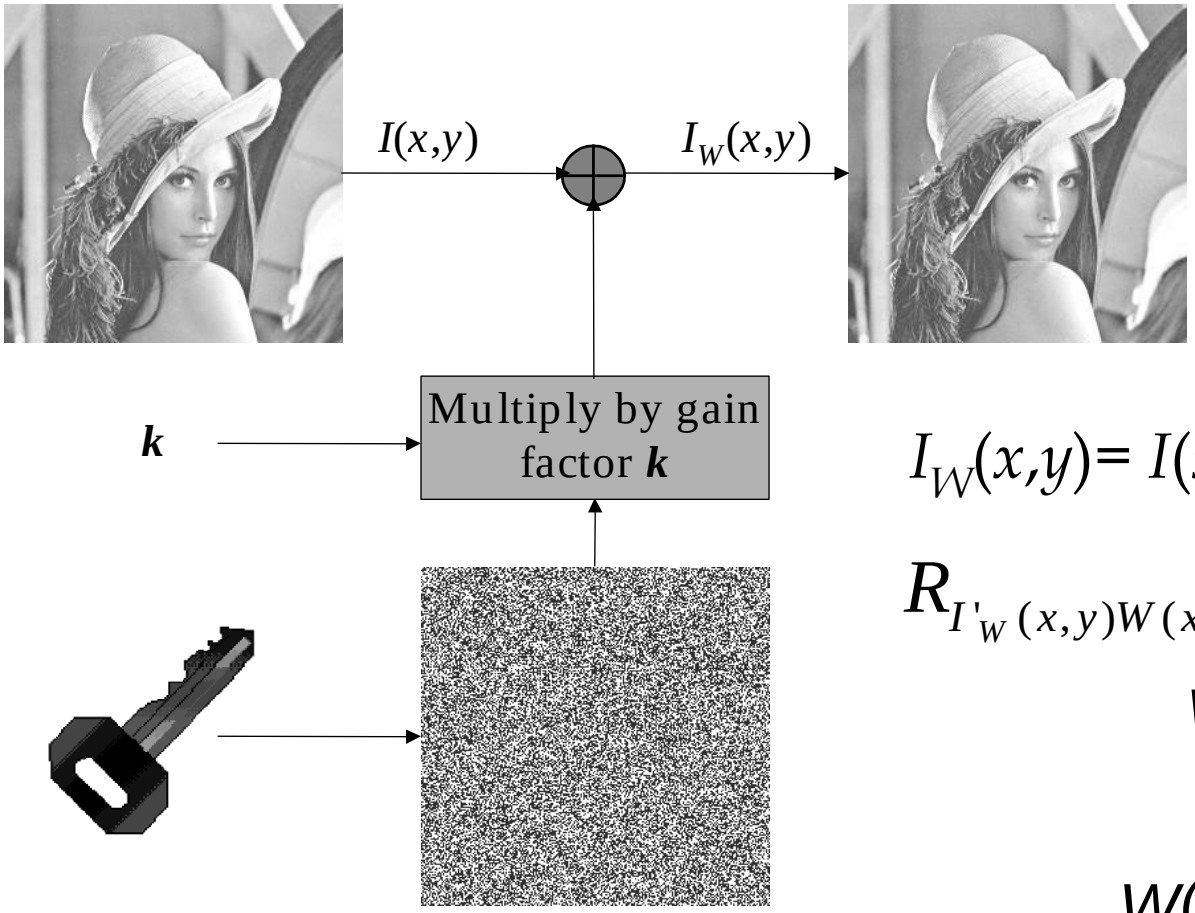
Image Watermarking

- Checksum
- Korišćenje spektara
- Hijerarhijski watermarking sa DCT
- Wavelet-based watermarking sa DWT
- DFT

Video Watermarking

- Raw video watermarking
  - DFT
  - DCT
  - DWT
- Watermarking I-frame (Mpeg-1,2)
- Watermarking video objekata (Mpeg-4)

Primer: Aditivni Watermark



$W(x,y)$: Pseudo Random Pattern {-1,0,1}

$$I_W(x,y) = I(x,y) + k \cdot W(x,y)$$

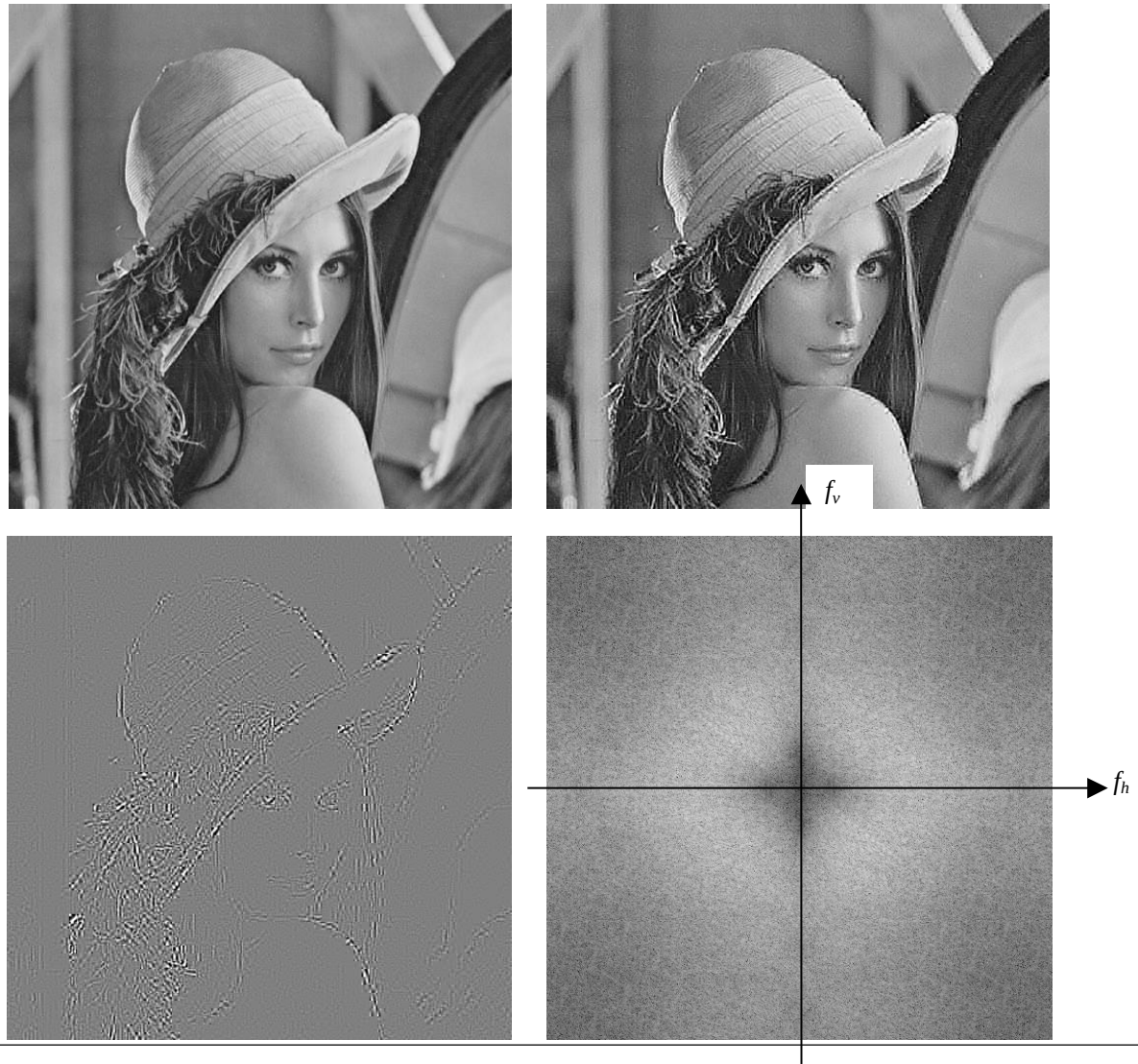
$$R_{I'_W(x,y)W(x,y)} > T \rightarrow$$

$W(x,y)$ detektovan

$$< T \rightarrow$$

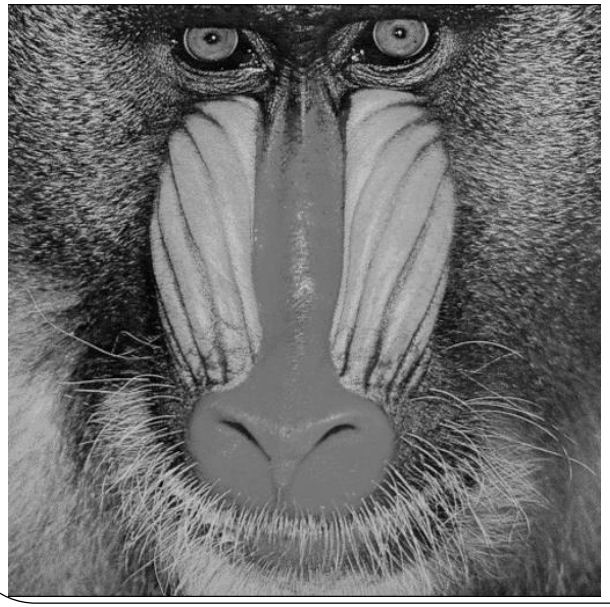
$W(x,y)$ nije detektovan

Aditivni watermark u transformacionom domenu

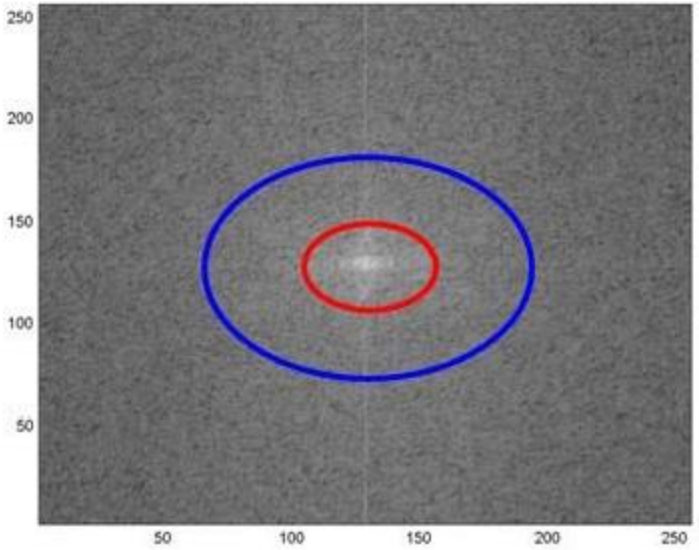


Originalna slika

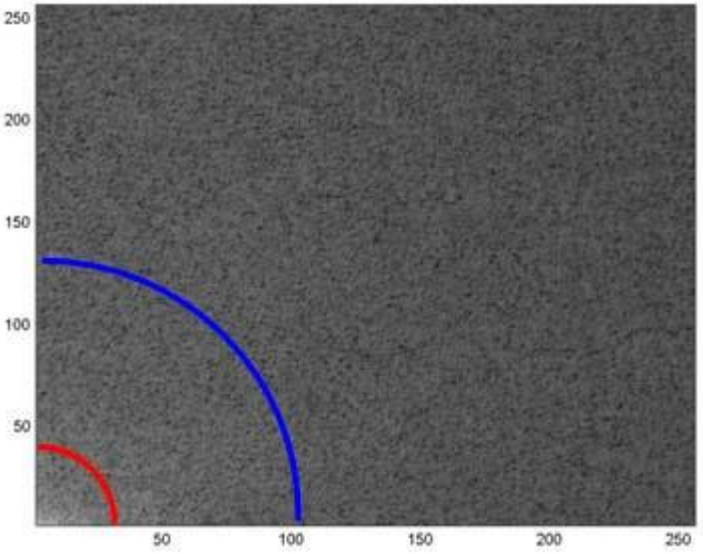
watermark



Primer:LSB Encoding



DFT Babuna



DCT Babuna

Zamena 4 i 7 LSBs originala

4 LSBs Watermarked

7 LSBs Watermarked

Aditivni - u vremenskm i prostornom domenu

Multiplikativni – u spektralnom domenu

$$I_W(x,y) = I(x,y) + k \cdot W(x,y)$$

$$I_W(x,y) = I(x,y) + k \cdot I(x,y)W(x,y)$$

Robusnost watermark sistema

Robusnost (otpornost na napade) i kvantifikacija robusnosti

Napadi na watermark

Uništavanje watermarka

Prevencija detekcije

Napadi lažnim svedočenjem i rupe u zakonu

Robusnost i njena kvantifikacija

- Robusnost tj. otpornost na napade watermarkinga obično je implementirana u dva područja: trajanje računa i količina distorzije, tj. robustnost se bazira na činjenici da, ukoliko želi da izbaci watermark, napadač mora da potroši preveliku količinu vremena ili unese u sadržaj preveliku distorziju.
- Definisanje robusnosti, tj. njena kvantifikacija u domenu slika i videa ne postoji službeno, dok se u audio tehnologiji pokušala definisati od strane International Federation of Phonografic Industry:

1) Watermark ne sme da smanji kvalitet sadržaja
2) Watermark ne treba da bude detektovan nakon operacija poput filtriranja, AD i DA uzastopne konverzije, MPEG i sličnih kompresija, dodavanja šuma, dodavanja drugog watermarka, menjanja snage pojedinih frekvencijskih opsega do 15 dB (npr. equilizerom) i slično
3) Ukoliko se watermark izvadi iz sadržaja, sadržaj mora biti neprepoznatljiv tj. nekoristan
4) Ukoliko je odnos signal-šum 20 dB, bandwidth watermarka mora imati 20 bps nakon error korekcije, nezavisno od nivoa i tipa signala

Napadi na watermark

1. ***Napadi na robusnost*** su npr. uništavanje watermarka, te su takvi napadi najočigledniji od četiri spomenute kategorije. Napadi ove kategorije kreću se od primene metode kompresije preko geometrijskih napada sve do specijalizovanih napada na sam watermark zavisno od metode ugrađivanja.
2. ***Prezentacioni napadi*** su napadi bazirani na sprečavanju detektora watermarka da uspešno obavi svoj posao, tj. na prevenciji detekcije. Umesto da se izbriše oznaka (tj. uništi watermark), on se promeni tako da pored detektora prođe bez detekcije.
3. ***Interpretacioni napadi*** su npr. napadi lažnim svedočenjem u kojima se, iako je uspešno detektovan, originalni sadržaj ili funkcija watermarka ne može ustanoviti pa sam watermark gubi smisao tj. ne znači ništa.
4. ***Rupe u zakonu*** se ne bave direktno uništavanjem watermarka, ali njihovim iskorišćavanjem gubi se osnovna namena watermarka (copyright).

1. Uništavanje watermarka

- ***Overmarking*** je jedna od metoda iz ove kategorije. Ukoliko se radi o javnom watermarku, pozicija (baš zato što je on javan) je uvek poznata, te je vrlo lako uništiti prvobitni watermark sa nekim drugim, čak ponekad i pomoću alata koji je poslužio za ubacivanje prvog, originalnog watermarka.
- ***Kompresija*** je vrlo česta na slikama, te se prilikom dizajna moraju uzeti u obzir poznati algoritmi, naročito lossy kompresija (JPEG). Watermark je po pravilu potrebno ubacivati u značajne komponente unutar frekventnog domena da bi se ovi napadi uspešno izbegli.
- ***Specijalni napadi*** su napadi bazirani na poznavanju metode watermarkinga koja se koristila prilikom ubacivanja. Tako je na primer watermark ubačen u Fourierovom domenu otporan na menjanje pixela u prostornom domenu, ali i vrlo osetljiv na menjanje koeficijenata u Fourierovom domenu. Baziranje robusnosti na temelju tajne metode implementacije watermarka je besmisleno.

2. Prevencija detekcije

- Da bi se watermark učinio nekorisnim nije ga potrebno izbrisati, dovoljno ga je učiniti nevidljivim za detektor. Takvi su sledeći napadi.

A) ***Napadi distorzijom*** su vrlo efikasni – iako je većina sistema otporna na klasične geometrijske transformacije, retko koja metoda je dovoljno robusna na njihove kombinacije a naročito ne na brojne slučajne male geometrijske distorzije. *Stirmark* je testni program koji na određenu sliku primenjuje različite distorzije poput sečenja (smicanja), i to u različitim smerovima i u različitom broju. Iako takve operacije plus JPEG kompresija ne uklanjaju watermark bitove, one sprečavaju detektor watermarka da ga nađe.

B) ***Mozaik napadi*** su napadi temeljeni na činjenici da je puno teže (ako ne i nemoguće) ubaciti watermark u malu sliku nego u veliku, te se ovim, u osnovi vrlo jednostavnim a uspešnim napadom jedna slika razbija na više malih. Naročito je ovaj napad primenljiv na webu, gde browser sam automatski spaja sve slike a detektor više ne može pronaći watermark u više malih sličica.

3) Napadi lažnim svedočenjem

Kod *napada na protokol*, napad se vrši ubacivanjem novog watermarka, ali ne s ciljem uništavanja drugog, nego kompromitovanja svrhe (copyright) prvog watermarka.

4) Rupe u zakonu

Copyright zakon podržavaju zemlje potpisnice Bernske konvencije – potrebno je samo pronaći zemlju koja nije potpisnik, te publikovati zaštićeni sadržaj u toj zemlji. Takođe, na internetu postoji gomila anonimnih servera, na koji se može publikovati zaštićeni sadržaj bez straha da će zakonski autor naći onog koga želi da tuži.

Praktična realizacija watermarka

Watermark u PPTu

Watermark u MS WORDu

Watermarking JPEG, GIF ili PNG slike korišćenjem PHP skripta i GD2 biblioteke za manipulisanje slikama u php-u

Primeri

DOC & watermark

- Ubacivanje watermarka u DOC fajl
- klip
- PageLayout – Watermark -

PPT & watermark

- Ubacivanje watermarka u PPT fajl:
- Klip

Praktična realizacija sa primerom

- PHP skripta kreira sliku sa watermarkom iz image fajla koji može biti u JPEG, GIF ili PNG formatu, gde je za watermark sliku najbolje uzeti sliku sa transparentnom pozadinom formata GIF ili PNG (npr. PNG slika napravljena u Photoshopu) i potrebno je da bude u istom direktorijumu gde je i skript.

- Skript pozivamo u html fajlu pomoću image taga na sledeći način:

  <img src="watermark1.php?path=imagepath"></img>

  gde je path u stvari relativna putanja do slike (npr. subdirectory/image.jpg)

Praktična realizacija sa primerom 1

- **Sadržaj fajla "watermark1.php"**

```
<?php
header ("Content-type: image/jpeg"); //header mora, definiše izlaz (output) php skripta
    koji se šalje primaocu


$putanja_slike =  $_GET['path'];
$tip_fajla = substr($putanja_slike,strlen($putanja_slike)-4,4);
$tip_fajla = strtolower($tip_fajla); //vraća string konvertovan u mala slova


if($tip_fajla == ".gif")  $slika = @imagecreatefromgif($putanja_slike);  //kreira novu
    sliku iz fajla ili URL-a
if($tip_fajla == ".jpg")  $slika = @imagecreatefromjpeg($putanja_slike);
if($tip_fajla == ".png")  $slika = @imagecreatefrompng($putanja_slike);
if (!$slika) die(); //die završava skript, ekvivalentno je sa exit()
```

Praktična realizacija sa primerom 1

```
$watermark = @imagecreatefrompng('yourname.png');
$slika_duzina = imagesx($slika); //imagesx uzima dužinu slike (width)
$slika_visina = imagesy($slika);  //imagesx uzima dužinu slike (height)
$watermark_duzina =  imagesx($watermark);
$watermark_visina =  imagesy($watermark);
$start_duzina = (($slika_duzina - $watermark_duzina)/2);
$start_visina = (($slika_visina - $watermark_visina)/2);
imagecopy($slika, $watermark,  $start_duzina, $start_visina, 0, 0, $watermark_duzina,
    $watermark_visina); //kopira definisane delove slike
imagejpeg($slika); //output slike u browser ili fajl
imagedestroy($slika); //oslobađa memoriju
imagedestroy($watermark);
?> EOF
```

Praktična realizacija sa primerom 1

- Rezultat primera pomoću watermark1.php fajla sa watermark-om, je slika:

Praktična realizacija sa primerom 2

- Takođe je moguće sem gotove watermark slike, uraditi **stamp** (pečat ili žig na slici), pri čemu možemo kreirati svoju sliku, kojoj definišemo dizajn pomoću gotovih GD2 funkcija. Primer koda :

```
$pechat = imagecreatetruecolor(100, 70);  //identifikator slike koji vraća crnu sliku datih razmera
imagefilledrectangle($pechat, 0, 0, 99, 99, 0x0000FF);  //x1, y1, x2, y2, boja
imagefilledrectangle($pechat, 9, 9, 90, 60, 0xFFFFFF);
imagestring($pechat, 5, 15, 18, 'Originalna slika', 0x0000FF);  //crta string prema datim koordinatama
imagestring($pechat, 5, 25, 40, 'Watermark', 0x0000FF);  // gde, font (od 1 do 5), x početak, y1 početak, tekst, boja
```

Praktična realizacija sa primerom 2

- Rezultat primera pomoću watermark2.php fajla sa generisanim pečatom ili ti žigom (stamp-om), je slika:

Pitanja