HOWIMETYOURMARK

Catch the Mark 2022

Roberta Bonaccorso
Matteo Darra
Leonardo Vicentini
Sofia Zanrosso

Embedding

DWT + SVD

Hybrid strategy based on various researches

Problems regarding existing papers

Direct usage of the watermark inside the embedding methods

New!

Novelty

Different **preprocessing method** - based on a "merit"

Preprocessing

Selection of n_blocks_to_embed based on a *"merit"*

Higher merit is given to:

- Blocks least attacked in an attack phase:
  - Blur, median, awgn, sharpening, resizing
- Blocks with higher values of a spatial function

The reference paper instead used edge detection* ⚠

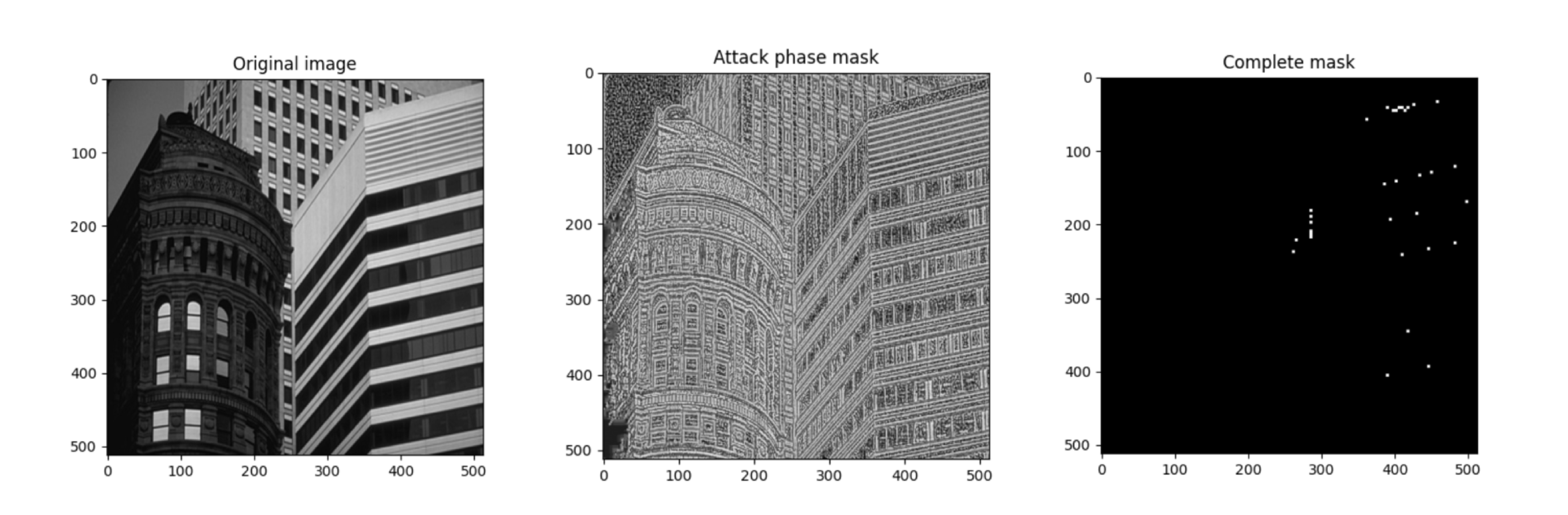
* "Towards Robust Reference Image Watermarking Using DWT-SVD and Edge Detection"
Satyanarayana Murty. P, Rajesh Kumar. P, 2013

HOWIMETYOURMARK

Novelty

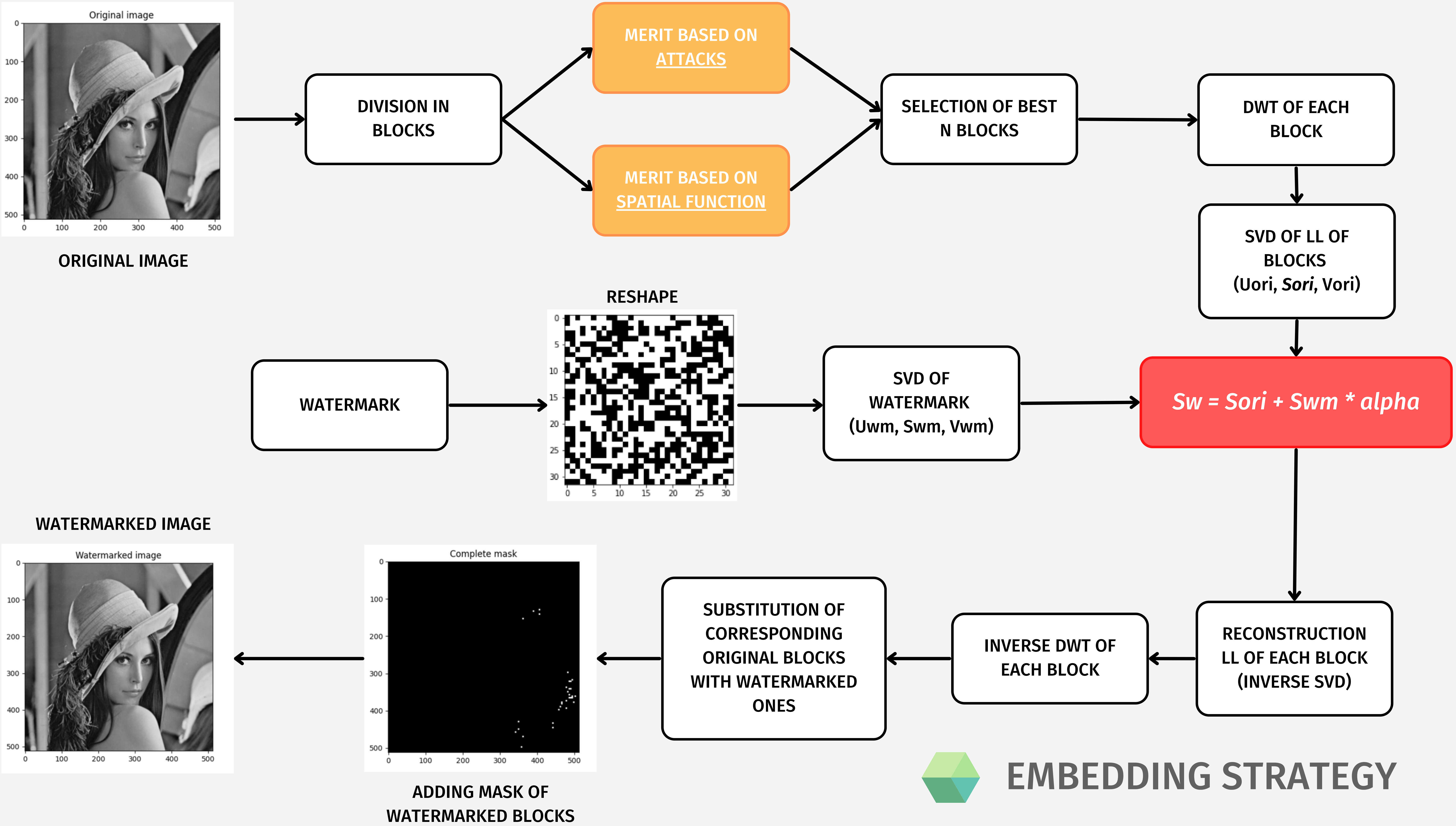
New!

Helpful during the detection phase



HOWIMETYOURMARK

EMBEDDING STRATEGY



ORIGINAL IMAGE

DIVISION IN BLOCKS

MERIT BASED ON ATTACKS

MERIT BASED ON SPATIAL FUNCTION

SELECTION OF BEST N BLOCKS

DWT OF EACH BLOCK

SVD OF LL OF BLOCKS (Uori, *Sori*, Vori)

WATERMARK

RESHAPE

SVD OF WATERMARK (Uwm, Swm, Vwm)

*Sw = Sori + Swm * alpha*

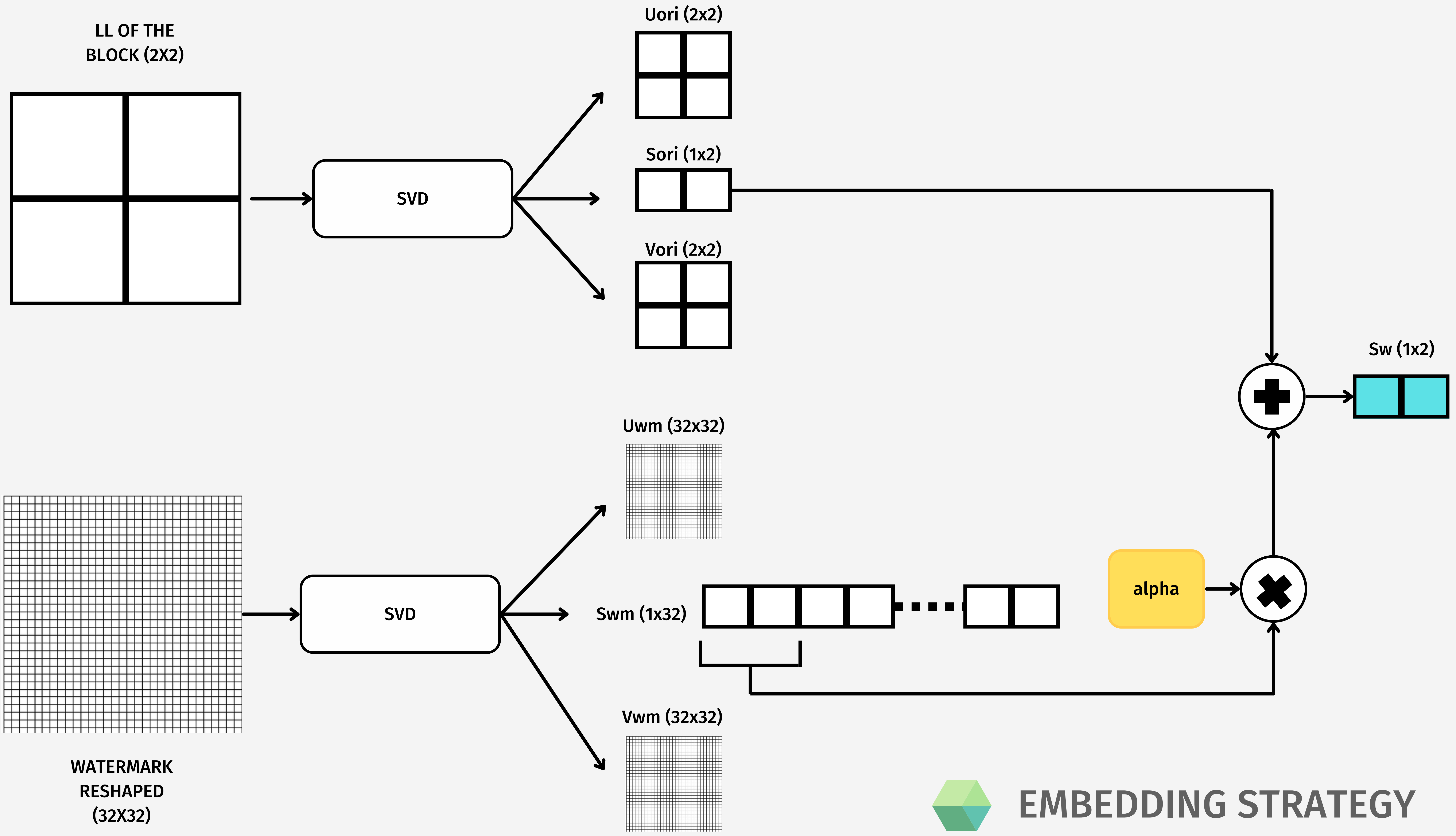
RECONSTRUCTION LL OF EACH BLOCK (INVERSE SVD)

INVERSE DWT OF EACH BLOCK

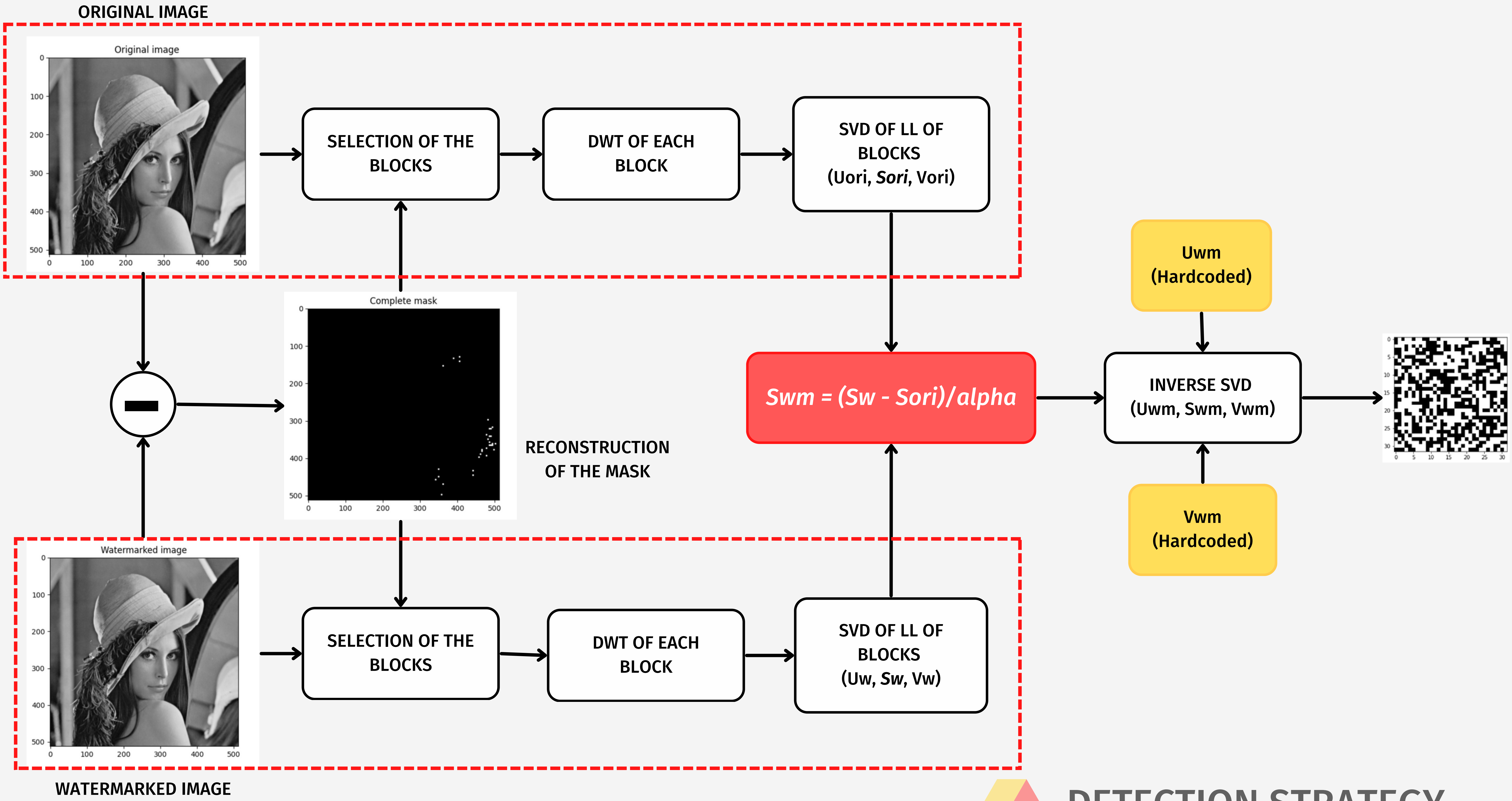
SUBSTITUTION OF CORRESPONDING ORIGINAL BLOCKS WITH WATERMARKED ONES

ADDING MASK OF WATERMARKED BLOCKS

WATERMARKED IMAGE



EMBEDDING STRATEGY



ORIGINAL IMAGE

SELECTION OF THE BLOCKS

DWT OF EACH BLOCK

SVD OF LL OF BLOCKS (Uori, ***Sori***, Vori)

RECONSTRUCTION OF THE MASK

Swm = (Sw - Sori)/alpha

Uwm (Hardcoded)

INVERSE SVD (Uwm, Swm, Vwm)

Vwm (Hardcoded)

SELECTION OF THE BLOCKS

DWT OF EACH BLOCK

SVD OF LL OF BLOCKS (Uw, ***Sw***, Vw)

WATERMARKED IMAGE

DETECTION STRATEGY

During the challenge

Precomputation of multiple thresholds (fpr 6.5%)

We have chosen the parameters that gave at least 66.00db and no more than 66.10db in all 3 images and succeeded in passing the detection test.

Parameters we focused on:

- Alpha
- n_blocks_to_embed (16, 32, 64)
- Weights given to calculate the merit:
  - Spatial function
  - Attack phase

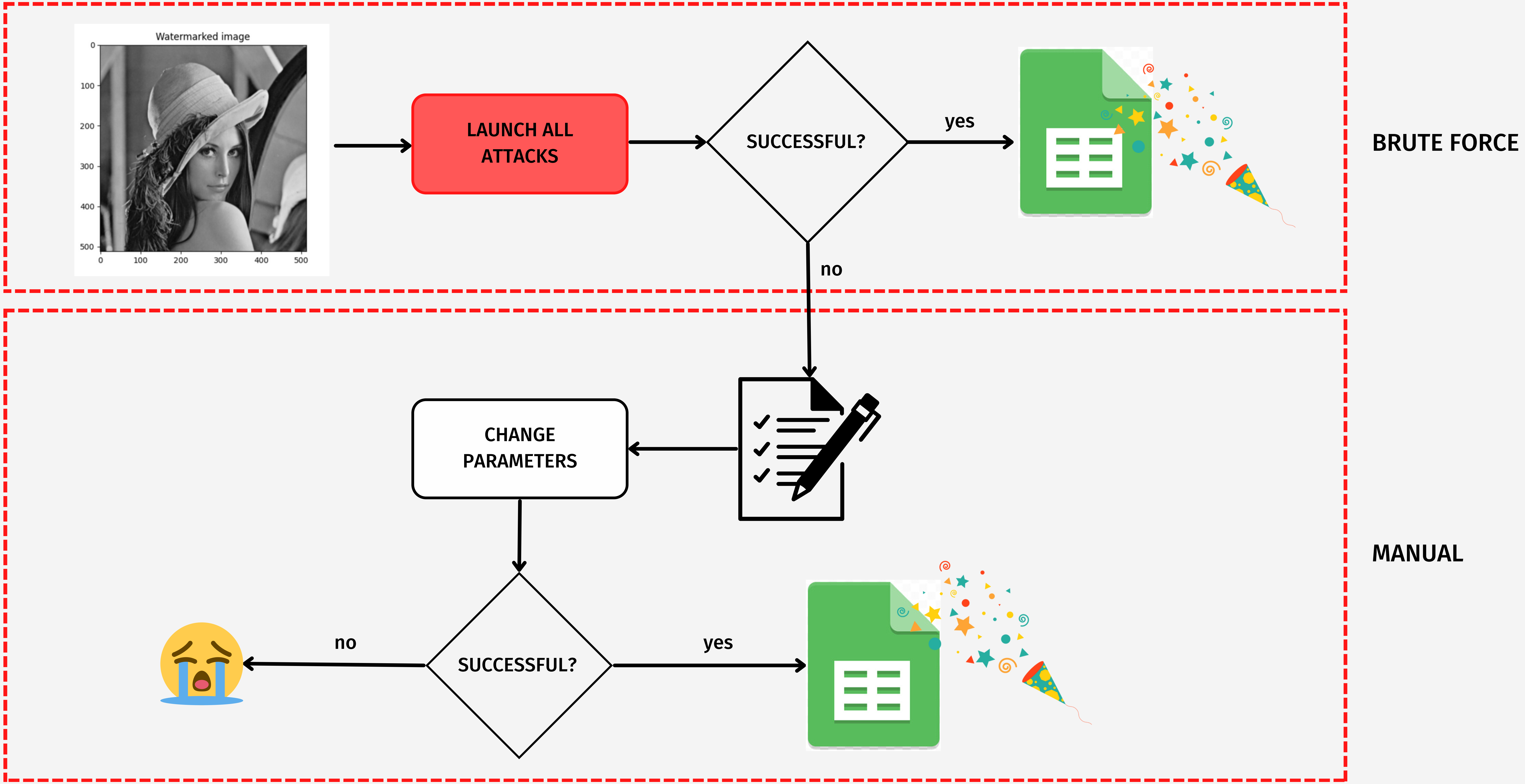
Attacks

Brute force attacks

WPSNR > 35 and mark removal

Manual attacks

Change pre-set parameters



LAUNCH ALL ATTACKS

SUCCESSFUL?

yes

no

BRUTE FORCE

CHANGE PARAMETERS

SUCCESSFUL?

no

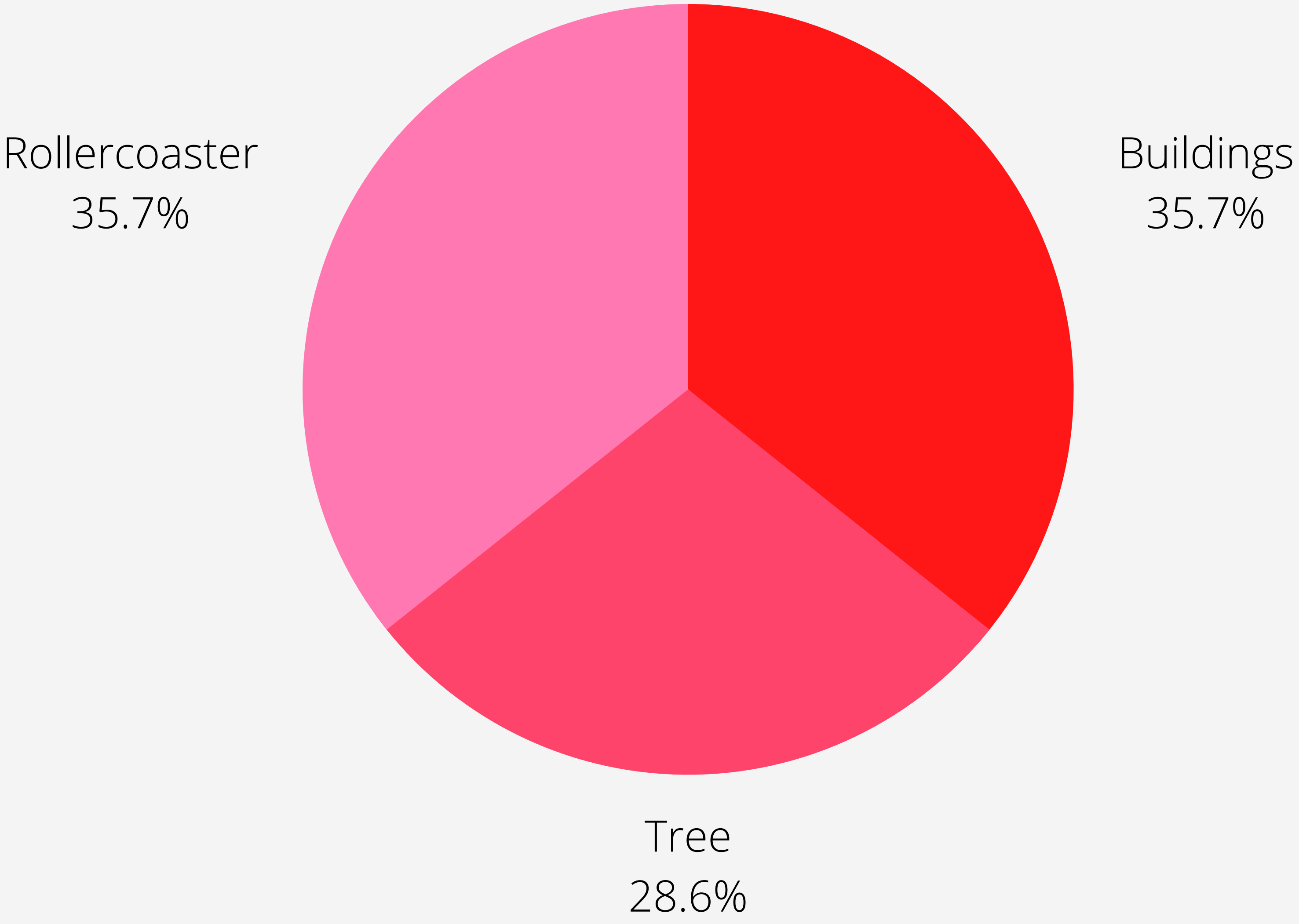
yes

MANUAL

HOWIMETYOURMARK

Attacks' results

Attacked images



Average time to attack a group: **15 min**

Parallelization with multiple users/pc

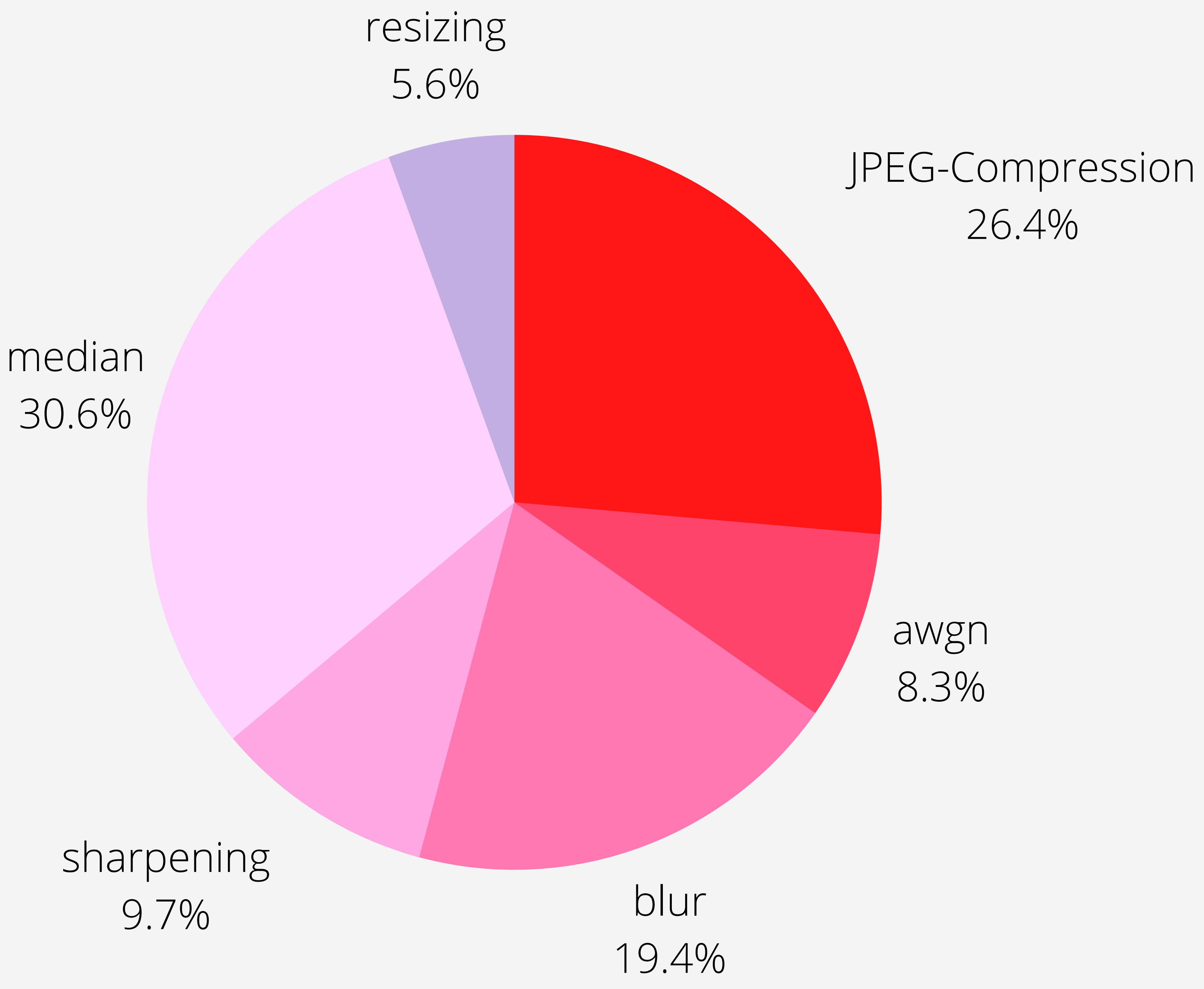
✓ Groups successfully attacked: **100%**

✓ Images successfully attacked: **93,3%**

HOWIMETYOURMARK

Attacks' results

Best attacks



Statistic	WPSNR
average	41,89
min	36,51
max	59,11

HOWIMETYOURMARK