5.2 Watermarking Using Side Information

Some Terrible Things for You

- Shannon's Theorem
- ...

Skip it.

5.3 Dirty-Paper Codes

Dirty-Paper Code

Classical notion of a code:

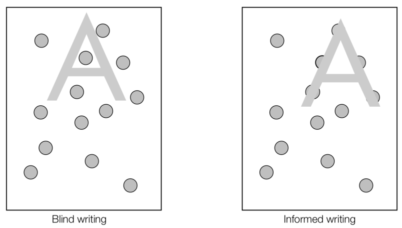
- One message, one code word.

Dirty-paper code

- One message, a set of candidate code words.

Find the code word fits best the host signal for a message.

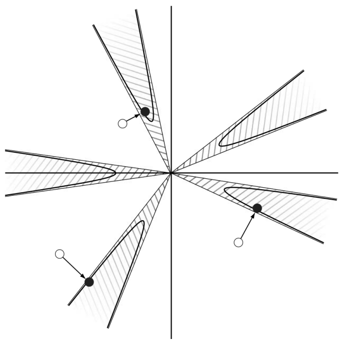
An Illustration



System 8: E_DIRTY_PAPER/D_DIRTY_PAPER

- Based on E_BLK_FIXED_R/D_BLK_CC
- TWO SETS of reference marks, $\mathcal{W}_0$ and $\mathcal{W}_1$, to encode ONE BIT of information.
- Embed 0: use the reference mark in $\mathcal{W}_0$
  - Has highest correlation with $\mathbf{v_o}$.
- Embed 1: use the reference mark in $\mathcal{W}_1$
  - Has highest correlation with $\mathbf{v_o}$.

Illustration



Performance

- False positive rate:

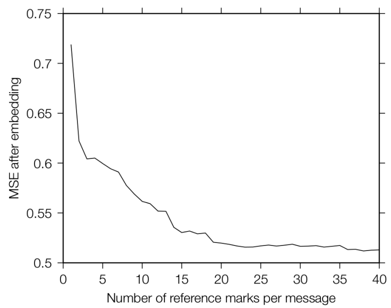
$$(|\mathcal{W}_0| + |\mathcal{W}_1|)P_{fp0}$$

  - Keep it constant: adjust numbers of reference marks and threshold.
- Constant payload (1-bit).
- Constant robustness.

Now why vary the number of reference marks?

- Fidelity.

Average Mean Squared Error



Limitation

The embedder and detector both use exhaustive search to find the best matches in $\mathcal{W}_0$ and $\mathcal{W}_1$, this system is only practical when the size of these sets is small.

Least significant bit (LSB) watermarking

Modify $\mathbf{c_o}$ so that the least significant bit encodes the message.

Embed 10000011

- Cover image $\Longrightarrow$ Watermarked image:

$$\begin{pmatrix} 00100111 \\ 11101001 \\ 11001000 \\ 00100111 \\ 11001000 \\ 11101001 \\ 11001000 \\ 00100111 \end{pmatrix} \Longrightarrow \begin{pmatrix} 00100111 \\ 11101000 \\ 11001000 \\ 00100110 \\ 11001000 \\ 11101000 \\ 11001001 \\ 00100111 \end{pmatrix}$$

Examples

1-bit

Examples

2-bit

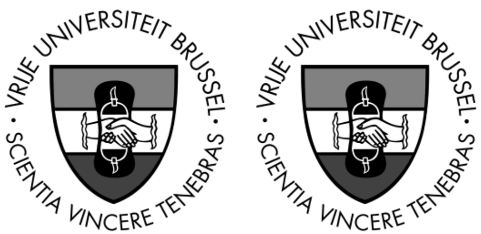
Examples

4-bit

Examples

6-bit

Examples



8-bit

Simple

Advantages

- High Payload
- Good fidelity for 1-bit only.

Drawbacks

- Not robust
- False positive probability?

Quantization Index Modulation

LSB is a QIM.

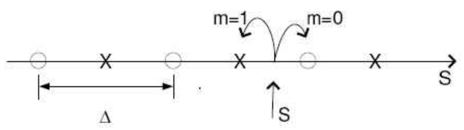
Separate the range of scalar into two sets

- even for 0
- odd for 1

Or in a 2-ary scalar watermarking, the code book $\mathcal{C}_0, \mathcal{C}_1$ are defined as

$$\mathcal{C}_m = \{(m + 2k) | k \in \mathbb{Z}, m \in \{0, 1\}\}\,. \qquad (1)$$

Illustration



The closest code.

Why Quantization?

From exhaustive search to simple rounding!

In General

For a M-ary scalar watermarking

- The code books $\mathcal{C}_m, m \in \{0, 1, \cdots, M-1\}$

$$\mathcal{C}_m = \{(m + kM)\Delta | k \in \mathbb{Z}\}.$$

- Embedding m into s: find k so that

$$\min_k |s - (m + kM)\Delta|.$$

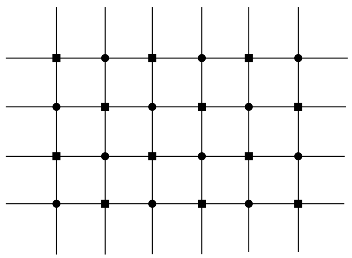
- Detection

$$[y/\Delta] \mod M.$$

Lattice Codes

From one dimension to two dimension

$$\mathcal{C}_0 = \{(k_1 + k_2) \mod 2 = 0\}$$
$$\mathcal{C}_1 = \{(k_1 + k_2) \mod 2 = 1\}.$$



More General

Binning scheme

- Hashing
- ...

Presentation: 8.2

General form of a perceptual model

Presentation: Project 1

- E_BLIND
- D_LC

The key points

- The tips
  - Scaling and shifting of the reference mark etc.
  - Noise from value clipping
    - Use low/high contrast image
- Performance: the plot of detection value
  - Using different reference mark
  - Using different cover work