

Sveučilište u Zagrebu

Prirodoslovno-matematički fakultet

Steganografija SVD

Naziv tima:

Glitch u matrici

Članovi tima:

Željka Baća, Nikola Kašnar, Ivana Kristić

Mentor:

prof. dr. sc. Zlatko Drmač

Zagreb, 29. studenoga 2024.

Sadržaj

1	Uvod	2
2	Singular Value Decomposition (SVD)	3
2.1	Motivacija	3
2.2	SVD	3
3	Proposed Watermarking Scheme	5
3.1	Dekompozicija slike	5
3.2	Umetanje vodenog žiga u D matricu	5
3.3	Umetanje vodenog žiga u U matricu	6
3.4	Konačna slika s vodenim žigom	7
4	Eksperimentalni rezultati	8
4.1	Steganografija na slici	8
5	Zaključak	15
6	Literatura	16

1 Uvod

Steganografija je tehnika skrivanja informacija unutar drugih, naizgled bezazlenih podataka, kako bi se prikrila prisutnost tajne poruke. Ova metoda se koristi od davnina, a s razvojem digitalnih tehnologija doživjela je značajan napredak, omogućujući sigurno i neprimjetno slanje informacija u digitalnom obliku. U kontekstu digitalne komunikacije, steganografija se često koristi za zaštitu privatnosti i osiguranje tajnosti podataka, čime se smanjuje rizik od otkrivanja osjetljivih informacija.

Jedna od glavnih prednosti steganografije u odnosu na druge metode skrivanja informacija, poput šifriranja, je ta što steganografija ne izaziva sumnju. Dok šifriranje jasno ukazuje da je informacija zaštićena, steganografija skriva samu činjenicu da se informacije razmjenjuju, što je osobito važno u vojnim i špijunskim aplikacijama, gdje je ključno da komunikacija ostane neprimjetna.

U ovom seminaru istražujemo primjenu steganografije u digitalnim medijima, s posebnim naglaskom na umetanje vodenih žigova u slike. Testirat ćemo i istražiti metodu Singular Value Decomposition (SVD), analizirajući njezinu učinkovitost i robusnost u skrivenju informacija. Cilj je istaknuti važnost ovih metoda u zaštiti digitalnih informacija, te prikazati mogućnosti SVD metode u praktičnoj primjeni.

2 Singular Value Decomposition (SVD)

2.1 Motivacija

Singular Value Decomposition (SVD) predstavlja jednu od najvažnijih tehnika u obradi podataka, a njezina široka primjena čini je ključnim alatom u različitim disciplinama. S obzirom na sve veći značaj obrade digitalnih informacija, SVD se ističe svojom sposobnošću da efikasno razlaže matricu na komponente, čime se omogućava pojednostavljanje složenih podataka.

Jedna od ključnih primjena SVD-a je u kompresiji slika, što omogućava smanjenje veličine datoteka bez značajnog gubitka kvalitete. U današnjem svijetu, gdje se suočavamo s velikim količinama vizualnih podataka, učinkovita kompresija slika postaje sve važnija.

Osim toga, SVD se koristi u rekonstrukciji preporučivih sustava, što pomaže u prepoznavanju obrazaca u korisničkim podacima i omogućava precizniju predikciju korisničkih preferencija. U kontekstu preporuka, SVD se koristi za analizu velikih skupova podataka i identifikaciju sličnosti među korisnicima i predmetima.

Dodatno, SVD se koristi u obnovi uništenih slika ljudskih lica, čime se omogućava popravak slika koje su oštećene ili uništene. Ova tehnika također igra važnu ulogu u klasifikaciji ručno pisanih znamenki, što poboljšava učinkovitost prepoznavanja obrazaca.

Iako SVD ima široku primjenu, u ovom seminaru fokusirat ćemo se na umetanje žigova u slike. Umetanje vodenih žigova predstavlja važnu metodu za zaštitu autorskih prava i integritet digitalnih sadržaja. Korištenjem SVD-a za umetanje žigova, istražit ćemo kako se informacije mogu sigurno integrirati u slike bez značajnih promjena u vizuelnoj kvaliteti, čime se doprinosi očuvanju autorskih prava u digitalnom okruženju.

U kontekstu digitalnog vodenog žigovanja, SVD igra ključnu ulogu u osiguravanju robustnosti umetnutih informacija. Ova metoda omogućuje umetanje vodenih žigova koji su otporni na različite vrste napada, čime se osigurava autentičnost i vlasništvo nad digitalnim sadržajem. Također, SVD se koristi u analizi korisničkih podataka u sustavima preporuka, što dodatno naglašava njegovu svestranost.

2.2 SVD

Za danu matricu A dimenzija $m \times n$ i ranga r , singularna vrijednosna dekompozicija omogućuje da se A izrazi kao produkt triju matrica:

$$A = U\Sigma V^*,$$

gdje:

U je unitarna matrica dimenzija $m \times m$, Matrica U sadrži lijeve singularne vektore matrice A kao svoje stupce. Budući da je U unitarna matrica, vrijedi $U^*U = I_m$, gdje je I_m identična matrica dimenzija $m \times m$.

Σ je dijagonalna matrica dimenzija $m \times n$ sa singularnim vrijednostima matrice A na glavnoj dijagonali, Matrica Σ je dijagonalna matrica dimenzija $m \times n$ sa singularnim vrijednostima σ_i na dijagonali:

$$\sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_r > 0.$$

Singularne vrijednosti σ_i definirane su kao kvadratni korijeni svojstvenih vrijednosti matrice A^*A .

V je unitarna matrica dimenzija $n \times n$, Matrica V sadrži desne singularne vektore matrice A kao svoje stupce i također je unitarna, što znači da $V^*V = I_n$, gdje je I_n identična matrica dimenzija $n \times n$.

V^* označava Hermitski konjugat matrice V (transponiranje i konjugiranje).

Matrica A može se izraziti kao:

$$A = U\Sigma V^*,$$

što znači da se A može rekonstruirati kao suma produkata:

$$A = \sum_{i=1}^r \sigma_i u_i v_i^*,$$

gdje su u_i lijevi singularni vektori (stupci matrice U), v_i desni singularni vektori (stupci matrice V), a σ_i singularne vrijednosti.

Singularne vrijednosti σ_i određene su kao kvadratni korijeni svojstvenih vrijednosti matrice A^*A :

$$\sigma_i = \sqrt{\lambda_i},$$

gdje su λ_i svojstvene vrijednosti matrice A^*A .

Lijevi i desni singularni vektori definirani su relacijama:

$$Av_i = \sigma_i u_i,$$

$$A^*u_i = \sigma_i v_i.$$

Ovdje su u_i lijevi singularni vektori, a v_i desni singularni vektori.

3 Proposed Watermarking Scheme

Predstaviti ćemo metodu umetanja vodenog žiga u slike baziranu na dekompoziciji slike pomoću SVD-a. U ovoj metodi, tehnike SVD-a koriste se za umetanje vodenog žiga u digitalnu sliku uz očuvanje kvalitete slike i otpornost na različite vrste napada. Posebno se koriste D i U matrice dobivene SVD-om, s primjenom Dither kvantizacije za kontrolu modifikacija.

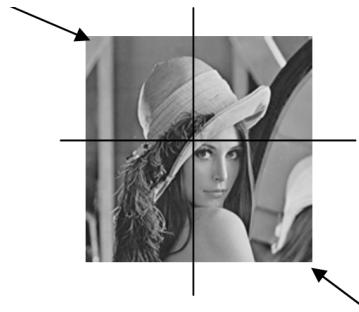
Glavni koraci metode su slijedeći:

3.1 Dekompozicija slike

Originalna slika $f(i, j)$ veličine $N \times N$ dijeli se na četiri pod-slike:

$$\begin{aligned} f_{tl}(p, q) & (\text{gore lijevo}) \\ f_{tr}(p, q) & (\text{gore desno}) \\ f_{bl}(p, q) & (\text{dolje lijevo}) \\ f_{br}(p, q) & (\text{dolje desno}) \end{aligned}$$

Vodeni žig ugraditi ćemo samo u pod-slike $f_{tl}(p, q)$ i $f_{br}(p, q)$ radi smanjenja vizualnih promjena i postizanja boljeg PSNR-a.



Slika 1: Podjela slike na blokove

3.2 Umetanje vodenog žiga u D matricu

Na svaki $M \times M$ blok pod-slike $f_{tl}(p, q)$ (gdje je $M \times M$ veličina vodenog žiga) primjenjuje se SVD, čime dobivamo D matricu.

Iz svakog bloka D -matrice uzimamo najveći koeficijent $D(1, 1)$ i formiramo matricu D_{large} koja odgovara veličini slike vodenog žiga.

Koristeći Dither kvantizaciju, elementi D_{large} mijenjaju se ovisno o vrijednosti bita vodenog žiga (1 ili 0) i kategoriji kvantizacijske tablice:

<i>bin no.</i>	d_{low}	d_{high}
1	$d_{min} - T$	d_{min}
2	d_{min}	$d_{min} + T$
3	$d_{min} + T$	$d_{min} + 2T$
b_{n-1}	$d_{max} - T$	d_{max}
.
.
b_n	d_{max}	$d_{max} + T$

Slika 2: Kvantizacijska tablica

Ako je bit vodenog žiga ‘1’, onda pripada intervalu Range1, gdje je Range1 definiran na slijedeći način:

$$\text{Range1} = d_{\text{low}}(n) \quad \text{do} \quad \frac{d_{\text{low}}(n) + d_{\text{high}}(n)}{2} \quad (1)$$

Tada se D_{large} mijenja u:

$$D_{\text{large}} = \frac{d_{\text{low}}(n) + (d_{\text{low}}(n) + d_{\text{high}}(n)) / 2}{2} \quad (2)$$

Ako je bit vodenog žiga ‘0’, onda pripada intervalu Range2, gdje je Range2 definiran na slijedeći način:

$$\text{Range2} = \frac{d_{\text{low}}(n) + d_{\text{high}}(n)}{2} \quad \text{do} \quad d_{\text{high}}(n) \quad (3)$$

Tada se D_{large} mijenja u:

$$D_{\text{large}} = \frac{d_{\text{high}}(n) + (d_{\text{low}}(n) + d_{\text{high}}(n)) / 2}{2} \quad (4)$$

Nakon modifikacija, inverznom SVD transformacijom dobijemo prvi dio slike s vodenim žigom.

3.3 Umetanje vodenog žiga u U matricu

Na pod-sliku $f_{br}(p, q)$ također primjenjujemo SVD u $M \times M$ blokovima, sada ciljajući U matricu za umetanje vodenog žiga.

Vodni žig $w(i, j)$, $1 \leq i \leq N/2M$ i $1 \leq j \leq N/2M$ umeće se u stupce svakog bloka U matrice. Za svaki $M \times M$ blok U matrice, u_{11} (prvi red, prvi stupac) i u_{21} (drugi red, prvi stupac) modificiraju se na sljedeći način:

$$u_{\text{diff}} = |u_{11}| - |u_{21}| \quad (5)$$

Ako je $w(i, j) = 1$ i $u_{\text{diff}} > \alpha$ ili $w(i, j) = 0$ i $u_{\text{diff}} < \alpha$, tada:

$$u_{21} = - \left| u_{21} - \frac{(\alpha - u_{\text{diff}})}{2} \right| \quad (6)$$

$$u_{11} = - \left| u_{11} + \frac{(\alpha - u_{\text{diff}})}{2} \right| \quad (7)$$

Ako je $w(i, j) = 1$ i $u_{\text{diff}} < \alpha$ ili $w(i, j) = 0$ i $u_{\text{diff}} > \alpha$, tada:

$$u_{21} = - \left| u_{21} - \frac{(\alpha + u_{\text{diff}})}{2} \right| \quad (8)$$

$$u_{11} = - \left| u_{11} + \frac{(\alpha + u_{\text{diff}})}{2} \right| \quad (9)$$

Nakon modifikacije U matrice, inverznim SVD-om na svakom bloku dobijemo drugi dio slike s vodenim žigom.

3.4 Konačna slika s vodenim žigom

Na kraju, sve pod-slike $f_{tlw}(p, q)$, $f_{tr}(p, q)$, $f_{bl}(p, q)$ i $f_{brw}(p, q)$ kombiniraju se u konačnu sliku s vodenim žigom $F(i, j)$.

Predložena metoda pruža visoku razinu otpornosti na uobičajene napade na digitalne slike, kao što su kompresija, rotacija i dodavanje šuma. Korištenjem Dither kvantizacije u procesu umetanja vodenog žiga postiže se precizno prilagođavanje vrijednosti u D matrici, čime se osigurava da vodiči žig ostane skriven, ali istovremeno i otporan na razne modifikacije slike.

Uzimajući u obzir kvalitetu vodenog žiga i neprimjetnost prisutnosti vodenog žiga, metoda nudi učinkovito rješenje za zaštitu autorskih prava i sigurnost digitalnih slika u raznim primjenama.

4 Eksperimentalni rezultati

4.1 Steganografija na slici

Sa sljedećim kodom koristimo steganografiju na primjeru slike mačke i psa gdje sliku psa sakrijemo u sliku mačke. Kod možete vidjeti na našem Github repozitoriju koji se nalazi na [4] pod nazivom "steganografija.m".



Slika 3: Originalne slike

```
1 % Definiramo imena fileova
2 orig_file = 'macka.jpg'; % Originalna slika
3 zig_file = 'pas.jpg'; % Maska slika
4
5 % Ucitamo i procesuiramo prvu sliku
6 coverImage = imread(orig_file);
7 % Pretvorimo ju u crno-bijelu sliku radi izgleda(makar ova
8 vec je
9 coverImage = rgb2gray(coverImage);
10 % Pretvorimo u tip double radi SVDa
11 coverImage = im2double(coverImage);
12 figure(1), imshow(coverImage), title('Originalna slika');
13
14 % Na njoj napravimo SVD
15 [U_cover, S_cover, V_cover] = svd(coverImage);
```

Slika 4: Prvi dio koda

```

1      % Napravimo isto procesiranje za drugu sliku
2      secretImage = imread(zig_file);
3      secretImage = rgb2gray(secretImage);
4      secretImage = im2double(secretImage);
5      [rows, cols] = size(coverImage);
6      % U slucaju da treba masku smanjimo/povecamo na na velicinu
7      % originala
8      secretImage = imresize(secretImage, [rows, cols]);
9      % Napravimo SVD na tajnoj slici
10     [U_secret, S_secret, V_secret] = svd(secretImage);
11     % Ovdje mozemo mijenjati alpha za steganometriju
12     alpha = 0.5;
13     S_stega = S_cover + alpha * S_secret;

14     % Napravimo steganometrijsku sliku
15     stegaImage = U_cover * S_stega * V_cover';
16
17     % Spremanje slike
18     figure(2), imshow(stegaImage), title('Steganoetrijska slika')
19 );
20     imwrite(stegaImage, 'stega_output.png');

21     % Ponovno u itamo stega sliku i napravimo svd na njoj
22     stegaImageReloaded = im2double(imread('stega_output.png'));
23     [U_stega, S_stega_reloaded, V_stega] = svd(
24     stegaImageReloaded);

25     % Pomo u poznate alphu izvucemo tajnu sliku
26     S_extracted_secret = (S_stega_reloaded - S_cover) / alpha;

27     % Rekonstruiramo staru sliku
28     extractedSecretImage = U_secret * S_extracted_secret *
29     V_secret';

30     figure(3), imshow(extractedSecretImage), title('Tajna slika')
31 );

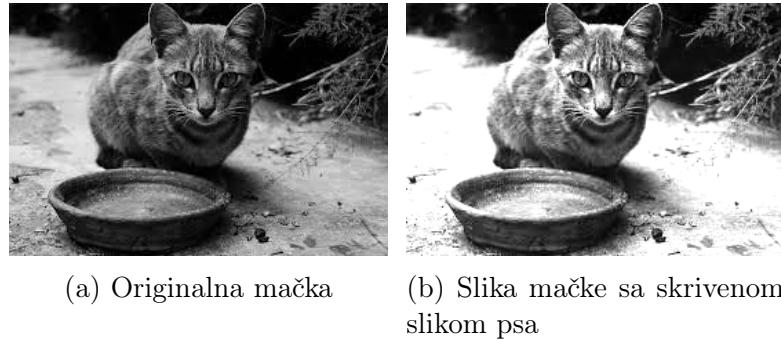
32     % Rekonstruiramo originalnu sliku iz stega slike
33     S_reconstructed_original = S_stega_reloaded - alpha *
34     S_secret;
35     reconstructedOriginal = U_stega * S_reconstructed_original *
36     V_stega';

37     figure(4), imshow(reconstructedOriginal), title(
38     'Rekonstruirana originalna slika');

```

Slika 5: Drugi dio koda

U ovom primjeru smo koristili da nam je $\alpha = 0.5$ te smo dobili sljedeći rezutat (sa strane stavljamo originalnu sliku za usporedbu):



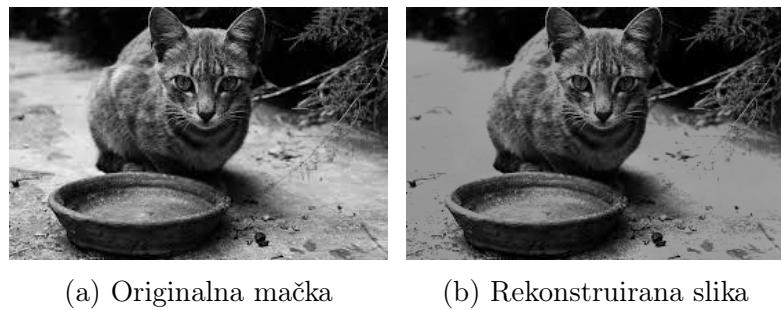
Slika 6: Steganometrija sa $\alpha = 0.5$

U ovom slučaju je α bio relativno velik pa se primjeti da je slika dosta svjetlija zbog toga. Ako uvrstimo $\alpha = 0.05$ razlika u odnosu na originalnu sliku se više baš i ne prepoznaje:



Slika 7: Steganometrija sa $\alpha = 0.05$

S obzirom da ponajemo α možemo i rekonstruirati sliku:



Slika je malo tamnija radi zaokruživanja te ne možemo dobiti potpuno istu sliku.

Ako povećamo α na tipa 0.9, steganografska slika će biti još svjetlijia:



(a) Originalna mačka (b) Rekonstruirana slika

Slika 9: Steganometrija sa $\alpha = 0.9$

Ujedno će i rekonstrukcija biti tamnija:



(a) Originalna mačka

(b) Rekonstruirana slika

To možemo primijetiti i na tajnoj slici koju radi poznavanja α možemo izvući iz steganografske slike:

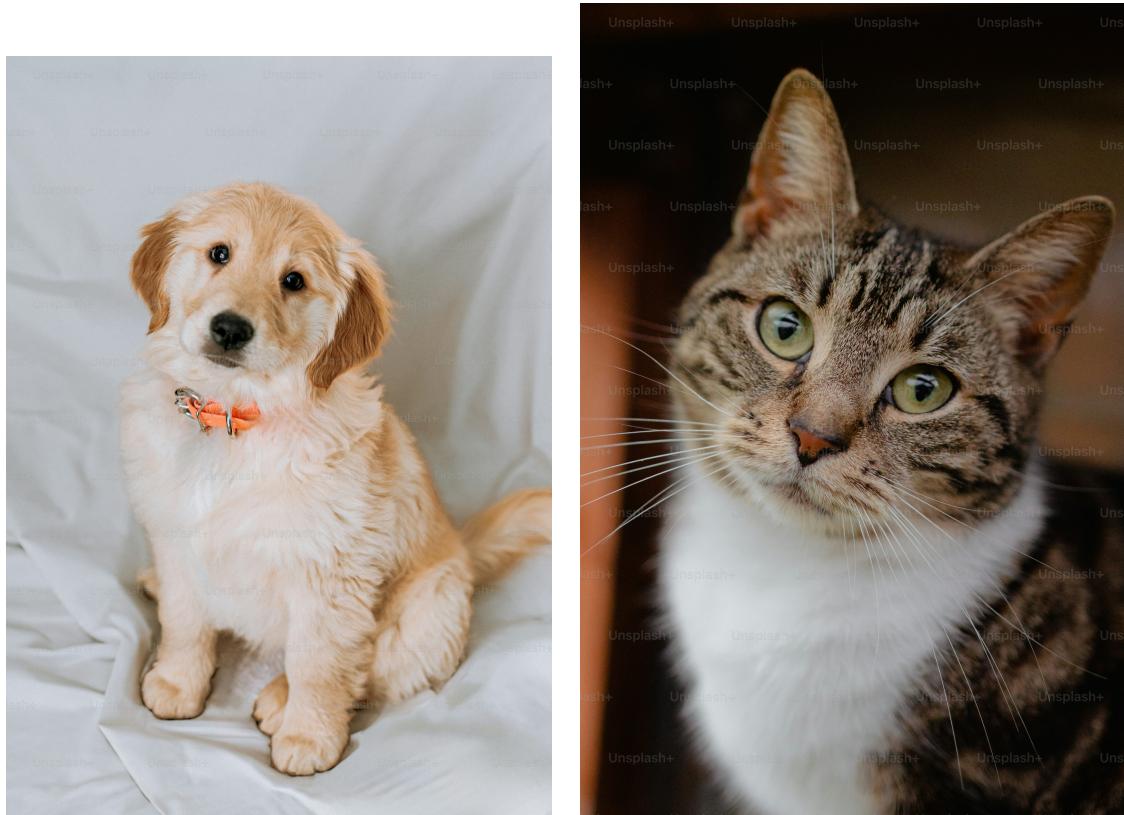


(a) Originalni pas

(b) Rekonstruirana tajna slika
psa

Osim toga, napravili smo i varijantu za slike u boji. Kod za tu varijantu se nalazi

u našem Github repozitoriju[4] pod nazivom "steganografijaColor.png". Ovo su dvije slike koje smo koristili:



Slika 12: originalne slike

U ovom slučaju smo malo obrnuli situaciju te spremili sliku mačke u sliku psa. pokretanjem kod smo dobili sljedeće:



(a) Originalni pas



(b) Slika pas sa skrivenom sli-
kom mačke

Slika 13: Stegenometrija sa $\alpha = 0.05$

Za situaciju gdje je $\alpha = 0.5$ opet dobijemo više primjetljivu razliku:



(a) Originalni pas



(b) Slika pas sa skrivenom sli-
kom mačke

Slika 14: Stegenometrija sa $\alpha = 0.05$

Također, pošto znamo α možemo izvući tajnu sliku



(a) Originalna mačka

(b) Rekonstruirana slika
mačke iz slike psa

5 Zaključak

6 Literatura

Literatura

- [1] B. Chandra Mohan, S. Srinivas Kumar, *A Robust Image Watermarking Scheme using Singular Value Decomposition*, JNTU College of Engineering, ECE Department, Kakinada, India
- [2] Ruizhen Liu, Tieniu Tan, *A SVD-Based Watermarking Scheme for Protecting Rightful Ownership*, National Lab of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences, P. O. Box 2728, Beijing, 100080, P. R. China
- [3] Zecheng Kuang, *Singular-Value Decomposition and its Applications*, Department of Mathematics, University of California San Diego, La Jolla, CA.
- [4] Naš Github repozitorij sa kodom: ([https://github.com/NikolaKasnar/
Image-watermarking-using-SVD](https://github.com/NikolaKasnar/Image-watermarking-using-SVD))