Multimedia Data Security
University of Trento

2 November 2020

Iquartz

Georgiana Bud, Matteo Golinelli, Francesco Penasa, Alessandro Sartori

Capture The Mark

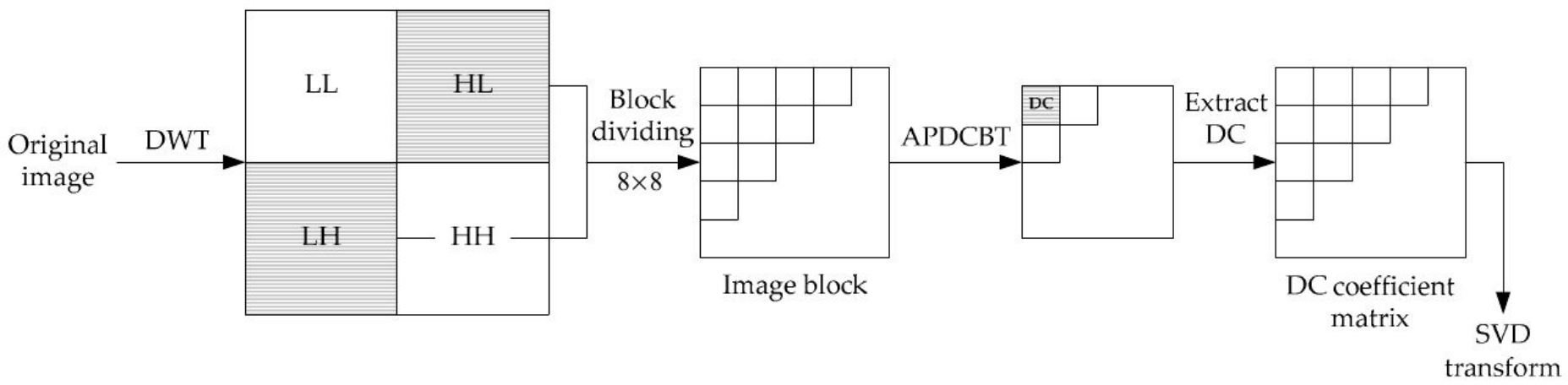
1. Defense strategy
2. Attack strategy
3. Results

Choosing our Strategy

“A Robust Image Watermarking Technique Based on DWT, APDCBT, and SVD”

- Explains the algorithm clearly
- Analyses and reports a high watermark robustness

Paper: Insertion Strategy



"A Robust Image Watermarking Technique Based on DWT, APDCBT, and SVD"

Example of embedding with paper algorithm

Lena, original

Lena, watermarked, alpha = 100

Implementation by Trial and Error

1. DWT + DCT full frame
2. DWT + APDCBT full frame
3. DWT + APDCBT on 8x8 blocks + DC extraction + SVD
4. DWT + APDCBT on 8x8 blocks

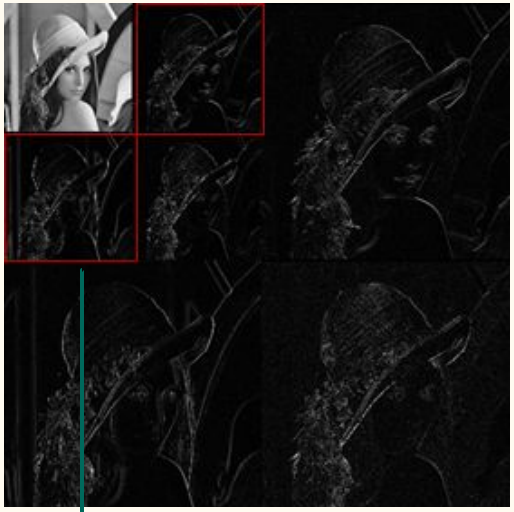
Final approach: Insertion

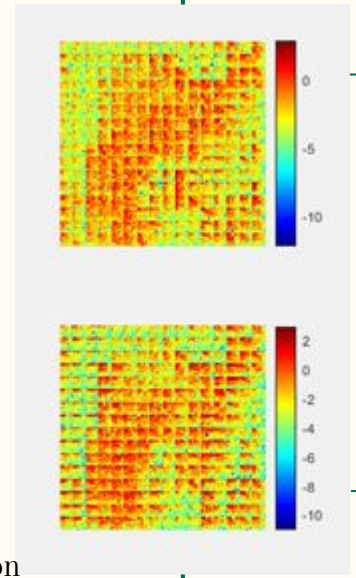
1 - Discrete Wavelet Transform, Level 2

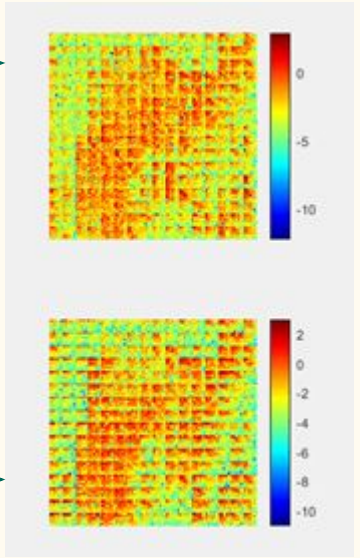
2.A - APDCBT on blocks on horizontal sub-band

3. Spread Spectrum additive in highest 1024 coefficients

watermarked = *original* + *1,2* x *watermark*





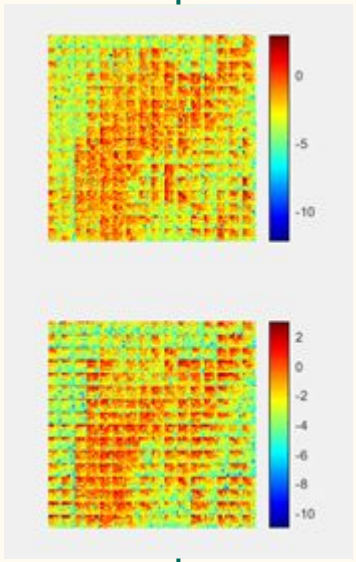


2.B - APDCBT on blocks on vertical sub-band

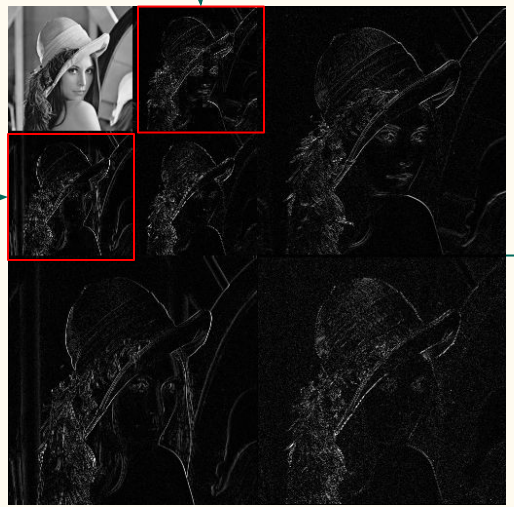
EXTRA: Change watermark to [-1, 1]

Insertion (continued)

3. Watermarked coefficients



4.A - IAPDCBT on horizontal sub-band

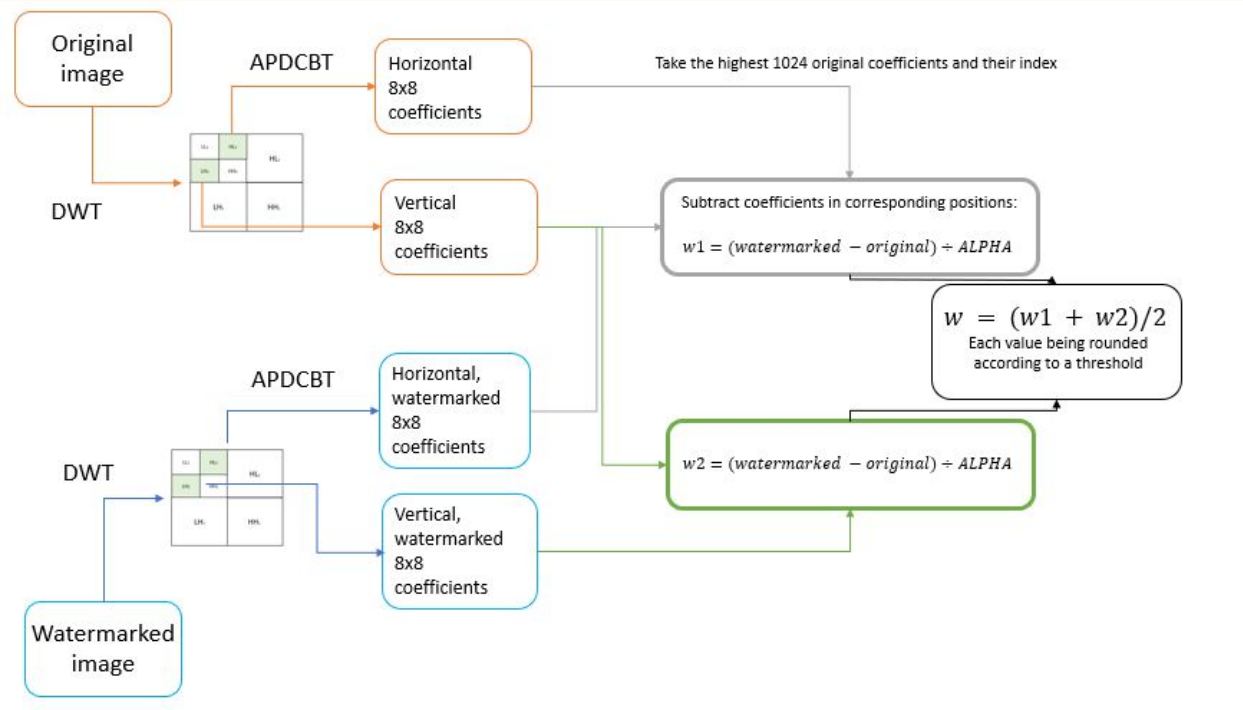


5 - Inverse DWT

Watermarked image

4.B - IAPDCBT on vertical sub-band

Detection



Extraction of original watermark w

Same procedure to extract attacked watermark w_a (change watermaked image with attacked one)

So when we have w and w_a we compare them based on a similarity measure

Embedding Results

- Average **embedding WPSNR**: 50.62 dB
- Average **robustness WPSNR**: 40.03 dB
  - Pretty good due to insertion in the **hybrid transform** domain and in the highest coefficients.
  - **Localisation** of the watermark in **textured areas**, **edges** and **surroundings.**

BUT

- Quite high visibility in the areas near the borders

Attacks: before the competition

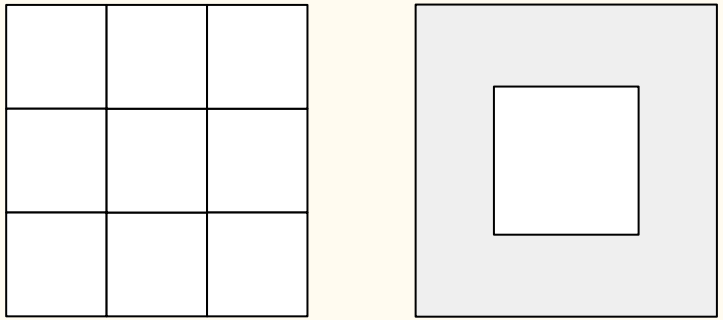
Attacks created

Standard

Combinations

AWGN + Median
AWGN + Median + jpeg
Median + jpeg
Resize + jpeg

Localized attacks
10 different zones



9 + 1

Attacks: before the competition

1. Python script for generating MATLAB attack scripts with different parameters
2. Automation script in MATLAB to automate the execution
3. R script to check the results table

Attacks: during the competition

1. Divide the groups to attack
2. Execute the automation script
3. Check the results of the attacks
4. Tune the most performing attacks to reach a higher WPSNR

Attacks Results

- **6 groups** attacked
- **16 images** attacked
- **Most effective:** AWGN & Median
  - 50% of successful attacks used awgn or median
- **Localization** played an important role in 6 attacks

Median filter on the upper half

References

MLA

Zhou, Xiao, Heng Zhang, and Chengyou Wang. "A robust image watermarking technique based on DWT, APDCBT, and SVD." Symmetry 10.3 (2018): 77.

Wang, C. Y., B. C. Jiang, and S. Z. Xie. "Properties of all phase biorthogonal transform matrix and its application in color image compression." *Journal of Computational Information Systems* 9.18 (2013): 7227-7234.