Digital Watermarking and Steganography

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

Chapter 4. Basic Message Coding

Lecturer: Jin HUANG

2015

4.1 Mapping Messages into Message Vectors

Overview

One bit only to more complicated message.

- Source coding: maps messages into sequences of symbols.
  - Direct message coding
  - Code separation
- Modulation: maps sequences of symbols into physical signals.
  - Time-division multiplexing
  - Space-division multiplexing
  - Frequency-division multiplexing
  - Code-division multiplexing

Direct Message Coding

A unique, predefined message mark $w \in \mathcal{W}$ to represent each message $m \in \mathcal{M}$.

- One-one mapping: $|\mathcal{W}| = |\mathcal{M}|$.

Detector: maximum likelihood detection

- $w(m)$ with the highest detection value.

Design of $\mathcal{W}$

- False positive rate
- Fidelity
- Robustness
- ...

Code separation: far away from each other.

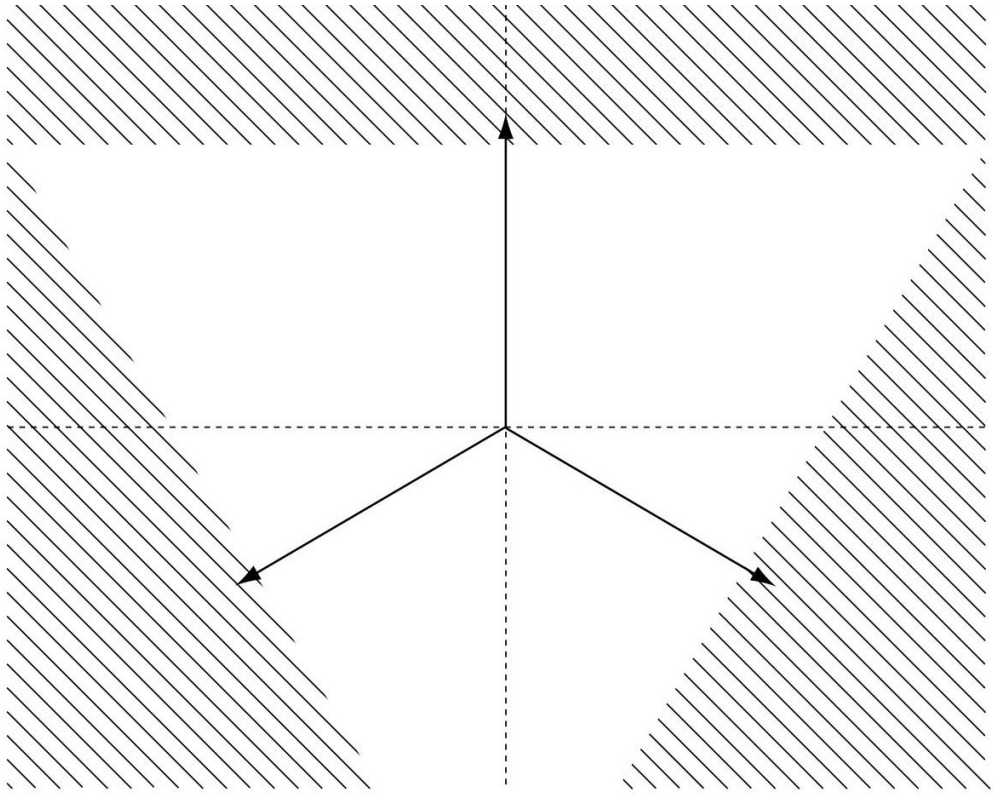
- To avoid confusion

Correlation in $\mathcal{W}$

- Low correlations with one another: good.
- Negative correlation with one another: better.
  - Embedding one **decreases** the other.
  - E.g. $m = \{0, 1\} \Rightarrow (2m - 1) = \{1, -1\}$.

More Messages

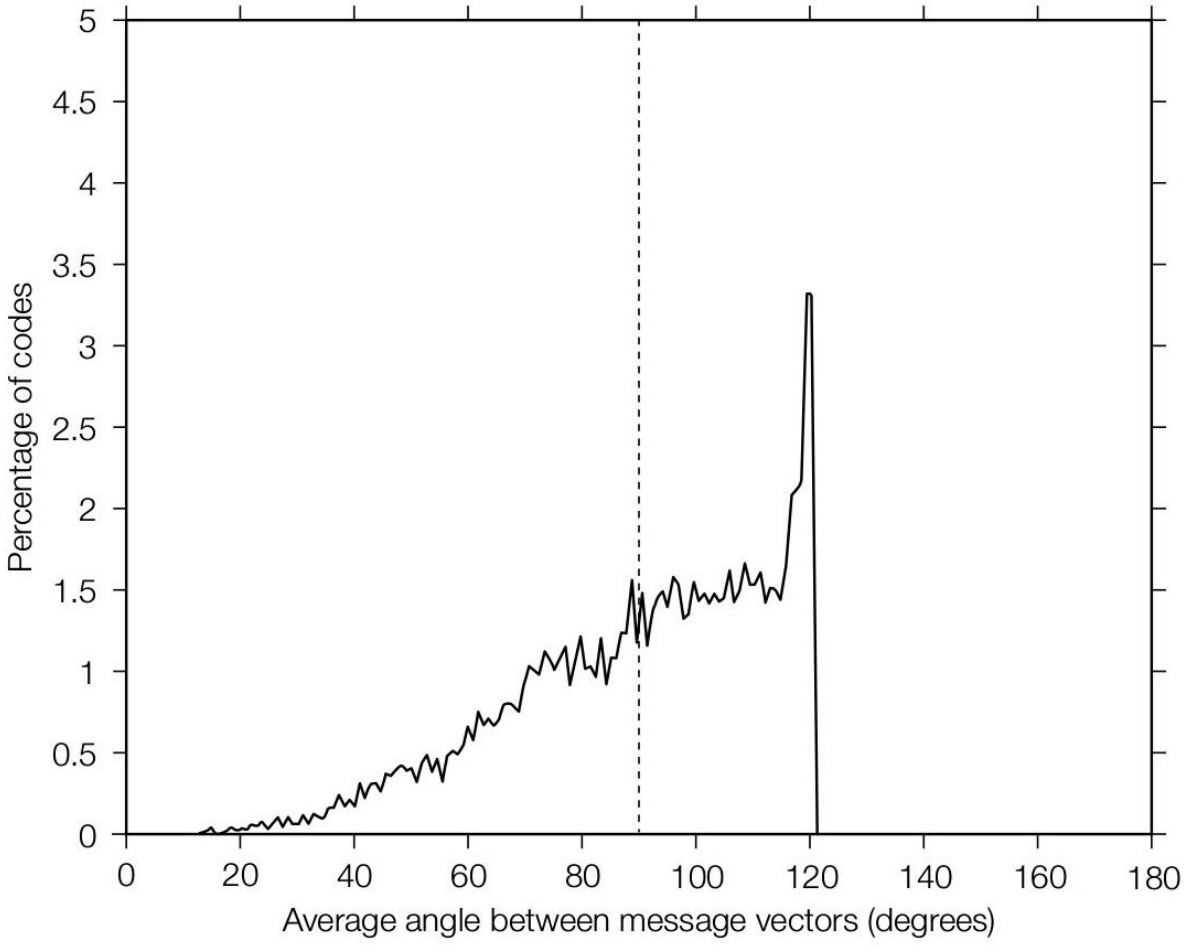
Placing $|\mathcal{M}|$ points on the surface of an N-dimensional sphere.



Three message mark vectors in a two-dimensional plane of marking space.

Low Dimension

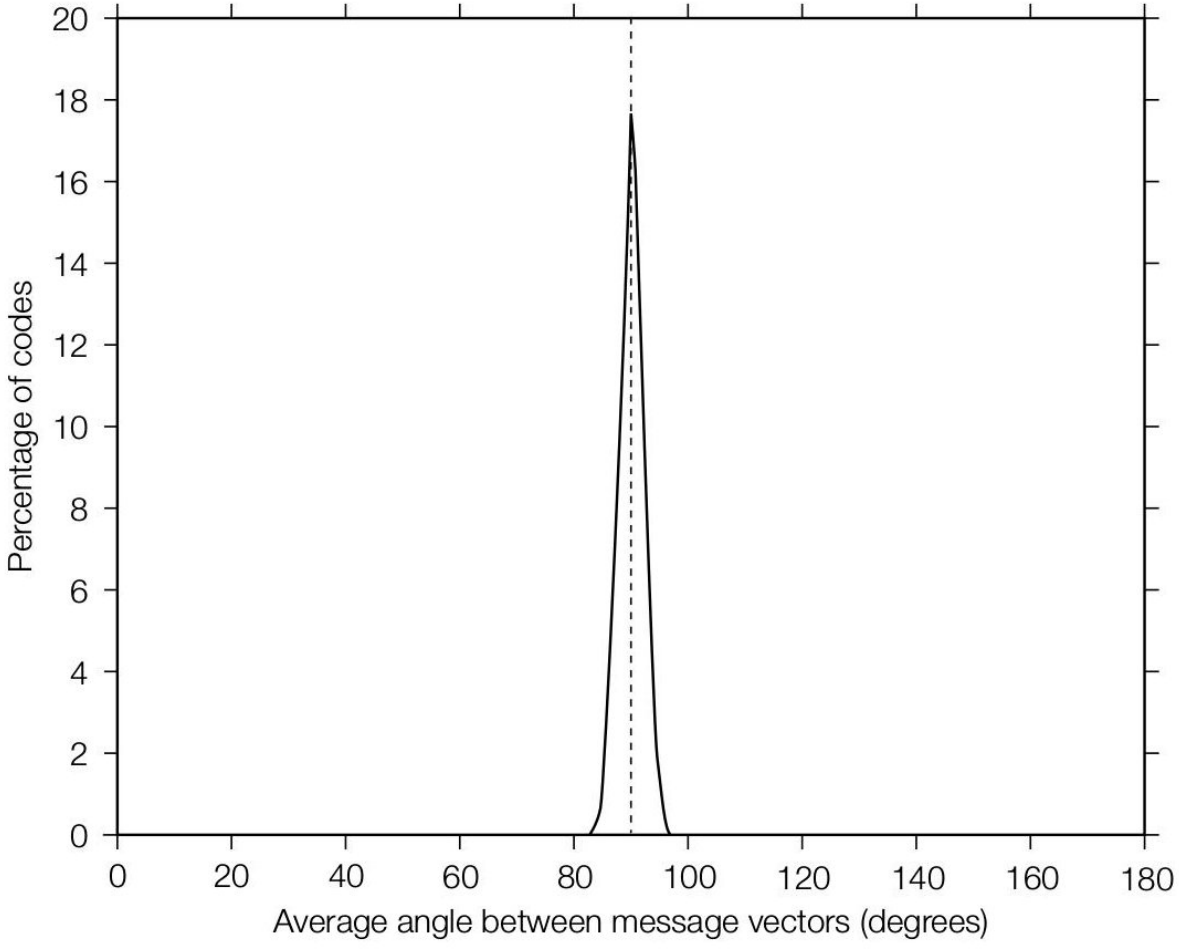
$N \leq |\mathcal{M}|$: randomly generated codes are good.



Three-message vectors in three-dimensional space.

High Dimension

$N \gg |\mathcal{M}|$: close to be orthogonal.

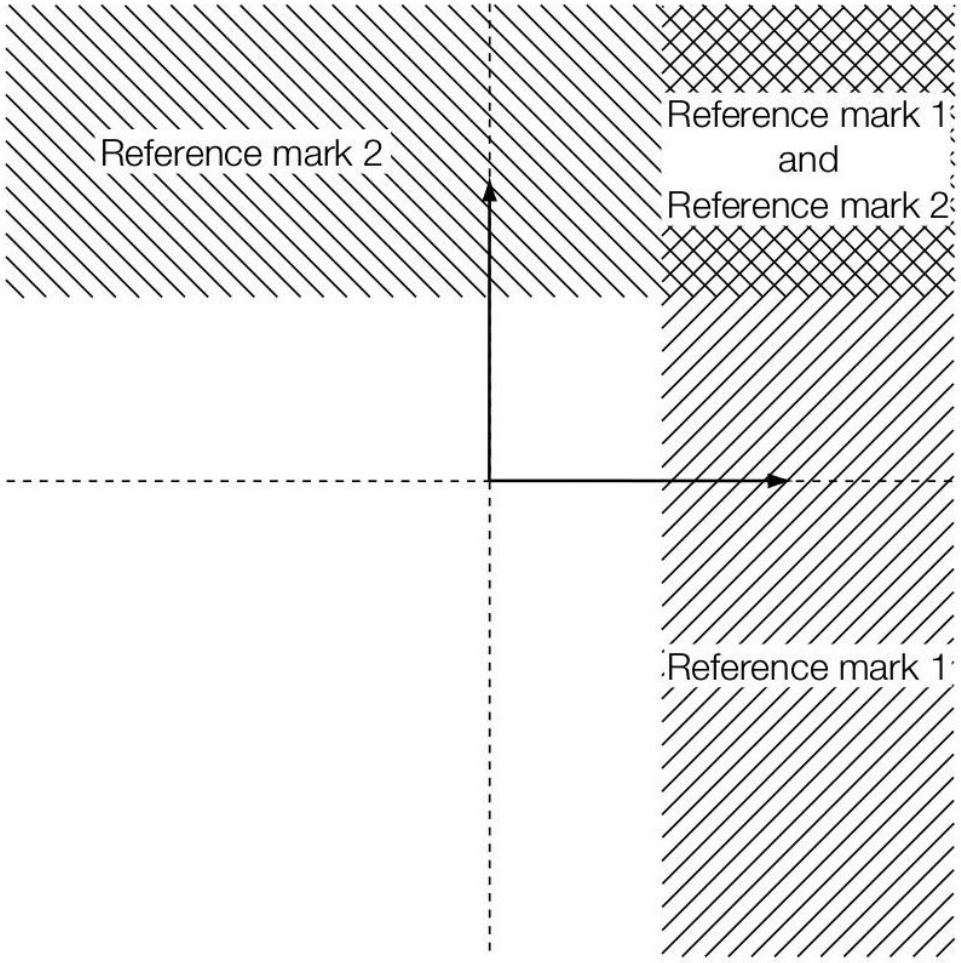


Three-message vectors in 256-dimensional space.

The Use of “Orthogonal”

Multiple messages in a work for

- Linear correlation.



Multisymbol Message Coding

Direct message coding is not efficient

- Detect for **all** marks.
- For a 16 bit information: 65536.
- Detector: compare with 65536 marks.

Multisymbol Message Coding!

Sequence of Symbols

Giving an alphabet $\mathcal{A}$, a length L **sequence**:

- $|\mathcal{A}|^L$ different messages.
- Sequence: the order is important!
- Direct message coding: $L = 1$.

16 bit information

- $|\mathcal{A}|^1 = 65536$ for direct message coding.
- $|\mathcal{A}|^8 = 65536$ for 4-symbol 8-length coding.
  - For each index/order: compare with 4 marks.

The Index/Order

- Time-division multiplexing
- Space-division multiplexing
- Frequency-division multiplexing
- Code-division multiplexing

Time- and Space-Division Multiplexing

Divide the work into disjoint regions

- In space or time
- One symbol in each part.

Samples: A length 4 sequence.

- Audio: 4 clips in $1/4$ length.
- Image: 4 blocks in 2×2 layout.

Frequency-Division Multiplexing

Disjoint bands in the frequency domain

- One symbol in each band.
- Frequency domain
  - Basis $\Phi[i]$: $\mathbf{f} = \sum_i \mathbf{x}[i]\Phi[i] = \Phi\mathbf{x}$.
  - Decomposition: $\mathbf{x} = \Phi^{-1}\mathbf{f}$.
  - Marking space
    - via a linear transformation $\mathcal{T}$ from media space.

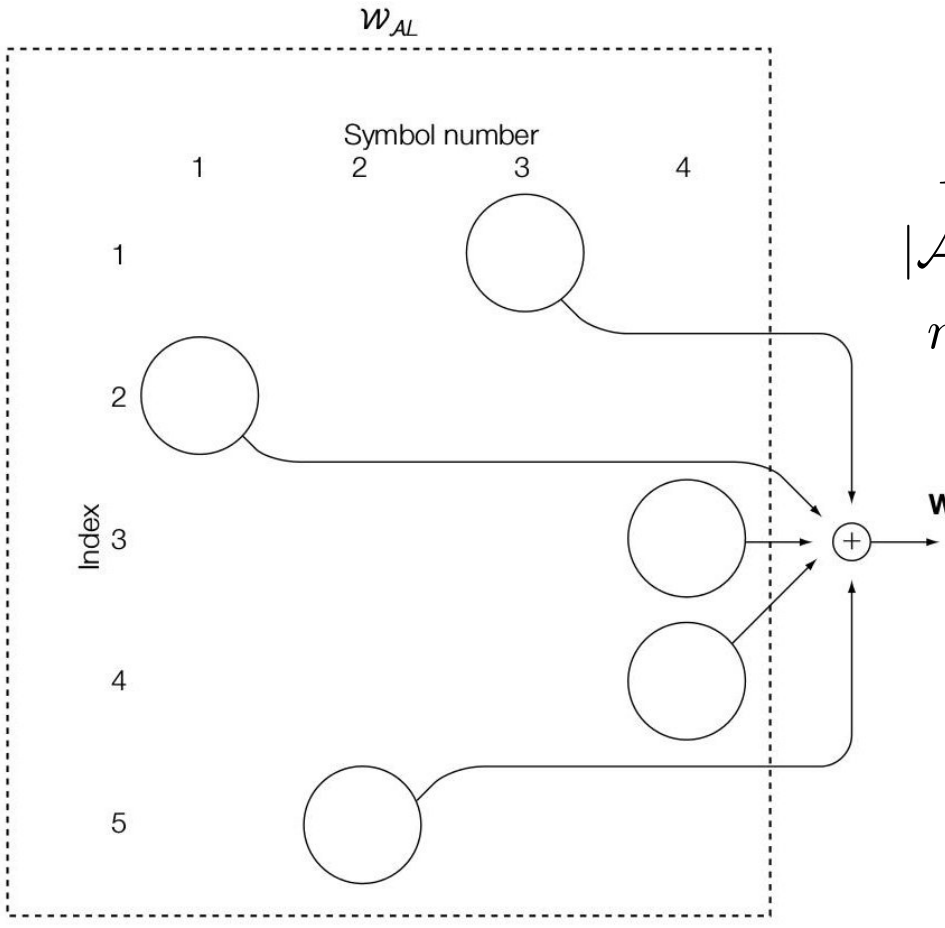
Samples:

- Audio: Fourier Transform
- Image: Discrete Cosine Transform

Code-Division Multiplexing

A table $\mathcal{W}_{\mathcal{AL}}$ in index and alphabet.

- $L \times |\mathcal{A}|$ reference marks.



$$
\begin{aligned}
L &= 5 \\
|\mathcal{A}| &= 4 \\
m &= \text{“31442”} \\
&\Longrightarrow \\
\mathbf{w}_m &= \mathcal{W}_{\mathcal{AL}}[1,3] \\
&\quad + \mathcal{W}_{\mathcal{AL}}[2,1] \\
&\quad + \mathcal{W}_{\mathcal{AL}}[3,4] \\
&\quad + \mathcal{W}_{\mathcal{AL}}[4,4] \\
&\quad + \mathcal{W}_{\mathcal{AL}}[5,2].
\end{aligned}
$$

Requirements on $\mathcal{W}_{\mathcal{AL}}$

Marks in $\mathbf{w}_m$:

- $m[i]$ and $m[j]$ have little correlation.
  - Close to orthogonal: concurrent presence.

$$\mathcal{W}_{\mathcal{AL}}[i,a] \cdot \mathcal{W}_{\mathcal{AL}}[j,b] \to 0, \text{if } i \neq j.$$

- Only one symbol in a index.
  - Negative correlation: distinguishable.

$$\mathcal{W}_{\mathcal{AL}}[i,a] \cdot \mathcal{W}_{\mathcal{AL}}[i,b] \to -1, \text{if } a \neq b. \qquad (1)$$

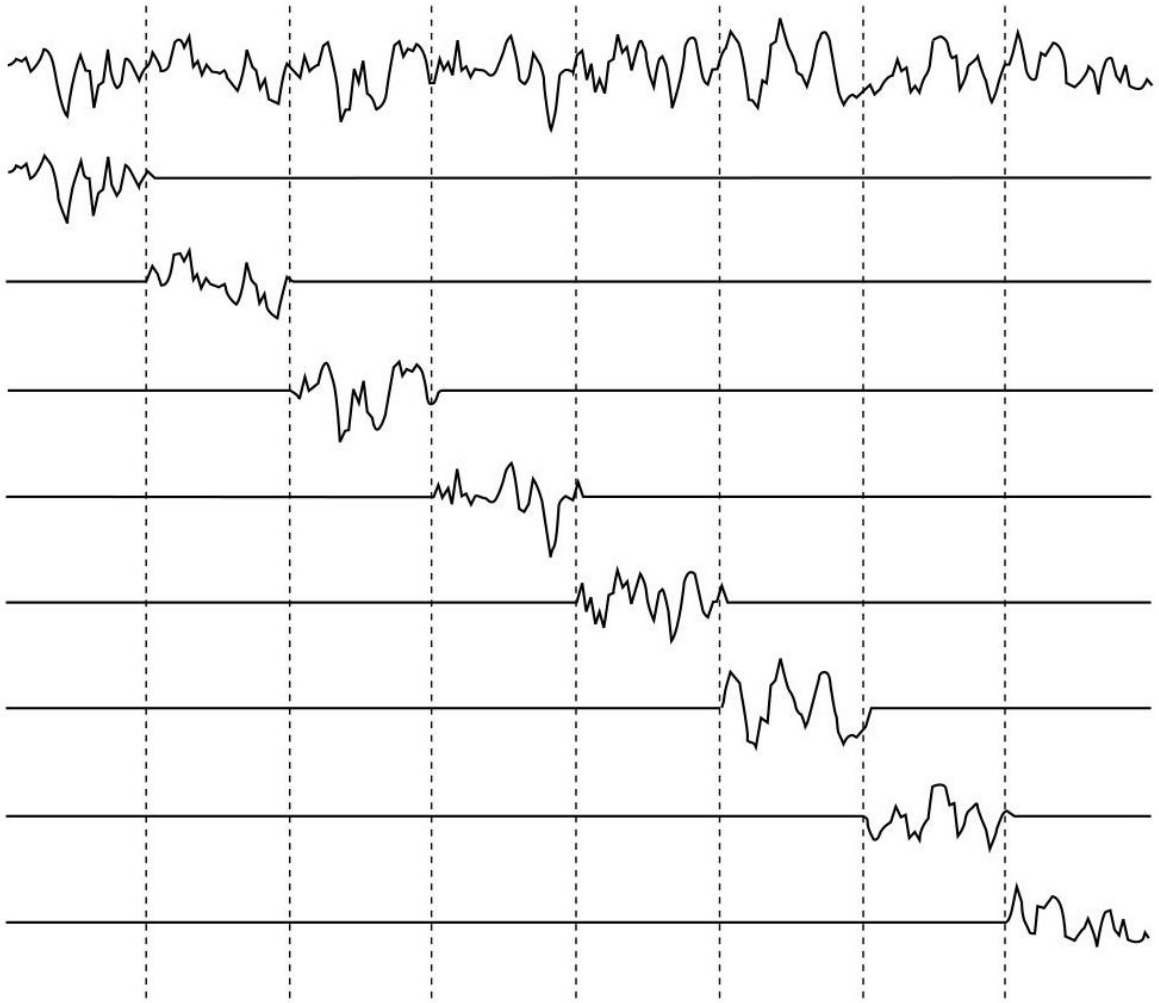
Distortion via shifting Δ

- Low cross-correlations

$$\mathcal{W}_{\mathcal{AL}}[i,a] \cdot \mathcal{W}_{\mathcal{AL}}[j+\Delta,b] \to 0, \text{if } i \neq j.$$

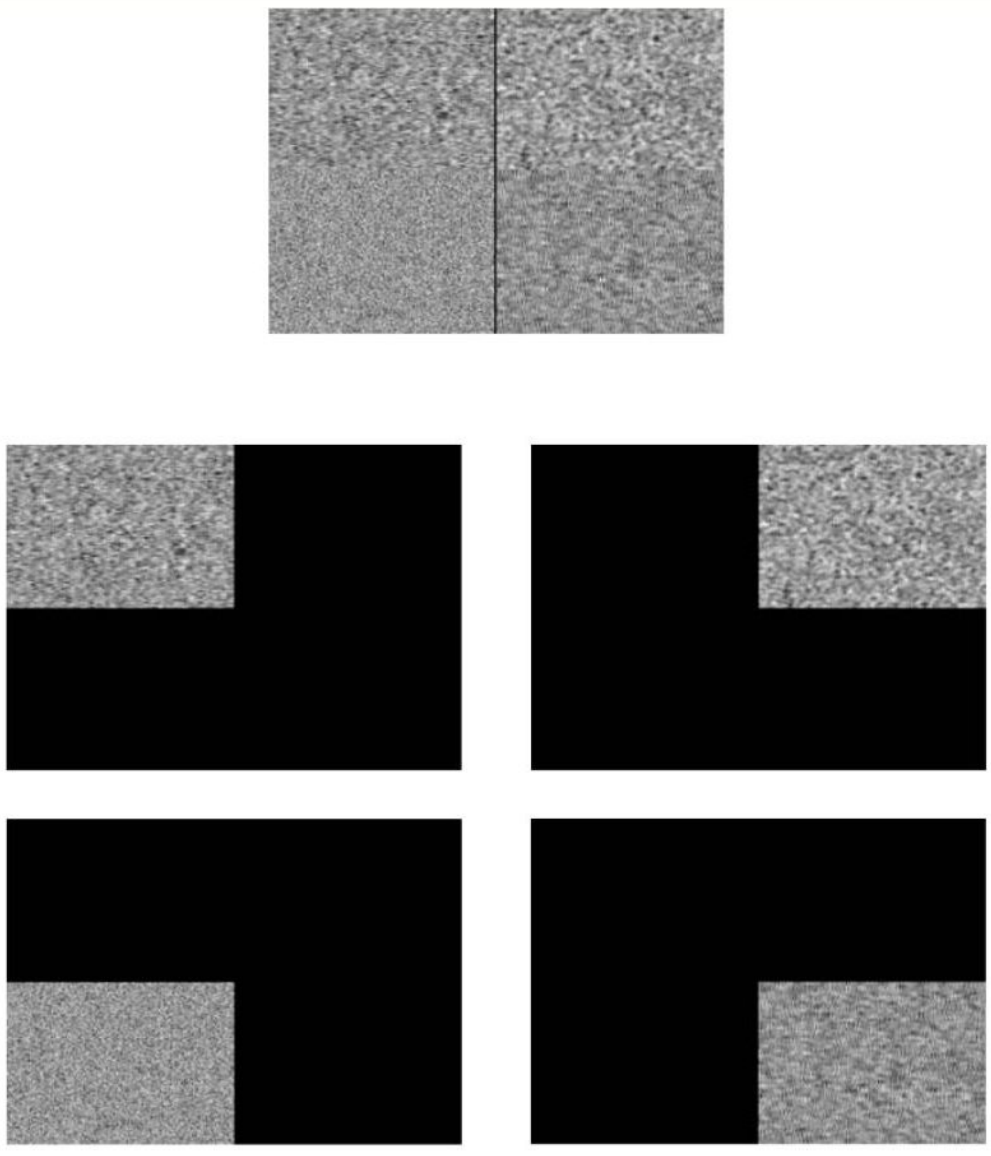
Equivalence to Time-Division

Pad the marks with zeros



Equivalence to Space-Division

Pad the marks with zeros



Equivalence to Frequency-Division

Convert symbols in each band back to the temporal or spatial domains.

If the transform is linear:

- Overlap in time or space.
- But zero correlation.

E_SIMPLE_8/D_SIMPLE_8 1

8-bit integer: length 8 binary string, $L = 8, |\mathcal{A}| = 2$.

- At each position
  - Distinguishable: negative correlation.
  - $\mathcal{W}_{\mathcal{AL}}[i, 1] = \mathbf{w}_{ri} = -\mathcal{W}_{\mathcal{AL}}[i, 0]$.
- Among positions
  - Gaussian distributions with zero mean.
- Normalize $\mathbf{w}_m$ to unit length.

E_SIMPLE_8/D_SIMPLE_8 2

Embedder

- $\mathbf{c}_w = \mathbf{c}_o + \alpha \mathbf{w}_m$

Detector

- For each i: check $\mathbf{w}_{ri}$.
- If is not watermarked
  - The output message is random. *read 4.3*

Performance

6 8-bit integers in each of 2000 images.

- Larger embedding strength $\alpha = 2$.
  - The message pattern is scaled to have unit standard deviation, thus $\alpha/\sqrt{8}$.
- 26 out of 12000 are wrong: confused by $m_a, m_b, a \neq b$.
- Reason:
  - Maximum correlation between two different message vectors is high.

Presentation: Hamming

- Hamming distance.
- Hamming code.
- Strategy of using Hamming code in watermark