Task 6

Watermark Embedding

Christian Riess (christian.riess@fau.de)

1 Summary

The main purpose of a digital watermark is to prove ownership of an image (or, more general, any type of media). The idea is to embed a binary random sequence (the "watermark") into the image. If ownership of the image has to be proven, it can be shown that the watermark is contained in the image. A watermarking algorithm always has to make a tradeoff between robustness (against, e.g., recompression), perceptual invisibility (the image should look like the non-watermarked version), and watermark capacity (the sequence length of the watermark).

On a technical level, watermarking algorithms typically

- transform the image into another domain (e.g., Fourier, Discrete Cosine, or Wavelet domain),
- perform an additive or multiplicative embedding of the watermark, and
- transform the image back.

Watermark detection is performed similarly. The image is transformed into the same domain as for the embedding, and then the watermark is correlated with the coefficients in that other domain.

In this exercise, we follow the paper by Barni, Bartolini, Piva: "Improved Wavelet-Based Watermark Through Pixel-Wise Masking", IEEE Transactions on Image Processing, vol. 10, no. 5, May 2001, pp. 783–791. You can access the paper from within our university network, the link is `http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=918570`.

2 Baseline Watermarking

Note that there is no template for this work sheet. However, we do not require a lot of tools for a baseline algorithm:

1. Create the watermark sequence x: a binary random sequence, with values ± 1. We will embed the watermark into the horizontal, vertical and diagonal detail coefficients of first decomposition level. Thus, the length of the watermark shall be 3/4 of the image.
2. Perform a one-level wavelet decomposition using the Daubechies-6 filters (`db6` in matlab).

3. Embed the watermark into the detail coefficients of the `lena` image by computing

$$\hat{I}_0^\theta(i,j) = I_0^\theta + \alpha x^\theta(i,j) \ , \tag{1}$$

where $\theta \in H, V, D$, i.e., I_0^θ denotes the detail coefficients at the first decomposition level, and x^θ denotes the respective substring of x. Furthermore, α is a user-selected parameter for the embedding strength. Larger α will make the watermark more robust, but will also lead to larger visual distortions.

4. Transform the image back, and display original and watermarked image side-by-side. Is the watermark indeed "invisible", or are the distortions from the watermark embedding visually disturbing?

5. Implement a check whether the watermark is present: perform again a 1-level wavelet decomposition of the original and the watermarked image, and correlate the detail coefficients with the watermark by computing

$$\rho = \frac{1}{3MN} \sum_{\theta=0}^{2} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} I_0^\theta(i,j) x^\theta(i,j) \ , \tag{2}$$

where M and N denote the x- and y-dimensions of the detail subband θ. If your method works, the correlation is considerable for the watermarked image.

6. Create another watermark y and check the correlation — the expected result is that the correlation is really low.

7. Perform JPEG-compression with quality factors 100, 90, 80, 50 on the watermarked image — is the correlation still high enough to confirm the presence of the watermark?

3 Watermarking with Perceptual Masking

Presumably, you noticed that the watermark can be made arbitrarily robust when increasing α — but this also introduces visibile artifacts into the image. We will now extend the baseline method a so-called "perceptual mask", which is a multiplier to the embedding strength for each of the detail coefficients used for the embedding. The idea is that we embed the watermark more strongly at locations where it can be less perceived by the eye.

1. Modify the code above to perform a 4-level Daubechy-6 wavelet decomposition.

2. In the paper by Barni, Bartolini, and Piva, Equation (2) states that the embedding function shall be

$$\hat{I}_0^\theta(i,j) = I_0^\theta + \alpha w^\theta(i,j) x^\theta(i,j) \ , \tag{3}$$

i.e., the difference to our baseline formulation is that we now have the perceptual mask w included. Equations (3) to (9) describe how w is computed. I think it is instructive to actually look at the equations: particularly (3) to (8) describe a general quantization scheme, but Eqn. (9) says that most of this is not required for our work. This is a common communication pattern in scientific literature.

Equation (9) states that

$$w^{\theta}(i,j) = q_0^{\theta}(i,j)/2 \ , \tag{4}$$

and $q_0^{\theta}(i,j)$ expands to

$$q_0^{\theta}(i,j) = \Theta(0,\theta)\Lambda(0,i,j)\Xi(0,i,j)^0.2 \ . \tag{5}$$

Here, Θ is set to $\sqrt{2}$ for the vertical detail coefficients, and to 1 otherwise. Λ is slightly more complicated (see Eqn. (5)-(7)):

$$\Lambda(0,i,j) = 1 + L'(0,i,j) \tag{6}$$

with

$$L'(0,i,j) = \begin{cases} 1 - L(0,i,j) & \text{if} L(0,i,j) < 0.5 \\ L(0,i,j) & \text{otherwise} \end{cases} \ , \tag{7}$$

and

$$L(0,i,j) = \frac{1}{256} I_3^L(1 + \lfloor i/8 \rfloor, 1 + \lfloor j/8 \rfloor) \ . \tag{8}$$

Thus, L is the overall brightness, as observed in the low-frequency component of the fourth decomposition level.

Finally, $\Xi(0,i,j)$ is a measure for texture, and is computed as

$$\Xi(0,i,j) = \sum_{k=0}^{3} \frac{1}{16^k} \sum_{\theta=0}^{2} \sum_{x=0}^{1} \sum_{y=0}^{1} (I_k^{\theta}\left(y + i/2^k, x + i/2^k\right))^2 \cdot \mathrm{Var}(I_3^3(1 + i/2^3, 1 + j/2^3)) \ , \tag{9}$$

where "Var" denotes the variance of the wavelet coefficients on the highest decomposition level in a 2×2 neighborhood (this is what is meant by the subscripts $x = 0, 1$, $y = 0, 1$ in Eqn. (8) of the paper).

3. Test your watermarking method again (maybe you need to modify α for beautiful results). Did it improve?

A final remark: one important aspect of watermarking research is the computation of guarantees for the watermark detection. We do not cover this in our implementation. Nevertheless, if you are curious, the detection threshold for watermark presence is given in Eqn. (15) and Eqn. (18) of the paper.