UNIVERSITY OF TRENTO – Italy
Department of Information Engineering and Computer Science

MULTIMEDIA DATA SECURITY

IMAGE WATERMARKING

GROUP :
STAKKASTAKKA

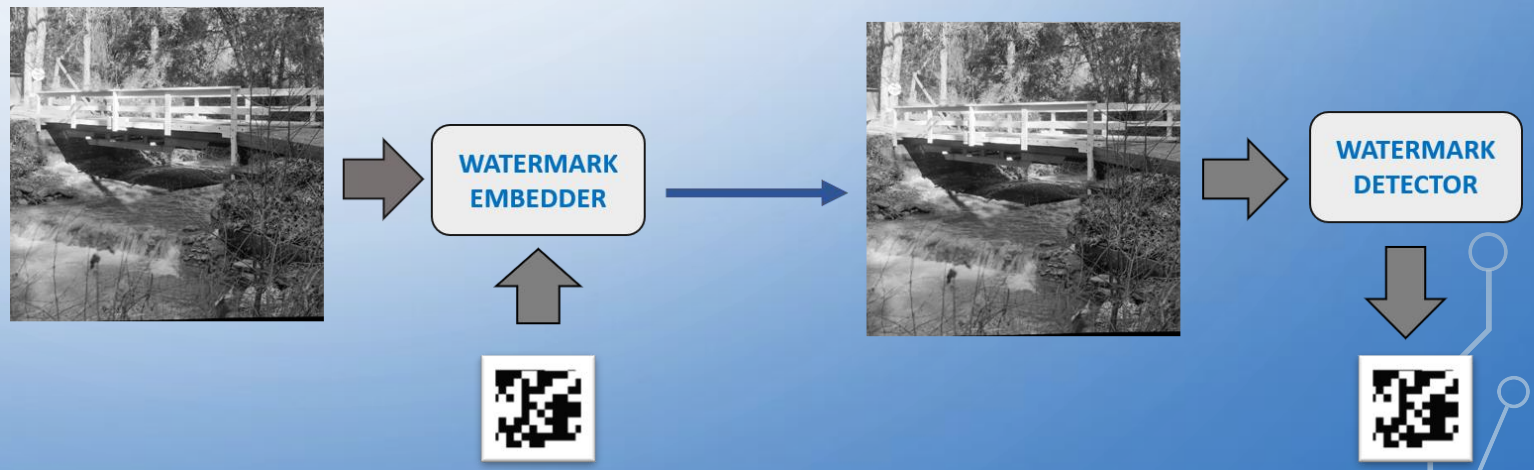
MULTIMEDIA DATA SECURITY COMPETITION

Objectives of the battle:

- Implement an embedding robust strategy maintaining original image quality
- Attack the watermarked image of the other groups without degrade too much the image quality

Explored solutions:

- Spread Spectrum
- Dwt - Dct - SVD
- Dwt - Dct
- Dwt - Dct - Arnold



EMBEDDING PHASE – ARNOLD TRANSFORM

1. Watermark Scrambling:

- Scrambling transform is applied on a watermark as a way of encryption, in order to obtain a more robust algorithm, it has been used Arnold Transform

Arnold Transform

- After scrambling transform, the spatial relationships of the pixels of a image has been destroyed completely, which makes it evenly distributed in all the space, so the robustness of the watermarking algorithm is improved in this way.

Original

Tranformed

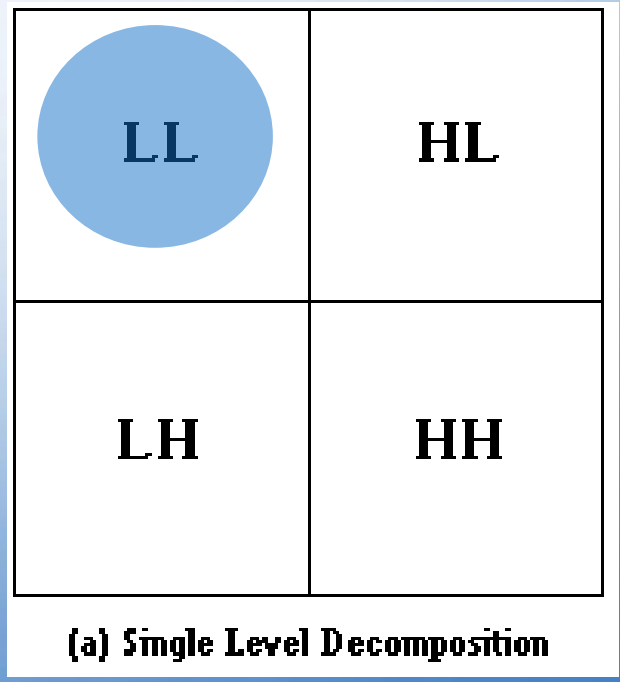
EMBEDDING PHASE - DWT

2. Computation of DWT, Discrete Wavelet Transform:

- DWT divides the image in four sub bands.
  The sub band highlighted in blue has been chosen to embed the water mark.

- Why chose this band?

  The lower frequency band contains the the biggest amount of energy, so embed in that bad results in a more roubust algorithm.



(a) Single Level Decomposition

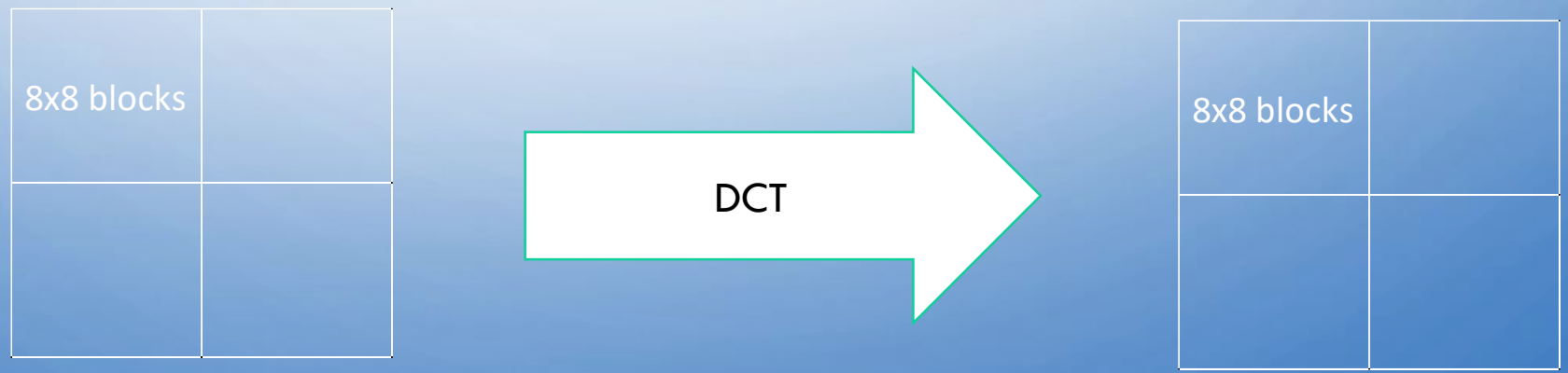
EMBEDDING PHASE – DCT

3. Computation of DCT coefficient:

- We have a watermark made of 1024 pixels so we found a way to encode this data in the most significant frequency of each transformed dwt sub block.

LL band is an image of 256x256 pixels, here is divided in 1024 blocks

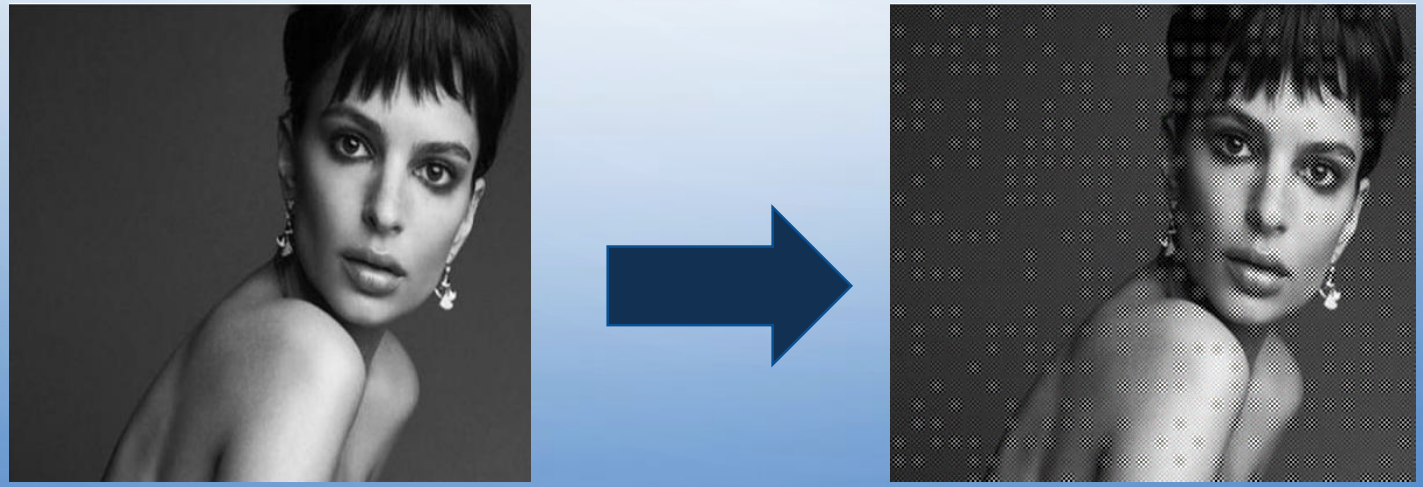
1024 blocks made of DCT coefficient



EMBEDDING PHASE – WATERMARK ISERTION

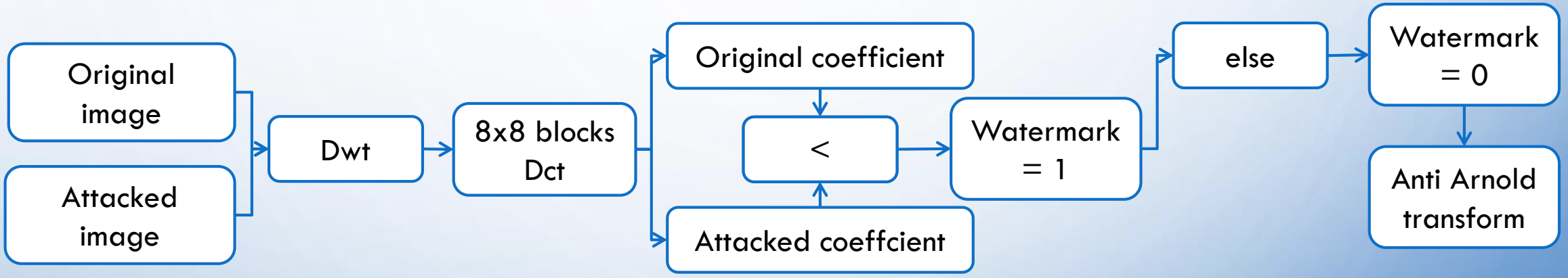
4. Watermark insertion:

- The watermark is composed by 0 and 1 so if it is zero decreases the coefficient in which is embedded otherwise if it is 1 increases the coefficient.
- In this way we can modify each cofficient of a significant quantity maintining a good wpsnr and a good robustnes.



DETECTION PHASE

- To detect the watermark the process seen before is applied to the original watermarked image and to the attacked image.



- During the detection is sufficient to check if a coefficient is larger or smaller then the orginal to retrieve the watermark.
- In case of attack even if the image is significantly modified the retrieve is possible because the detection is based on the direction of the variation of the coefficient modified by the embedding algorithm.

ATTACK PHASE

Implementation of the attack code:

- Choice of parameters for attack functions.
- The function are executed in loop
- Checking the condition
  - ***If (WPSNR < 35)*** → *Break*
  - ***If (ispresent == 0)*** → *save the image and pass to the following attack.*
- Save parameters on file:
  - *Image name.*
  - *Attack name.*
  - *List of parameters.*
  - *WPSNR value.*