


Geometric attack resistant watermarking in wavelet transform domain

Geometric attacks

-  Flipping
- Scaling
- Rotation
- Shearing
- Cropping
- Translation along (x, y)
- Row / Column removal
- Aspect ratio manipulation

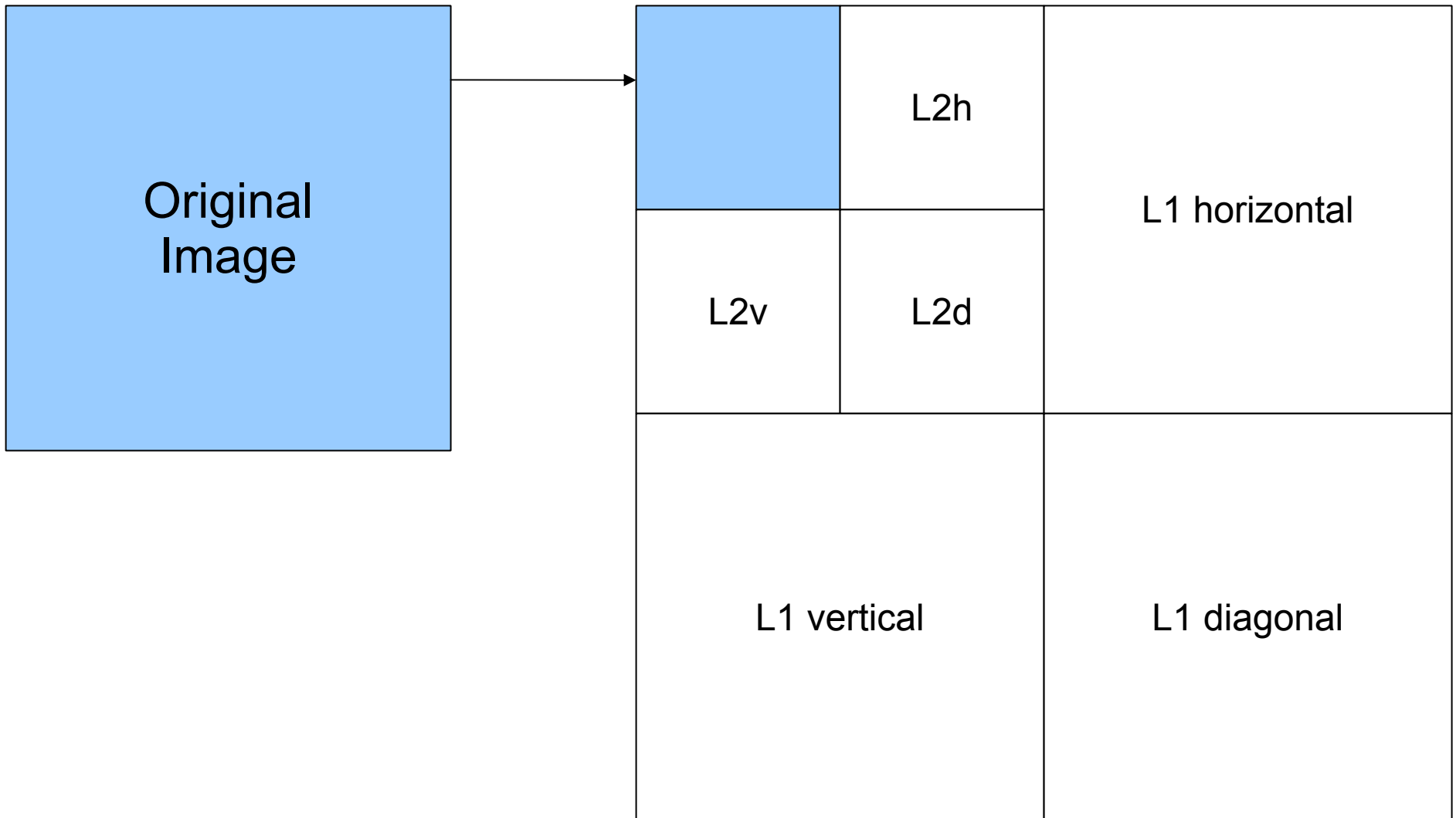
Preparing the cover image

- The cover image is first modified to have a high periodic correlation with itself
- This gives the resulting image stronger AC peaks, which are critical to accurate removal of the geometric attack
- The image is preprocessed using the Wiener highpass filter, and the 'noise' is isolated by

$$\text{Noise} = \text{Im} - \text{FilteredIm}$$

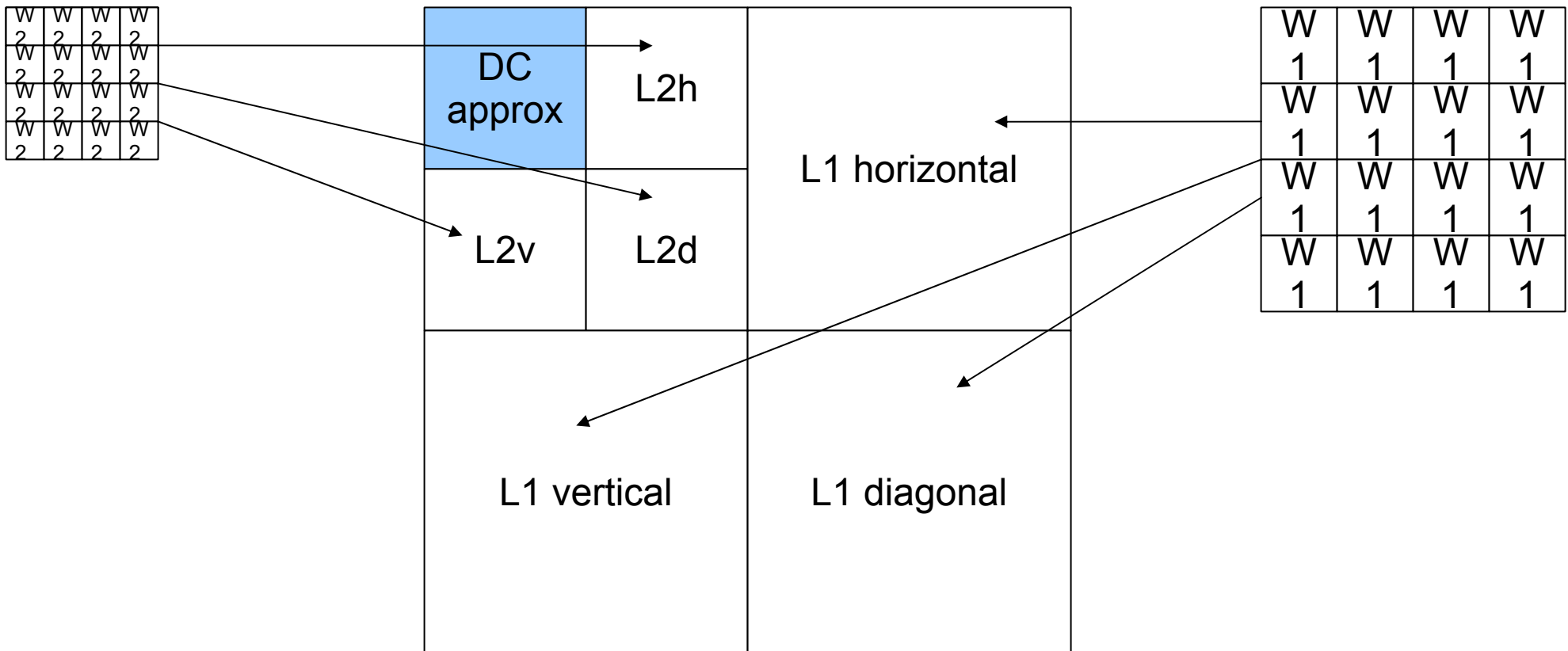
Embedding the watermark

Perform level-2 DWT on target image.



Embedding the watermark

Generate two periodic watermarks



Embedding the watermark

The periodic watermarks will be embedded into each sub-band with varying strength based on a weighting formula:

$$\text{MarkedSub-band}(x, y) = \text{Sub-band}(x, y) + \alpha * (\lambda(x, y) * \text{Watermark}(x, y))$$

Here, α represents a user-defined weight factor,

λ represents a dynamically calculated weight factor.

Embedding the watermark



- The local weighting factor λ is determined based on the relative noise of the surrounding pixels.*
- The watermark can be embedded more heavily in areas with high noise.*
- A 'noise visibility' function is used to set the value of λ , resulting in higher values for high-noise areas (textured regions) and lower values for low-noise areas (smooth regions).*


Extracting the watermark



Two step process:


- Any geometric attacks must be estimated, and reversed if possible.
- The restored image is analyzed for the presence of a watermark

Geometric attack estimation

 Before the periodicity of the watermark can be extracted from the spatial domain, the Wiener high-pass filter must be applied to the watermarked image. This step is identical to the autocorrelation pre-processing step.

$$\text{Noise} = \text{Im} - \text{FilteredIm}$$

Geometric attack estimation

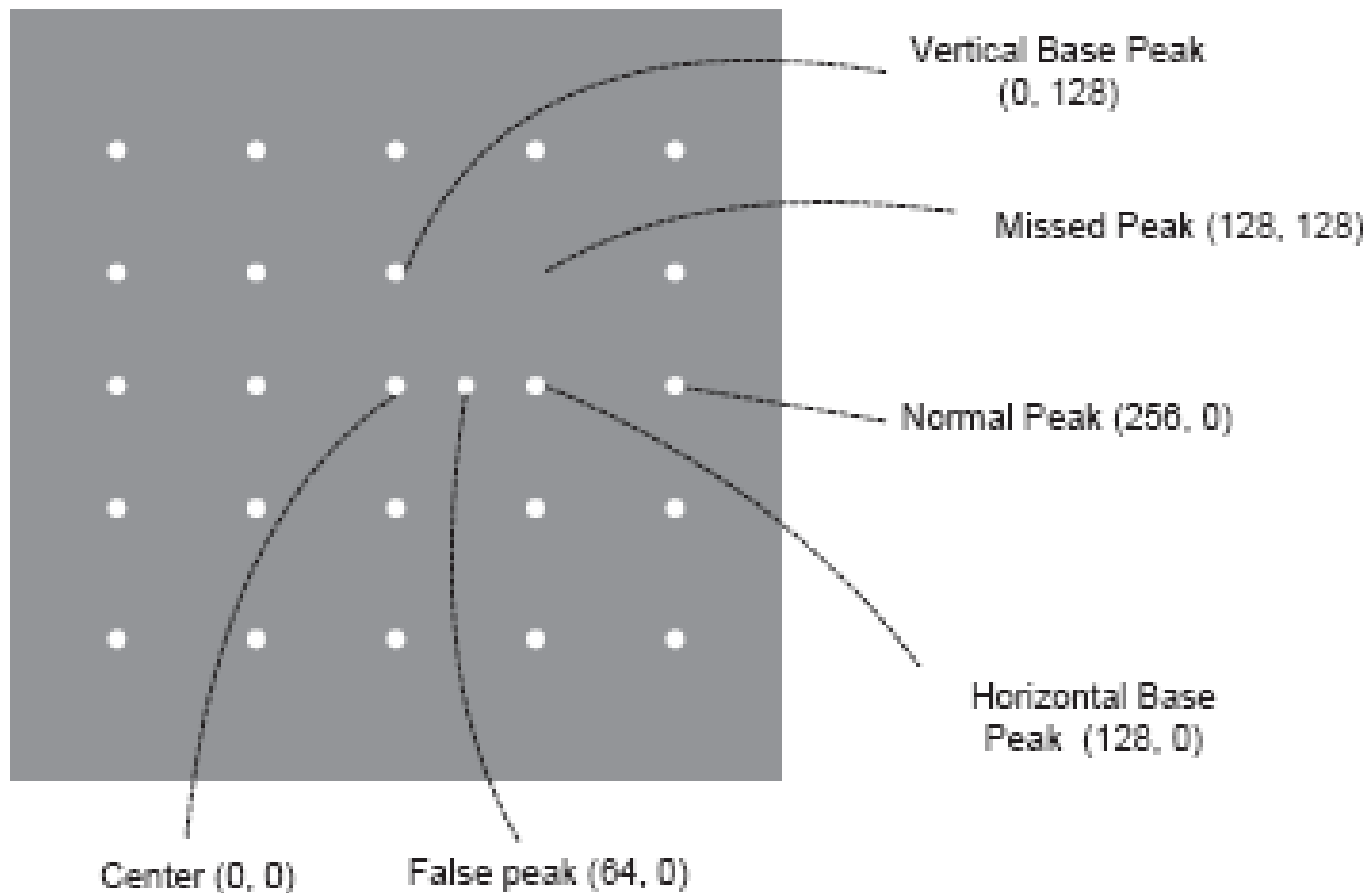
 The ACF function is then calculated for the extracted signal. This results in a matrix ACF with dimension equal to the watermarked image.

- Peaks are found in matrix ACF by finding values $ACF(x, y)$ such that:

$$ACF(x, y) > \text{Mean}(ACF) + \text{StdDev}(ACF)$$

Geometric attack estimation

 The ACF peaks can be visualized as follows:



Geometric attack estimation

 **Base peaks** are found from previous image.

- Base peaks are the two peaks closest to the center of the image.
- The algorithm for finding the correct peaks was modified. First, the peaks are given a weight based on their distance. Correct base peaks will share a common distance from the center. Using this knowledge, a weight is assigned by

if(peak1.distance == peak2.distance)

PeakWeight(peak1, peak2) += peak1.distance / m

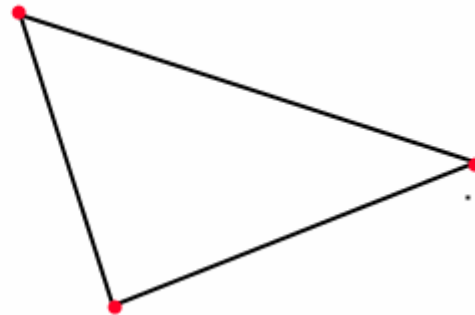
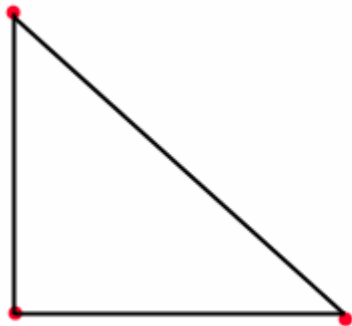
Geometric attack estimation



- The peaks are then given additional weight based on how many correct peaks can be found using their x , y positions.
- After the base peaks are chosen, the geometric attack on the image can be approximated and reversed, which will restore the original image.
- After the geometric attack has been reversed, the watermark can be detected.

Geometric attack estimation

- Using the information from the base peak pair, a triangle is formed.
- The affine transformation A is found that converts triangle C to C' . This transformation is applied to the image.



Extracting the watermark

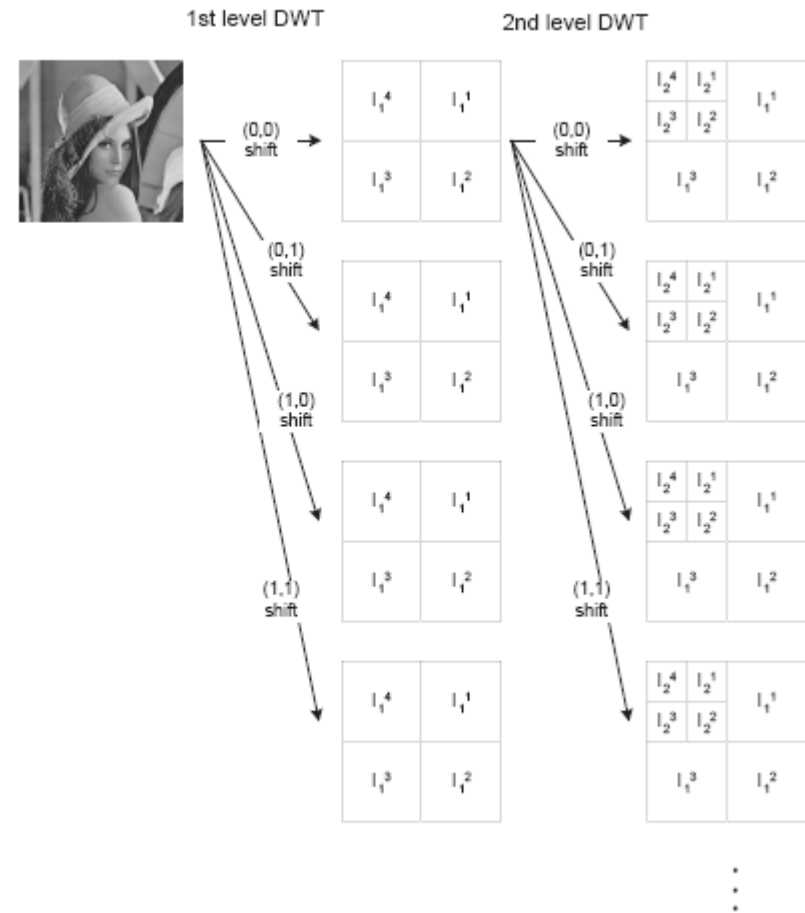


- The image is segmented into blocks of size $M \times M$, and the average of these blocks is found.
- Four sets of DWT sub-bands are generated for Level 1, three have 1 pixel shifts applied to them
- The image is shifted by $(0, 1)$, by $(1, 0)$, and $(1, 1)$ respectively
- The same is done for Level 2, on the shifted DC approximation of Level 1.


Extracting the watermark



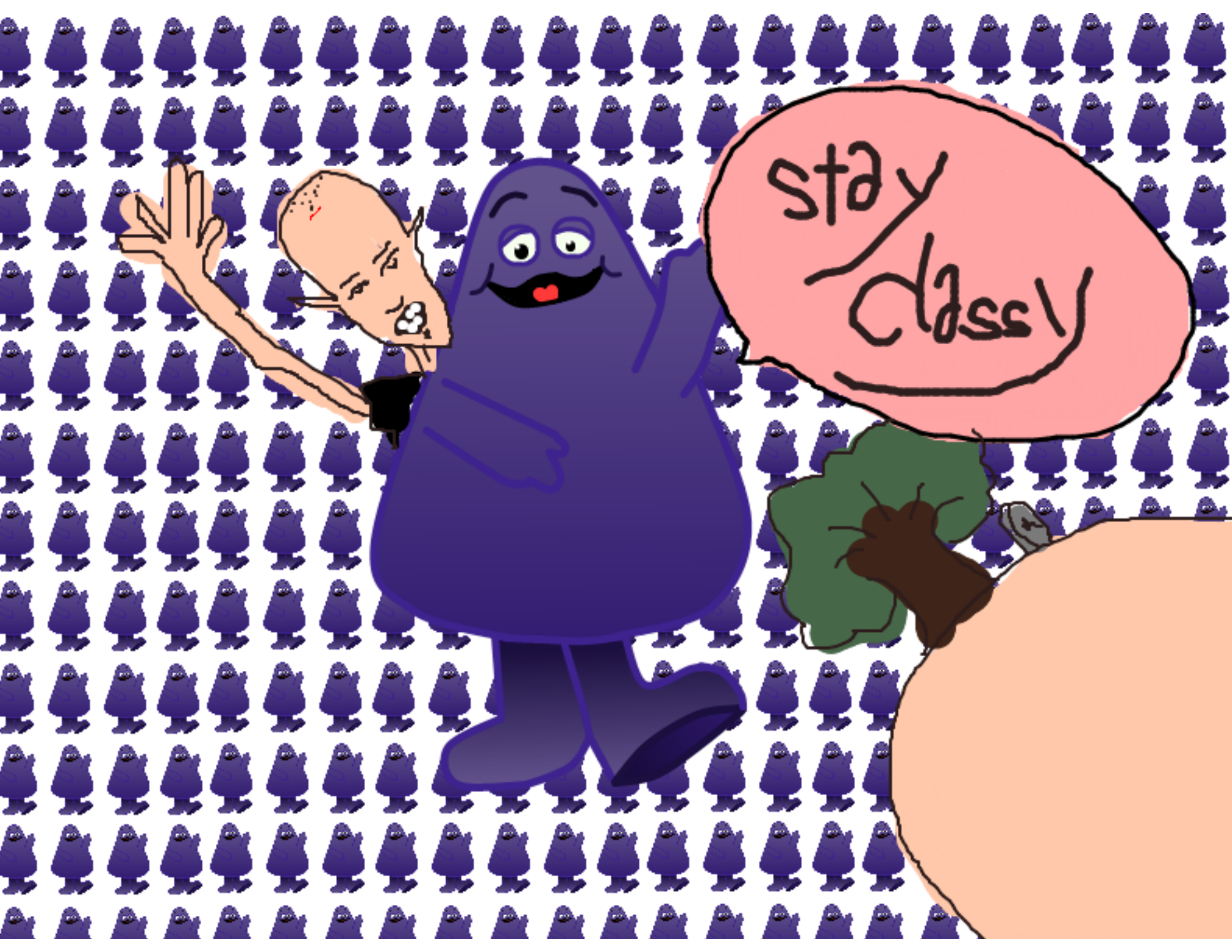
- Four Level-2 sub-bands are generated for each Level-1 DC approximation, resulting in a total of 20 generated sub-bands (4 Level-1, 16 Level-2)
- By shifting each sub-band by every possible offset, every possible shift in the spatial domain can be expressed.



Extracting the watermark

-  The ACF is taken of each shift for each sub-band, and the maximum values for each decomposition level are chosen (Max1 and Max2)
- A threshold is calculated for each decomposition level. If $\text{Max1} > \text{Thresh1}$ or $\text{Max2} > \text{Thresh2}$, the image is marked.

$$\text{Thresh}_n > \text{Mean}(\text{MaxBlock}_n) + \text{StdDev}(\text{MaxBlock}_n)$$



stay
class!