Digital Watermarking and Steganography

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

Chapter 6. Practical Dirty-Paper Codes

Lecturer: Jin HUANG

2015

6.1 Practical Considerations for Dirty-Paper Codes

Practical

- Efficiently find the closest code to:
  - The cover work.
  - The received work.
- High payload.

Efficient Encoding Algorithms

Low cost:

- Low distortion to the cover work.
  - Many different measurements: perceptual models.
- Efficiently in computation/searching.

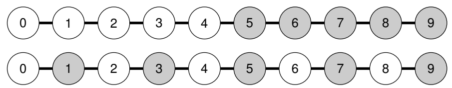
Efficient Decoding Algorithms

Good metric:

- Robust against some distortions: brightening etc.
- Efficiently in computation/searching.

Tradeoff between Robustness and Encoding Cost

- code separation: distance between different messages.
  - Larger for better robustness.
- coset formation: structure between codes for each message.
  - Good structure for efficient search, e.g. lattice.
  - Wide but close spacing for low cost.



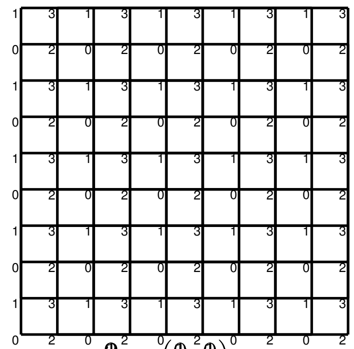
6.3 A Simple Lattice Code

N-Dimensional Lattice

N unit orthogonal basis $\mathbf{w}_{\mathbf{r}1}, \cdots, \mathbf{w}_{\mathbf{r}N}$

- Points in the lattice $\mathbf{p} = \sum_i k_i \mathbf{w}_{\mathbf{r}i}, k_i \in \mathbb{Z}$.
- A template sub-lattice $2\mathbf{w}_{\mathbf{r}1}, \cdots, 2\mathbf{w}_{\mathbf{r}N}$.
  - Points in the template sub-lattice:
    $$\sum_i k_i (2\mathbf{w}_{\mathbf{r}i}), k_i \in \mathbb{Z}.$$
  - Shifting it along bases according to $(b_1, \cdots, b_n), b_i \in \{0, 1\}$.
  - Points in the sub-lattice with message $(b_1, \cdots, b_n)$:
    $$\sum_i (b_i + 2k_i)\mathbf{w}_{\mathbf{r}i}.$$

Illustration



N-Dimensional Lattice

Can be 2^N messages

- Encoded as length N binary sequences.

How about use template sub-lattice $(h\mathbf{w}_{\mathbf{r}1}, \cdots, h\mathbf{w}_{\mathbf{r}N})$ for $h = 3$?

Embedding

Giving a vector $\mathbf{v}$ and a message $m = (b_1, \cdots, b_N)$:

- Project along each basis i:

$$p[i] = \frac{\mathbf{v}}{\|\mathbf{w}_{\mathbf{r}i}\|} \cdot \frac{\mathbf{w}_{\mathbf{r}i}}{\|\mathbf{w}_{\mathbf{r}i}\|}.$$

- Quantize to the nearest code (Book has error):

$$q[i] = 2\left\lfloor \frac{p[i] - b_i + 1}{2} \right\rfloor + b_i.$$

- Reconstruct

$$\mathbf{v}_m + = \sum_i (q[i] - p[i])\mathbf{w}_{\mathbf{r}i}.$$

Illustration

In one-dimensional case $\mathbf{w}_\mathbf{r} = 1$.

Encode message into 47:

m	p	q	$\mathbf{v}_m$
0	47	48	48
1	47	47	47

Detection

Giving a vector $\mathbf{v}$

- Project/Measure along ith basis:

$$p[i] = \mathbf{v} \cdot \mathbf{w}_{\mathbf{r}i}.$$

- Quantize to the nearest lattice point:

$$q[i] = \lfloor p[i] + 0.5 \rfloor.$$

- Decode the message:

$$m = (q[1] \bmod 2, \cdots, q[N] \bmod 2).$$

A Question

Why not

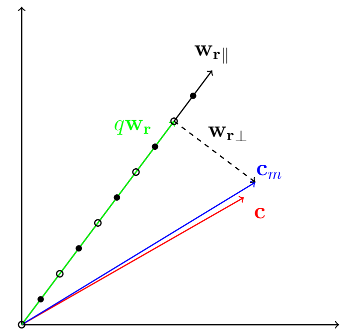
$$\mathbf{v}_m = \sum_i q[i]\mathbf{w}_{\mathbf{r}i}.$$

Number of basis is less than the dimension of $\mathbf{v}$.

Embedding one bit into 2 pixels $(7, 4)$ with $w_r = [0.6, 0.8]$.

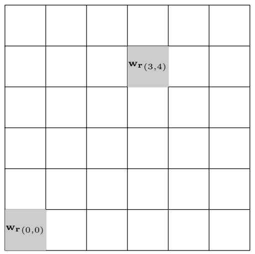
m	p	q	$\mathbf{v}_m$	$q\mathbf{w}_\mathbf{r}$
0	7.4	8	(7.36, 4.48)	(4.8,6.4)

Illustration



System 9: E_LATTICE/D_LATTICE

- N bits $(b_1, \cdots, b_N)$.
- N bases $\mathbf{w}_{\mathbf{r}1}, \cdots \mathbf{w}_{\mathbf{r}N}$.
  - Orthogonality by spatial division.



High Payload

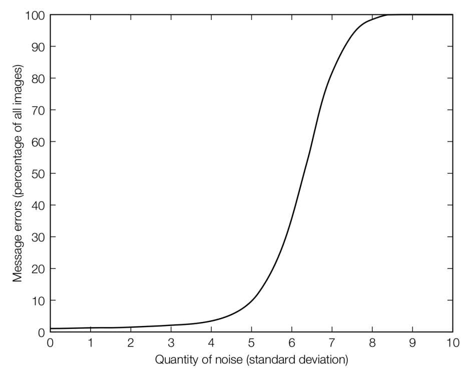
Indeed

- One block one bit.
- Or, N images N bit.

But we can use other way for orthogonality.

- Gram-Schmidt process.
- ...

Performance



Presentation: 8.3.1

- Basic idea of DCT
  - Kinds of Fourier transformation
- Watsons DCT-Based Visual Mode