Digital Watermarking and Steganography

by Ingemar Cox, Matthew Miller, Jeffrey Bloom, Jessica Fridrich, Ton Kalker

Chapter 9. Robust Watermarking

Lecturer: Jin HUANG

2015

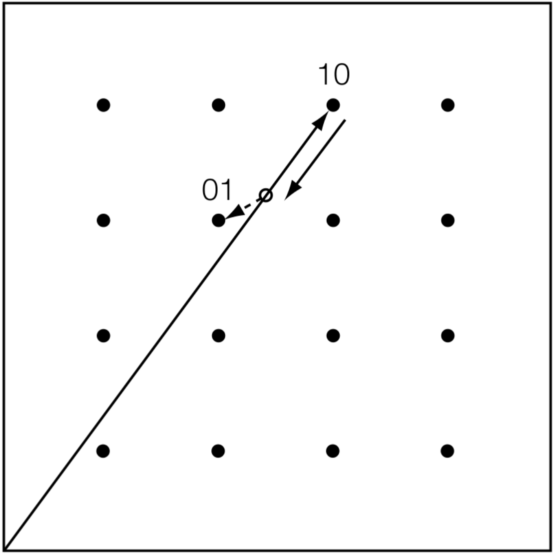
Valumetric Scaling

$\mathbf{c} * 0.8$

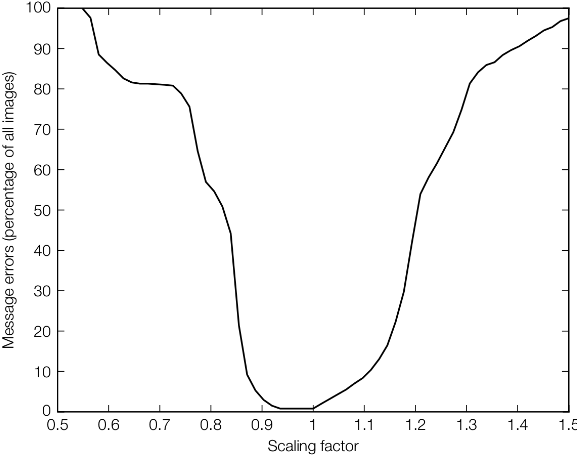
$\mathbf{c} * 1.0$

$\mathbf{c} * 1.2$

QIM is not Robust



Error Illustration



Valumetric scaling on the E_LATTICE/D_LATTICE system.

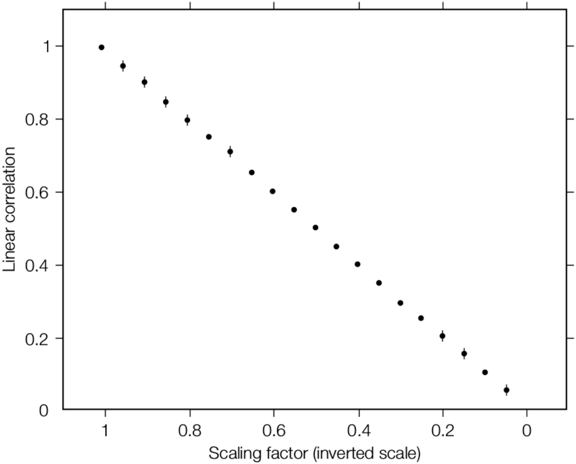
Reason

$$
\begin{aligned}
z_{lc}(s) &= (s\mathbf{c_w}) \cdot \mathbf{w_r} \\
&= s(\mathbf{c_w}) \cdot \mathbf{w_r}) \\
&= s \cdot z_{lc}.
\end{aligned}
$$

Possible solution?

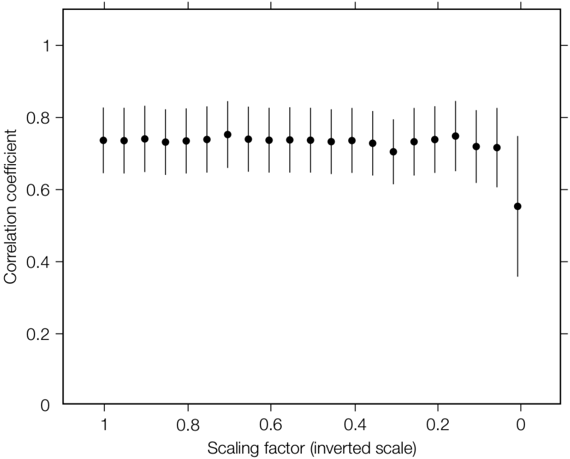
$$
\begin{aligned}
z_{nc}(s) &= \frac{s\mathbf{c_w}}{\|s\mathbf{c_w}\|} \cdot \mathbf{w_r} \\
&= \frac{\mathbf{c_w}}{\|\mathbf{c_w}\|} \cdot \mathbf{w_r} \\
&= \cos(\theta(\mathbf{c_w}, \mathbf{w_r})).
\end{aligned}
$$

Linear Correlation



E_FIXED_LC/D_LC.

Correlation Coefficients

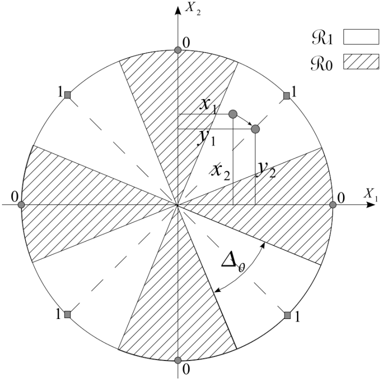


E_BLK_FIXED_R/D_BLK_CC.

z_{nc} with Dirty Paper

Angle QIM (Ourique et al. ICASSP 2005.):

- Snap work to the closest "grid angle".



2-Dimensional Case

- Choosing two bases $\mathbf{X}_1, \mathbf{X}_2$.
- Get coordinates x_1, x_2.
- Evaluate the length and angle:

$$r = \sqrt{x_1^2 + x_2^2}, \quad \theta = \arctan(x_2/x_2).$$

- Angle QIM:

$$\theta^Q = Q_{m,\Delta}(\theta) = \left\lfloor \frac{\theta + m\Delta}{2\Delta} \right\rfloor 2\Delta + m\Delta.$$

- Restore:

$$x_1' = r\cos(\theta^Q), \quad x_2' = r\sin(\theta^Q).$$

L-Dimensional Case

- L bases: $\mathbf{X}_i, i = 1, \cdots, L$.
- L coordinates: $\mathbf{x}_i, i = 1, \cdots, L$.
- $L-1$ angles: $\mathbf{x}_i, i = 1, \cdots, L-1$.

$$\theta_1 = \arctan(x_2/x_1)$$
$$\theta_i = \arctan \frac{x_{i+1}}{\sqrt{\sum_{k=1}^{i} x_k^2}}, i = 2, \cdots L-1.$$

- Restore:

$$x_1' = r\Pi_{k=1}^{L-1} \cos\theta_k^Q$$
$$x_i' = r\sin\theta_{i-1}^Q \Pi_{k=i}^{L-1} \cos\theta_k^Q, i = 2, \cdots, L.$$

Digital Watermarking and Steganography

by Ingemar Cox, Matthew Miller, Jeffrey Bloom, Jessica Fridrich, Ton Kalker

Chapter 10. Watermark Security

Lecturer: Jin HUANG

2015

Ambiguity Attacks with Blind Detection

I am the True Owner!

The owner hold $\mathbf{c_o}$ privately, and distribute $\mathbf{c_d} = \mathbf{c_o} + \mathbf{w_r}$.

If other people claim the ownership with $\mathbf{c_d}$.

- $\mathbf{c_d}$ containing $\mathbf{w_r}$.
- AND ONLY the owner has a copy $\mathbf{c_o}$ without $\mathbf{w_r}$.

Example

Ownership

	$\mathbf{c_o}$	$\mathbf{c_d}$	$\mathbf{c_f}$
$\mathbf{w_r}$	-0.016	0.973	0.971
$\mathbf{w_f}$	0.968	0.970	0.005

$\mathbf{w_f}$ and $\mathbf{c_f}$

- $\mathbf{w_f}$: large z_{lc} for $\mathbf{c_o}$ and $\mathbf{c_d}$

$$\mathbf{c_o} \cdot \mathbf{w_f}, \quad (\mathbf{c_o} + \mathbf{w_r}) \cdot \mathbf{w_f}.$$

- $\mathbf{c_f}$:

$$\text{small } \mathbf{c_f} \cdot \mathbf{w_f}, \quad \text{large } \mathbf{c_o} \cdot \mathbf{w_f}.$$

- Idea:
  - $\mathbf{w_f}$ has high correlation with $\mathbf{c_o}$: $\mathbf{w_f} \cdot \mathbf{c_o} = 1$.
  - $\mathbf{c_f} = \mathbf{c_o} - \mathbf{w_f}$.

A Naive Solution

- Directly using $\mathbf{c_d}$ as $\mathbf{w_f}$
  - $\mathbf{c_f}$ has poor fidelity
- Find a noisy $\mathbf{w_f}$ but has high z_{lc} to $\mathbf{c_o}$.

A Better Solution

Using the Fourier transformation F:

- Project to Fourier bases:

$$\mathbf{c_d^1} = F\mathbf{c_d}.$$

- Scaling $\tilde{\mathbf{c}}_\mathbf{d}$ by a random diagonal matrix D into a random vector:

$$\mathbf{c_d^2} = D\mathbf{c_d^1}.$$

- Reconstruct it back:

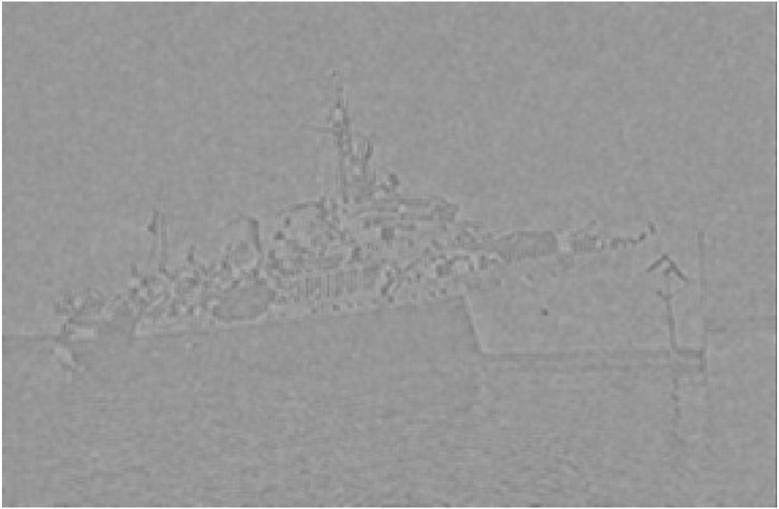
$$\mathbf{w_f} = F^T\mathbf{c_d^2}.$$

Check

$$
\begin{aligned}
\mathbf{w_f} \cdot \mathbf{c_o} &= (F^T D F)(\mathbf{c_d}) \cdot \mathbf{c_o} \\
&= \mathbf{c_o}^T (F^T D F) \mathbf{c_d} \\
&= (D^{1/2} F \mathbf{c_o})^T (D^{1/2} F (\mathbf{c_o} + \mathbf{w_r}) \\
&= \mathbf{c}'_{\mathbf{o}} \cdot \mathbf{c}'_{\mathbf{o}} + \mathbf{c}'_{\mathbf{o}} \cdot \mathbf{w}'_{\mathbf{r}} \\
&\approx \mathbf{c}'_{\mathbf{o}} \cdot \mathbf{c}'_{\mathbf{o}}.
\end{aligned}
$$

High correlation!

Illustration



More like noisy image, but not enough.

A Refinement

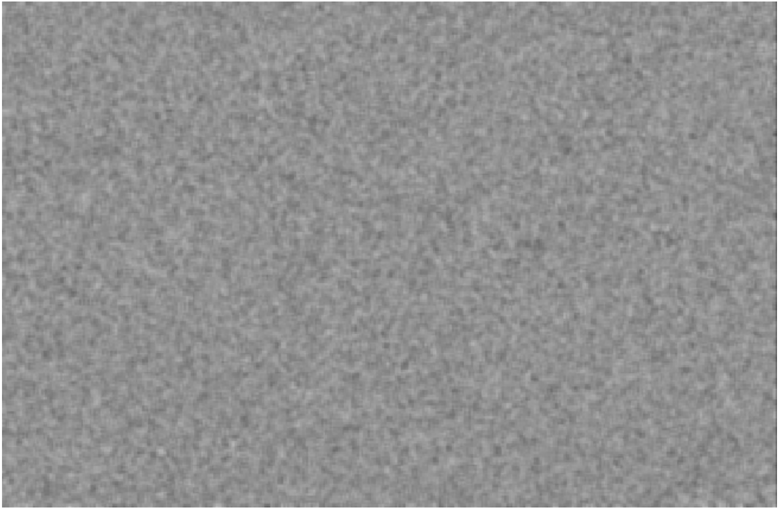
Add noise before applying Fourier transformation.

$$\mathbf{w_f} = (F^T D F)(\mathbf{c_d} + \mathbf{n}).$$

Check:

$$\begin{aligned}
\mathbf{w_f} \cdot \mathbf{c_o} &= (F^T D F)(\mathbf{c_d} + \mathbf{n}) \cdot \mathbf{c_o} \\
&= (D^{1/2} F \mathbf{c_o})^T (D^{1/2} F (\mathbf{c_d} + \mathbf{n})) \\
&\approx \mathbf{c_o'} \cdot \mathbf{c_o'} + \mathbf{c_o'} \cdot \mathbf{n'} \\
&\approx \mathbf{c_o'} \cdot \mathbf{c_o'}
\end{aligned}$$

Illustration



A noisy image, but high correlation to $\mathbf{c_o}$.

$\mathbf{c_f}$

$$\mathbf{c_f} = \mathbf{c_d} - 0.995\mathbf{w_f}.$$

Ownership

	$\mathbf{c_o}$	$\mathbf{c_d}$	$\mathbf{c_f}$
$\mathbf{w_r}$	-0.016	0.973	0.971
$\mathbf{w_f}$	0.968	0.970	0.005

Countering Ambiguity Attacks

Make the reference pattern dependent on $\mathbf{c_o}$.

- No $\mathbf{c_o}$, no reference pattern.

Using the md5 of the $\mathbf{c_o}$ as the seed of pseudo-noise generator.

- Adding a constraint: $\mathbf{w_r} = \text{PN}(\text{md5}(\mathbf{w_c}))$.
- Difficult to find a $\mathbf{w_f}$
  - $\mathbf{w_f} \cdot \mathbf{c_o}$ is high,
  - AND $\mathbf{w_f} = \text{PN}(\text{md5}(\mathbf{w_f}))$.