A DCT-domain system for robust image watermarking

M Barni, F Bartolini, V Cappellini, A Piva

Signal processing, 1998 - Elsevier

MyungJoon Kwon (kwon19@kaist.ac.kr)
May 7th, 2019

Contents

Intro

- A digital watermark is a code carrying information about the copyright of multimedia data.
- A watermark should be
  - Unobtrusive : statistically and perceptually invisible -> data quality is not degraded and the mark can’t be detected
  - Readily extractable
  - Robust : resistant to signal processing techniques
  - Unambiguous : its retrieval should unambiguously identify the data owner
  - Innumerable : possible to generate a great number of watermarks, distinguishable from each other

Intro

- To completely define a image watermarking technique operating in a transformed domain, we need to specify:
  1. Image transformation
     - DCT/DFT/other transforms
     - Applying transform to the image as a whole / to some blocks
  2. Watermark casting
     - Tradeoff between perceptual invisibility and robustness
  3. Watermark recovery
     - Comparing with the original image or other methods

Intro

I

Original image

DCT

DCTed

Insert Watermark

DCTed and Watermarked

IDCT

Watermarked

I'

Release on the Internet

I^*

Watermarked and corrupted

DCT

watermarked, corrupted, and DCTed

Recover Watermark

Related work – Cox's

- I.J. Cox, J. Kilian, T. Leighton, T. Shamoon, Secure spread spectrum watermarking for images, audio and video, Proc. IEEE Internat. Conf. on Image Processing (ICIPÕ96), Vol. III, Lausanne, Switzerland, 16-19 September 1996, pp. 243-246.

Related work – Cox's

1. Image transformation
   - DCT
   - Applying transform to the image as a whole
2. Watermark casting
   - Watermark $X = \{x_1, x_2, \cdots, x_M\}$ where $x_i \sim N(0,1)$ (independently).
   - After DCTing the whole image, select the M largest DCT coefficients(excluding the DC term), say $T = \{t_1, t_2, \cdots, t_M\}$.
   - Insert watermark by modifying T as $t_i' = t_i + \alpha t_i x_i$.
   - EX: $M = 1000, \alpha = 0.1$
3. Watermark recovery
   - Comparing with the original image
   - Reverse the casting process to obtain X^*. We can do this since we know t_i. i.e., $x_i^* = \frac{t_i^* - t_i}{\alpha t_i}$
   - Measure the similarity of Y and X^* by $sim(Y, X^*) = \frac{Y \cdot X^*}{\sqrt{X^* \cdot X^*}}$.
     - If $sim(Y, X^*) > threshold$ then we can say X = Y, i.e., the watermark is detected.

Related work – Cox's

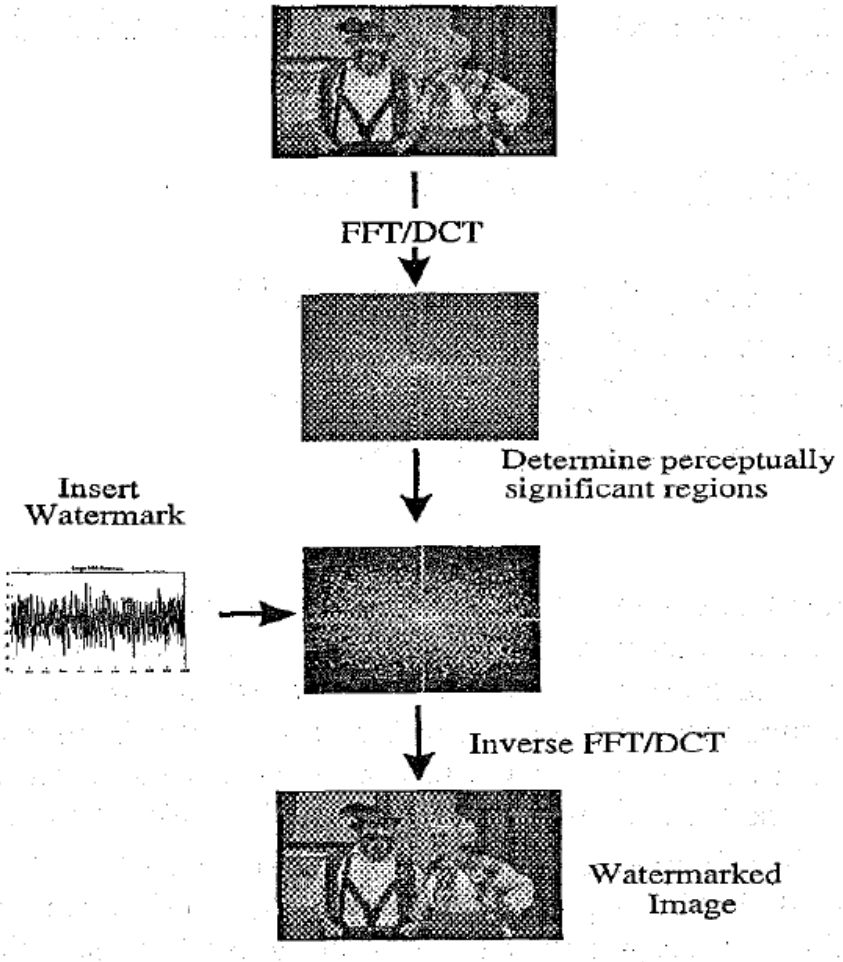


Figure 1: Stages of watermark insertion procedure.

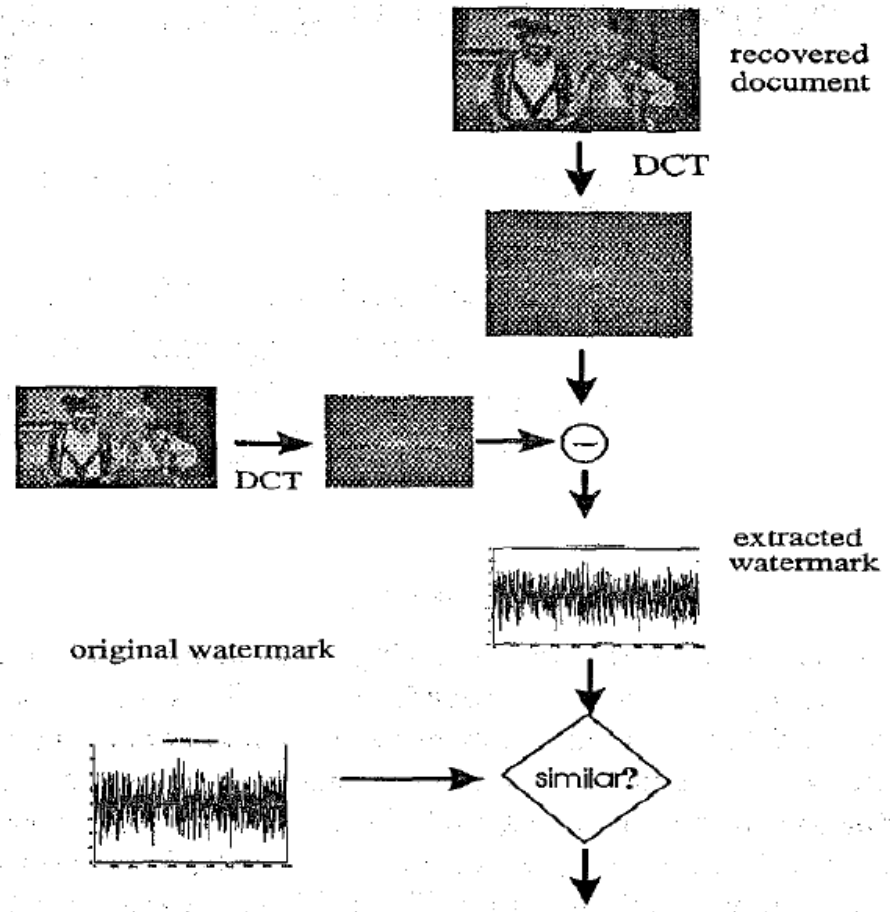


Figure 2: Stages of watermark extraction procedure.

Method

1. Image transformation
   - DCT
   - Applying transform to the image as a whole
2. Watermark casting
   - Watermark $X = \{x_1, x_2, \cdots, x_M\}$ where $x_i \sim N(0,1)$ (independently).
   - After DCTing the whole image, order the coefficients in zig-zag scan. Then select the coefficients from the $(L+1)$th to the $(L+M)$th, say $T = \{t_1, t_2, \cdots, t_M\}$.
   - Insert watermark by modifying T as $t_i' = t_i + \alpha|t_i|x_i$.
   - EX: $L = M = 16000, \alpha = 0.1$
3. Watermark recovery
   - DCT the possibly corrupted image to obtain T^*.
     - We can't obtain X^* since we are not using the original image. i.e., we don't know t_i.
   - Measure the correlation z of T^* and Y by $z = \frac{1}{M} Y \cdot T^* = \frac{1}{M} \Sigma_{i=1}^{M} y_i t_i^*$ where Y is the arbitrary mark.
     - z is higher if $\mathrm{X} = \mathrm{Y}$ compared to $\mathrm{X} \neq \mathrm{Y}$ (proof: see the theoretical analysis).
     - If $z > T_z$ then we can say $\mathrm{X} = \mathrm{Y}$, i.e., the watermark is detected.

$$x_i^* = \frac{t_i^* - t_i}{\alpha|t_i|}$$

Theoretical Analysis

- So far, we have
  - $x_i, y_i \sim N(0,1)$, $E(t_i) = 0$ (all independent)
  - $t_i' = t_i + \alpha|t_i| x_i = t_i^*$ (Assume the image is not corrupted)
  - $z = \frac{1}{M} Y \cdot T^* = \frac{1}{M} \Sigma_{i=1}^{M} y_i t_i^* = \frac{1}{M} \Sigma_{i=1}^{M} (y_i t_i + y_i \alpha |t_i| x_i)$
- Claim: $\mu_z = \begin{cases} \alpha \mu_{|t|} & \text{if } X = Y \\ 0 & \text{if } X \neq Y \\ 0 & \text{if no mark is present} \end{cases}$
- Claim: $\sigma_z^2 = \begin{cases} \frac{1+2\alpha^2}{M} \sigma_t^2 + \frac{\alpha^2}{M} \sigma_{|t|}^2 & \text{if } X = Y \\ \frac{1+\alpha^2}{M} \sigma_t^2 & \text{if } X \neq Y \\ \frac{1}{M} \sigma_t^2 & \text{if no mark is present} \end{cases}$

Theoretical Analysis

- $z = \frac{1}{M}\Sigma_{i=1}^{M}(y_i t_i + y_i \alpha |t_i| x_i)$

Case 1 $X = Y$

Then $x_i = y_i$ for all i.

Thus $z = \frac{1}{M}\sum_i (x_i t_i + \alpha |t_i| x_i^2)$

$$\mu_z = E(z) = E\left[\frac{1}{M}\sum_i (x_i t_i + \alpha |t_i| x_i^2)\right]$$

linearity

$$= \frac{1}{M}\sum_i \left[E(x_i t_i) + \alpha E(|t_i| x_i^2)\right]$$

$E(x_i)E(t_i)$ ($\because x_i \perp\!\!\!\perp t_i$)

$E(|t_i|)E(x_i^2)$ ($\because |t_i| \perp\!\!\!\perp x_i^2$)

$$= \frac{1}{M}\sum_i \left[E(x)E(t) + \alpha E(|t|)E(x^2)\right]$$

$\sum_i$: M; $E(x)$: 0; $E(x^2)$: 1 ($\because Var(x) = E(x^2) - E(x)^2$; $Var(x)$: 1; $E(x)^2$: 0)

$$= \alpha E(|t|) = \alpha \mu_{|t|}$$

Theoretical Analysis

- $z = \frac{1}{M}\Sigma_{i=1}^{M}(y_i t_i + y_i \alpha |t_i| x_i)$

$$\sigma_z^2 = \frac{1}{M^2}\,\mathrm{Var}\left[\sum_i (x_i t_i + \alpha |t_i| x_i^2)\right] \quad \text{independence (covariance = 0)}$$

$$= \frac{1}{M^2}\sum_i \left[\mathrm{Var}(x_i t_i) + \alpha^2 \mathrm{Var}(|t_i| x_i^2)\right] \qquad \sum_i \to M$$

$$= \frac{1}{M}\left[\underbrace{E(x_i^2 t_i^2)}_{E(x_i^2)E(t_i^2)} - \underbrace{E(x_i t_i)^2}_{[E(x_i)E(t_i)]^2} + \underbrace{\alpha^2 (t_i^2 x_i^4)}_{\alpha^2 E(t_i^2)E(x_i^4)} - \underbrace{\alpha^2 E(|t_i| x_i^2)^2}_{-\alpha^2 E(|t_i|)^2 E(x_i^2)^2}\right]$$

$E(x_i^2) \to 1$, $E(t_i^2) \to \sigma_t^2$, $E(x_i) \to 0$, $E(x_i^4) \to 3$ (using the moment generating function)

$\sigma_t^2 - \sigma_{|t|}^2$ $\because$ $\mathrm{Var}(|t_i|) = E(|t_i|^2) - E(|t_i|)^2$, with $\mathrm{Var}(|t_i|) \to \sigma_{|t|}^2$ and $E(|t_i|^2) \to E(t_i^2) = \sigma_t^2$

$\because$ $\mathrm{Var}(t_i) = E(t_i^2) - E(t_i)^2$, with $\mathrm{Var}(t_i) = \sigma_t^2$ and $E(t_i) \to 0$

$$= \frac{1}{M}\left[\sigma_t^2 + 3\alpha^2\sigma_t^2 - \alpha^2\sigma_t^2 + \alpha^2\sigma_{|t|}^2\right]$$

$$= \frac{1}{M}\left[\sigma_t^2(1 + 2\alpha^2) + \alpha^2\sigma_{|t|}^2\right]$$

Theoretical Analysis

- $z = \frac{1}{M}\Sigma_{i=1}^{M}(y_i t_i + y_i \alpha |t_i| x_i)$

Case 2 $X \neq Y$

$$\mu_Z = E(z) = E\left[\frac{1}{M}\sum_i (y_i t_i + y_i \alpha |t_i| x_i)\right]$$

$$= \frac{1}{M}\sum_i \left[\underbrace{E(y_i t_i)}_{\text{independence}} + \alpha \underbrace{E(y_i |t_i| x_i)}_{\text{independence}} \right]$$

$$E(y_i)\underbrace{E(t_i)}_{0} \qquad E(y_i)E((t_i))\underbrace{E(x_i)}_{0}$$

$$= 0$$

Theoretical Analysis

- $z = \frac{1}{M}\Sigma_{i=1}^{M}(y_i t_i + y_i \alpha |t_i| x_i)$

$$\sigma_z^2 = Var(z) = Var\ \frac{1}{M}\sum_i (y_i t_i + y_i \alpha |t_i| x_i)$$

$$= \frac{1}{M^2}\sum_i \left[Var(y_i t_i) + \alpha^2 Var(y_i |t_i| x_i)\right]$$

$\sum_i \rightarrow M$

$$= \frac{1}{M}\left[E(y^2t^2) - E(yt)^2 + \alpha^2 E(y^2t^2x^2) - \alpha^2 E(y|t|x)^2\right]$$

$E(y^2t^2) \rightarrow E(y^2)E(t^2) \rightarrow 1$

$E(yt) \rightarrow E(y)E(t) \rightarrow 0$

$E(y^2t^2x^2) \rightarrow E(y^2)E(t^2)E(x^2) \rightarrow 1$

$E(y|t|x)^2 \rightarrow E(y)E(|t|)E(x) \rightarrow 0$

$$= \frac{1}{M}\left[E(t^2) + \alpha^2 E(t^2)\right]$$

σ_t^2 (∵ proved before)

$$= \frac{\sigma_t^2}{M}(1+\alpha^2)$$

Theoretical Analysis

- $z = \frac{1}{M}\Sigma_{i=1}^{M}(y_i t_i + y_i \alpha |t_i| x_i)$

Case 3 No mark exists.

This means, $t_i' = t_i + \alpha |t_i| x_i = t_i$

$\therefore \alpha = 0$ for $X \neq Y$ case.

Plug $\alpha = 0$ to $\begin{cases} \mu_z = 0 \\ \sigma_z^2 = \frac{\sigma_\epsilon^2}{M}(1+\alpha) \end{cases} \xrightarrow{\alpha=0} \begin{cases} \mu_z = 0 \\ \sigma_z^2 = \frac{\sigma_t^2}{M} \end{cases}$

Theoretical Analysis

- $\mu_z = \begin{cases} \alpha\mu_{|t|} & \text{if } X = Y \\ 0 & \text{if } X \neq Y \\ 0 & \text{if no mark is present} \end{cases}$
- $\sigma_z^2 = \begin{cases} \frac{1+2\alpha^2}{M}\sigma_t^2 + \frac{\alpha^2}{M}\sigma_{|t|}^2 & \text{if } X = Y \\ \frac{1+\alpha^2}{M}\sigma_t^2 & \text{if } X \neq Y \\ \frac{1}{M}\sigma_t^2 & \text{if no mark is present} \end{cases}$
- Note $\sigma_{|t|}^2 < \sigma_t^2$ and assume $\alpha^2 \ll 1$. Then $\sigma_z^2 = \frac{\sigma_t^2}{M}$ for all cases.

Theoretical Analysis

- $\mu_z = \begin{cases} \alpha\mu_{|t|} & \text{if } X = Y \\ 0 & \text{if } X \neq Y \\ 0 & \text{if no mark is present} \end{cases}$
- $\sigma_z^2 = \frac{\sigma_t^2}{M}$
- This is why $t_i' = t_i + \alpha|t_i|x_i$ is used.
  - If no abs, then $\mu_{|t|} = 0$.

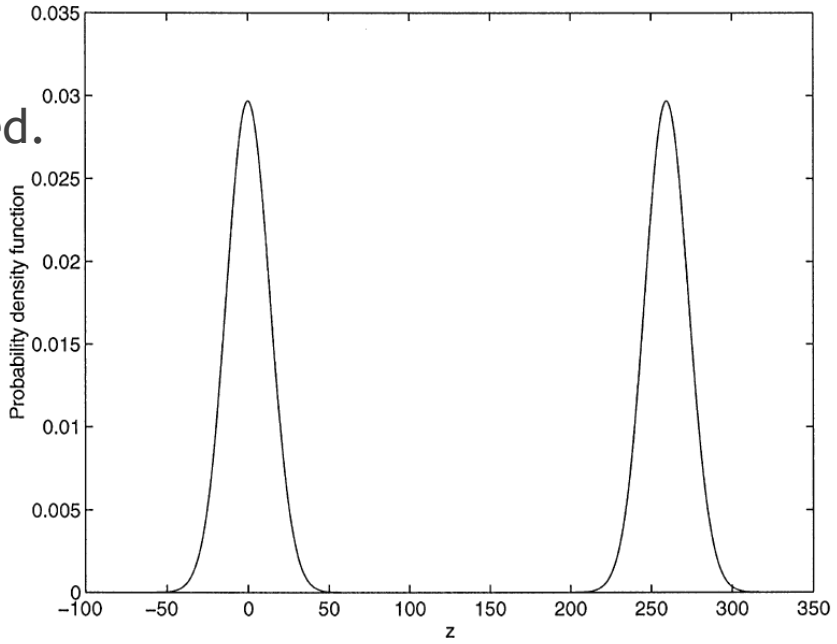
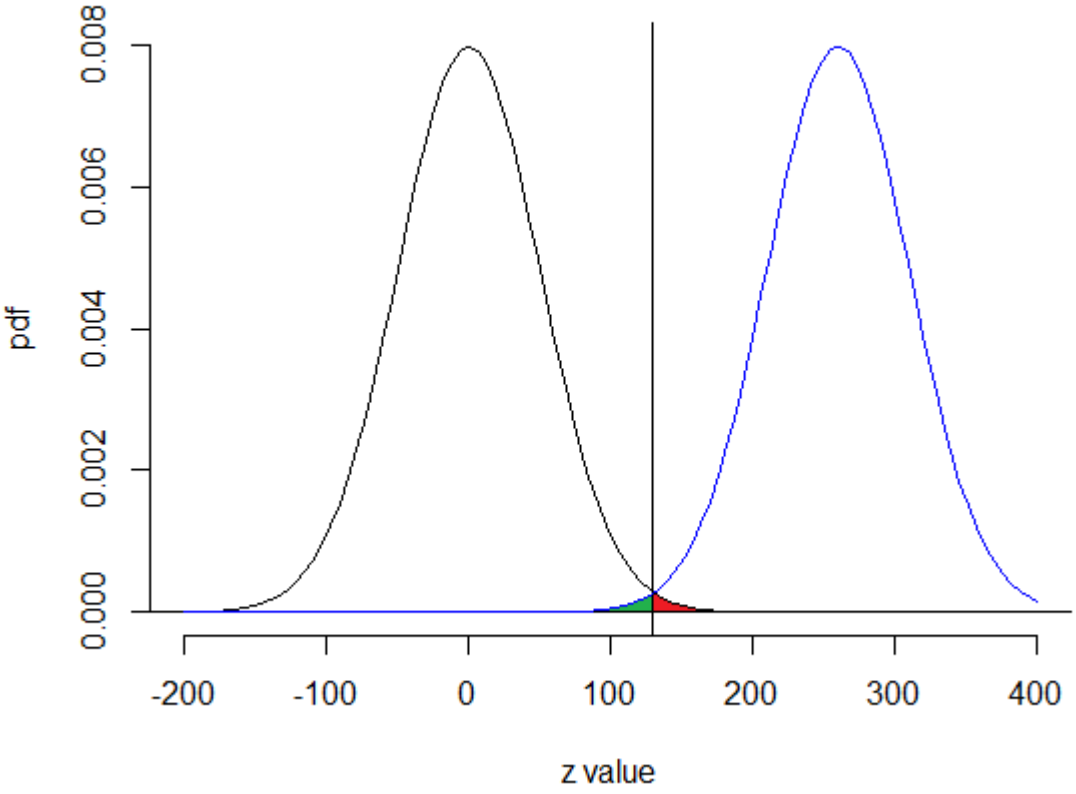


Fig. 1. Probability density functions of the random variable z, when the watermark detected does not match the embedded one (Left), and when the watermark matches the embedded one (Right).

Theoretical Analysis

- If we assume $T_z = \frac{\mu_{z_2}}{2}$ and $\sigma_{z_1} = \sigma_{z_2} = \sigma_z$, then we have the error probability $P_e = \frac{1}{\sqrt{2\pi\sigma_z^2}} \int_{T_z}^{\infty} e^{-x^2/2\sigma_z^2}\, dx.$

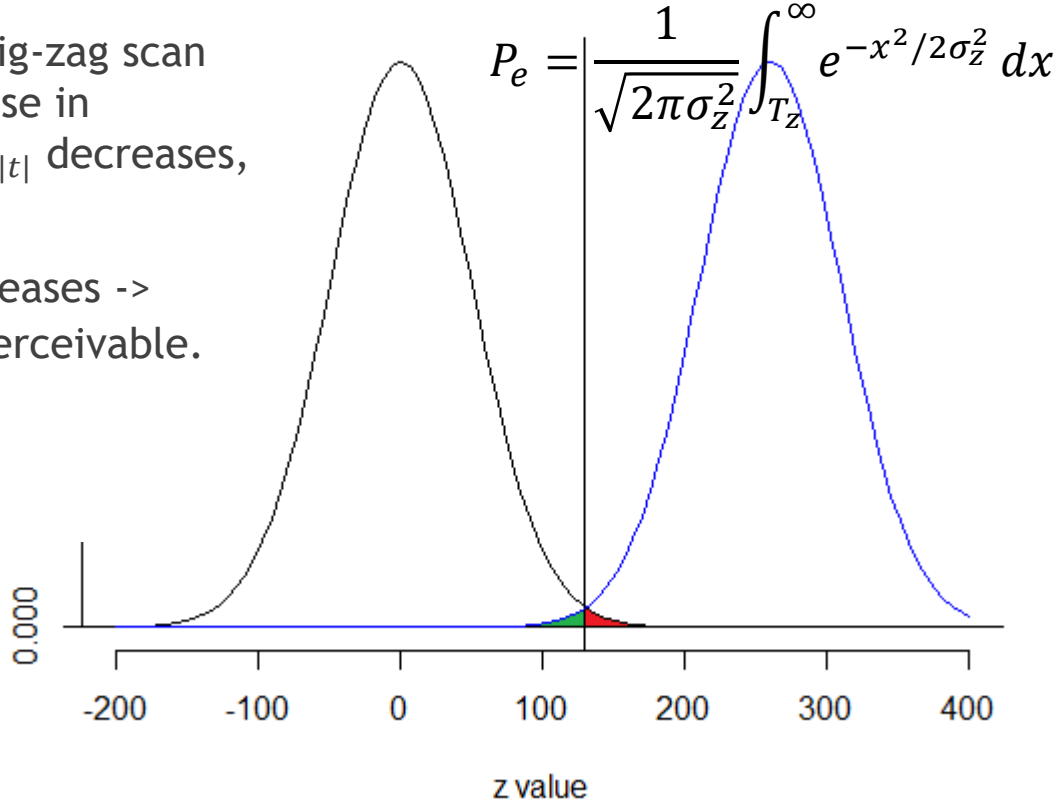


Theoretical Analysis

- To reduce the error, we need to increase $\mu_{z_2} = \alpha\mu_{|t|}$ or decrease $\sigma_z = \frac{\sigma_t^2}{M}$.
  - If M increases, then σ_z decreases -> error decreases but more perceivable.
  - If L increases, then in the zig-zag scan the DCT coefficients decrease in absolute value. So σ_t^2 and $\mu_{|t|}$ decreases, but σ_t^2 decreases faster.
  - If α increases, then μ_{z_2} increases -> error decreases but more perceivable.

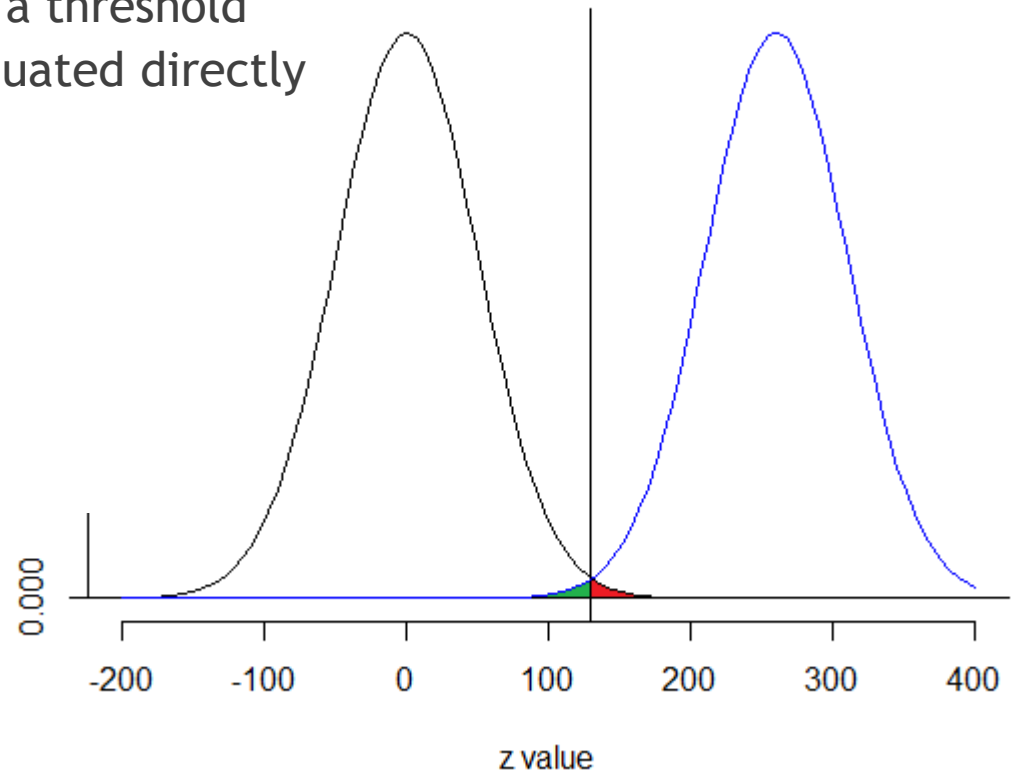
$$T_z = \frac{\mu_{z_2}}{2} = \frac{\alpha\mu_{|t|}}{2}$$

$$P_e = \frac{1}{\sqrt{2\pi\sigma_z^2}} \int_{T_z}^{\infty} e^{-x^2/2\sigma_z^2}\, dx$$



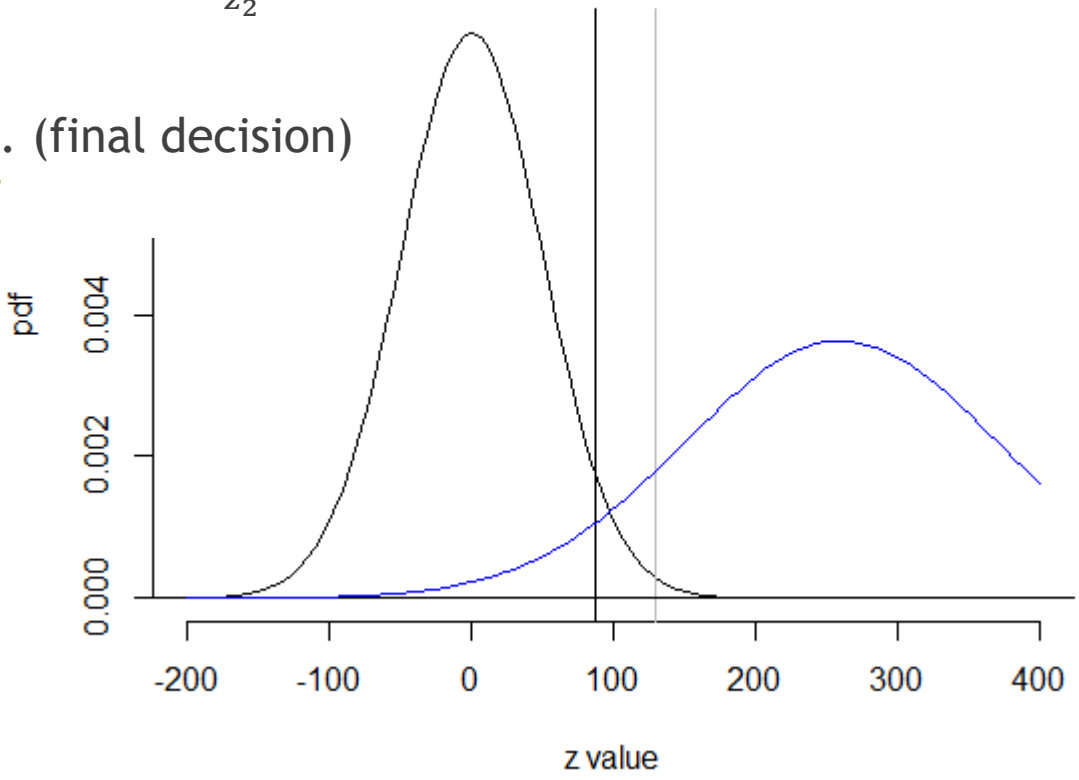
Theoretical Analysis

- It's hard to derive $\mu_{|t|}$ or σ_t since the expected value of t_i over all possible images should be computed. So it is hard to compute $T_z = \frac{\alpha \mu_{|t|}}{2}$.
- In practical application, use a threshold $T_z' = \frac{\alpha}{2M} \Sigma_{i=1}^{M} |t_i'|$ which is evaluated directly on the marked image.



Theoretical Analysis

- Now consider the case when the images is corrupted.
- Experimental results show that when the image has been corrupted, σ_{z_1} remains approximately the same, whereas σ_{z_2} increases significantly.
- So we set $T_z' = \frac{\alpha}{3M}\Sigma_{i=1}^{M}|t_i^*|$. (final decision)



Visual Masking

- The algorithm we've discussed so far changes DCT coefficients equally over the whole image not concerning the regional characteristics.
- To enhance the invisibility of the watermark, the spatial masking characteristics of the HVS are exploited.
- $y''_{i,j} = y_{i,j}(1 - \beta_{i,j}) + \beta_{i,j} y'_{i,j}$ where $y_{i,j}$: original pixel, $y'_{i,j}$: watermarked pixel, $\beta_{i,j}$: local weighting factor.
  - $\beta_{i,j} \approx 1$ for highly textured region (watermarking is easy)
  - $\beta_{i,j} \approx 0$ for uniform region (watermarking is hard)
  - Choose $\beta_{i,j}$ by the normalized sample variance of an $R \times R$ block centered at $y_{i,j}$.
  - α can be chosen in such a way that its mean value over the image, after weighting by factor $\beta_{i,j}$, becomes $\bar{\alpha} = 0.2$. ($\bar{\alpha} = \alpha E(\beta)$)

Experiments

- 1000 watermarks were randomly generated.
- M=L=16000, R=9, $\bar{\alpha} = 0.2$

Results

- 1. Original / 2. Watermarked

Fig. 2. Original image 'Boat' (Left), and watermarked image 'Boat' with parameters $\bar{x} = 0.2$, $M = L = 16\,000$, and block size $R = 9$ (Right).

Results

- 2. Watermarked

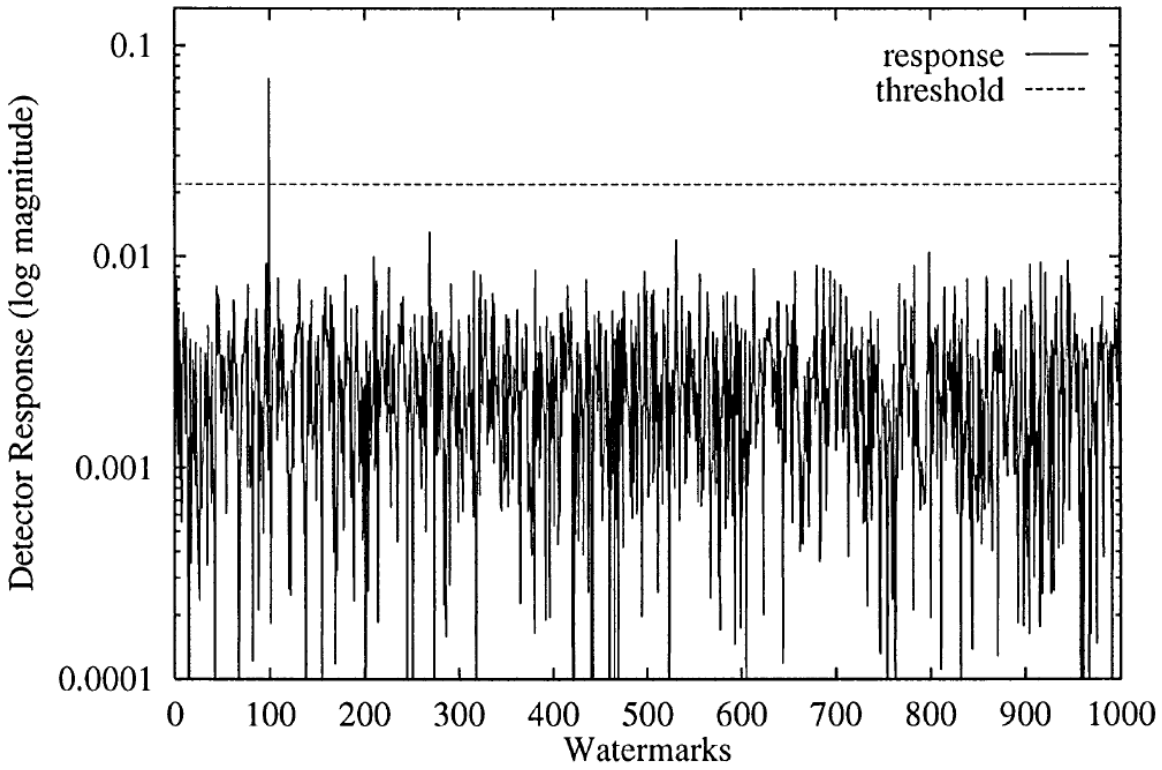


Fig. 3. The log of the magnitude of the detector response of the watermarked image in Fig. 2 (Right) to 1000 randomly generated watermarks. Only watermark number 100 matches that embedded.

Results

- 3. Jpeg compressed

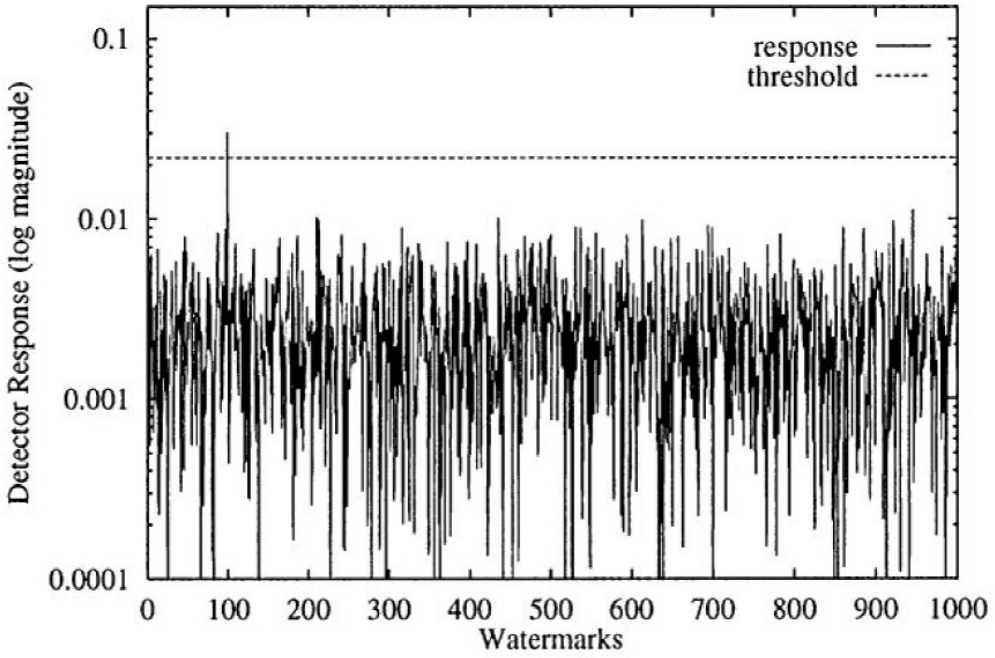


Fig. 4. JPEG compressed copy of the watermarked image 'Boat', with 4% quality and 0% smoothing (Left), and the corresponding log of the magnitude of the detector response (Right).

Results

- 4. low-pass filtered

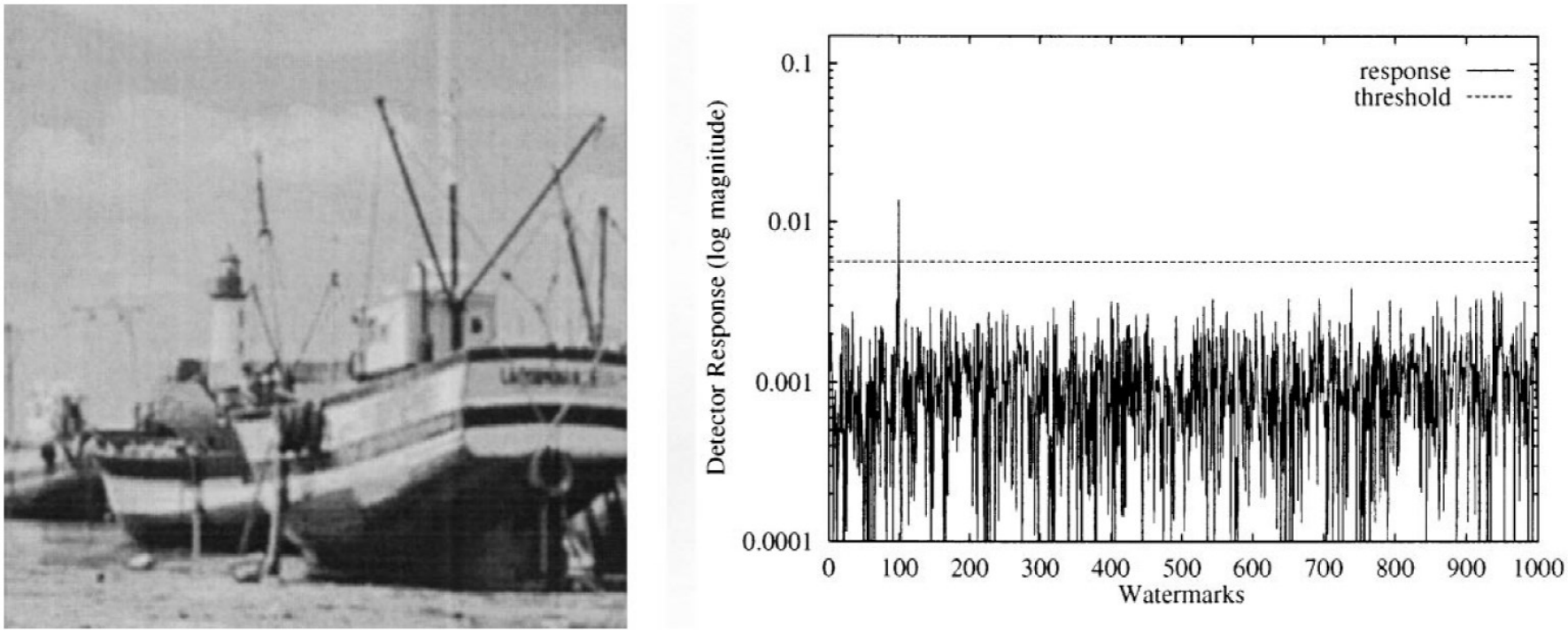


Fig. 5. Watermarked image 'Boat' low pass filtered 5×5 (Left), and the corresponding log of the magnitude of the detector response (Right).

Results

- 5. Median filtered

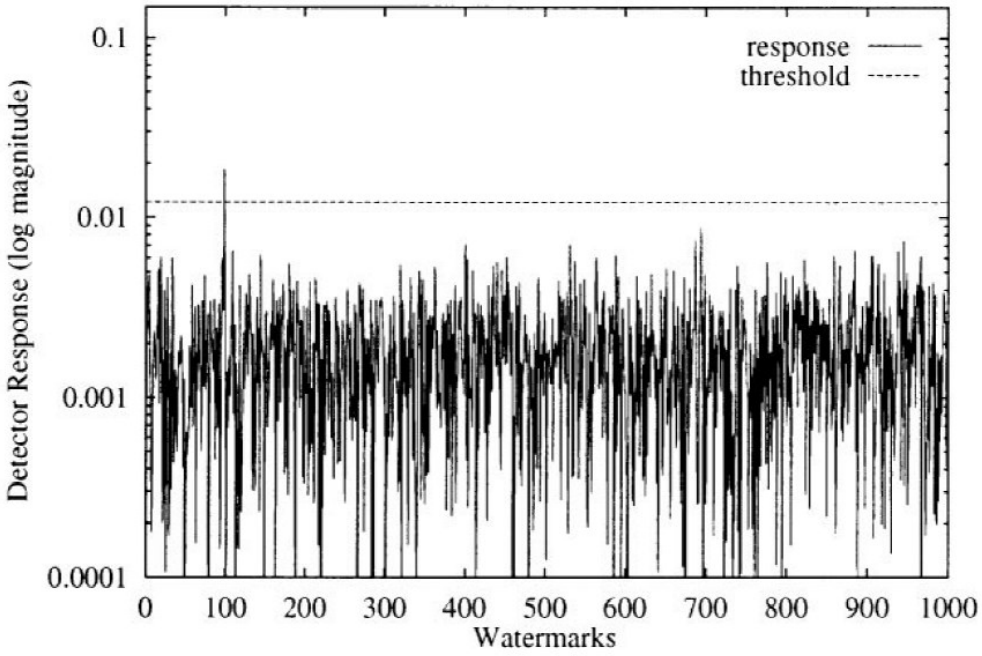
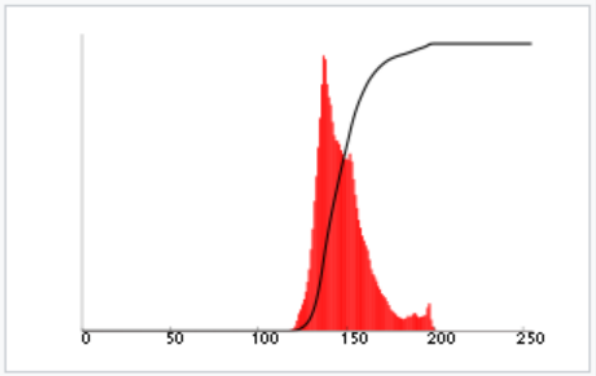


Fig. 6. Watermarked image 'Boat' median filtered 5×5 (Left), and the corresponding log of the magnitude of the detector response (Right).

Results

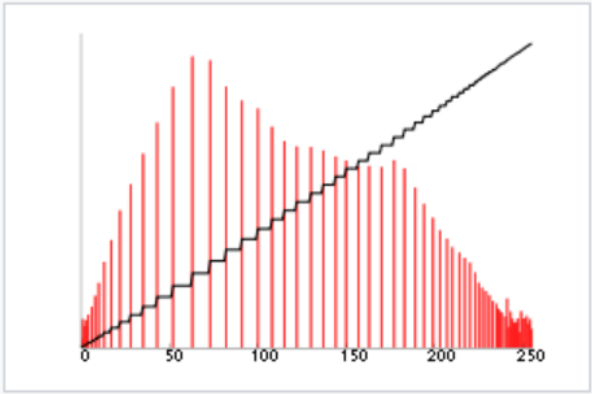
- 6. Applied histogram equalizing

Before Histogram Equalization



Corresponding histogram (red) and cumulative histogram (black)

After Histogram Equalization



Corresponding histogram (red) and cumulative histogram (black)

Results

- 6. Applied histogram equalizing

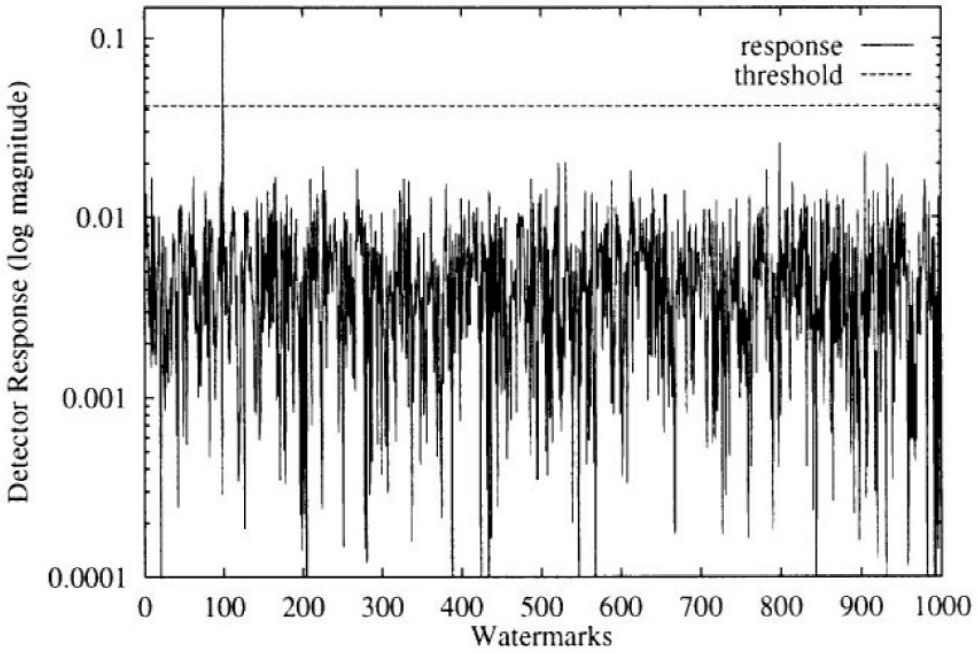


Fig. 7. Watermarked image 'Boat' after histogram equalization (Left), and the corresponding log of the magnitude of the detector response (Right).

- Detector response of the embedded watermark increases w.r.t response obtained on the unprocessed watermarked image

Results

- 7. Applied histogram stretching

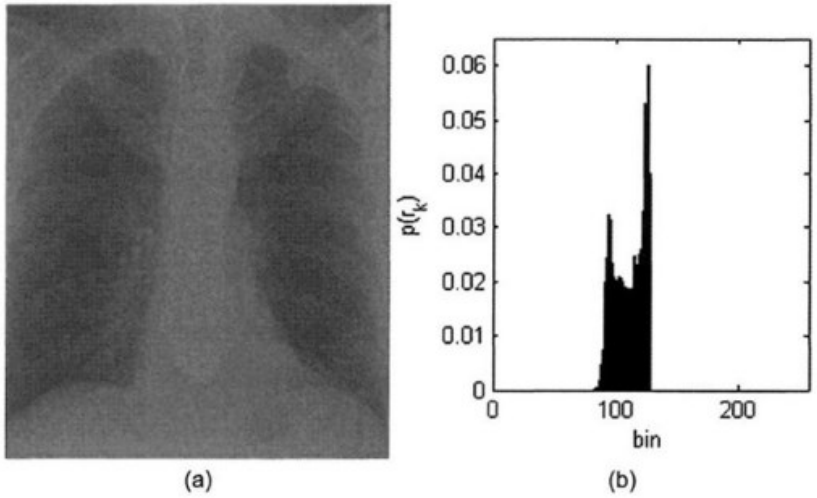


Figure 3-4. X-ray image courtesy of SRS-X, http://www.radiology.co.uk/srs-x. (a) Low contrast chest x-ray image, (b) Low contrast histogram.

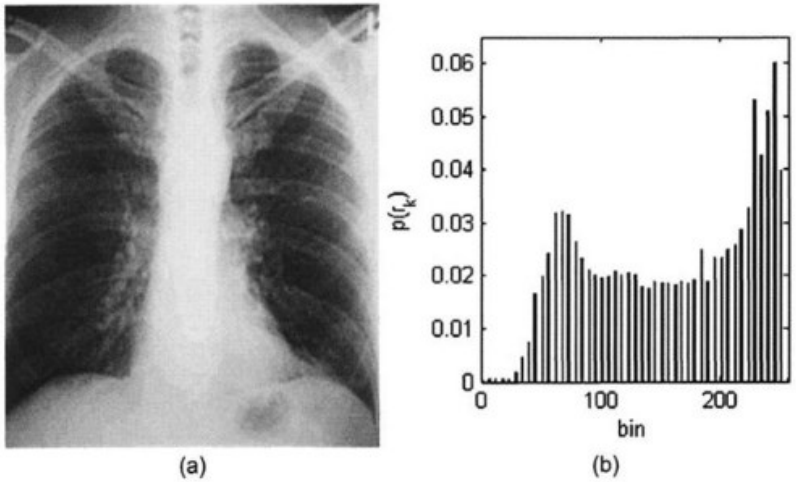


Figure 3-5. (a) Contrast-stretched chest x-ray image, (b) Modified histogram.

Results

- 7. Applied histogram stretching

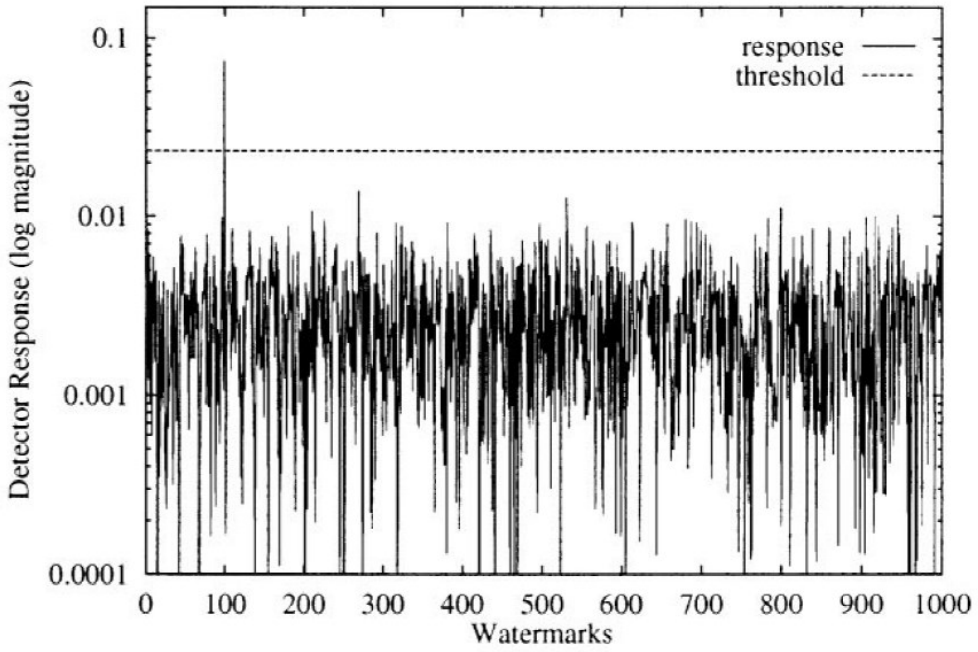


Fig. 8. Watermarked image 'Boat' after histogram stretching (Left), and the corresponding log of the magnitude of the detector response (Right).

- Detector response of the embedded watermark increases w.r.t response obtained on the unprocessed watermarked image

Results

- 8. Applied Gaussian noise

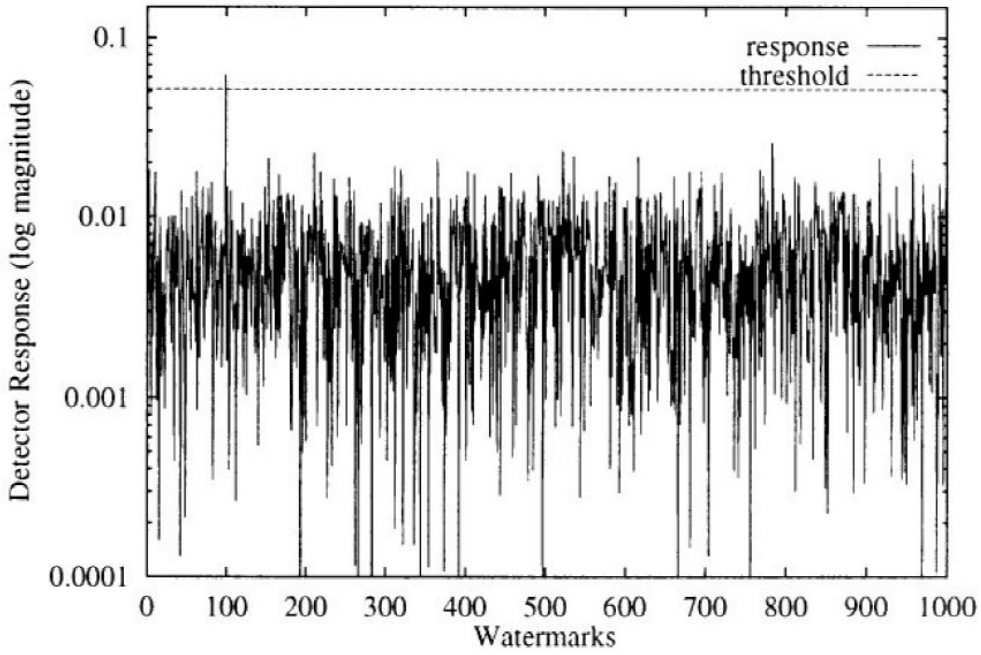
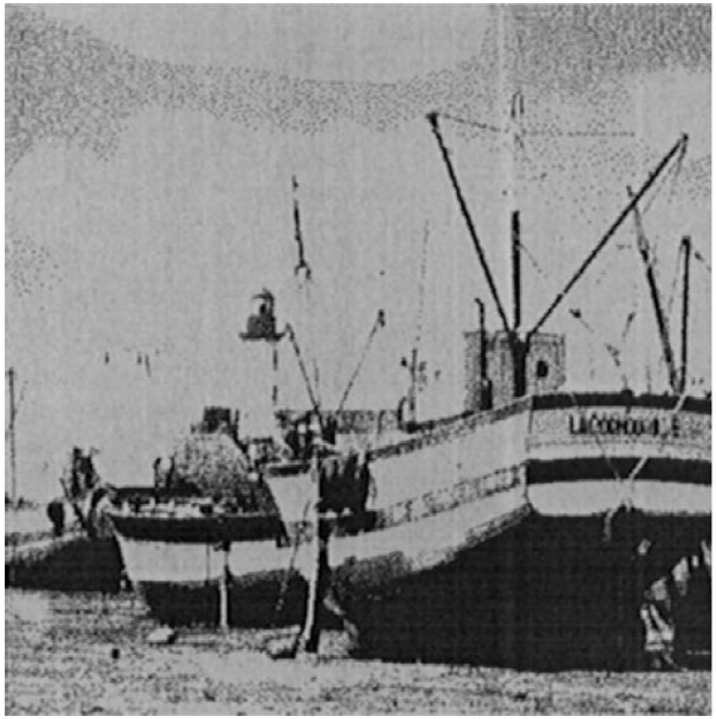


Fig. 9. Watermarked image 'Boat' with Gaussian noise having variance $\sigma^2 = 4000$ (Left), and the corresponding log of the magnitude of the detector response (Right).

Results

- 9. Applied dithering



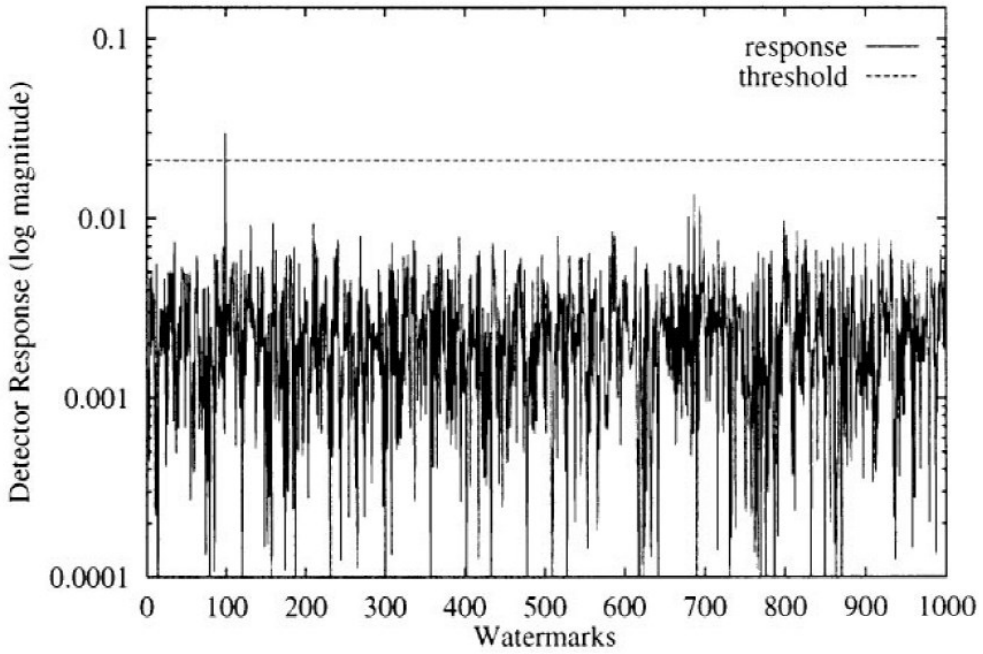


Fig. 10. Watermarked image 'Boat' after dithering (Left), and the corresponding log of the magnitude of the detector response (Right).

- Dithering converts the grayscale image to the binary (black and white) image.
- The high resistance of the watermark to dithering suggests the system is also robust against all digital-to-analog conversions based on such techniques.

Results

- 10. Resized

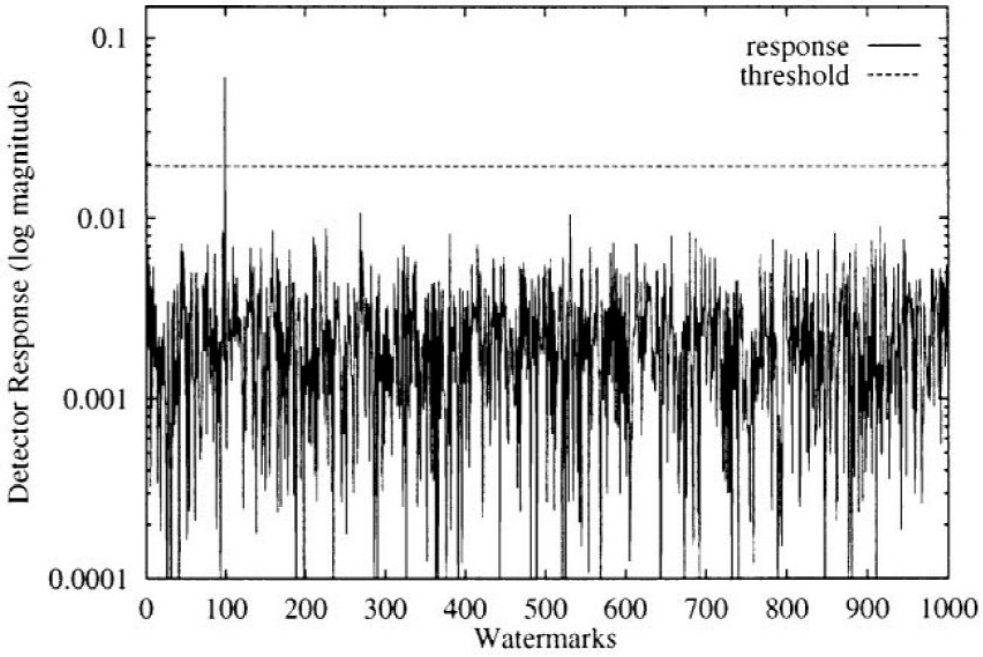


Fig. 12. Watermarked image 'Boat' after resizing from 512×512 to 256×256 (Left), and the corresponding log of the magnitude of the detector response (Right).

Results

- 10. Resized

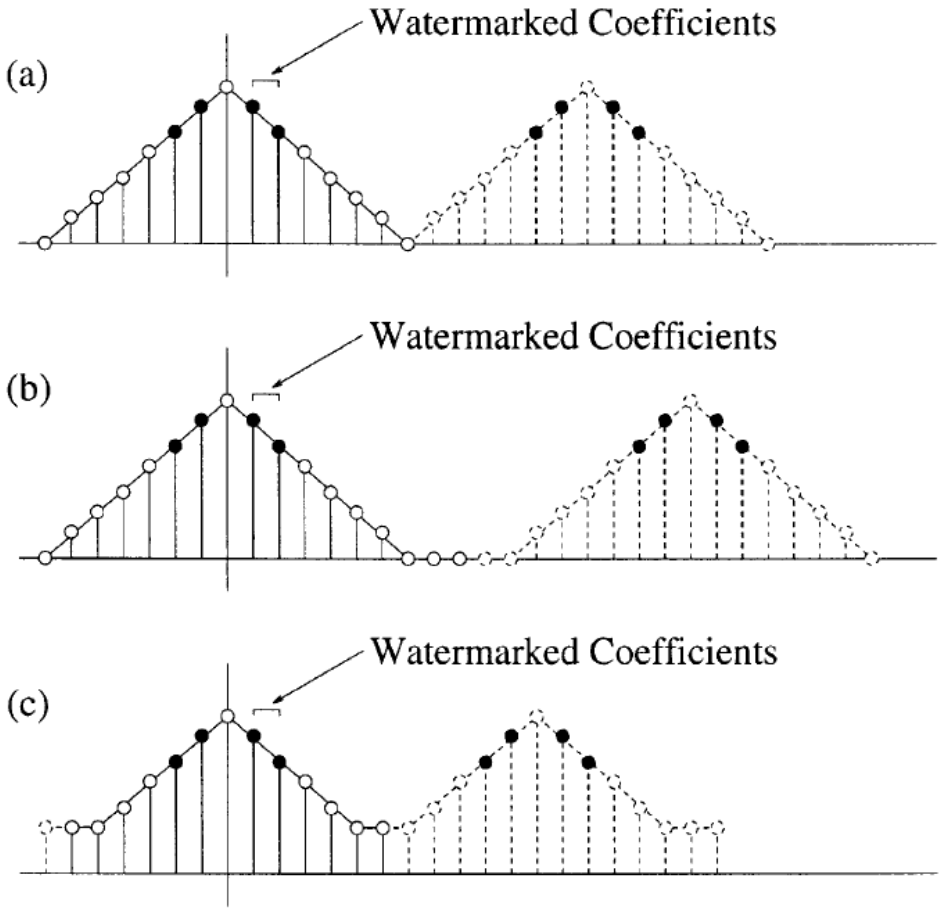


Fig. 11. Example of the effects of image resizing on DCT coefficients. The DCT spectrum of the uncorrupted watermarked image (a) is shown, as well as that of a magnified (b) and a shrunk (c) copies.

Results

- 11. Cropped

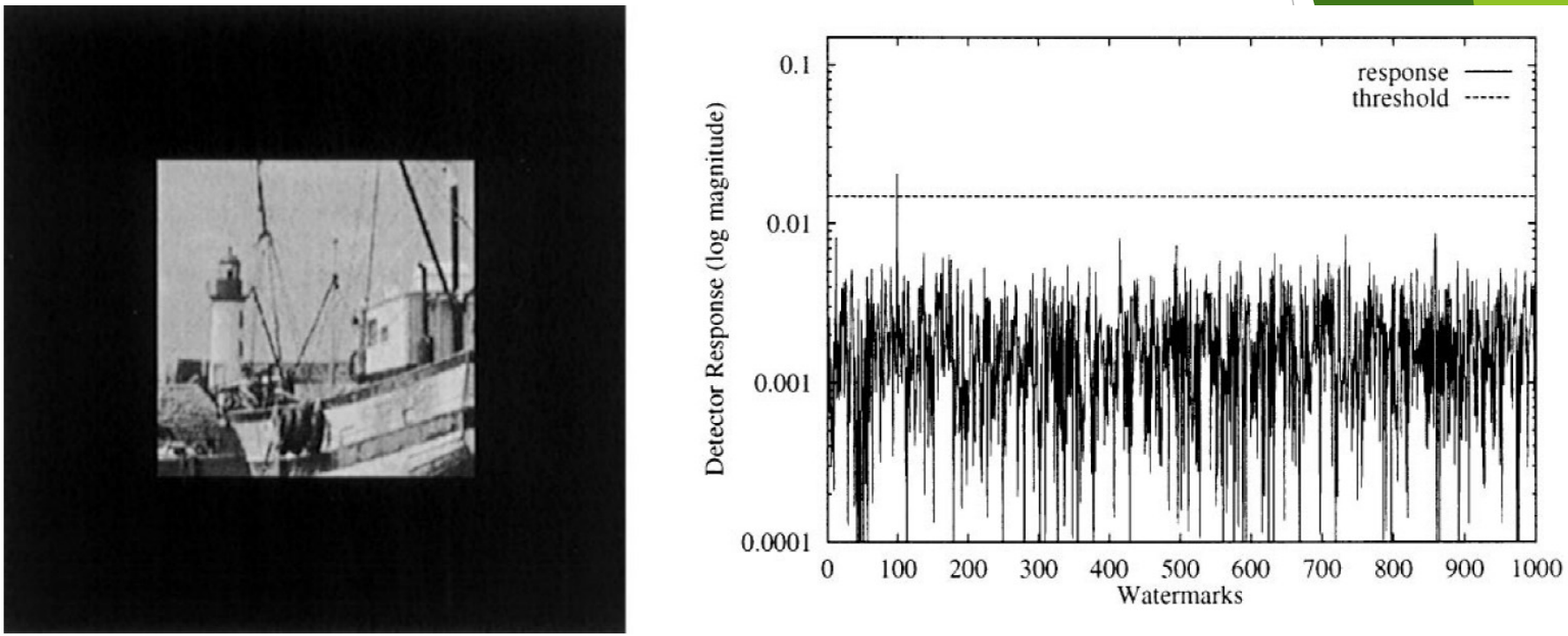


Fig. 13. Watermarked image 'Boat' after cropping (Left), and the corresponding log of the magnitude of the detector response (Right).

- If the subimage is placed at exactly the same position it occupied in the original picture, the proposed system can detect the watermark if the cropped part is at least 40% of the original image.

Results

- 12. Multiple watermarks

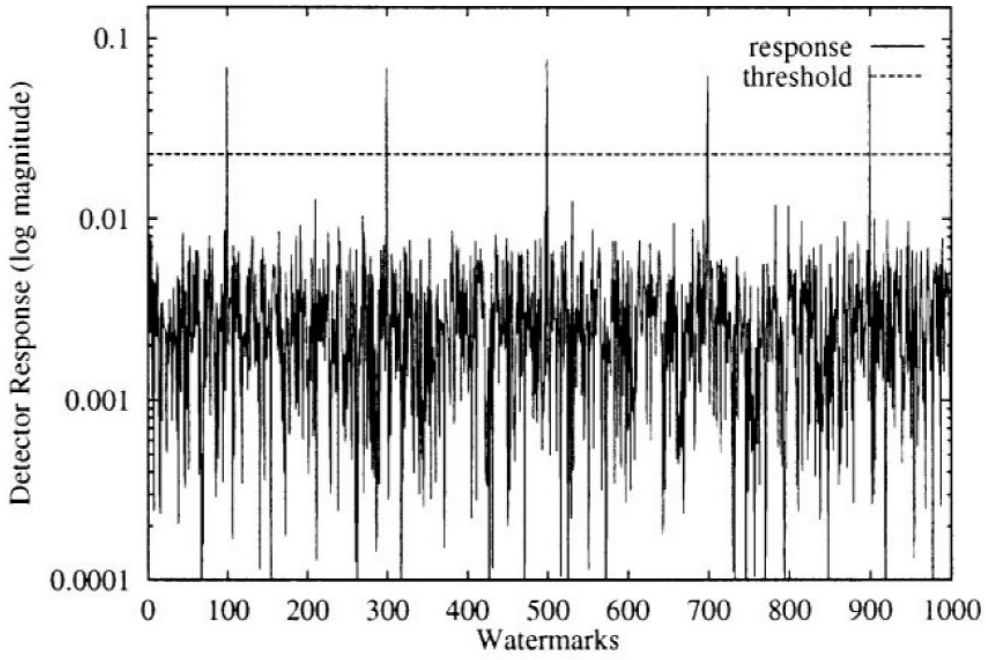
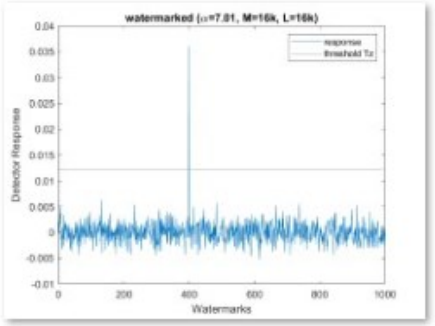


Fig. 14. Image 'Boat' with five different watermarks (Left), and the corresponding log of the magnitude of the detector response (Right).

Results

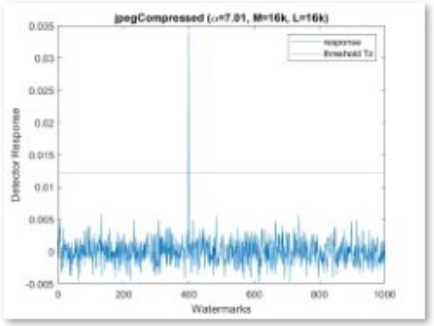
- Matlab implementation

1_2_watermarked_IU.jpg



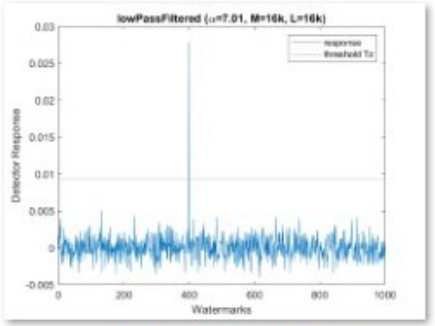
1_2_watermarked_IU.jpg.png

1_3_jpegCompressed_IU.jpg.jpg



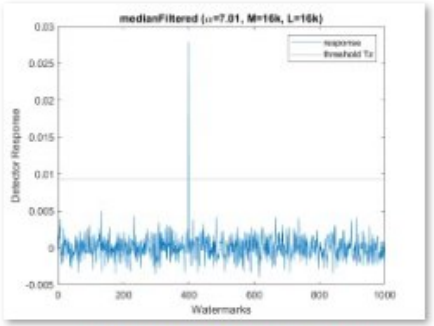
1_3_jpegCompressed_IU.jpg.png

1_4_lowPassFiltered_IU.jpg

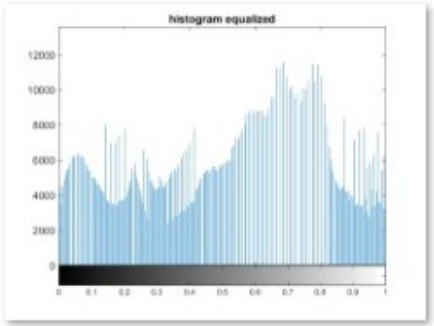


1_4_lowPassFiltered_IU.jpg.png

1_5_medianFiltered_IU.jpg

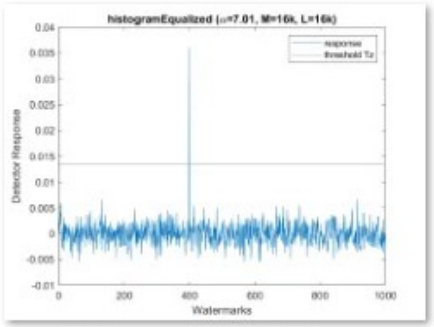


1_5_medianFiltered_IU.jpg.png

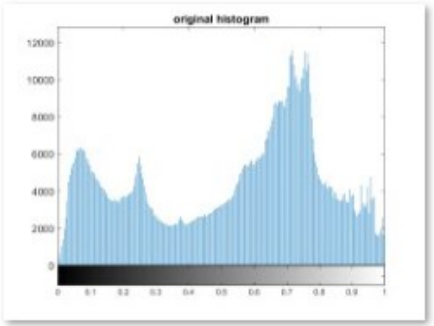


1_6_histogram equalized_IU.jpg.png

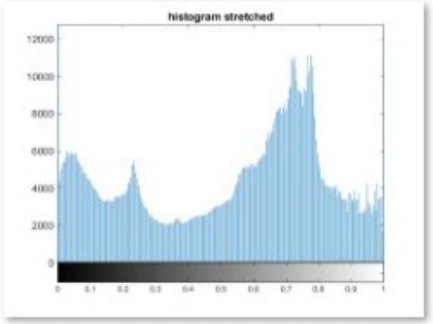
1_6_histogramEqualized_IU.jpg



1_6_histogramEqualized_IU.jpg.png

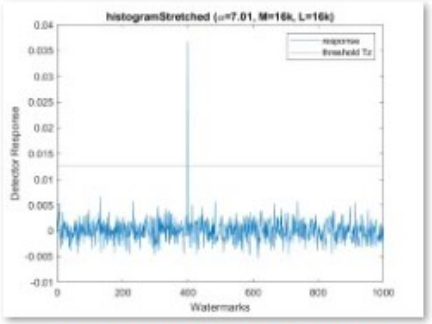


1_6_original histogram_IU.jpg.png

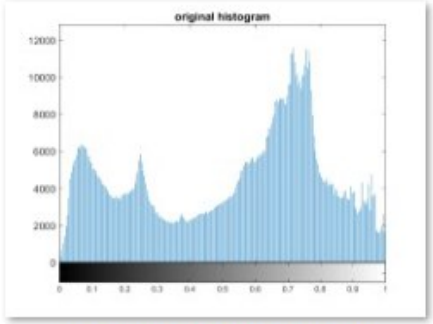


1_7_histogram stretched_IU.jpg.png

1_7_histogramStretched_IU.jpg

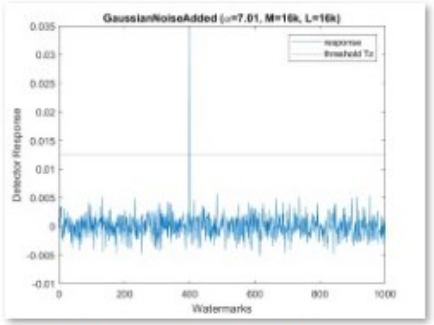


1_7_histogramStretched_IU.jpg.png



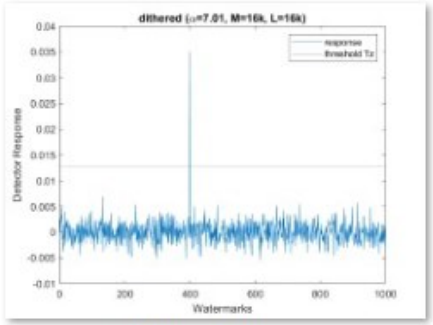
1_7_original histogram_IU.jpg.png

1_8_GaussianNoiseAdded_IU.jpg



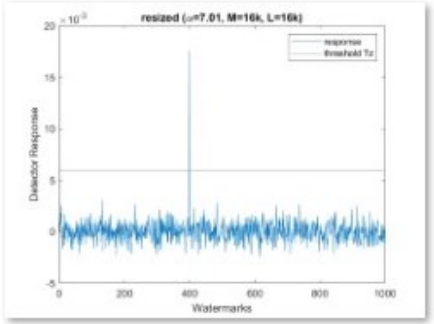
1_8_GaussianNoiseAdded_IU.jpg.png

1_9_dithered_IU.jpg



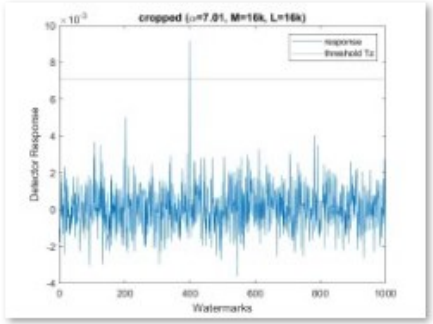
1_9_dithered_IU.jpg.png

1_10_resized_IU.jpg



1_10_resized_IU.jpg.png

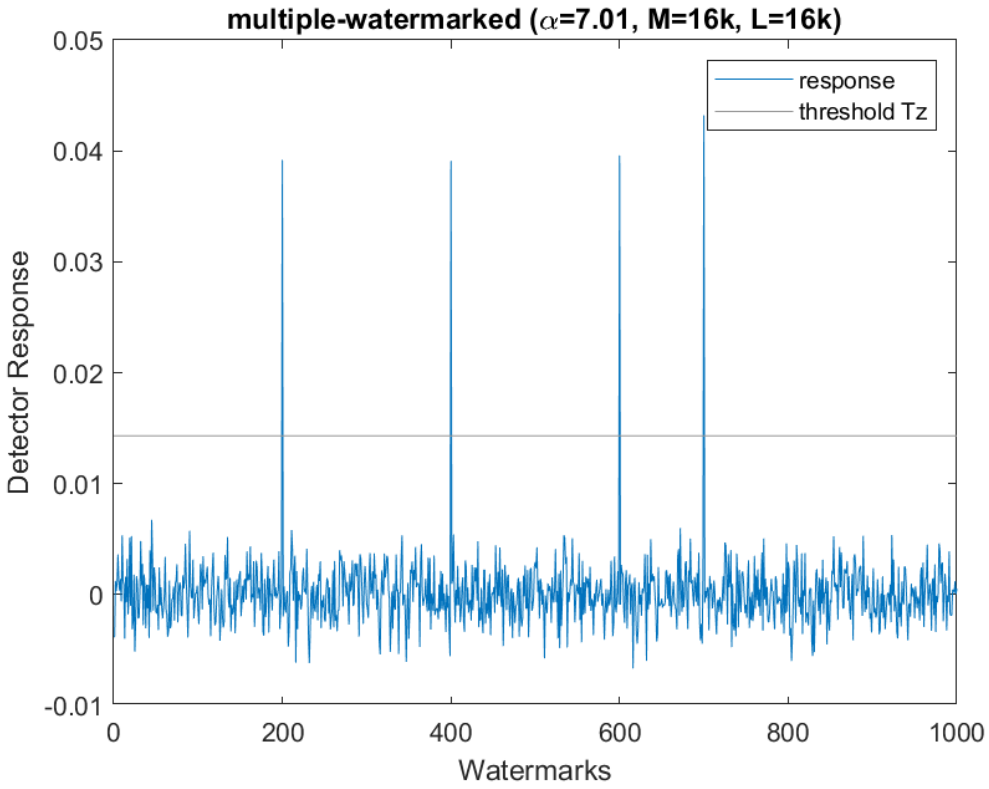
1_11_cropped_IU.jpg



1_11_cropped_IU.jpg.png

Results

- 12. Multiple watermarks



Results

- More experiments not in the paper
- Targeted to fail the proposed method
  - Translation
  - Scaling with different x and y scale
  - Rotation

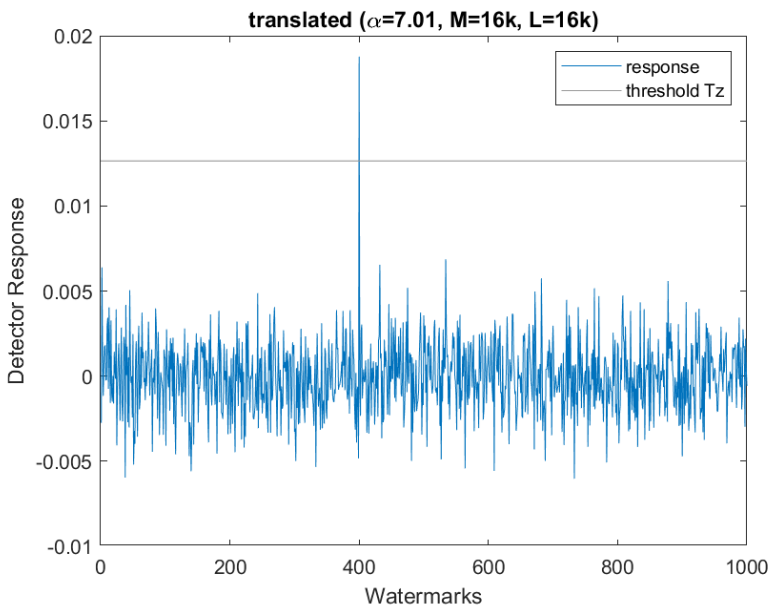
Results

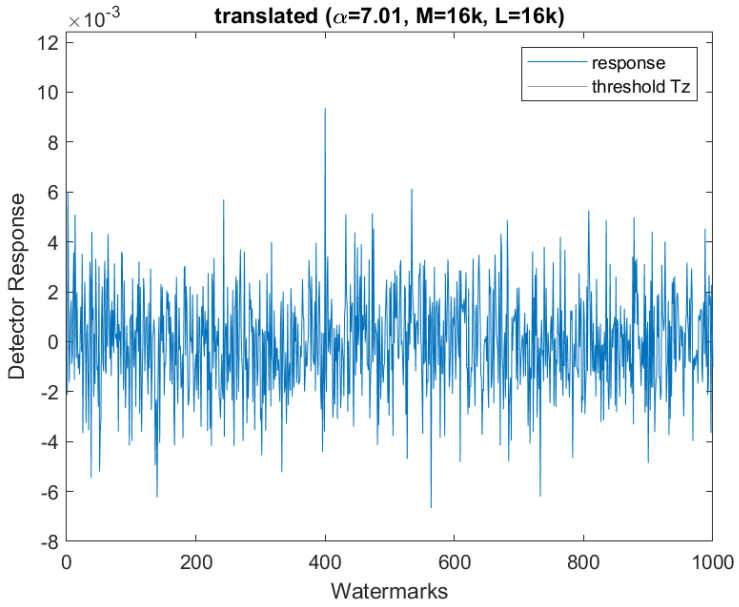
- 13. translation

- Translate the image

main.m | translate.m

```
function outputImage = translate(image, titleStrin
d=1;
[Y,X]=size(image);
outputImage=zeros([Y,X]);
outputImage(1+d:Y,:)=image(1:(Y-d),:);
imwrite(outputImage,strcat('output/',string(imageI
```





- top: d=3pixels, bottom: d=4pixels
- Original image size = 1080x1080

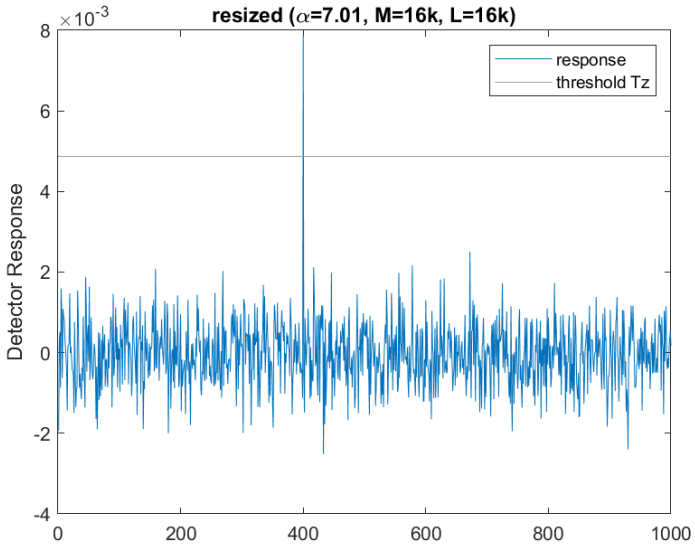
Results

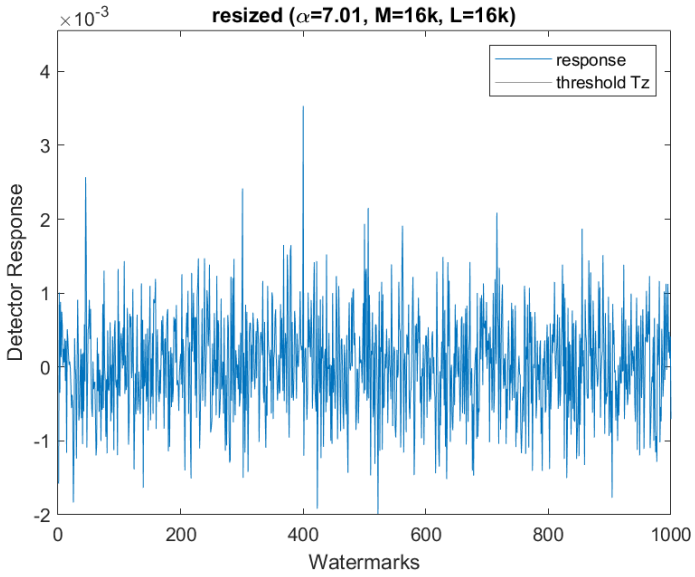
- 14. resizing with different x and y scale

- Scale the image

main.m | resize2.m

```
1   function outputImage = resize2(image, titleString, plotNumb
2 -  scale=0.2;
3 -  resizedFileName=strcat('output/',string(imageIndex),'_',str
4 -  [Y,X]=size(image);
5 -  image=imresize(image,[Y,X*scale]);
6 -  imwrite(image,resizedFileName);
7 -  outputImage=im2double(imread(resizedFileName));
8 -  try
9 -      outputImage = rgb2gray(outputImage);
10 -  catch
11 -  end
```





- Very robust to scaling
- top: scale=0.20(216x1080), bottom: scale=0.18(195x1080)
- Original image size = 1080x1080

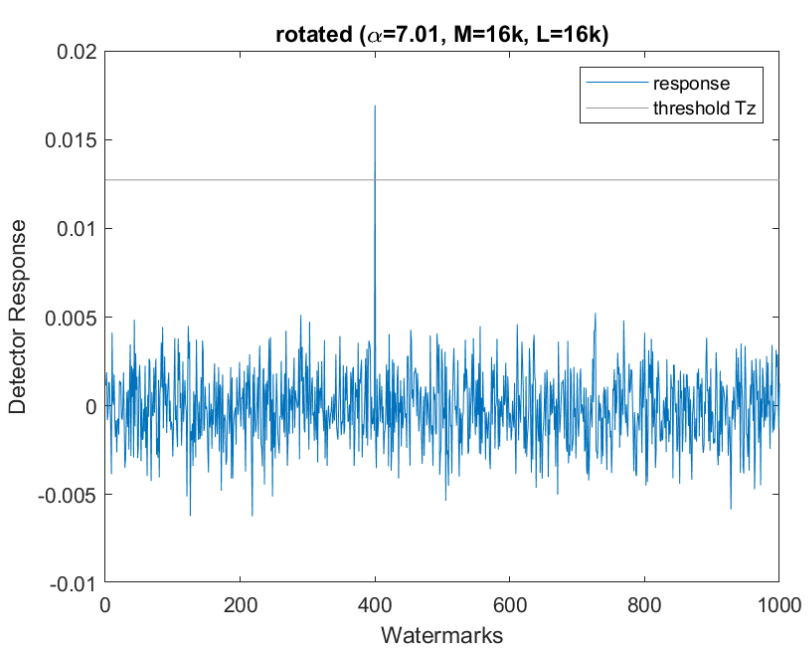
Results

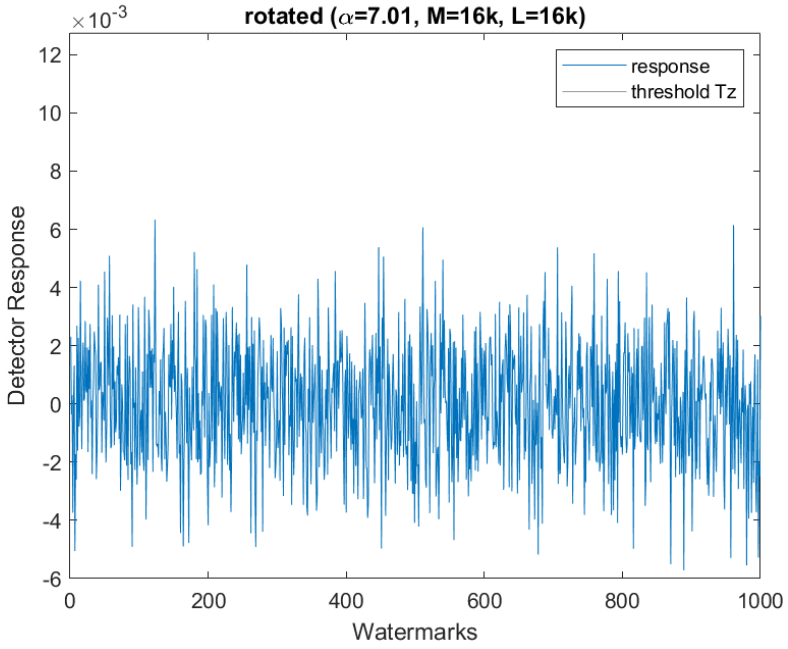
- 15. rotation

- Rotate the image

main.m | rotate.m

```
1   function outputImage = rotate(image, titleString, plot
2 -     angle=1; % angle in degree
3 -     outputImage=imrotate(image,angle,'bilinear','crop');
4 -     imwrite(outputImage,strcat('output/',string(imageIndex
```





- Fails even in 1 degree. (top: angle=0.4, bottom: angle=1)

Conclusions

- In this paper a watermarking algorithm for digital images operating in the frequency domain is presented :
  - A pseudo-random sequence of real numbers having standard normal distribution is embedded in a selected set of DCT coefficients.
  - After embedding, the watermark is adapted to the image being signed by exploiting the characteristics of noise masking of the HVS.
- Original image is not needed to recover the watermark.
- Experimental results demonstrate that the watermark is robust to several signal processing techniques.
- Multiple watermarking is possible.

Discussion

- The watermark is detectable only if the image is placed at the exactly same location. So a ‘smart' image matching algorithm is needed to use the proposed method in real internet world.

Thank you