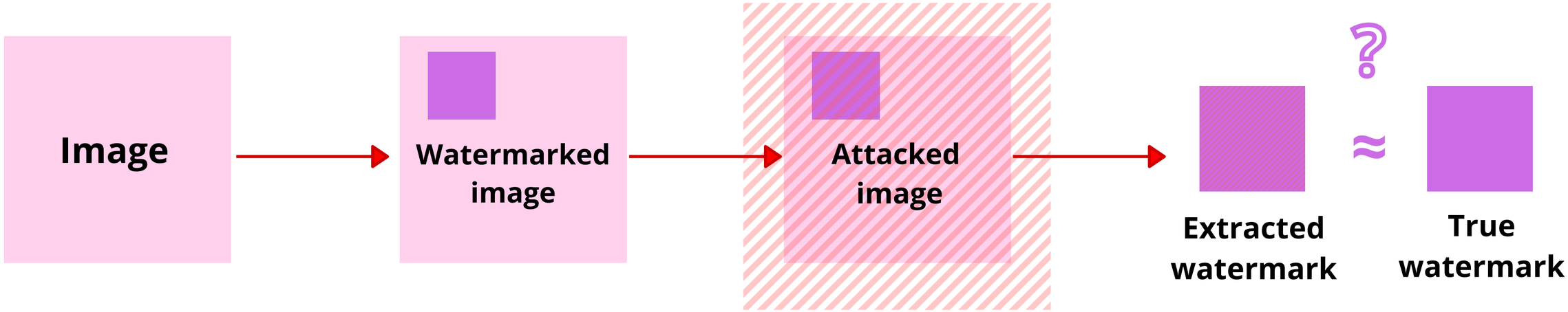
Watermarking colored image using SVD

JULIA MOROZ
OLGA GOLDOBINA
ALEXANDER TELEPOV
MAKSIM PANKRATOV

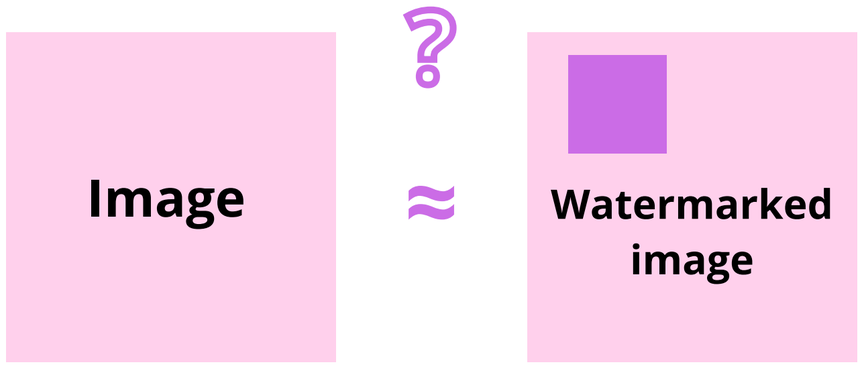
Problem statement

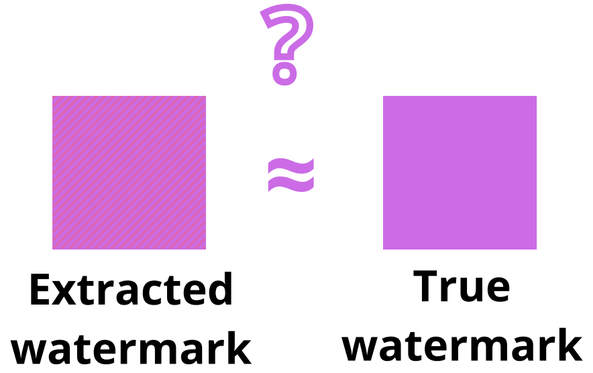


Applications:

- Owner identification
- Copyright protection
- Source tracking

Problem statement





Metrics:

$$MSE(Im, Im^{noisy}) = \frac{1}{KNM} \sum_{k=0}^{K} \sum_{i=0}^{N} \sum_{j=0}^{M} (Im_{ijk} - Im_{ijk}^{noisy})^2$$

$$PSNR(Im, Im^{noisy}) = 10 \log_{10}(\frac{V_{max}^2}{MSE(Im, Im^{noisy})})$$

V_{max} - maximal possible pixel value

Algorithm

Intuition behind algorithm:

Singular values of an image have very good stability.

Thus, when a small perturbation is added to an image, its singular values do not change significantly. So we can make a watermark by adding noise to singular values.

Algorithm: Encode $\mathcal{O}(n^3)$

Starting with RGB image: $I(x, y) \rightarrow [r(x, y), g(x, y), b(x, y)]$

- For each color decompose image*;
- Apply watermark to diagonal matrix of singular values;
- Decompose the result of previous step;
- Use new singular values in initial SVD decomposition;

$$I = UDV^T$$
$$\downarrow$$
$$D^{'} = D + \alpha W$$
$$\downarrow$$
$$D^{'} = U^{'} D^{''} V^{'T}$$
$$\downarrow$$
$$I^w = UD^{''}V^T$$

*can be replaced with DWT of each color

Algorithm: Decode $\mathcal{O}(n^3)$

Now we start with watermarked (probably distorted) image

- Decompose it;

$$I^w = U^w D^w V^{wT}$$

$$\downarrow$$

- Construct new matrix using unitary matrices from previous slide;

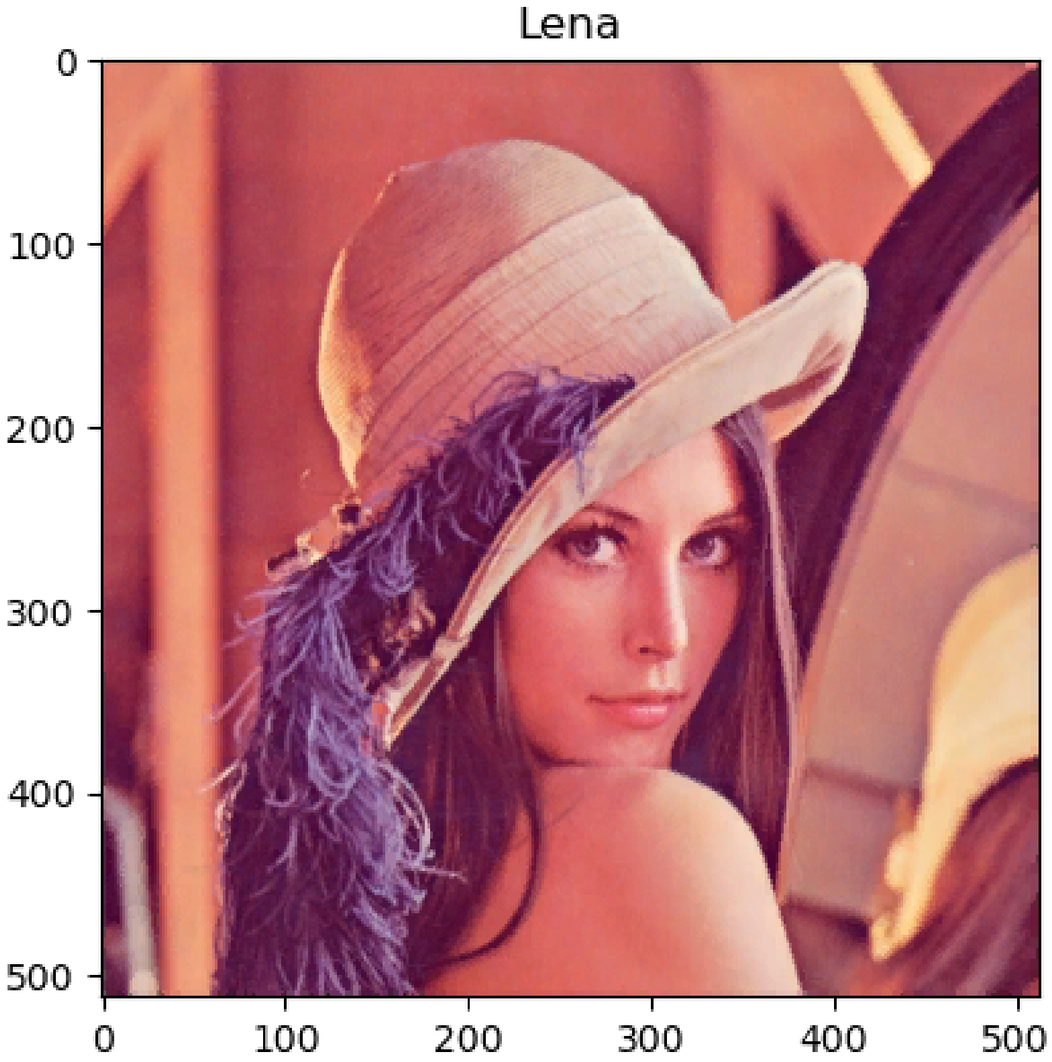
$$E = U^{'} D^w V^{'T}$$

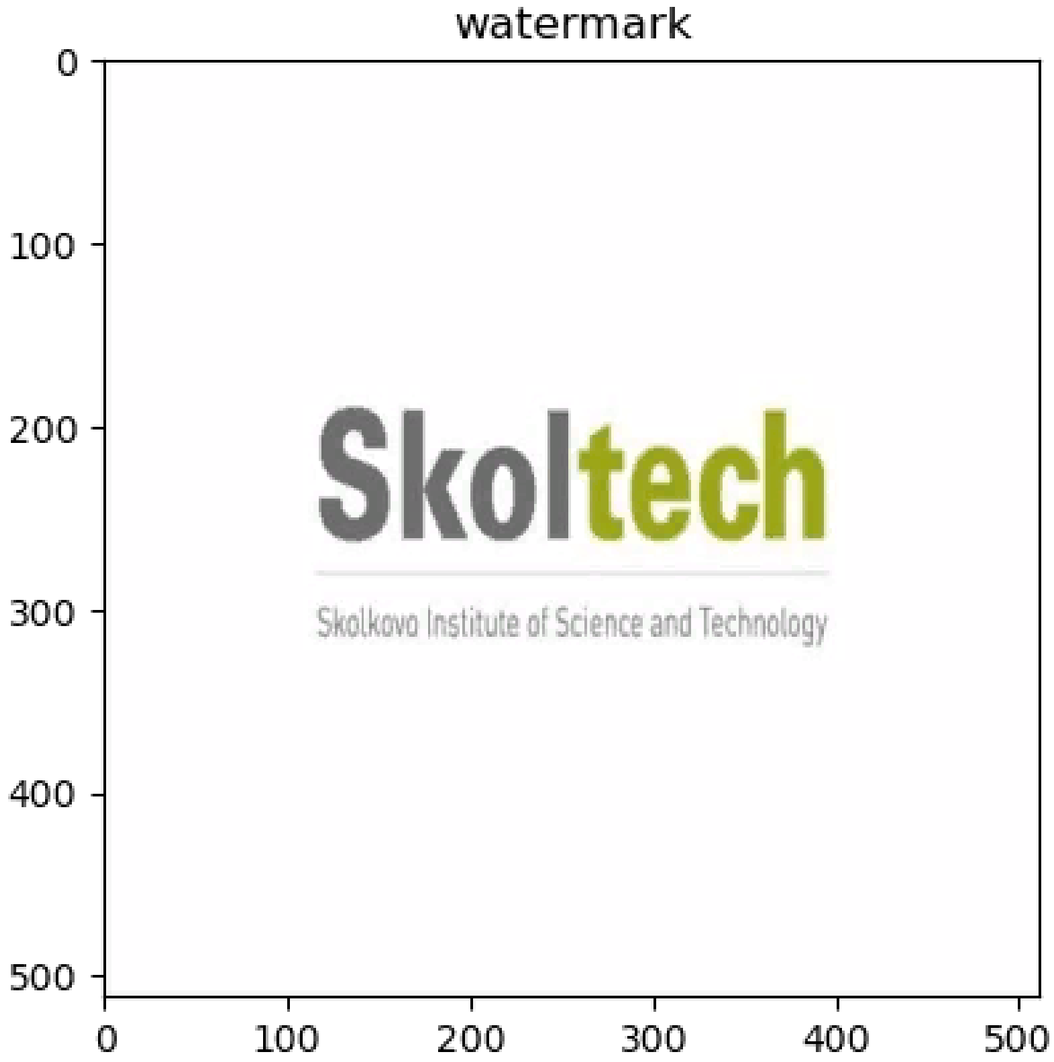
$$\downarrow$$

- Compute extracted watermark using formula

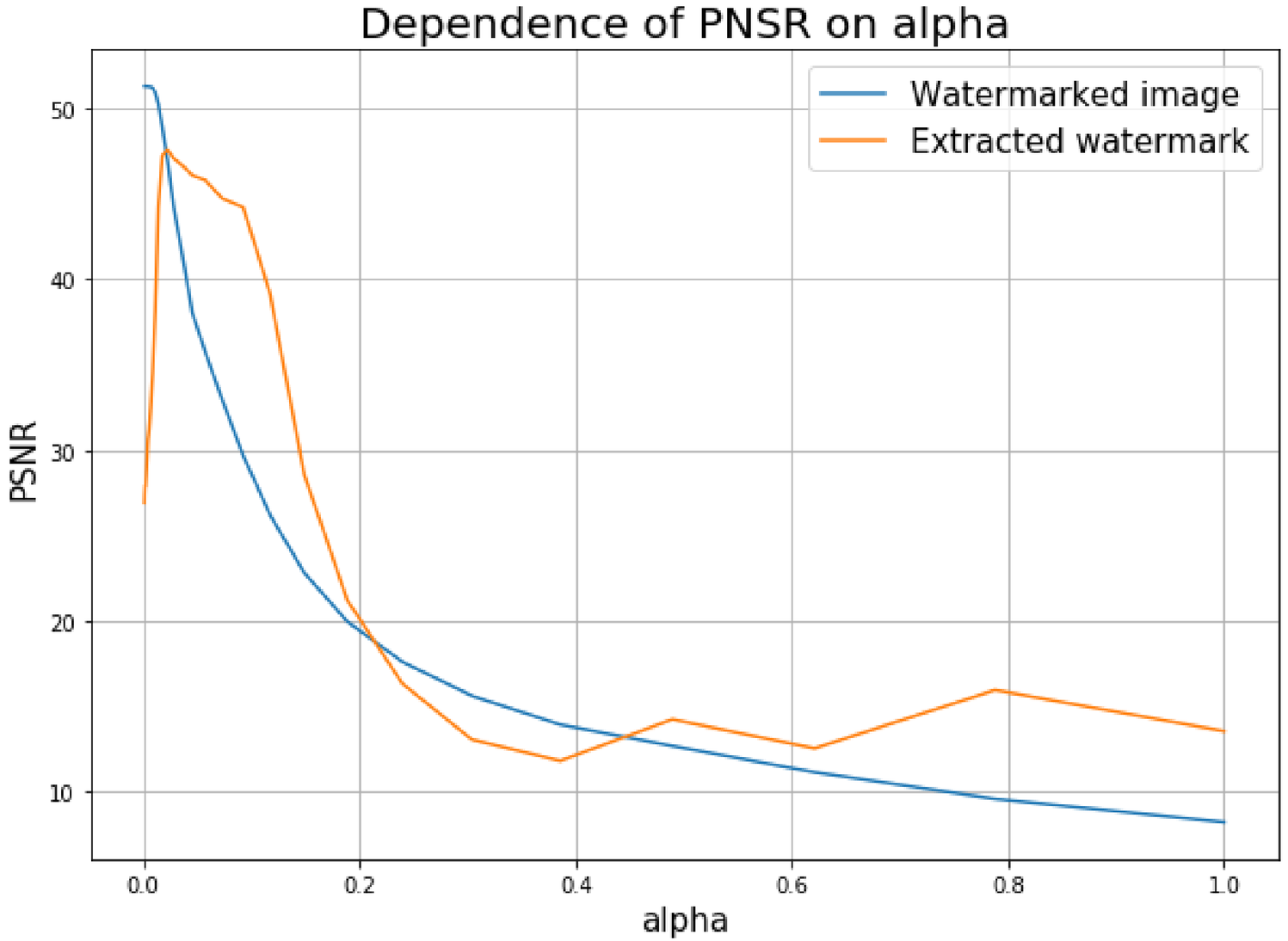
$$W^e = \frac{E - D}{\alpha} = \frac{U^{'} D^w V^{'T} - D}{\alpha}$$

Input images



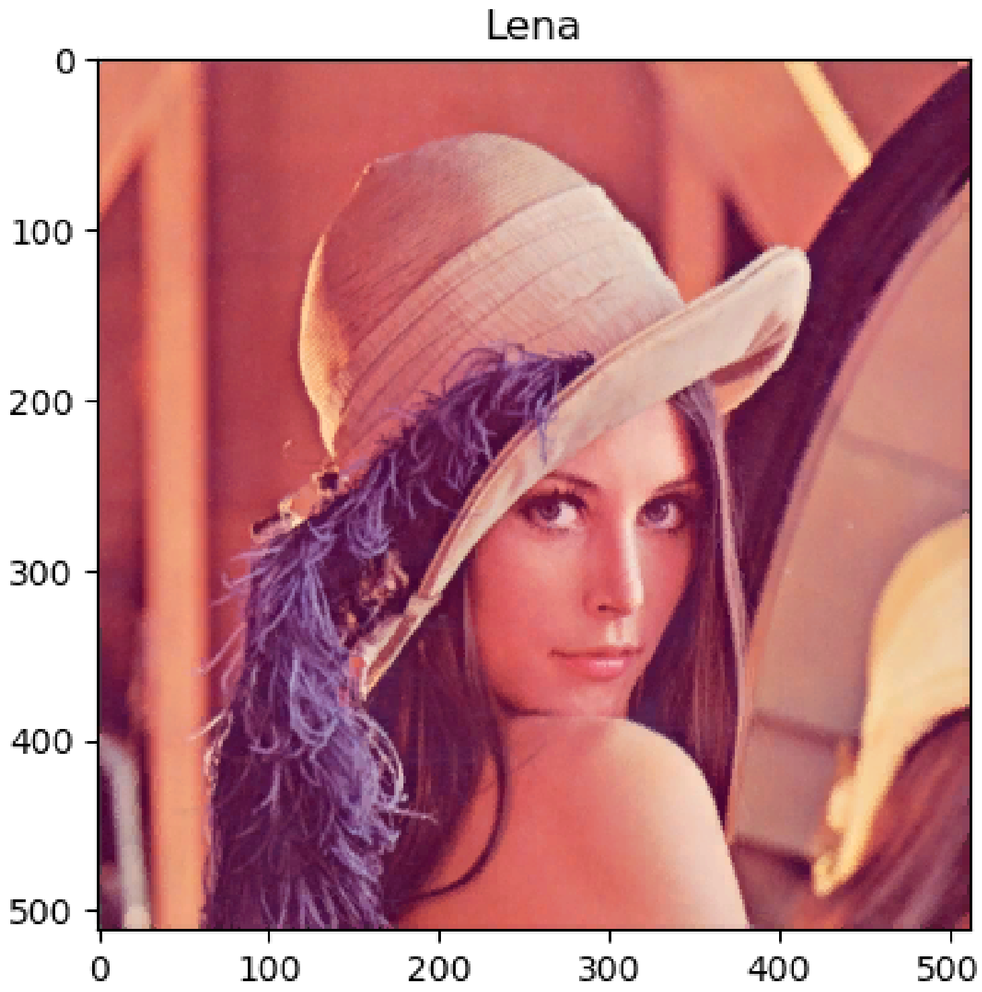


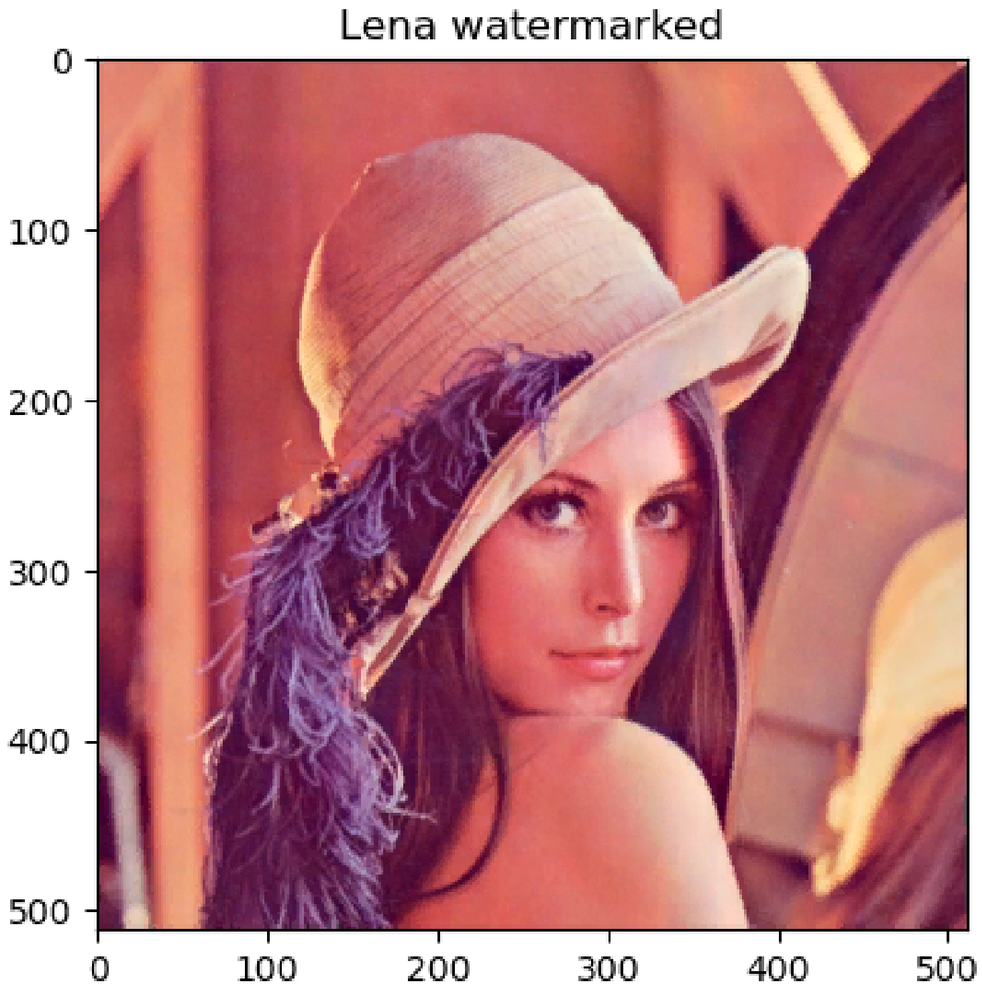
Choosing alpha



Best alpha ≈ 0.05

Applying watermark

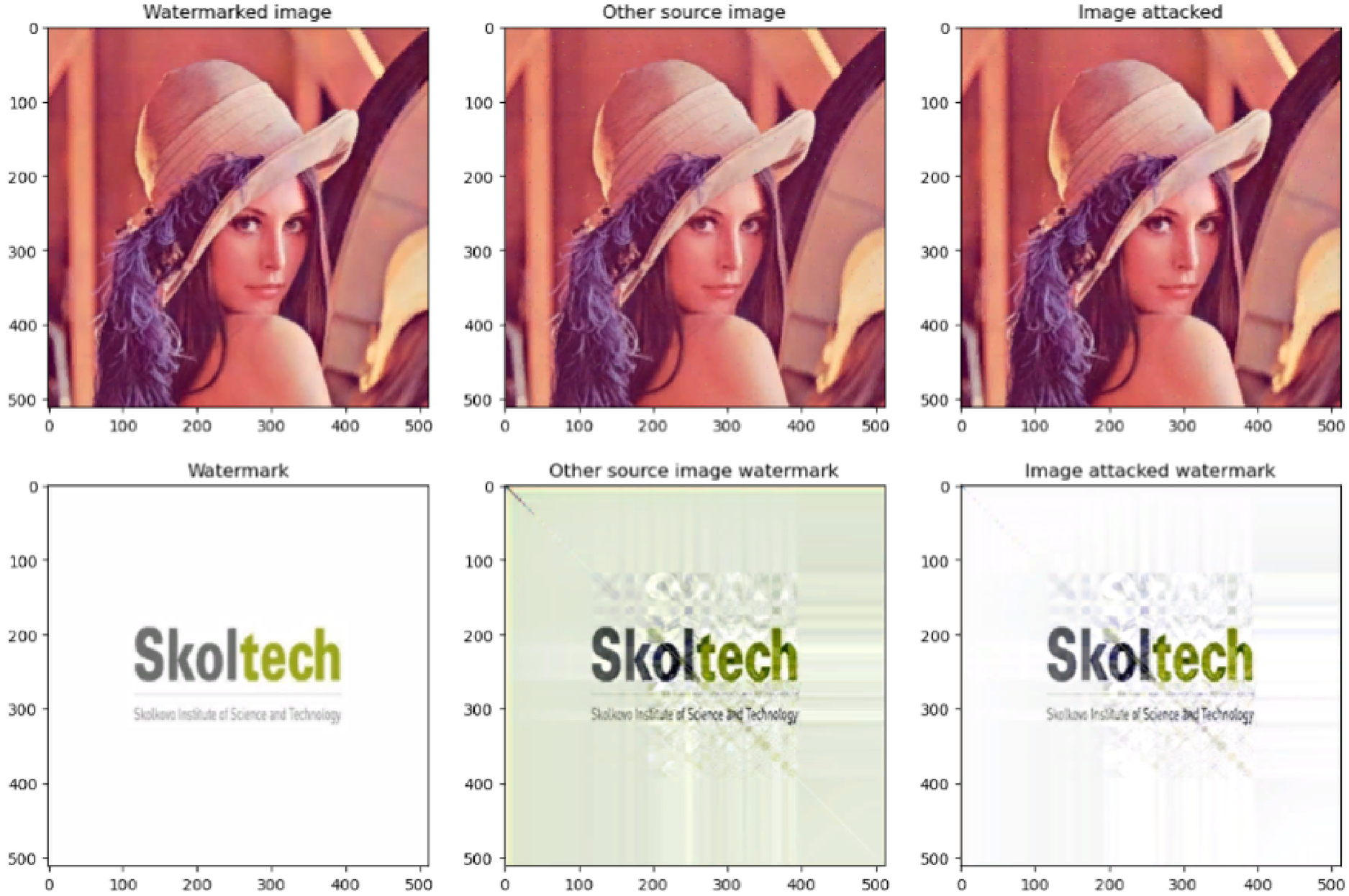




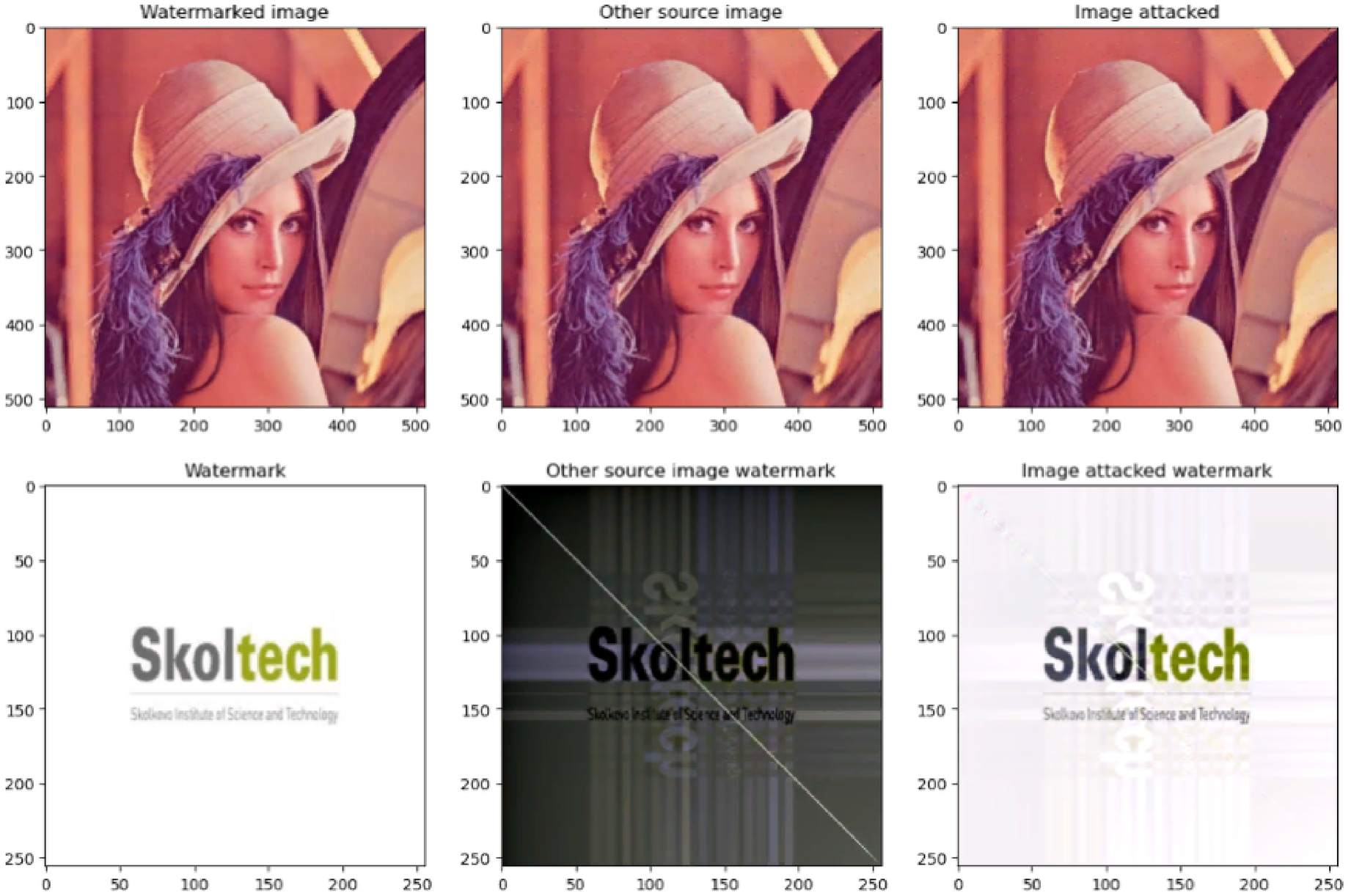
MSE = 13.630, PNSR = 36.786

A couple of experiments...

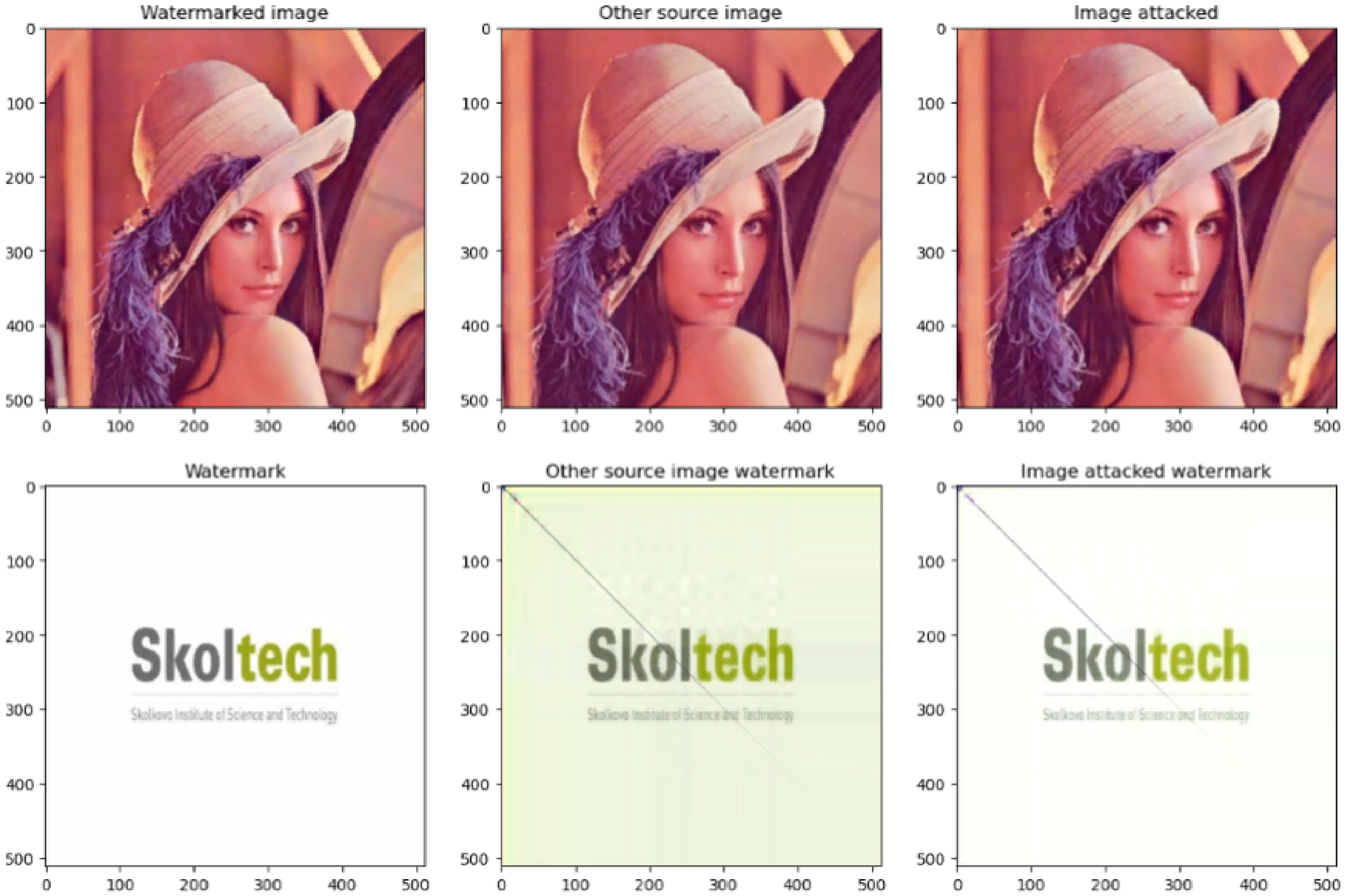
Salt&pepper noise



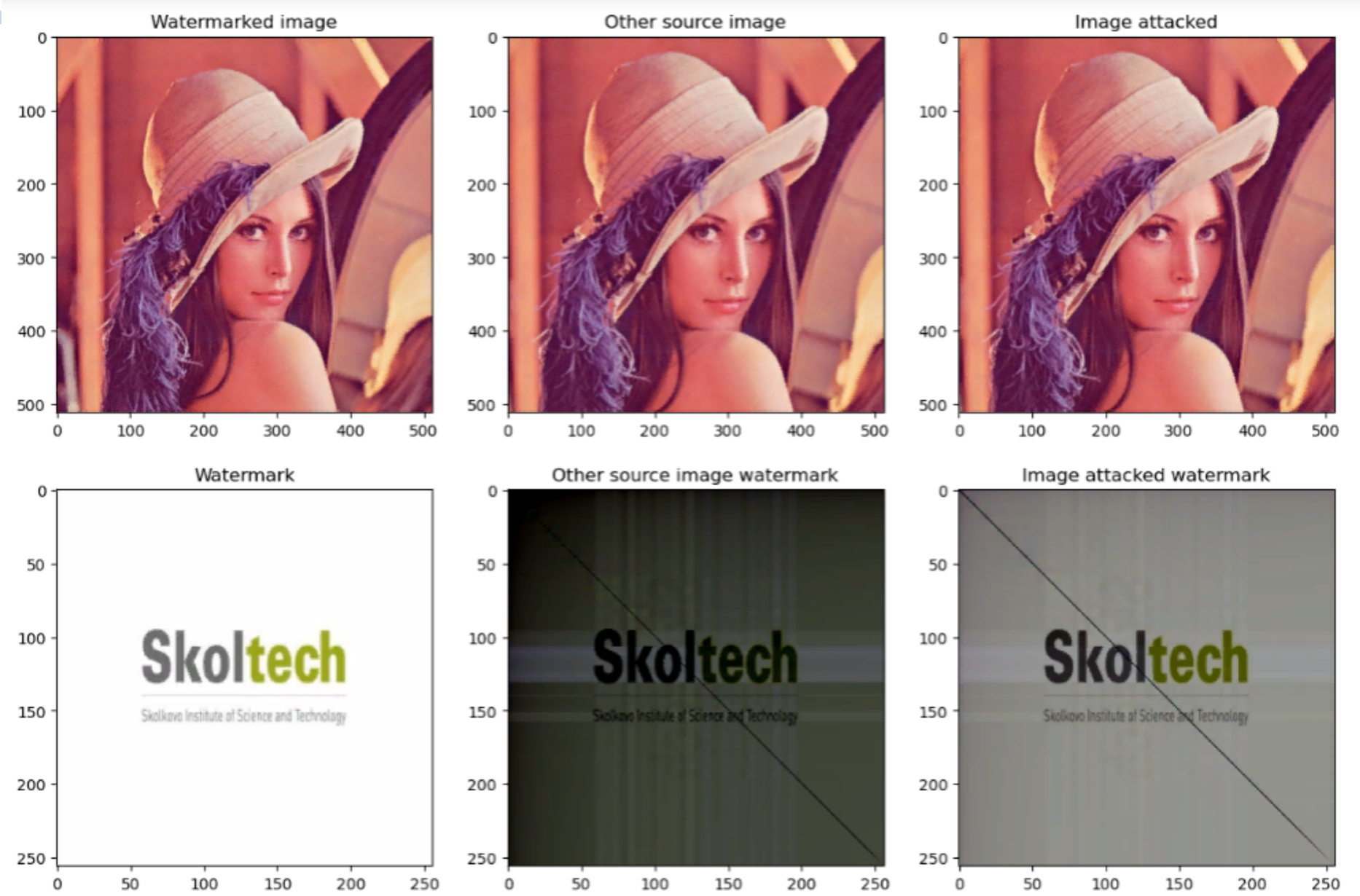
Salt&pepper noise (DWT)



Cropping


Watermarked image
Other source image
Image attacked
Watermark
Other source image watermark
Image attacked watermark
Skoltech
Skolkovo Institute of Science and Technology

Cropping (DWT)



Experiments metrics

Images

	pnsr_img_attacked	pnsr_img_other_source	mse_img_attacked	mse_img_other_source
sp_noise	32.46147	31.09300	36.89213	50.55689
rotate	10.32986	10.33867	6026.90544	6014.69024
blur	32.84674	32.40626	33.76032	37.36410
cropped	15.37378	15.40434	1886.69903	1873.46953
sharpened	5.06885	5.08301	20239.27372	20173.39373
compressed_100	37.68402	34.53477	11.08355	22.88774

Extracted watermarks

	pnsr_wm_attacked	pnsr_wm_other_source	mse_wm_attacked	mse_wm_other_source
sp_noise	25.46994	2.32160	184.53826	38099.60198
rotate	2.12548	2.07023	39859.50643	40369.82611
blur	2.71275	1.94811	34818.11775	41521.14531
cropped	6.66577	2.14102	14012.10816	39717.16479
sharpened	11.83142	10.20719	4265.18902	6199.56836
compressed_100	22.69754	2.34751	349.40298	37872.93997

Results

- The algorithm allows **implementing a watermark without changes in the original image** noticeable to human eyes.
- This method **does not completely save us from false-positive** errors, but at the same time, the **watermark is extracted from watermarked images more clearly**.
- This method is **resistant to most of the considered attacks**.

References

- CHIH-CHIN LAI, CHENG-CHIH TSAI, DIGITAL IMAGE WATERMARKING USING DISCRETE WAVELET TRANSFORM AND SINGULAR VALUE DECOMPOSITION, HTTPS://IEEEXPLORE.IEEE.ORG/DOCUMENT/5560822

- FITA A, ENDEBU B, WATERMARKING COLORED DIGITAL IMAGE USING SINGULAR VALUE DECOMPOSITION FOR DATA PROTECTION, HTTPS://WWW.RESEARCHGATE.NET/PUBLICATION/330727358_WATERMARKING_COLORED_DIGITAL_IMAGE_USING_SINGULAR_VALUE_DECOMPOSITION_FOR_DATA_PROTECTION

Thank you!

LET US KNOW IF YOU HAVE
QUESTIONS OR CLARIFICATIONS.