ammhackati

CAPTURE THE MARK 2024

University of Trento

Embedding

Multilevel DWT

To increase robustness

Modular alpha

To adapt the embedding to different layers and sub-bands

Perceptual mask

To increase invisibility

M. Barni, F. Bartolini and A. Piva, "Improved wavelet-based watermarking through pixel-wise masking," in IEEE Transactions on Image Processing, May 2001, doi: 10.1109/83.918570.

Multilevel DWT

compute

modular alpha

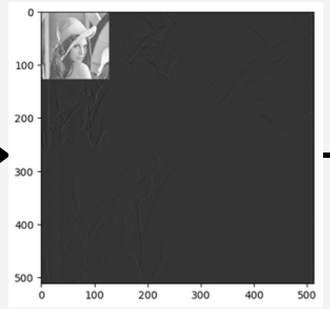
perceptual mask

best locations

Watermark
011011...001011

$$Loc_{wm} = Loc_{original} \cdot (1 + (mask \cdot \alpha_{\theta l} \cdot mark))$$

Multilevel
iDWT



compute

modular alpha

perceptual mask

best locations

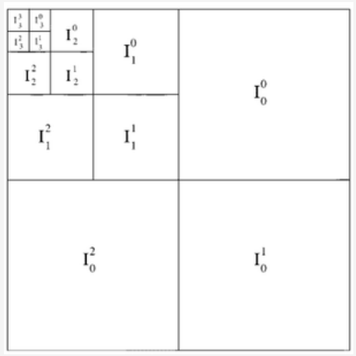
Watermark
011011...001011

$$Loc_{wm} = Loc_{original} \cdot (1 + (mask \cdot \alpha_{\theta l} \cdot mark))$$

Multilevel
iDWT

Multilevel DWT

compute



perceptual mask

best locations

Watermark
011011...001011

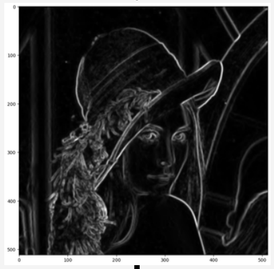
$$Loc_{wm} = Loc_{original} \cdot (1 + (mask \cdot \alpha_{\theta l} \cdot mark))$$

Multilevel
iDWT

Multilevel DWT

compute

modular alpha



best locations

Watermark
011011...001011

$$Loc_{wm} = Loc_{original} \cdot (1 + (mask \cdot \alpha_{\theta l} \cdot mark))$$

Multilevel iDWT

Detection

Original

Multilevel DWT

modular alpha

perceptual mask

best locations

$$WM_{bit} = \frac{Loc_{wm} - Loc_{or}}{\alpha_{\theta l} \cdot mask \cdot Loc_{or}}$$

mean between same layer

Original Watermark
011011...001011

Watermarked

Multilevel DWT

modular alpha

perceptual mask

best locations

Detection

Attacked

Multilevel DWT

modular alpha

perceptual mask

best locations

$$WM_{bit} = \frac{Loc_{wm} - Loc_{or}}{\alpha_{\theta l} \cdot mask \cdot Loc_{or}}$$

mean between same layer

best similarity score

Original Watermark
011011...001011

Extracted watermark
011011...001011

Defense phase

Parameters we chose for the embedding

Number of layers	Alpha	Perceptual mask
3	8.4	only edges

Tested against both **global** and **localized** attacks

- awgn
- blur_gauss
- jpeg_compression
- sharp
- blur_median
- resize
- gauss_dwt
- median_dwt
- gauss_edge

Results

LAYERS	ALPHA	INVISIBILITY	ROBUSTNESS
3	0.88	3	4
3	8.4	1	6
2	0.2	6	0
2	1.4	2	5
1	20	1	6

Attack phase

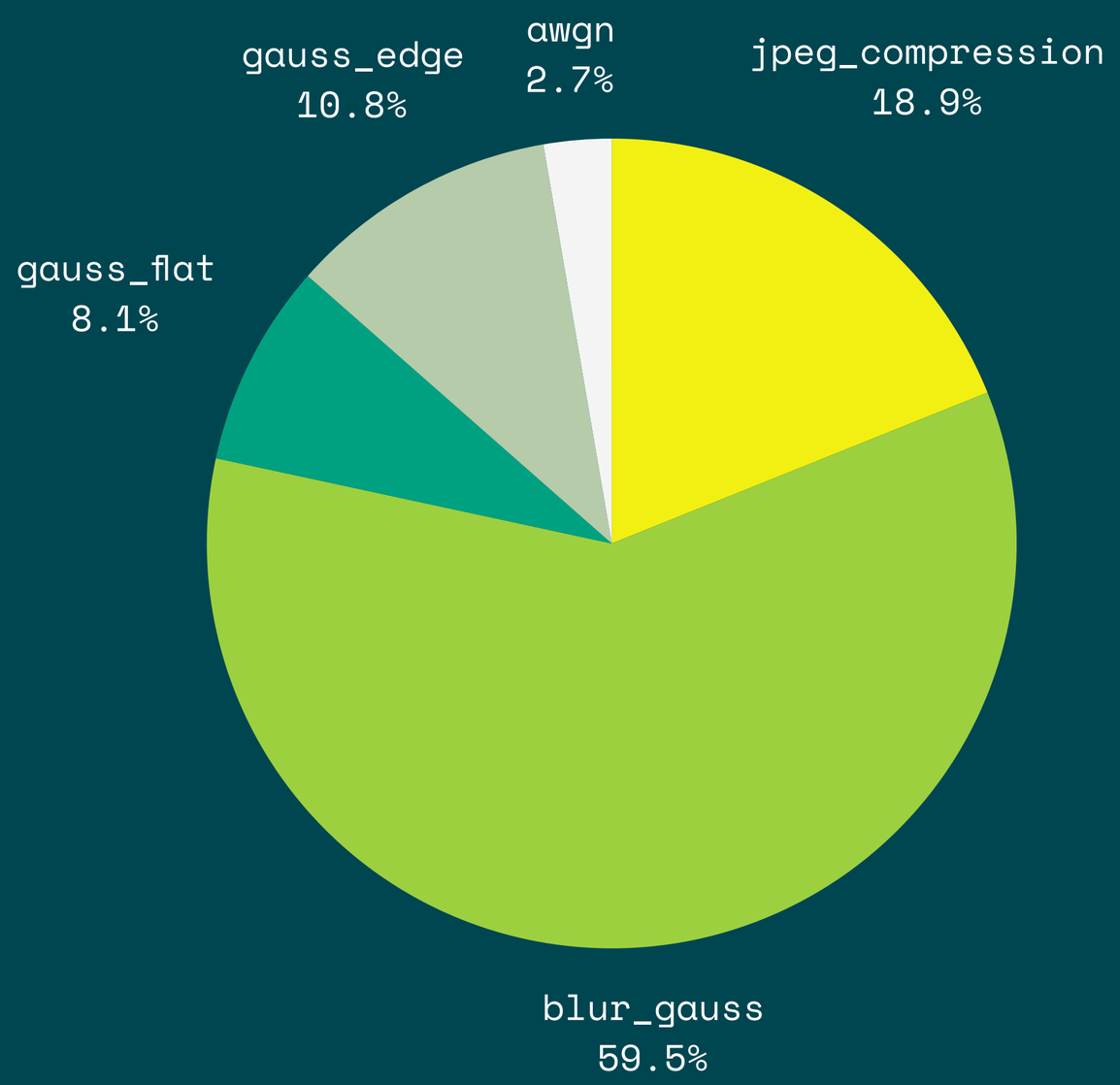
The Attack function allowed to specify the attack to use and the corresponding parameters.

- **Global attacks**
- **Localized attacks**
- **Combination attacks**
- **Wavelet transform attacks**

During the challenge we manually chose which one to apply, trying different parmeters in order to remove the watermark.

Results

STATISTICS	WPSNR
max	73.71 (9999)
avg	~43
min	36.06



Further improvements and things we tried

SVD / Hashing

ECC

- Hamming codes
- Reed-Solomon codes
- Low-Density Parity Check

Limit quantization errors

ammhackati

THANK YOU