Catch The Mark 2022 - PIXEL

Multimedia Data Security

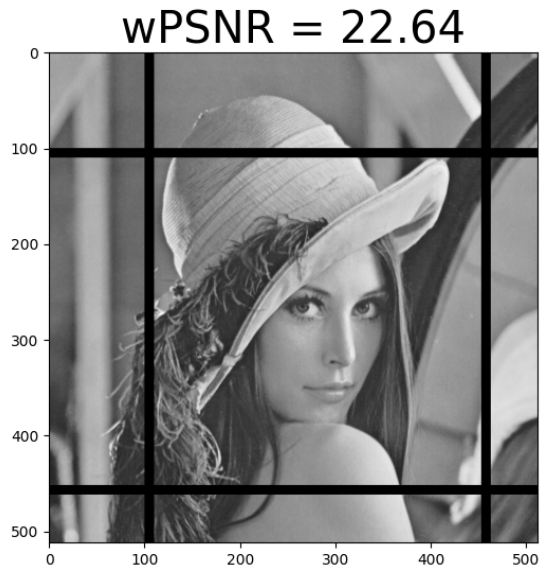
FREGONA Giacomo, GASSINE Alan,
HAVERMANS Stephan

Supervised by: Prof. Giulia Boato & Dott. Andrea Montibeller

Nov 9, 2022

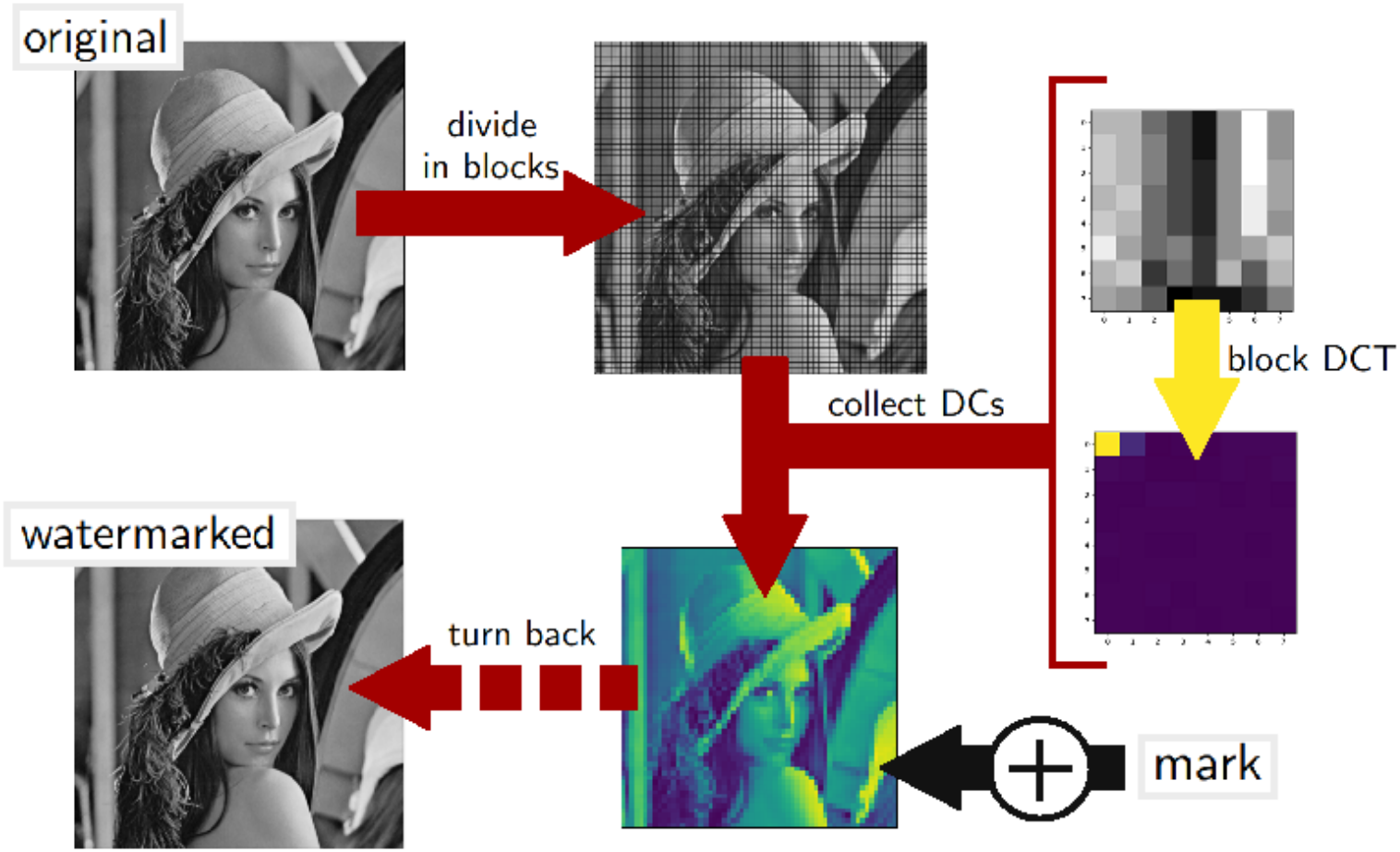
Summary

Motivation of our code

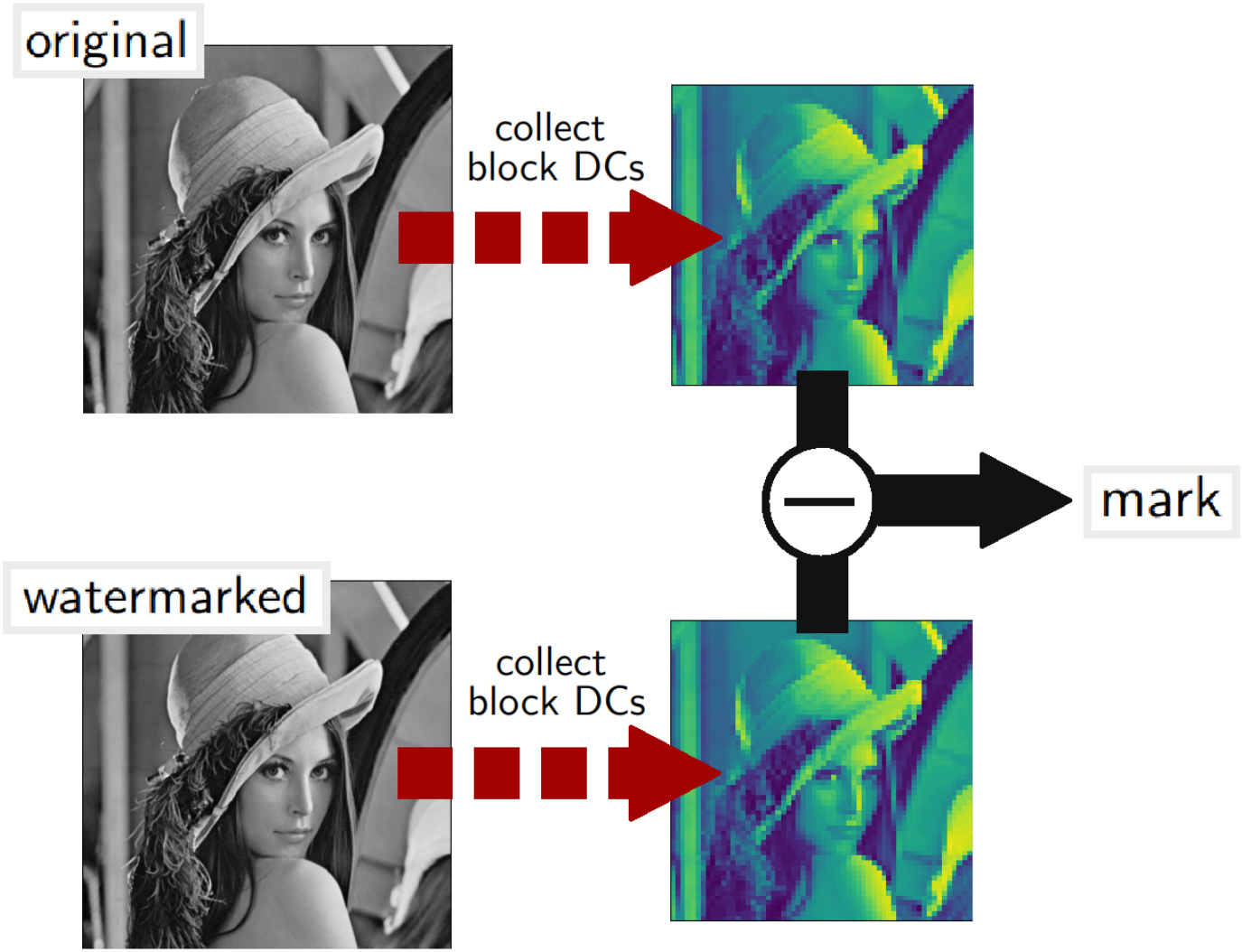


- The wPSNR function used in the competition is not sensitive in the borders! Hence:
  - additive watermark has easy wPSNR behaviour,
  - the watermark location is a relevant quality parameter.
- Let's use the DC component of 8×8 blocks to be robust against Jpeg compression.

Embedding


original
divide
in blocks
block DCT
collect DCs
watermarked
turn back
mark

Detection


original
collect
block DCs
mark
watermarked
collect
block DCs

Our strategy in practice

In practice:

- substitute the mark with its encoding;
- to represent a 1 bit, add a constant value α to all the pixels of a block instead of modifying the DC component;
- to represent a 0 bit, leave unchanged the block;
- extract each bit with the following formula:

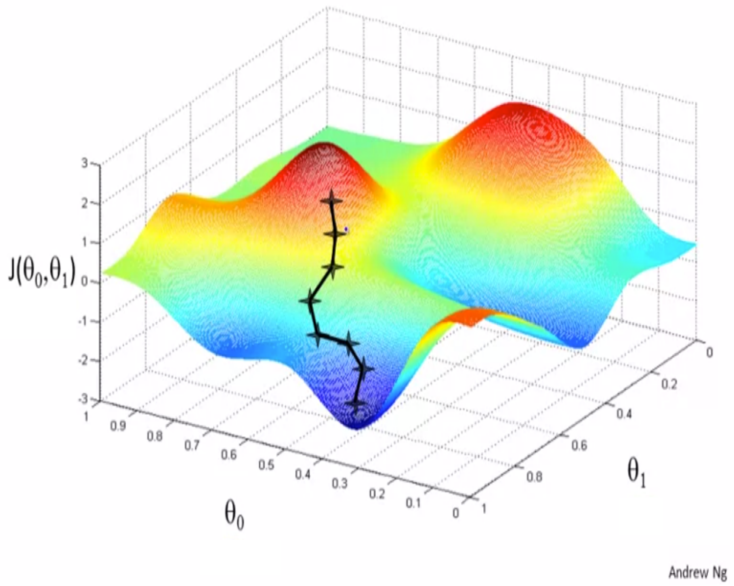
$$bit_{extracted} = \frac{\sum_i (block_w - block_o)_i}{64 \times \alpha};$$

- decode the mark using the extracted bits. Return 0 if you have no information for a bit position.

Last minute problem: comparison attack

- Idea: represent zeros adding α and ones leaving unchanged the block. In this way:
  - the locations where we inserted the ones will not be visible,
  - locations of the zeros will be visible but could probably be recovered exploiting the decoding strategy if strongly attacked.
- Problem: mark detected in the original image.

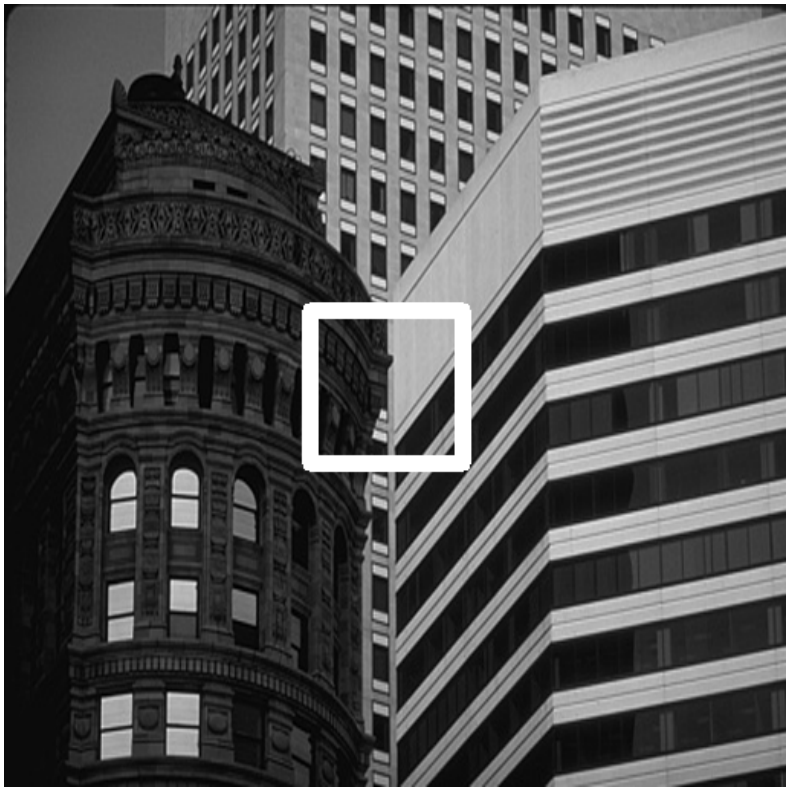
Attack - Automated



Auto-Attack Strategy

- Use every basic attack
- 3 different parameters
- Every image
- Detect watermark
- Output results in DataFrame

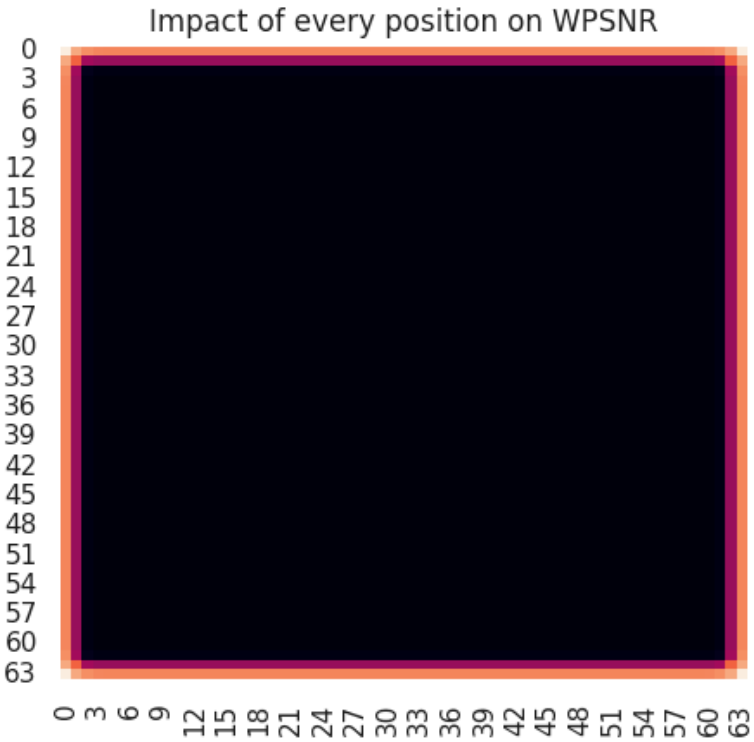
Attack - Local



Local Attack Strategy

- Avoid unmarked sections
- Higher WPSNR
- Partial removal
- Watermark undetectable

Attack - Border



Border JPEG Compression

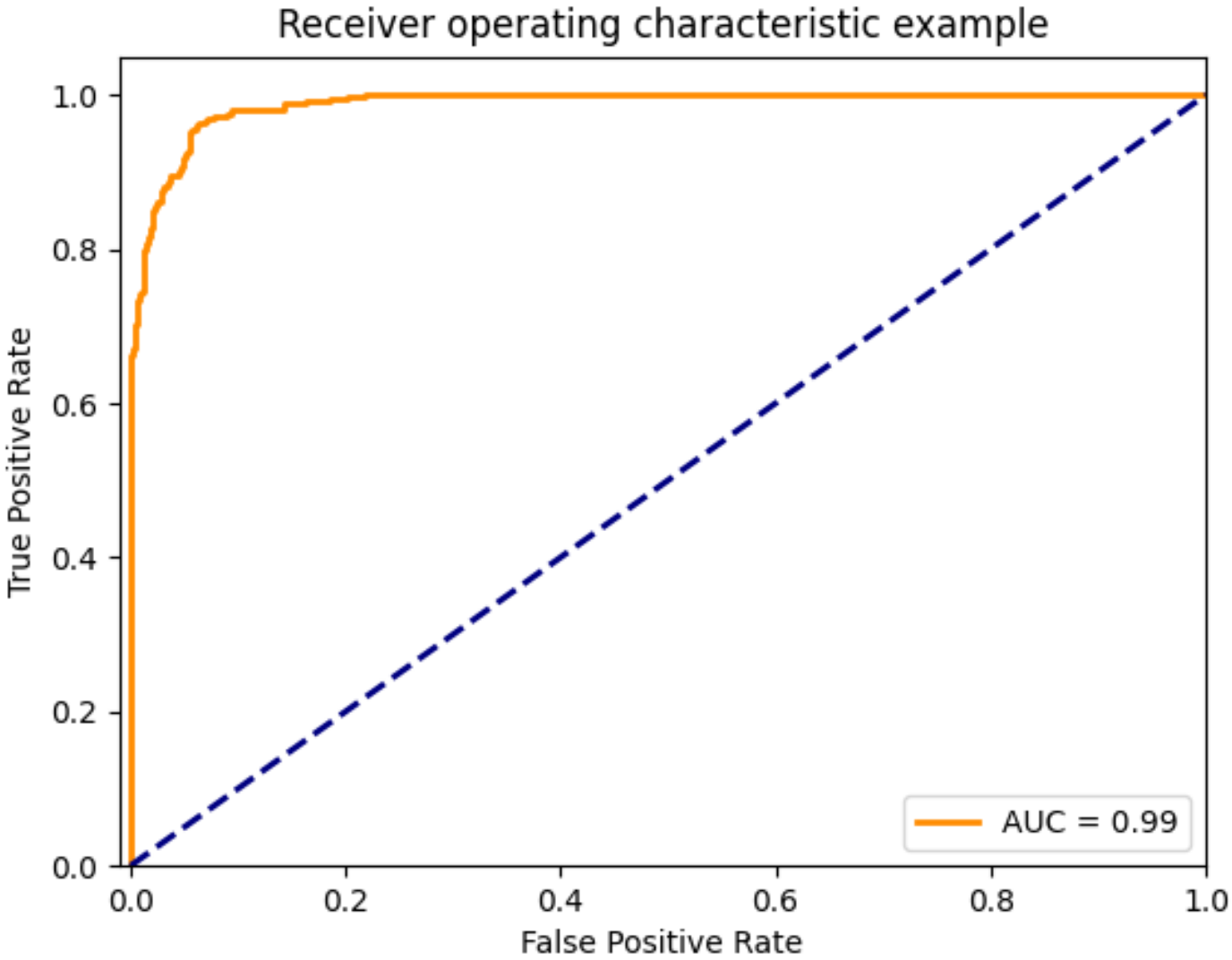
- Convolution → Non-uniform impact
- Suspected spot for watermarks
- Aggressive JPEG Compression

Results - Strategy

What really happened:

- The auto-attack and border strategies were very useful
- We made no use of the localized attacks
- Our threshold computation method seemed successful

Results - ROC Curve & Threshold



Results - Attacks (1)

Image	Group	WPSNR	Attack(s) with parameters
building	dinkleberg	39.89	median filtering with kernel_size = [3,5]
rollercoaster		38	median filtering with kernel_size = [3,5]
tree		35.87	sharpening with sigma = 0.5 and alpha = 1
Image	Group	WPSNR	Attack(s) with parameters
building	weusedlsb	37.48	jpeg compression with QF = 8
rollercoaster		38.2	jpeg compression with QF = 8
tree			
Image	Group	WPSNR	Attack(s) with parameters
building	omega		
rollercoaster		46.68	jpeg compression with QF = 25
tree			
Image	Group	WPSNR	Attack(s) with parameters
building	ef26420c		
rollercoaster		35.69	blur with sigma = [1.4, 1.2]
tree			
Image	Group	WPSNR	Attack(s) with parameters
building	failedfouriertransform	35.93	blur with sigma = [1.5,0.5]
rollercoaster		41.86	jpeg compression with QF = 1 on the borders
tree		36.63	blur with sigma = [1.5,9]

Results - Attacks (2)

Image	Group	WPSNR	Attack(s) with parameters
building	you_shall_not_mark	42.9	resizing of scale 0.7
rollercoaster		50.31	blur with sigma = [0.45, 0.45]
tree		42.04	resizing of scale 0.8
Image	Group	WPSNR	Attack(s) with parameters
building	howimetyourmark	35.45	jpeg compression with QF = 6
rollercoaster		36.11	jpeg compression with QF = 6
tree			
Image	Group	WPSNR	Attack(s) with parameters
building	theyarethesamepicture	36.52	jpeg compression with QF = 7
rollercoaster			
tree			
Image	Group	WPSNR	Attack(s) with parameters
building	blitz	132.2	jpeg compression with QF = 1 on the borders
rollercoaster		132.49	jpeg compression with QF = 1 on the borders
tree		130.78	jpeg compression with QF = 1 on the borders
Image	Group	WPSNR	Attack(s) with parameters
building	thebavarians	132.64	jpeg compression with QF = 1 on the borders
rollercoaster			
tree			

Thanks for your attention

Any Questions?

FREGONA Giacomo, GASSINE Alan,
HAVERMANS Stephan

Supervised by: Prof. Giulia Boato & Dott. Andrea Montibeller

Nov 9, 2022