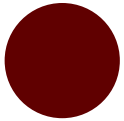
ŠTO SE SKRIVA U FOTOGRAFIJAMA?

dr. sc. Dijana Tralić
Zavod za radiokomunikacije
Fakultet elektrotehnike i računarstva

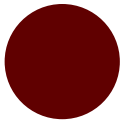
Sadržaj

- **Uvod u digitalnu forenziku slike**
- Detekcija izmjena na slikama
- Skrivanje sadržaja u sliku
- Šifriranje sadržaja slike
- Zaštita sadržaja slike
- Zaključak

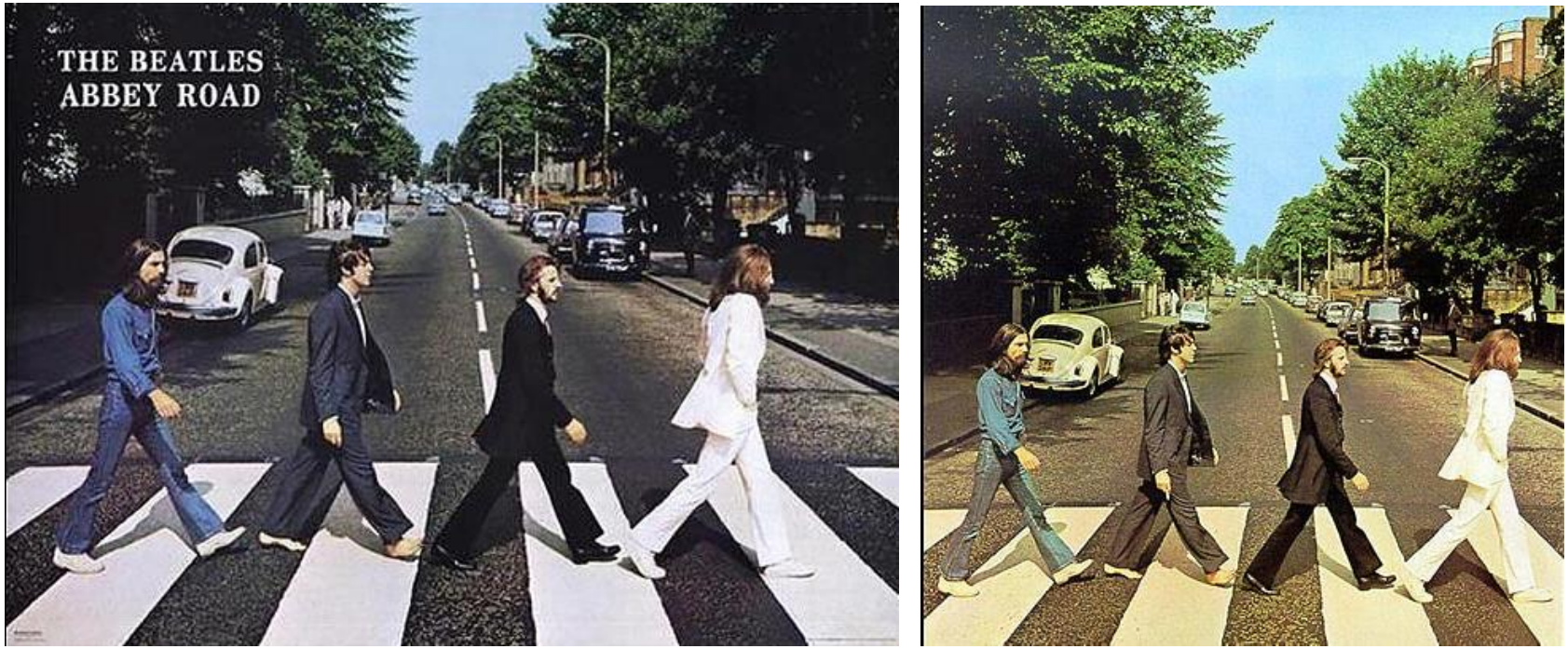


Uvod u digitalnu forenziku slike

- Digitalna foreznika slika (eng. *digital image forensics*) uključuje različite metode usmjerene na:
  - identifikaciju izmjena sadržaja digitalnih slika,
  - određivanje autentičnosti slika.
- Cilj izmjene sadržaja slike je skrivanje/dodavanje objekta/osoba na sliku ili izmjena karakteristika slike (boje, svjetline i sl.).
- Rezultat - nemogućnost razlikovanja originalnih i izmijenjenih digitalnih slika.



Uvod u digitalnu forenziku slike



Poster grupe The Beatles, 1969.
Na posteru (lijevo) je uklonjena cigareta iz ruke Paula McCartneya vidljiva na originalu (desno).

Izvor: http://content.time.com

Uvod u digitalnu forenziku slike

Iransko testiranje Shahab-3 raketa, 2008.
Sepah News objavili su editiranu sliku testiranja raketa (lijevo) kako bi prikrili neupješno lansiranje jedne rakete vidljivo na originalnoj slici (desno).

Izvor: http://content.time.com

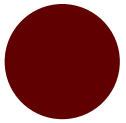
Uvod u digitalnu forenziku slike

Sastanak Hitlera i Leni Riefenstahla, 1937.
Joseph Goebbels izbrisan je s originalne fotografije sastanka (desno). Ostaje nepoznato zašto je Hitler tražio da se s fotografije ukloni jednog od njegovih najbližih suradnika (lijevo).

Izvor: http://content.time.com

Sadržaj

- Uvod u digitalnu forenziku slike
- **Detekcija izmjena na slikama**
- Skrivanje sadržaja u sliku
- Šifriranje sadržaja slike
- Zaštita sadržaja slike
- Zaključak



Detekcija izmjena na slikama

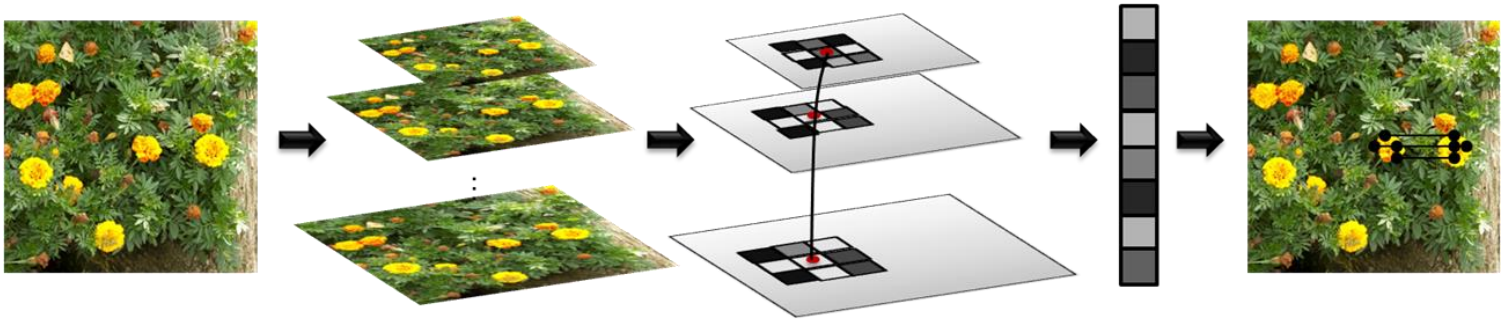
Izmjene na digitalnim slikama

Izmjene uporabom jedne slike

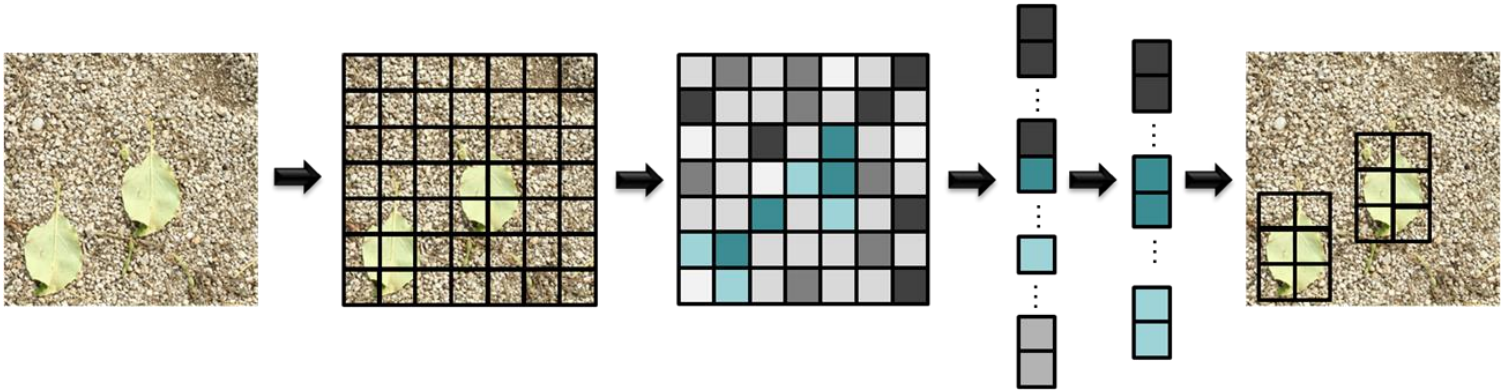
Izmjene kombinacijom više slika

Izvor: Bayram et. al., A survey of copy-move forgery detection techniques
http://www.imediaethics.org/

Detekcija izmjena na jednoj slici



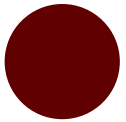
Pristup temeljen na ključnim točkama



Pristup temeljen na podjeli u preklapajuće blokove

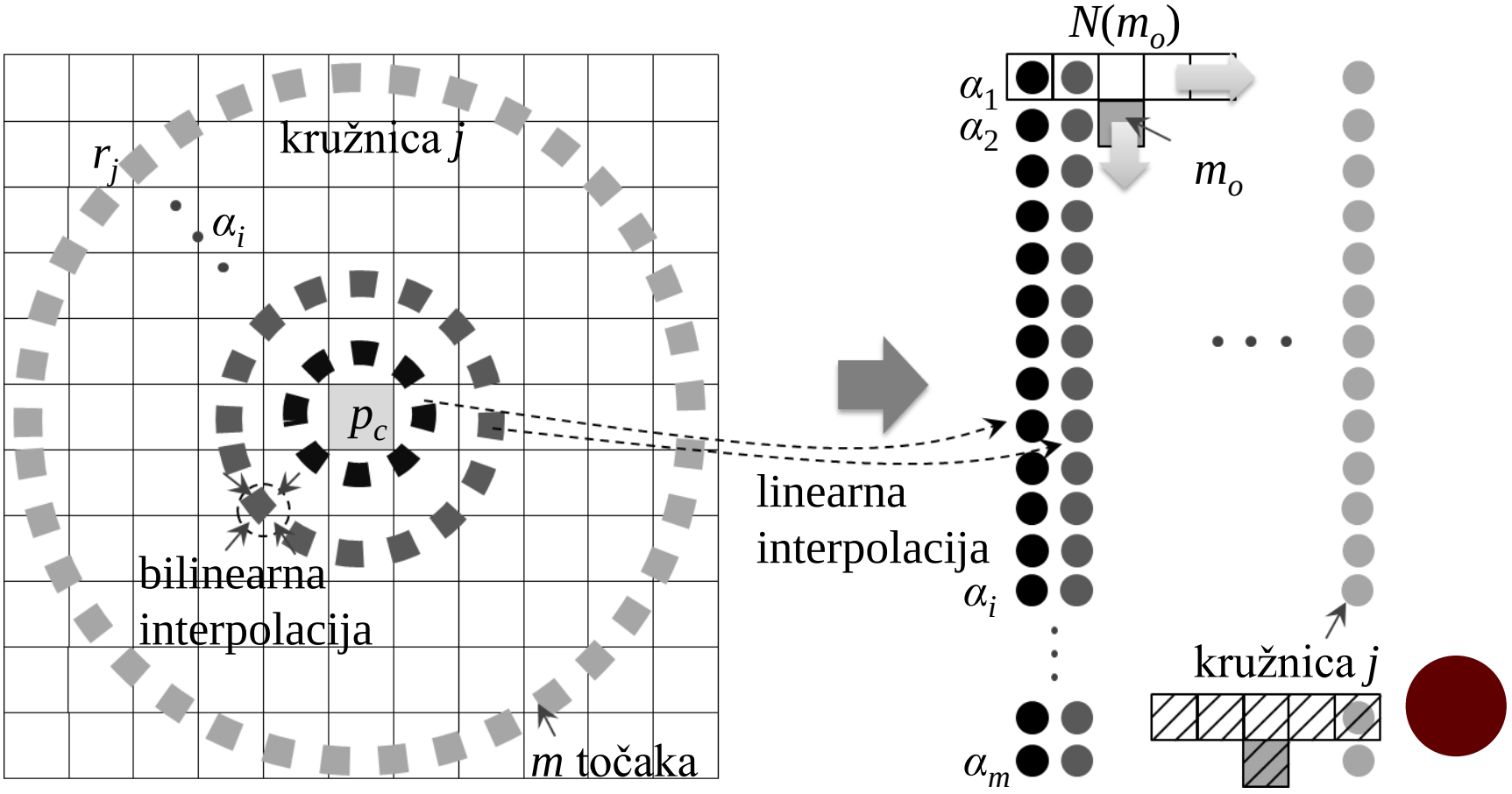
Detekcija izmjena na jednoj slici

- Osnovni probem – kako odrediti ključne točke/sažeti opis blokova?
- Ključne točke – SIFT, SURF
- Opis blokova:
  - Transformacije – DCT, DWT, Zernike,
  - Momenti – Hu,
  - Analiza vrijednosti elemenata – srednja vrijednost,
  - Sažimanje opisa – PCA.
- Cilj je osigurati što kraći i jednostavniji opis, koji je robustan na razne transformacije i naknadnu obradu slike.



Detekcija izmjena na jednoj slici

- Kombinacija staničnog automata i lokalnog binarnog uzorka – opis bloka binarnim nizom!



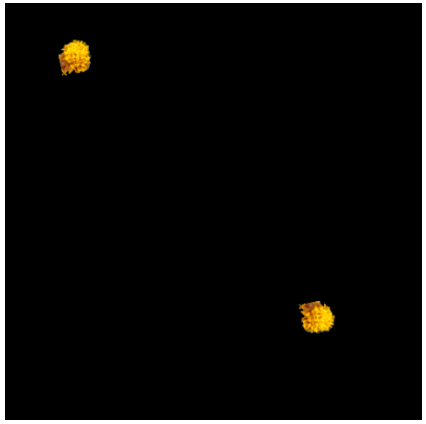
Detekcija izmjena na jednoj slici

$F = 0{,}9828$

$F = 0{,}9827$

Translacija: Originalna slika (prvi stupac), izmijenjena slika (drugi stupac), očekivani rezultat (treći stupac), postignuti rezultat (četvrti stupac)

Detekcija izmjena na jednoj slici


$\alpha = 90°$, $F = 0{,}7384$

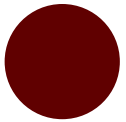


$f = 95\ \%$, $F = 0{,}5681$

Rotacija za kut α i skaliranje za faktor f: Izmijenjena slika (prvi stupac), očekivani rezultat (drugi stupac), postignuti rezultat (treći stupac)

Detekcija izmjena na jednoj slici

- Moguće je uspješno detektirati:
  - Translaciju objekta na novu lokaciju neovisno o veličini objekta;
  - Dodavanje šuma – Gaussov šum varijance < 0.01
  - Zamućenje slike – 3×3, 5×5;
  - JPEG kompresiju za faktore > 40%;
  - Rotaciju – kuteve < 10 ° ili višekratnike od 90°;
  - Skaliranje – smanjenje i povećanje površine do 10 %.



Detekcija izmjena JPEG slike

- Dvostruka kompresija nastaje pri izmijeni JPEG slike – slika se kvantizira s različitim faktorima kvantizacije
- Detekcija dvostruke kvantizacije:

$$diff(x,y) = \left|I(x,y) - I_q(x,y)\right|$$

$$D(x,y) = \frac{1}{8^2}\sum_{m=0}^{7}\sum_{n=0}^{7} diff(x+m, y+n)$$

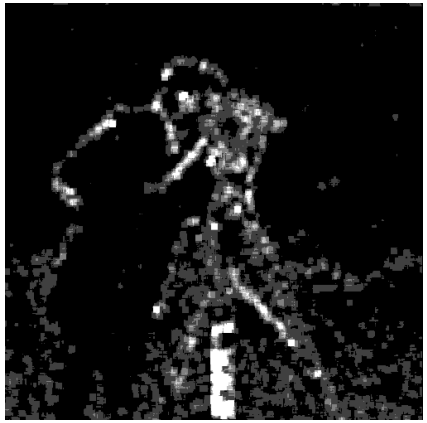
- Problem – nemoguće detektirati izmjenu slike pohranjene s istim stupnjem kompresije.

Detekcija izmjena JPEG slike

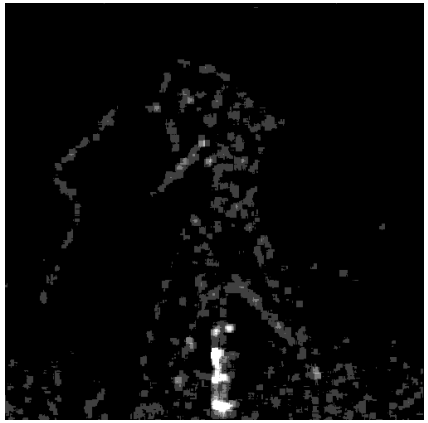
Originalna slika

Izmijenjena slika

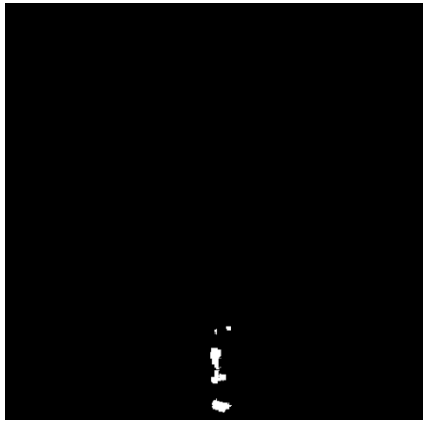
Faktor $q = 6$



Faktor $q = 8$



Faktor $q = 9$



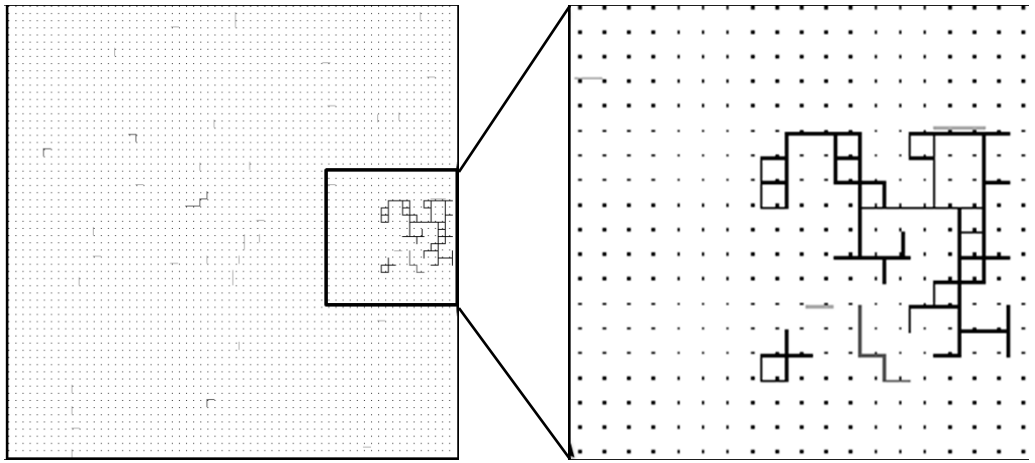
Rezultat detekcije

Detekcija izmjena JPEG slike

- Analiza mreže DCT blokova preko lokalnog efekta:

$$LE = \sqrt{\frac{\sum_{i=7||j=7} {S_{ij}}^2}{{S_{11}}^2}}$$

Izmijenjena slika

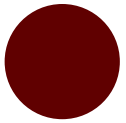


Mreža DCT blokova

Detektirano neslaganje

Detekcija kombiniranja slika

- Kombiniranje slika moguće je detektirati analizom:
  - Svojstva kamere,
  - Fizičkih osobina slike – poput osvjetljenja,
  - Geometrijskih odnosa na slici,
  - Statistika višeg reda.



Detekcija kombiniranja slika

Kombiniranje fotografija

Osvjetljenje (prikazano zutim strjelicama) nije konzistentno. Odsjaj u očima pokazuje da osobe nisu fotografirane u istim uvjetima.

Izvor:H. Farid: digital Image Forensics, SCIENTIFIC AMERICAN, 2008.

Detekcija kombiniranja slika

Fotografija turista na WTC, 11. rujan 2001.
Balans boja nije odgovarajući – avion bi imao više žutog tona da je snimljen istom kamerom.

Izvor: http://www.snopes.com/rumors/photos/tourist.asp

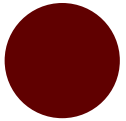
Sadržaj

- Uvod u digitalnu forenziku slike
- Detekcija izmjena na slikama
- **Skrivanje sadržaja u sliku**
- Šifriranje sadržaja slike
- Zaštita sadržaja slike
- Zaključak

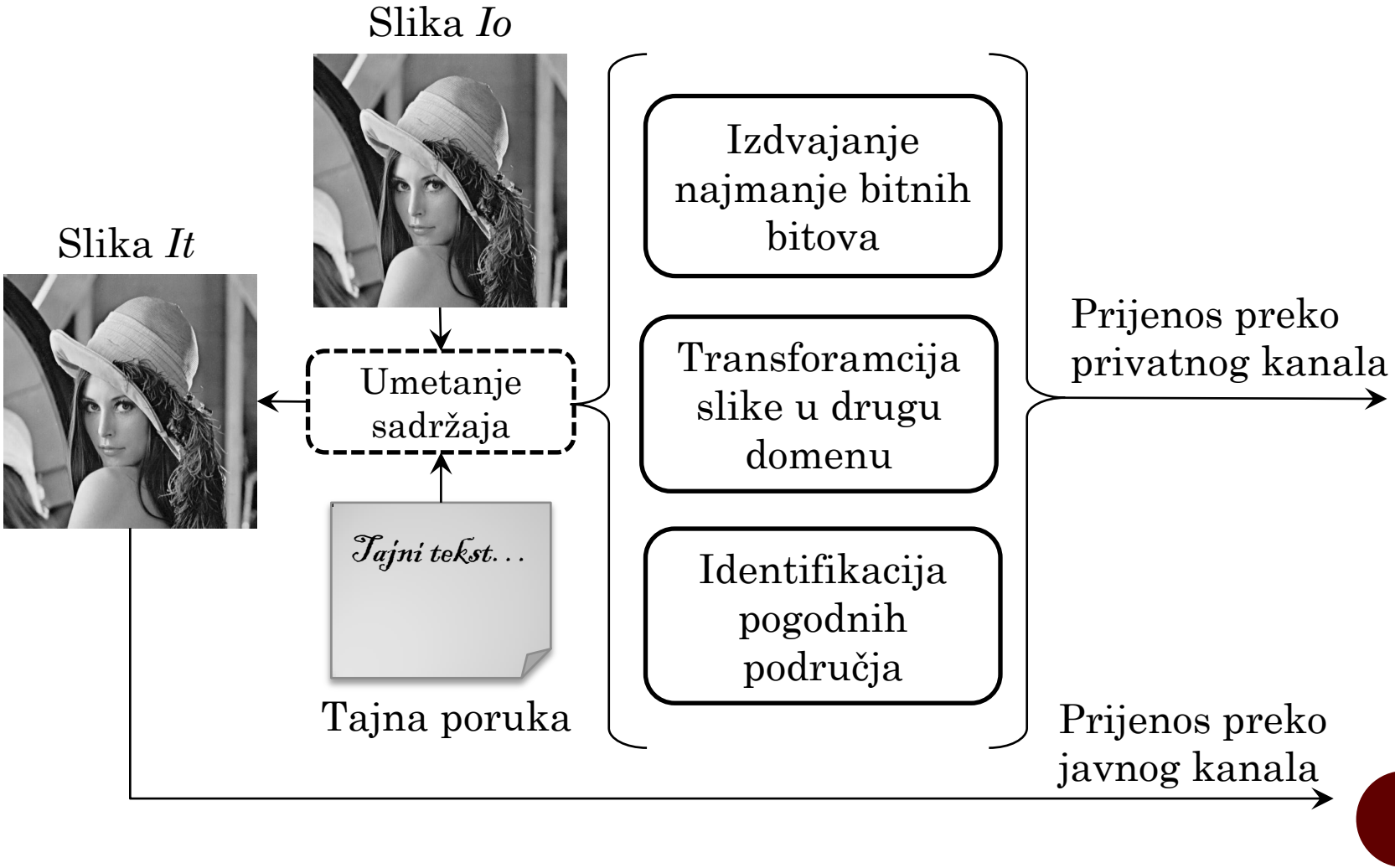
Skrivanje sadržaja u sliku

- Podrazumijeva umetanje tajnog sadržaja u sliku, koji može biti tekst, video ili audio.

- Umetanje sadržaja obavlja se na način da se:
  - Osigura kvaliteta slike – umetnuti sadržaj ne smije biti vidljiv,
  - Zaštiti umetnuti sadržaj od gubitaka pri prijenosu – šum u kanalu,
  - Spriječi slučajno otkviranje tajnog sadržaja.



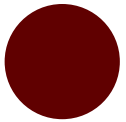
Skrivanje sadržaja u sliku



Skrivanje sadržaja u sliku

- Umetanje sadržaja u DCT (eng. *discrete cosine transform*) komponente
  - Zadržanje kvalitete slike,
  - Otpornost na razne transformacije i naknadnu obradu slike.

- Šifriranje sadržaja uporabom staničnog automata
  - Jednodimenzionalna pravila,
  - Nemogućnost detekcije sadržaja bez poznavanja odgovarajućeg pravila.



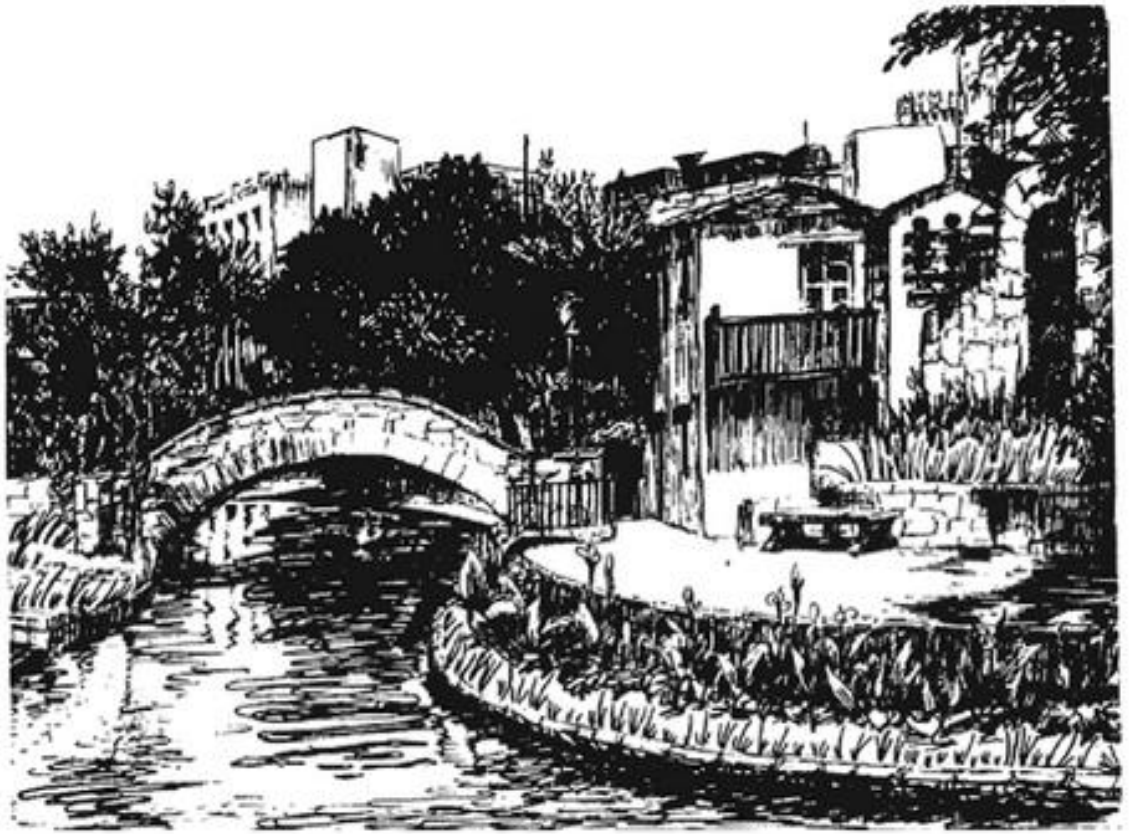
Skrivanje sadržaja u sliku

Sastanak sutra u 10 sati na trgu.

Originalna slika

Slika sa skrivenim sadržajem

Skrivanje sadržaja u sliku



Crtež rijeke San Antonio, 1945.
Morseov kod je skriven u travu uzduž rijeke – duga trava predstavlja crtu, a kratka točku.

Izvor: F.L.Bauer, Decrypted Secrets: Methods and Maxims of Cryptology, 4. ed., Springer-Verlag, Berlin, 2007.

Skrivanje sadržaja u sliku

Washington, DC
Slika koja sadrži tajnu poruku skrivenu u najmanje značajne bitove slike

Izvor: http://www.garykessler.net/library/fsc_stego.html

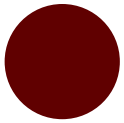
Skrivanje sadržaja u sliku

Zračna luka Burlington, Vermont
Slika skrivena u prethodnu sliku

Izvor: http://www.garykessler.net/library/fsc_stego.html

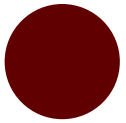
Sadržaj

- Uvod u digitalnu forenziku slike
- Detekcija izmjena na slikama
- Skrivanje sadržaja u sliku
- **Šifriranje sadržaja slike**
- Zaštita sadržaja slike
- Zaključak

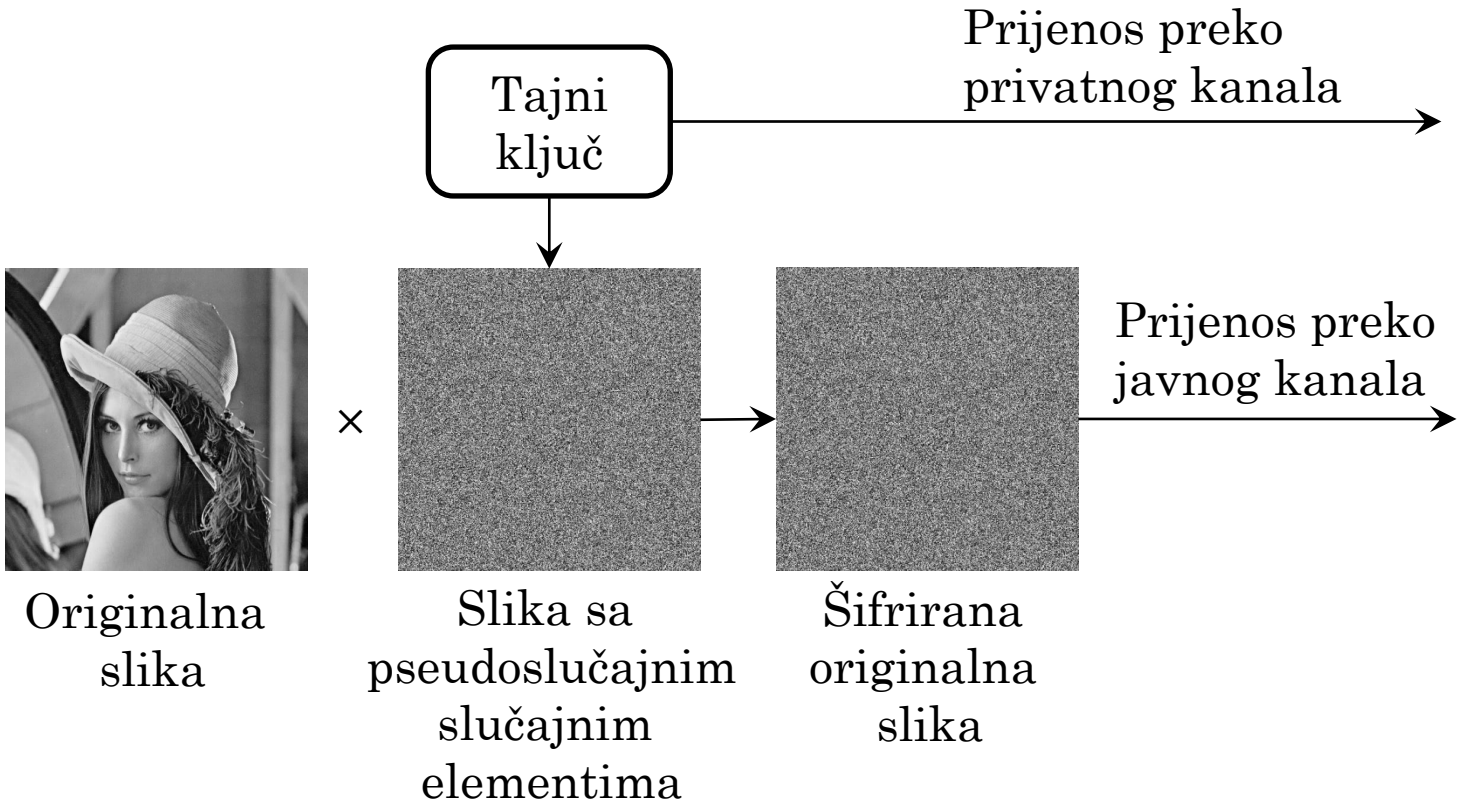


Šifriranje sadržaja slike

- Podrazumjeva izmjenu vrijednosti elemenata slike:
  - Zamijenom lokacija elementima slike,
  - Kombiniranjem vrijednosti elemenata slike s pseudo slučajnim vrijednostima.
- Tajni ključ se koristi kako bi se spriječilo neovlašteno dešifriranje slike.
- Metoda mora biti otporna na razne vrste statističkih analiza te osigurati veliki volumen tajnog ključa.



Šifriranje sadržaja slike

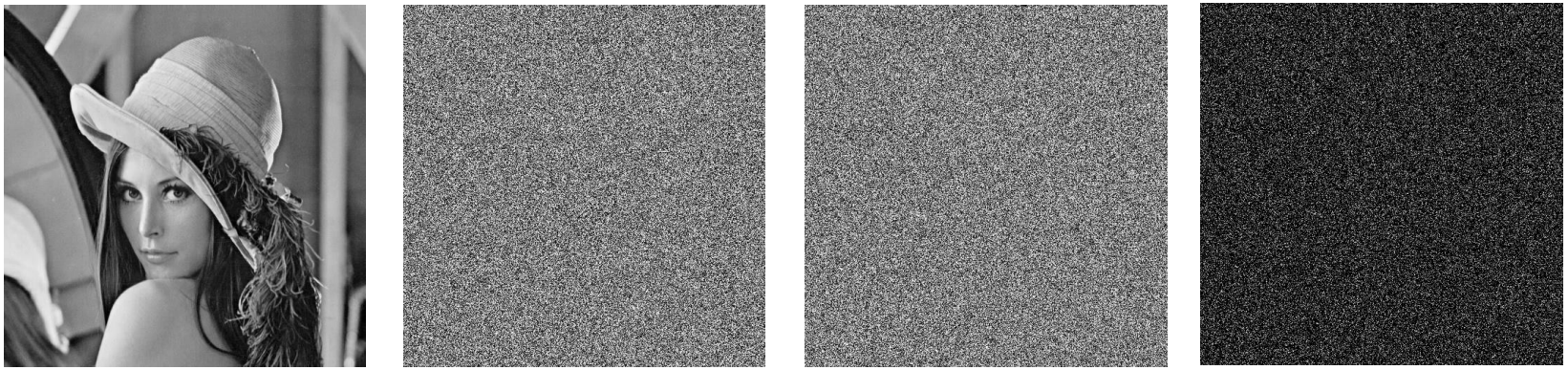


Šifriranje sadržaja slike

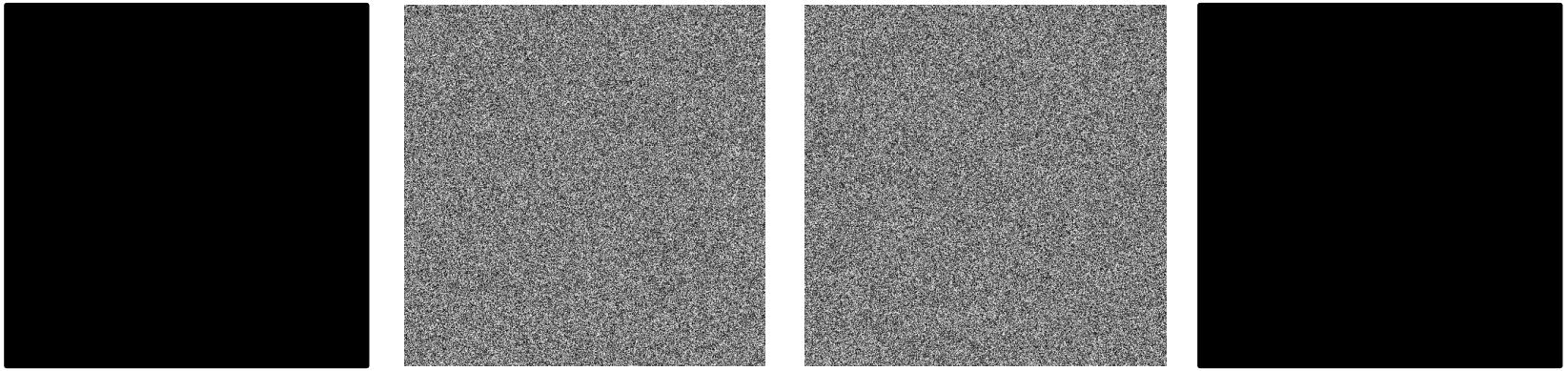
- Osnovni problem – kako generirati pseudoslučajne vrijednosti?
- Stanični automat:
  - Dvodimenzionalnost,
  - Prošireno Moore susjedstvo – 25 elemenata slike,
  - Balansirana pravila – podjednak broj jednicia i nula,
  - Primjena na svaku binarnu ravninu slike posebno.
- Volumen tajnog ključa:

$$V = \binom{2^{25}}{2^{24}}^{8}$$

Šifriranje sadržaja slike

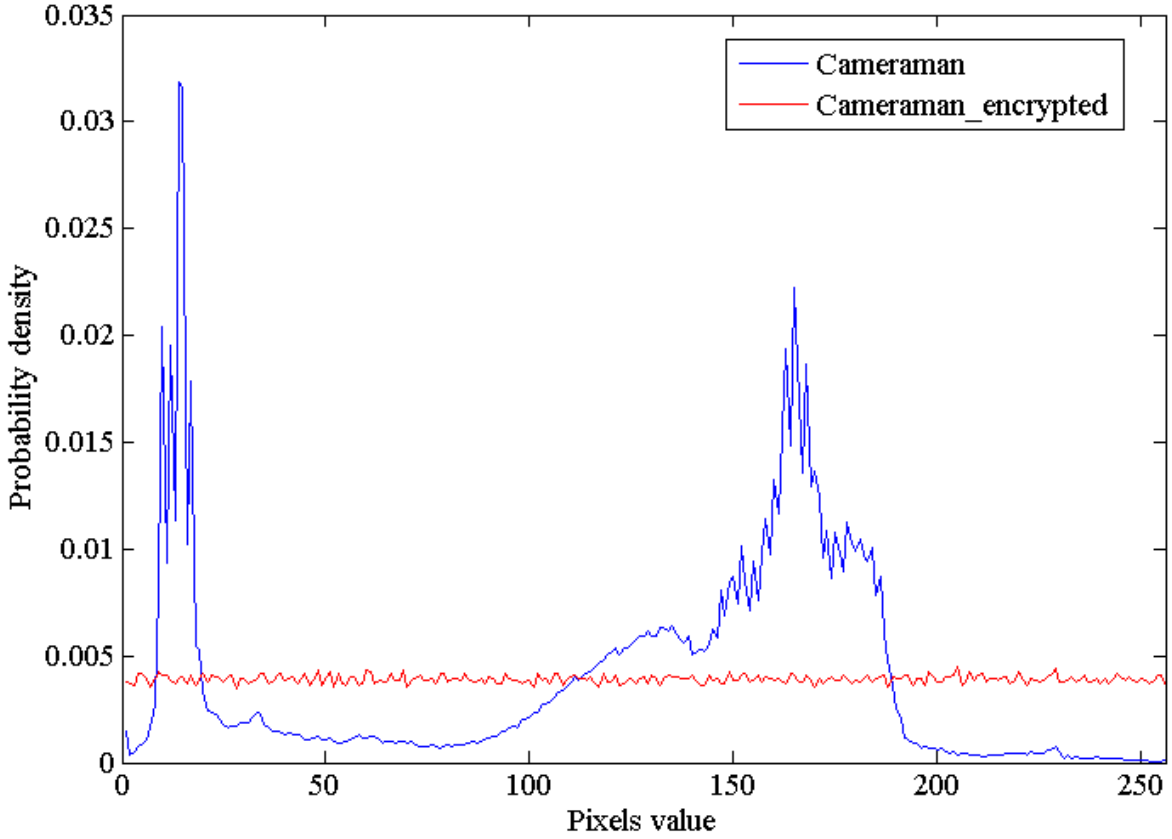


Lena sifrirana s ključvima koji se razlikuju u 1 bit i razlika rezultata



Slika s uniformnim vrijednostima šifrirana s jednim ključem te dešifrirana s pogrešnim i ispravnim ključem

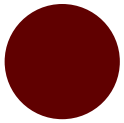
ŠIFRIRANJE SADRŽAJA SLIKE



Pdf funkcije originalne i šifrirane slike – entropije originalne slike: 7.0843, entropije šifrirane slike: 7.9983

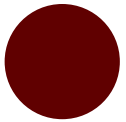
Sadržaj

- Uvod u digitalnu forenziku slike
- Detekcija izmjena na slikama
- Skrivanje sadržaja u sliku
- Šifriranje sadržaja slike
- **Zaštita sadržaja slike**
- Zaključak



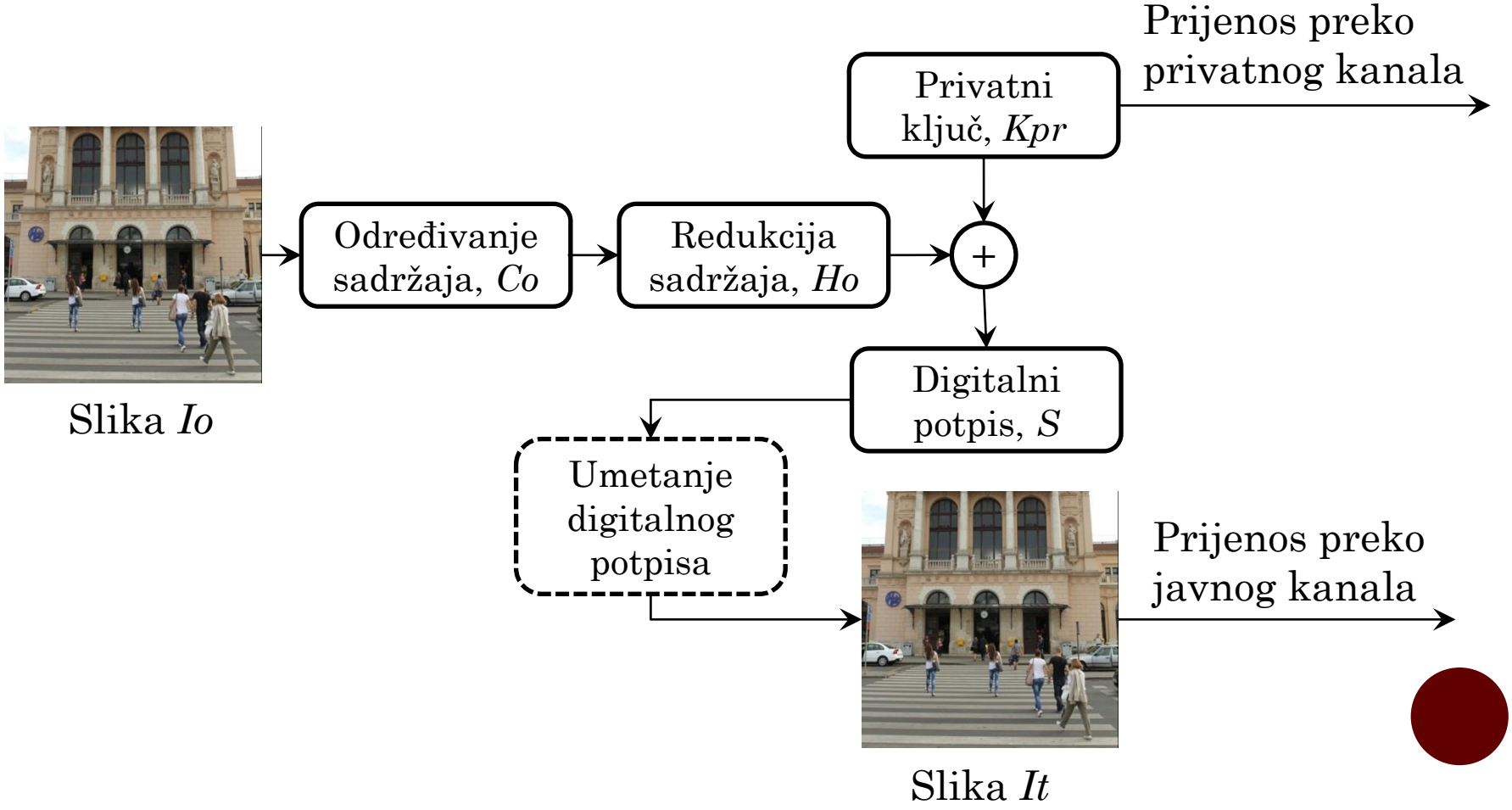
Zaštita sadržaja slike

- Podrazumijeva ugradnju određenih informacija u sliku.
- Promjena sadržaja slike povlači izmjenu i ugrađene informacije.
- Detekcija izmjene na slici obavlja se analizom ugrađene informacije.
- Osnovna dva primjera su:
  - digitalni potpisi (eng. *digital signatures*),
  - vodeni žigovi (eng. *watermarks*).



DIGITALNI POTPISI

- Sadržaj se određuje iz same slike: $S = f_h(f_o(I_o)) \oplus K_{pr}$



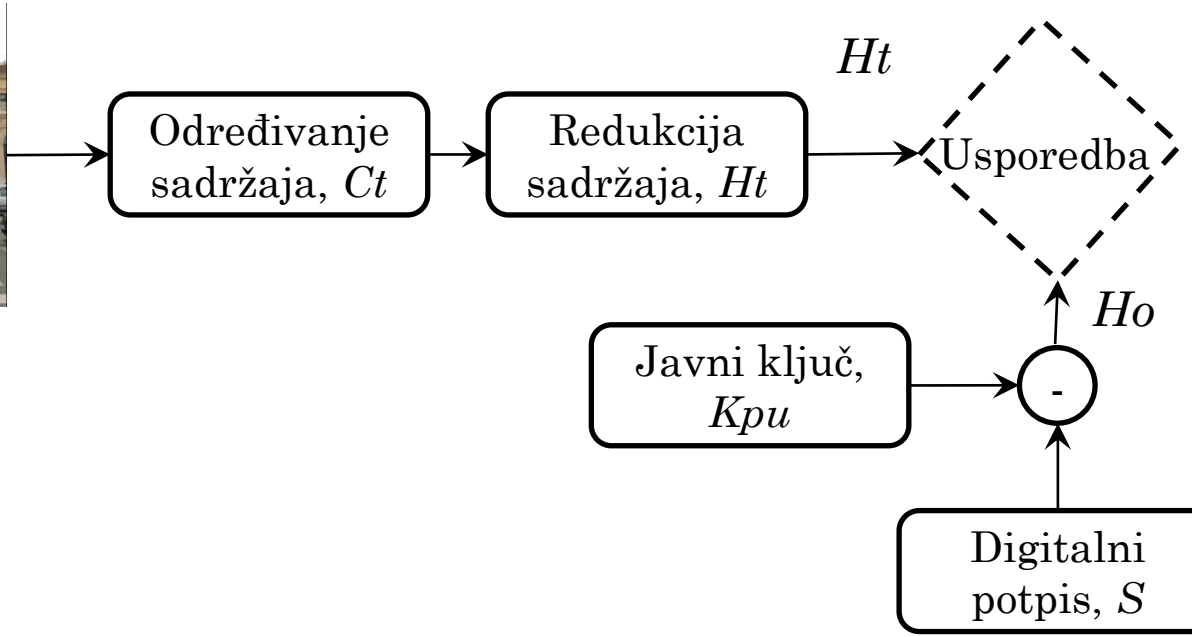
DIGITALNI POTPISI

- Detektirani sadržaj mora odgovarati umetnutom sadržaju:

$$H_t = f_h(f_o(I_t))$$

$$\|H - H_t\| \leq \text{prag}$$

Slika *It*



DIGITALNI POTPISI

Digitalni potpis: originalna slika (lijevo), slika s digitalnim potpisom (desno)

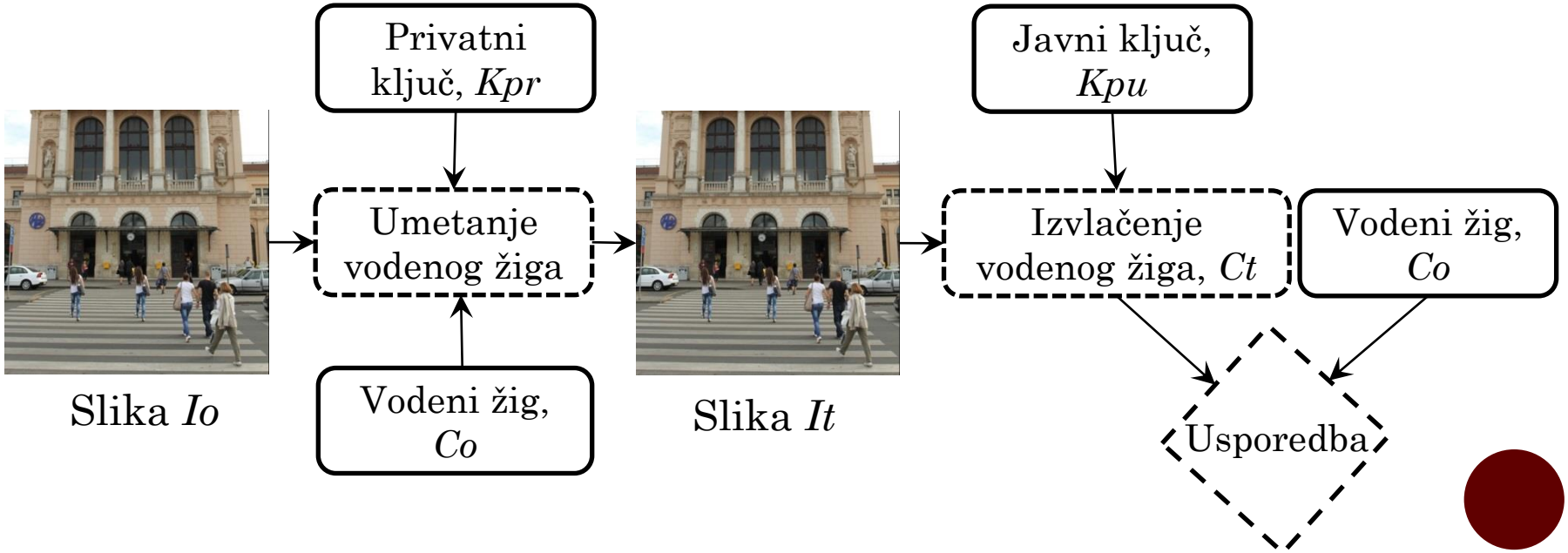
Izvori M: Kutter, F. Jordan, F. Bossen: Digital Signature of Color Images using Amplitude Modulation, SPIE Proceedings, 1997.

VODENI ŽIGOVI

- Informacija je neovisna o slici, a detektirana informacija mora odgovarati umetnutoj:

$$C_o \oplus K_{pr}$$

$$\|C_o - C_t\| \leq \text{prag}$$



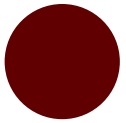
VODENI ŽIGOVI

Vidiljivi i nevidljivi (ime autora) vodeni žig

Izvori: https://www.watermark-image.com/gallery.aspx
http://www.alpvision.com/watermarking.html

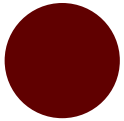
Sadržaj

- Uvod u digitalnu forenziku slike
- Detekcija izmjena na slikama
- Skrivanje sadržaja u sliku
- Šifriranje sadržaja slike
- Zaštita sadržaja slike
- **Zaključak**



Zaključak

- Digitalne slike omogućile su jednostavnu manipulaciju sadržajem.
- Autentičnost digitalnih slika nije moguće utvrditi jednostavnim promatranjem slike.
- Analizom raznih statističkih svojstava digitalnih slika moguće je detektirati veliki broj manipulacija.
- Ne postoji jedinstveno rješenje koje pruža odgovor o autentičnosti slike.
- Još uvijek je jednostavnije provesti manipulaciju sadržaja digitalne slike, nego detekciju te manipulacije.



Hvala na pozornosti…