Spread Spectrum Watermarking

Spread Spectrum Watermarking

- One of the first valid digital watermarking approaches proposed in the literature
- Design for digital images (but can be extended to audio, video and other multimedia data)
- An independent and identically distributed (i.i.d.) Gaussian random vector (the watermark) is imperceptibly inserted in a spread-spectrum-like fashion into the perceptually most significant spectral components of the data

Cox, Kilian, Leighton, Shamoon, "Secure Spread Spectrum Watermarking for Multimedia", IEEE Transactions on Image Processing, vol.6, no.12, Dec 1997

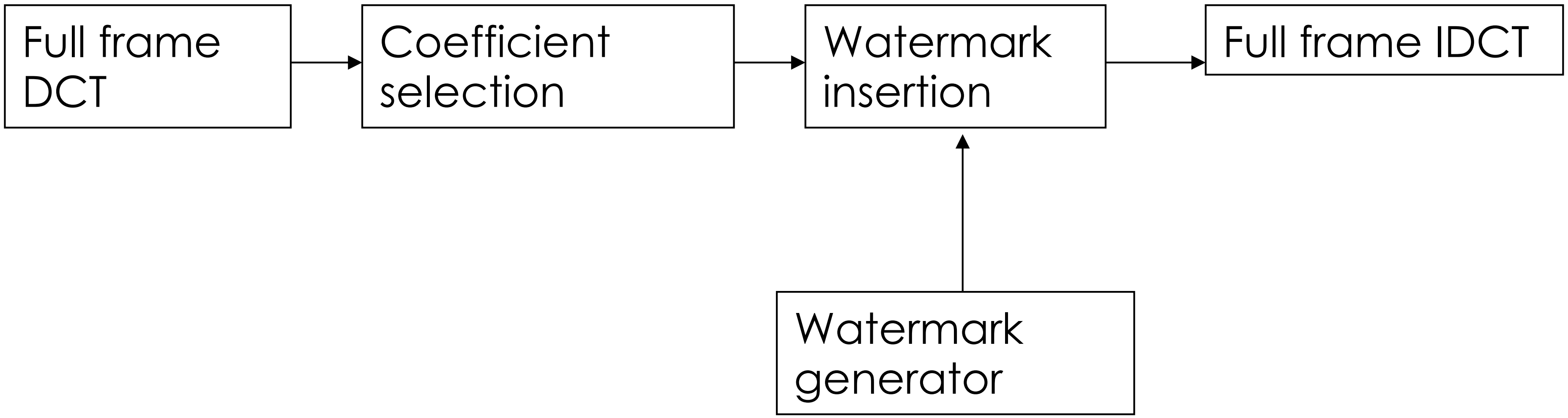
Spread Spectrum Watermarking

- A digital watermark is intended to complement cryptographic processes. It is a preferably invisible identification code that is permanently embedded in the data and remains present within the data after any decryption process.
- The watermark should be perceptually invisible, or its presence should not interfere with the media being protected.
- The watermark must be difficult (hopefully impossible) to remove. Attempts to remove it should result in severe degradation in fidelity before the watermark is lost.

Spread Spectrum Watermarking

- The watermark should be robust against:
  - Common signal processing: resampling, re-quantization, re-compression, signal enhancement, etc.
  - Common geometric distortions: rotation, translation, cropping, scaling, etc.
  - Combination of the above distortions
  - Collusion of multiple individuals who each possess a watermarked copy of the data

Watermark embedding



- Significant components have perceptual capacity that allows watermark insertion without perceptual degradation.
- Most processing techniques applied to media data tend to leave the perceptually significant components intact.

Watermark embedding

- Spread Spectrum Communication: transmits a narrowband signal over a much larger bandwidth such that the signal energy present in any single frequency is undetectable.
- The watermark is spread over many frequency bins so that the energy in each bin is very small and certainly undetectable.
- Because the watermark verification process knows the location and content of the watermark, it is possible to concentrate these many weak signals into a single output with high SNR (signal-to-noise-ratio).
- To destroy such a watermark would require noise of high amplitude to be added to all frequency bins.

Watermark embedding

- Each coefficient in the frequency domain has a perceptual capacity: a quantity of additional information can be added without any (or with minimal) impact to the perceptual fidelity of the data.

- To determine the perceptual capacity of each frequency one can use models for the appropriate perceptual system or simple experimentation.

Watermark embedding

- Compute the N x N DCT of an N x N gray scale cover image I
- The watermark must be composed of random numbers drawn from a Gaussian distribution (N(0,1), where N(μ,σ²) denotes a normal distribution with mean μ, and variance σ²)
  - Embed a sequence of real values $X = x_1, x_2, \ldots, x_n$, according to N(0,1), into the n largest magnitude DCT coefficients, excluding the DC component

$$\text{Additive-SS}: v_i' = v_i + \alpha x_i$$

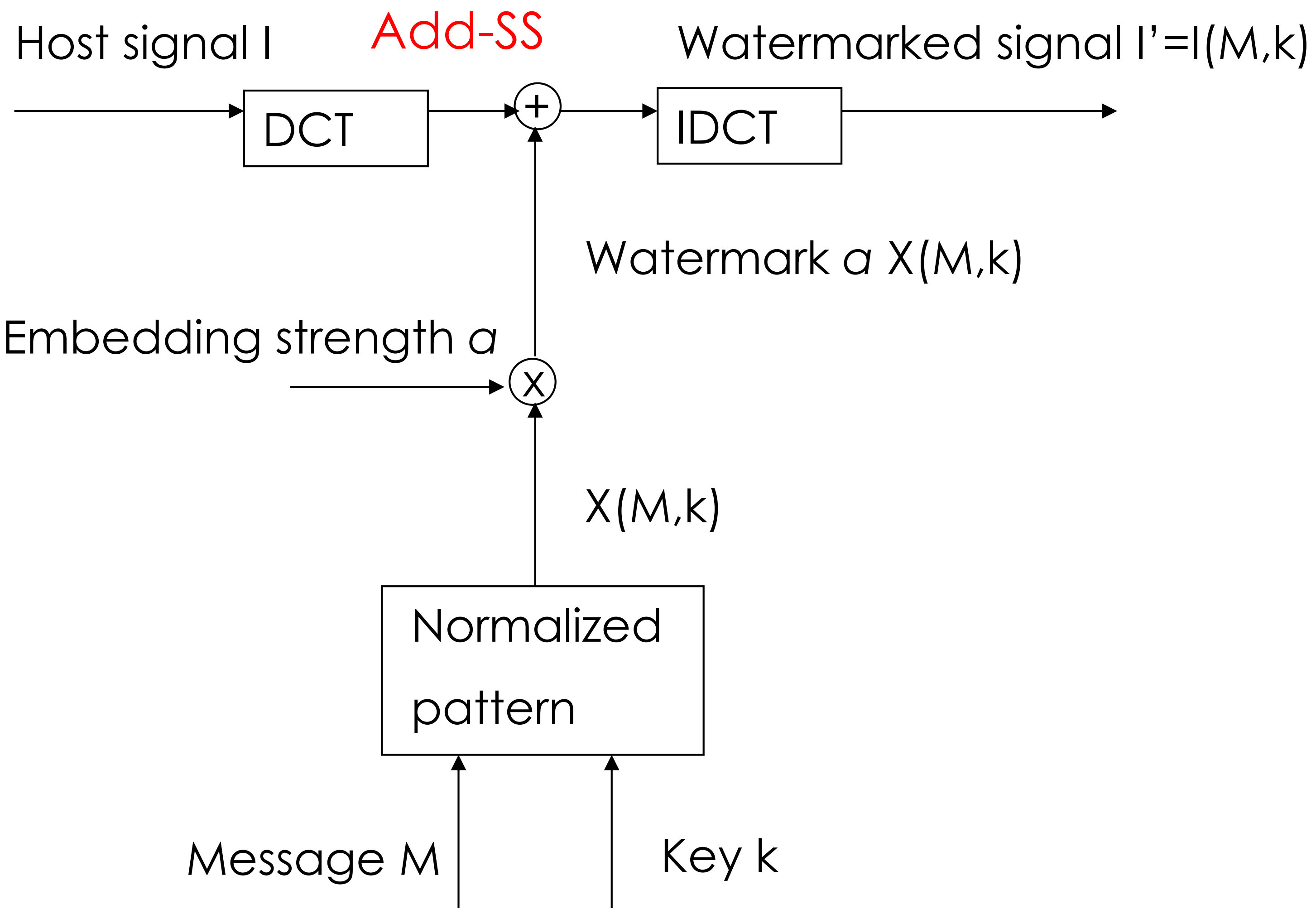
$$\text{Multiplicative-SS}: v_i' = v_i(1+\alpha x_i) \quad i = 1, \ldots, n$$

- Compute the inverse DCT to obtain the watermarked cover image I'

Watermark embedding

- The Discrete Cosine Transform (DCT)
  - The DCT represents an image as a sum of sinusoids of varying magnitudes and frequencies
  - The DCT has the property that, for a typical image, most of the visually significant information about the image is concentrated in just a few coefficients of the DCT
  - The DCT is at the heart of the international standard lossy image compression algorithm known as JPEG
- Place the watermark in perceptually significant spectrum (for robustness)

Watermark embedding



Watermark embedding

- Use long random noise-like vector as watermark (for robustness and security and imperceptibility)
- Attacker does not know secret pattern X
- Typically X=pseudo-random noise (PRN) sequence
- k=seed to PRN generator
- A watermark length of 1000 was used
- The watermark was added to the image by modifying 1000 of the more perceptually significant DCT coefficients of the image
- The DC term was excluded in the embedding process
- The value of the scaling factor *a* was 0.1

Watermark detection

- Compute the DCT of the watermarked (and possibly attacked) cover image I*
- Extract the watermark X*

$$\text{Additive-SS}: x_i^* = (v_i^* - v_i)/\alpha$$

$$\text{Multiplicative-SS}: x_i^* = (v_i^* - v_i)/\alpha v_i, i = 1,\ldots,n$$

- Evaluate the similarity of X* and X using

$$\mathrm{sim}(X, X^*) = \frac{X \cdot X^*}{\sqrt{X^* \cdot X^*}}$$

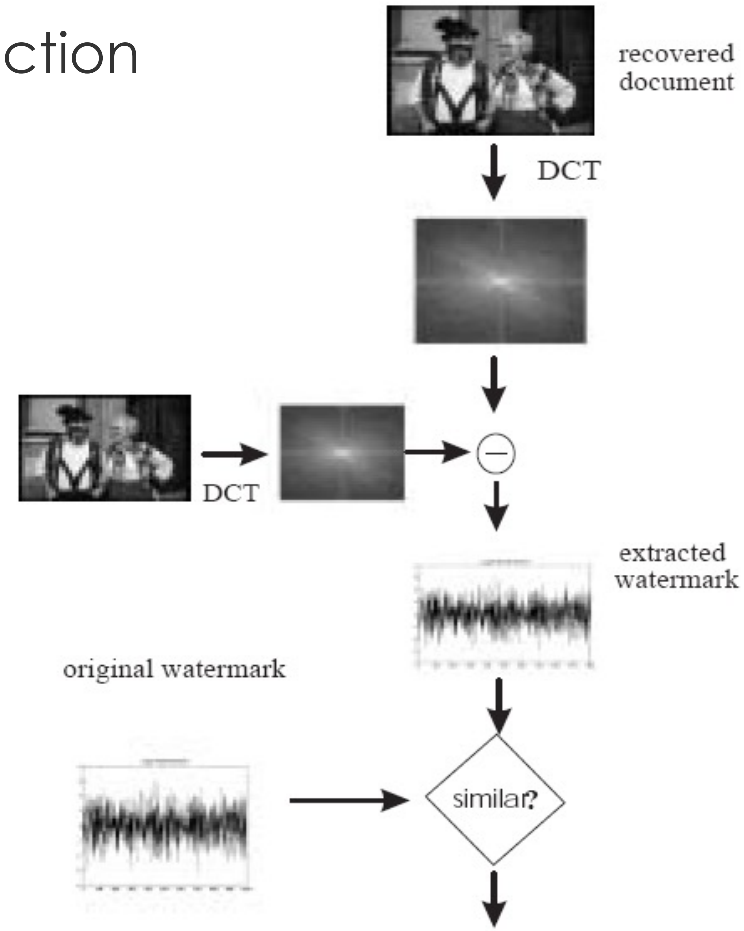
If sim (X,X*) > T, a given threshold, the watermark exists

Watermark detection

- Setting the detection threshold is a classical decision estimation problem in which we wish to minimize both the rate of false negatives (missed detections) and false positives (false alarms).
- Other possible measures are standard correlation coefficient or normalized correlation.

Watermark detection

- Non-blind detection



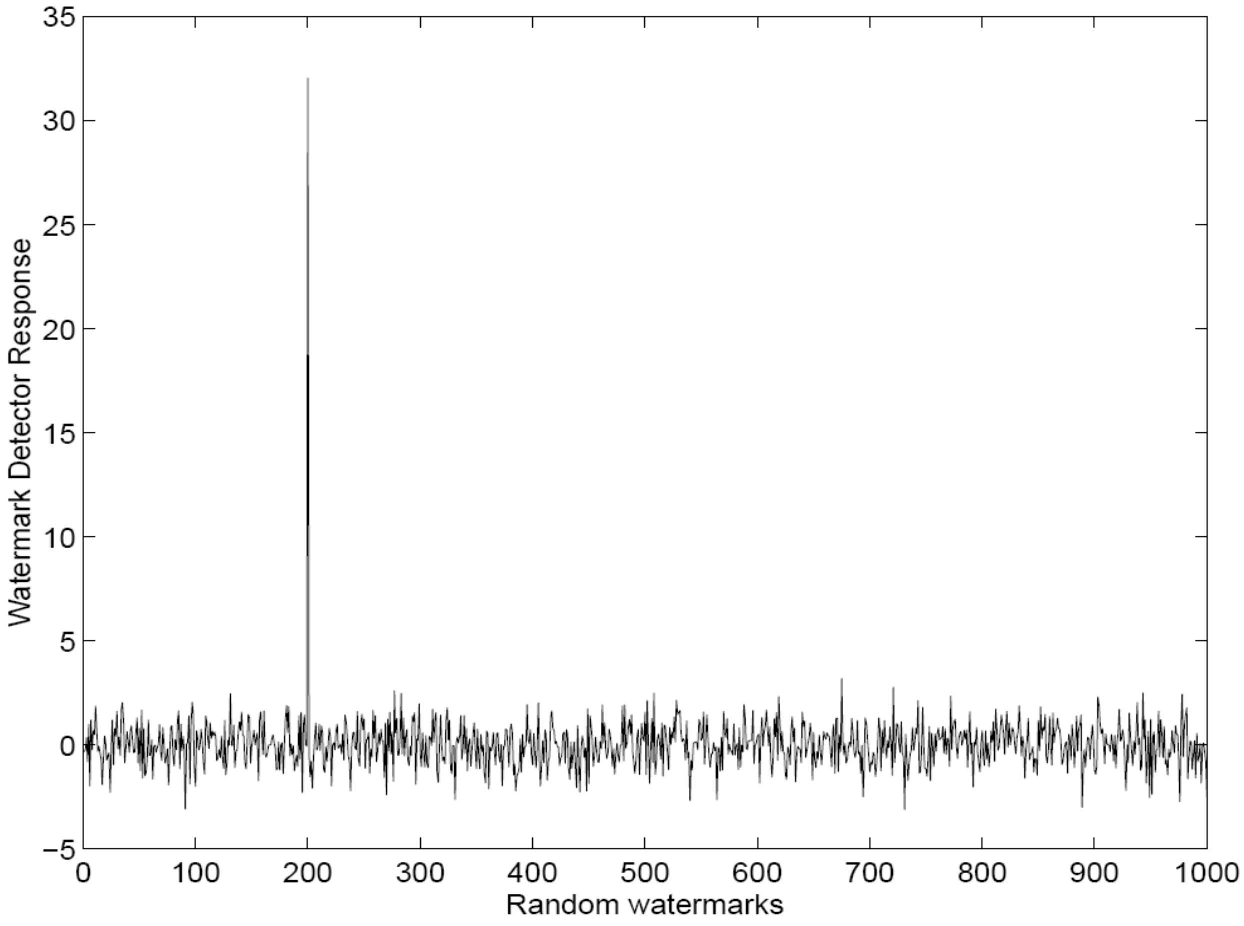
Watermark detection

Figure 4: "Bavarian Couple" courtesy of Corel Stock Photo Library.

Figure 5: Watermarked version of "Bavarian Couple".

Watermark detection

- Watermark detector response to 1000 randomly generated watermarks. Only one watermark (the one to which the detector was set to respond) matches that present in Figure (5)



Watermark detection

- The watermark is robust to signal processing operations (such as lossy compression, filtering, digital-analog and analog-digital conversion, re-quantization, etc.), and common geometric transformations (such as cropping, scaling, translation, and rotation) provided that the original image is available.

Watermark detection

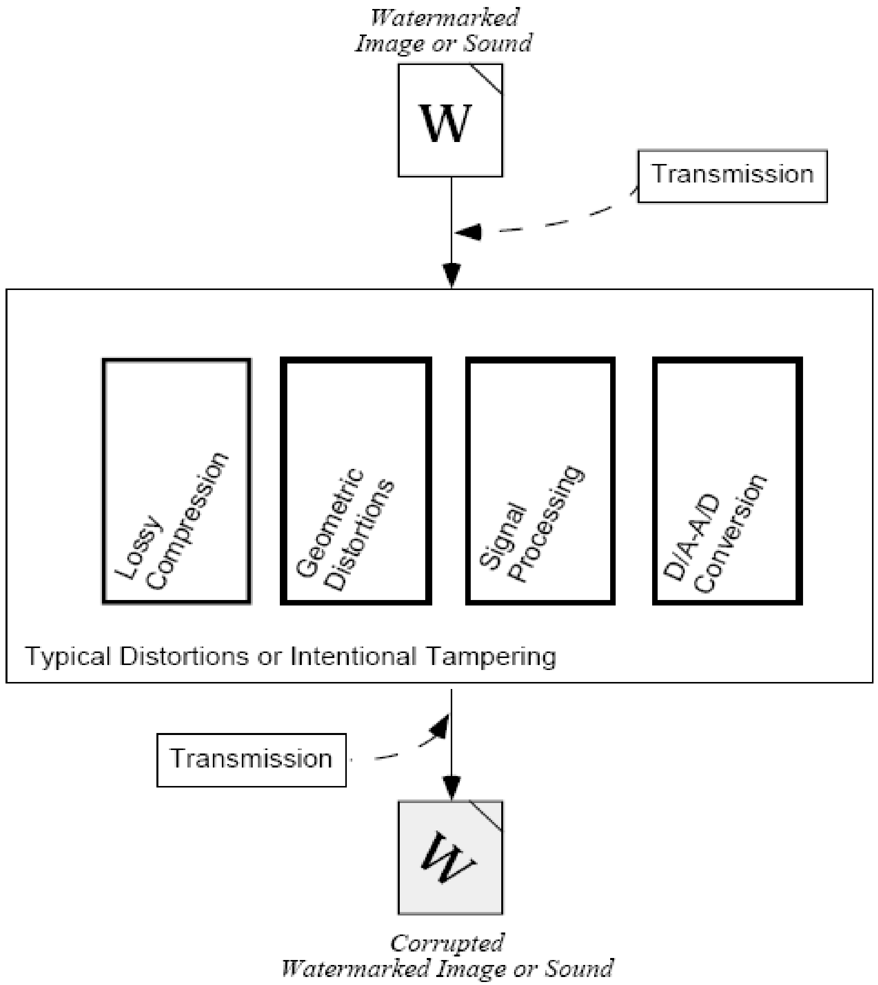


Image scaling

- The response of the watermark detector for the real watermark is 13.4. The response is higher than those of the fake watermarks!

Figure 7: (a) Low pass filtered, 0.5 scaled image of "Bavarian Couple", (b) re-scaled image showing noticable loss of fine detail.

JPEG compression

- The response of the watermark detector for the real watermark is 22.8 (Fig. 8) - 13.9 (Fig. 9). The responses are higher than those of the fake watermarks!

Figure 8: JPEG encoded version of “Bavarian Couple” with 10% quality and 0% smoothing.

Figure 9: JPEG encoded version of “Bavarian Couple” with 5% quality and 0% smoothing.

Dithering

- The response of the watermark detector for the real watermark is 5.2. The response is higher than those of the fake watermarks!

Figure 10: Dithered version of "Bavarian Couple".

Cropping

- The response of the watermark detector for the real watermark is 14.6.The response is higher than those of the fake watermarks!

Figure 11: (a) Clipped version of watermarked "Bavarian Couple", (b) Restored version of "Bavarian Couple" in which missing portions have been replaced with imagery from the original unwatermarked image of Figure (4).

JPEG and cropping

- The response of the watermark detector for the real watermark is 10.6.The response is higher than those of the fake watermarks!

Figure 12: (a) Clipped version of JPEG encoded (10% quality, 0% smoothing) "Bavarian Couple", (b) Restored version of "Bavarian Couple" in which missing portions have been replaced with imagery from the original unwatermarked image of Figure (4).

Print, xerox, and scan

- The response of the watermark detector for the real watermark is 4.0. The response is higher than those of the fake watermarks!

Re-watermarking

Figure 14: Image of "Bavarian Couple" after five successive watermarks have been added.

Re-watermarking

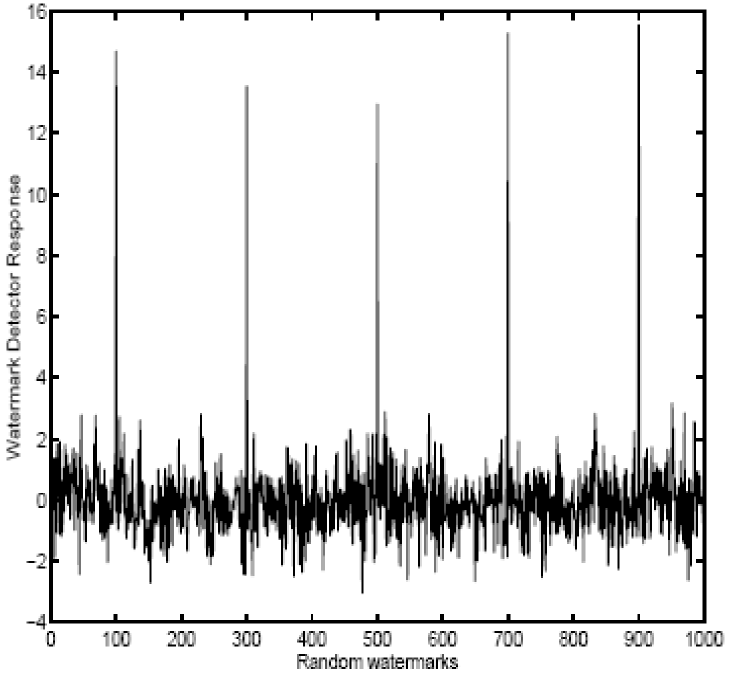


Figure 15: Watermark detector response to 1000 randomly generated watermarks (including the 5 specific watermarks) for the watermarked image of Figure (14). Each of the five watermarks is clearly indicated.

Collusion

- The watermark should be robust to collusion by multiple individuals who each possess a watermarked copy of the data. The watermark should be robust to combining copies of the same data set to destroy the marks.
- It must be impossible for colluders to combine their images to generate a different valid watermarked image with the intention of framing a third party.

Collusion

Figure 16: Image of "Bavarian Couple" after averaging together five independently watermarks versions of the "Bavarian Couple" image.

Collusion

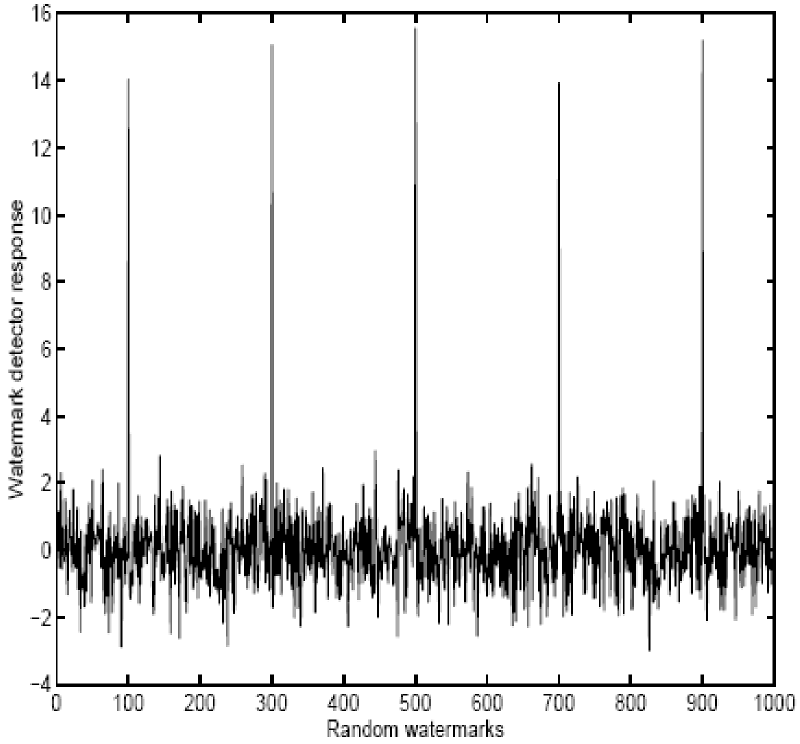


Figure 17: Watermark detector response to 1000 randomly generated watermarks (including the 5 specific watermarks) for the watermarked image of Figure (16). Each of the five watermarks is clearly detected, indicating that collusion by averaging is ineffective.