Performance

- Without ECC
  - Length 4, 1 bit difference for different message.
  - Min inner product: $N(4 - 2 \times 1) = 2N$.
- With ECC
  - Length 7, at least 3 bit differences for different message.
  - Min inner product: $N(7 - 2 \times 3) = N$.

Expand the Alphabet

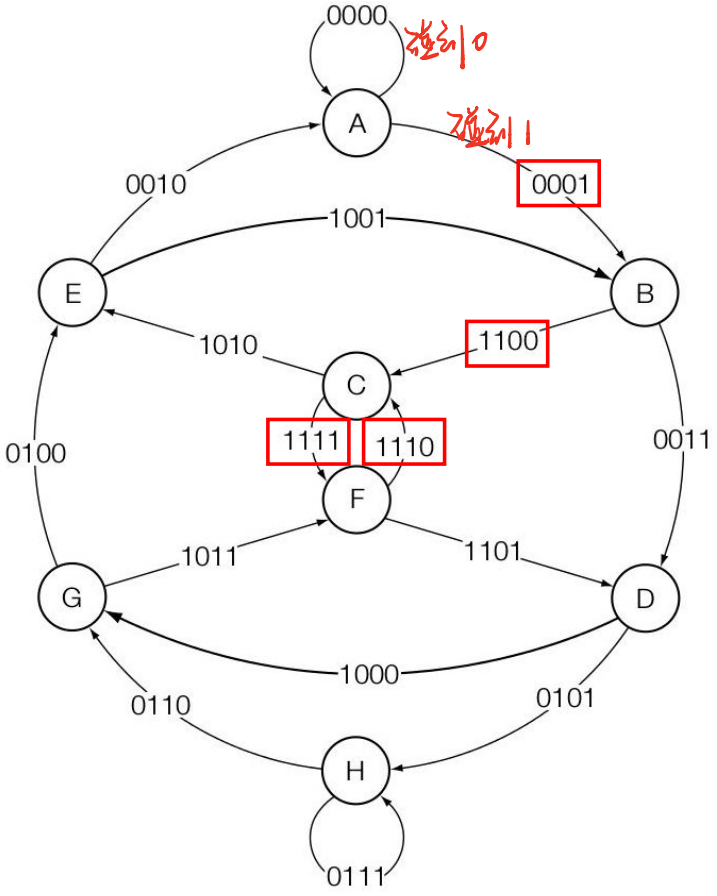
From $|\mathcal{A}| = 2$ to $|\mathcal{A}'| = 4$.

- Less typical.
- Equivalent to increase length in capacity.
- But different in modulation.

Trellis Codes

$$1010 \Rightarrow 0001\ 1100\ 1111\ 1110$$

State machine



4bit ⇒ 16 bit

Trellis-coded Modulation

- Summing L symbols (watermarking keys).
  - Zero correction: random in high dimensional space.
- Expand the alphabet to $2^4 = 16$ symbols.
  - Negative correction: uniformly distribute 16 points on a sphere.

Convolutional Coding

- Trellis code is a special convolutional code.
  - Not blocks of message+parity.
  - A sequence of parity.
  - Message is reconstructed from the parity in a **slicing** window.
    - The windows are overlapped.
    - Each time, slide one bit.

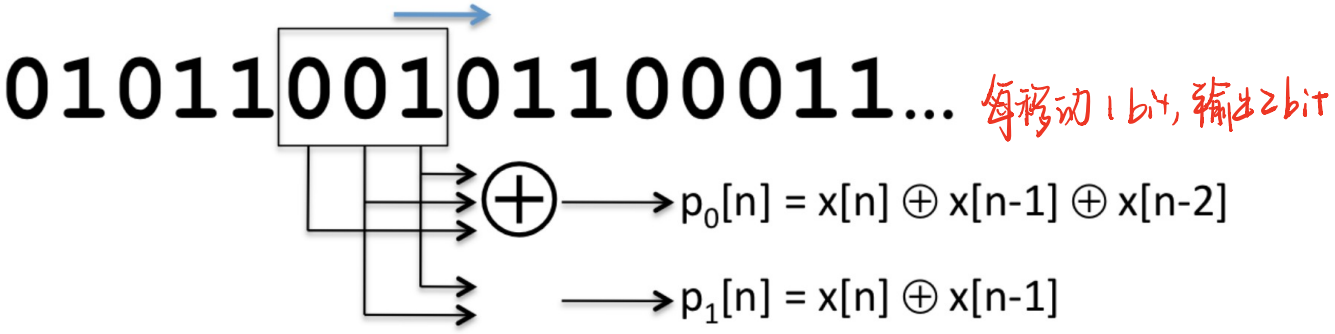
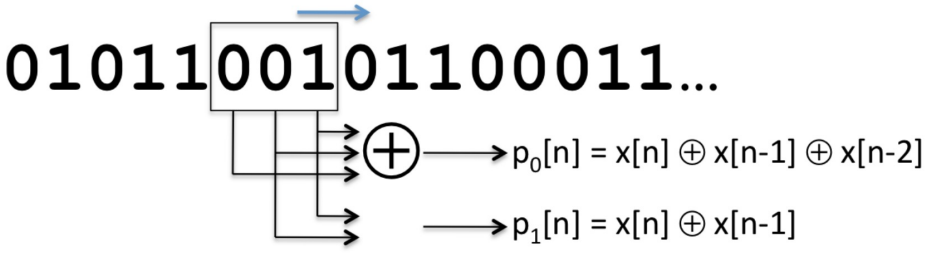
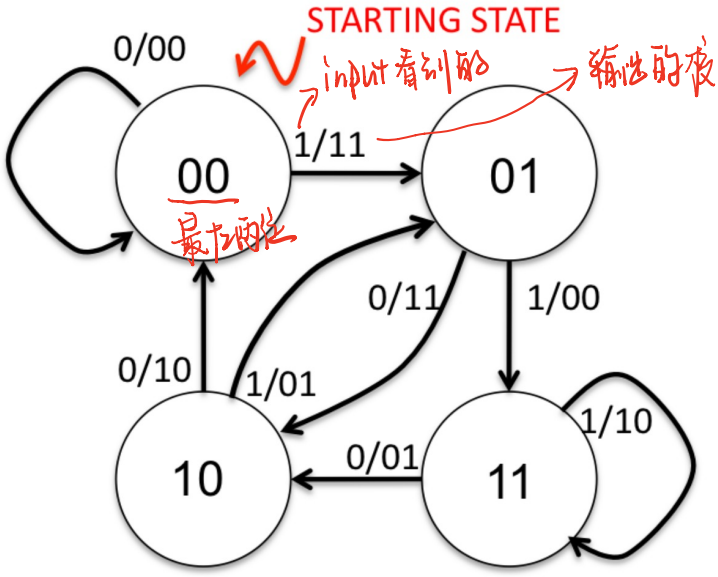


Illustration of Convolutional Code



可视会考.

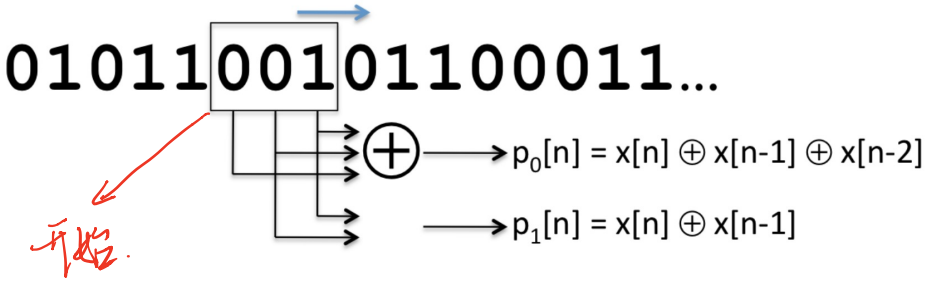
在每一种 parity 条件下都会生 trellis code.

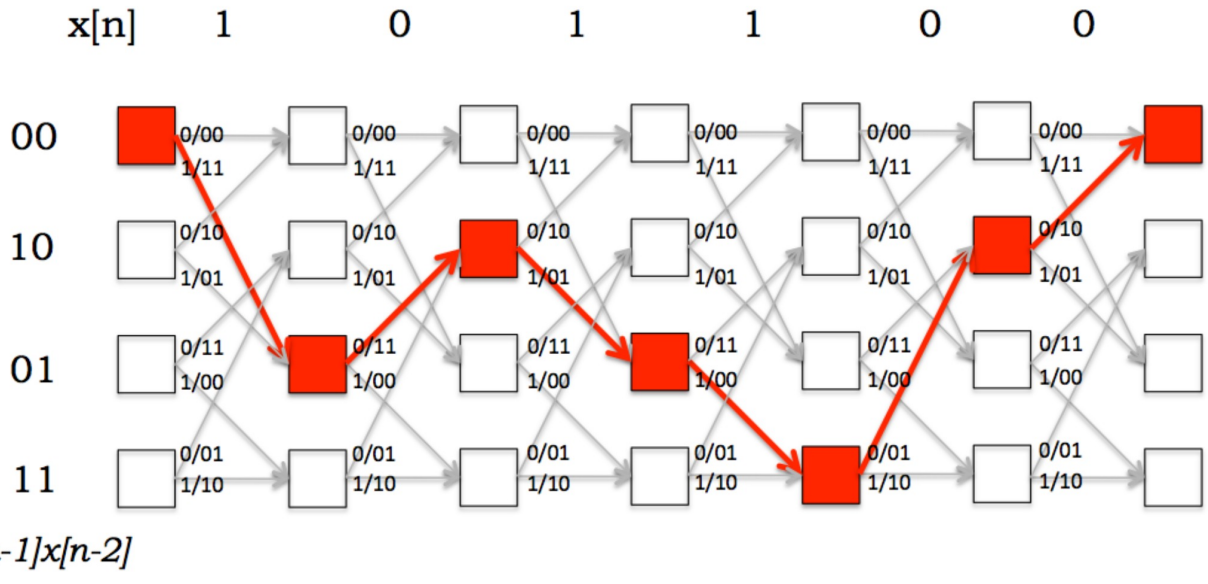


input 看到的

输出的校验位 $P_0[n]$, $P_1[n]$

Illustration of Convolutional Code

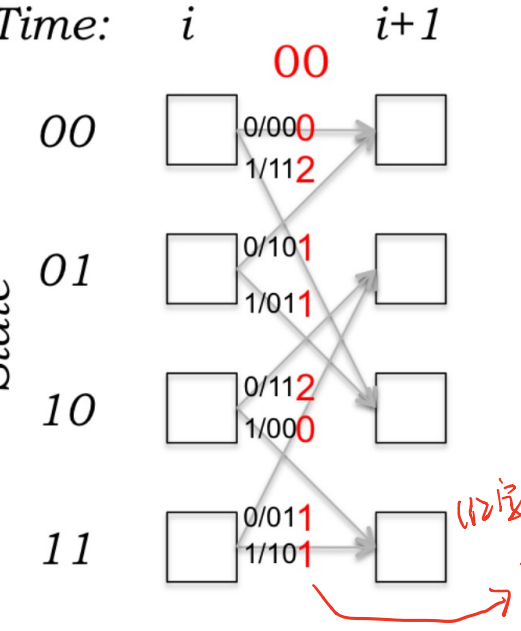




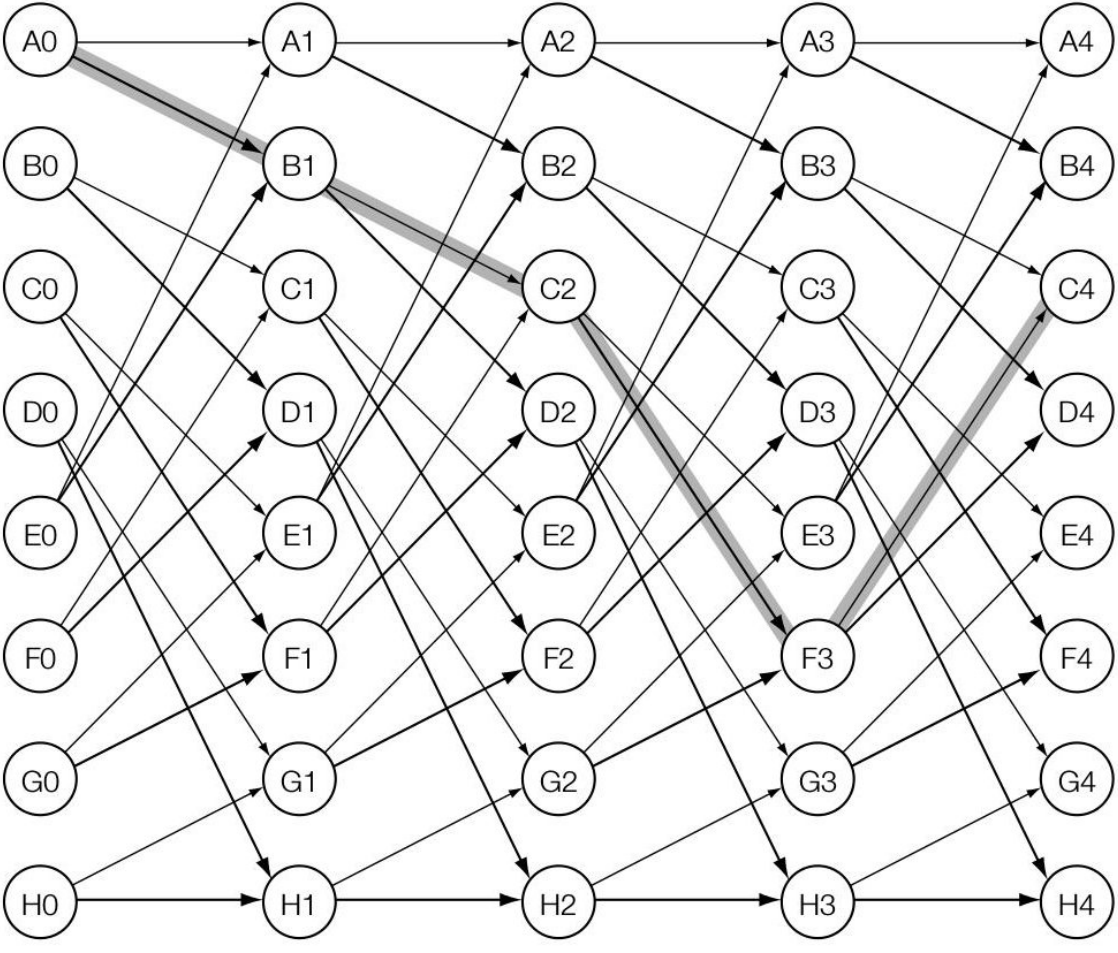
Viterbi Decoding

- Find most closest code (most-likely path).
  - dynamic programming (not exhausting search).
  - Add branch metric B into path metric P.

$$P(s, i+1) = \min(P(\alpha, i)+B(\alpha, s), P(\beta, i)+B(\beta, s)).$$



Trellis Diagram in Book



Performance of E_TRELLIS_8/D_TRELLIS_8

The same to E_SIMPLE_8/D_SIMPLE_8:

- 8-bit message instead of 4-bit.
  - Pad two more zero at the end: 10-bit indeed.
  - More redundancy: a priory for accuracy.
- 6 integers in each of 2000 images.

Much better accuracy

- 1 out of 12000 is wrong.

4.3 Detecting Multisymbol Watermarks

False Positive

If there is no watermark

- Direct message encoding
  - The most likely one is still poor in correction.
- Multisymbol system:
  - The corrections for all the symbols are not good enough.
  - How to define “good”.

trellis code 纠错功能会使无水印也变有水印.

Valid Messages

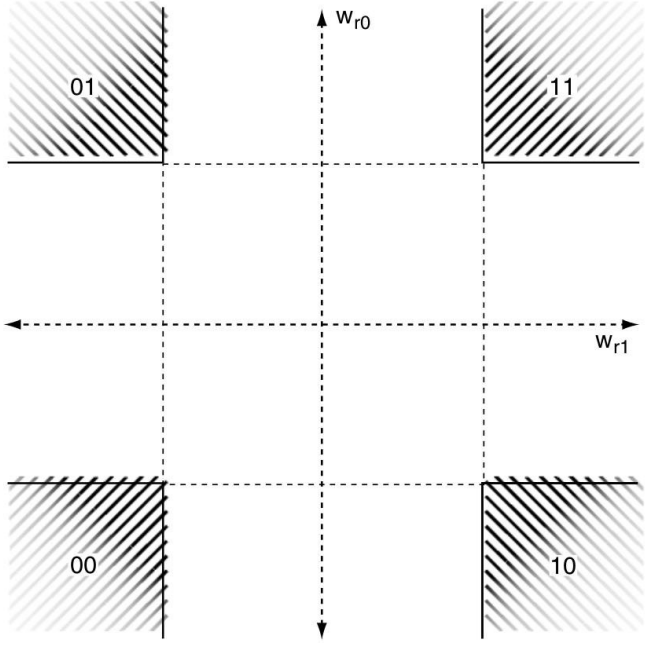
An intelligible message or a garbage.

- Checksum for verification
  - 16-bits message: m.
  - 9-bits checksum: $c = m[1:8] + m[9:16]$.
  - 25-bits watermarking: (m, c). 降低 fpr
- Detector
  - Extractor 25-bits watermarking (m, c). 会丢纠错 ECC. 可以 trellis pad 会降低 fpr.
  - Compare c and $m[1:8] + m[9:16]$.
- False positive probability: $P_{fp} = \frac{1}{2^9}$.

Individual Symbols 1

All symbols are reliable (high correlated).

- Watermark presence.



2-bit system in linear correlation.

Individual Symbols 2

False positive probability

- Single reference mark: P_{fp0}.
- In each index/position/order
  - If one mark in $\mathcal{A}$

$$P_{fp1} \approx |\mathcal{A}| P_{fp0}.$$

- For the whole length L sequence.
  - All of them is high

$$P_{fp} = (P_{fp1})^L \approx (|\mathcal{A}| P_{fp0})^L.$$

Normalized Correlation 1

- Multiple-symbol embedding 归一化后内积
  - $\mathbf{w}_{ri}$ orthogonal to each other and unit.

$$\mathbf{v}_L = \mathbf{v}_o + \sum_{i=1}^{L} \mathbf{w}_{ri}, \quad \|\mathbf{v}_L\| \approx \sqrt{L}.$$

在marking space. (前面有个N8是这个原因).

  - Linear correlation: independent of L 与L无关

$$z_{lc}(\mathbf{v}_L, \mathbf{w}_{r1}) = \mathbf{v}_o \cdot \mathbf{w}_{r1} + \mathbf{w}_{r1} \cdot \mathbf{w}_{r1} = \varepsilon + 1.$$

  - Normalized correlation: difficult for larger L

$$z_{nc}(\mathbf{v}_L, \mathbf{w}_{r1}) = \frac{\mathbf{v}_L}{\|\mathbf{v}_L\|} \cdot \mathbf{w}_{r1} = \frac{\varepsilon + 1}{\sqrt{L}}.$$

与L有关

已单位化

会再小pr.

Normalized Correlation 2

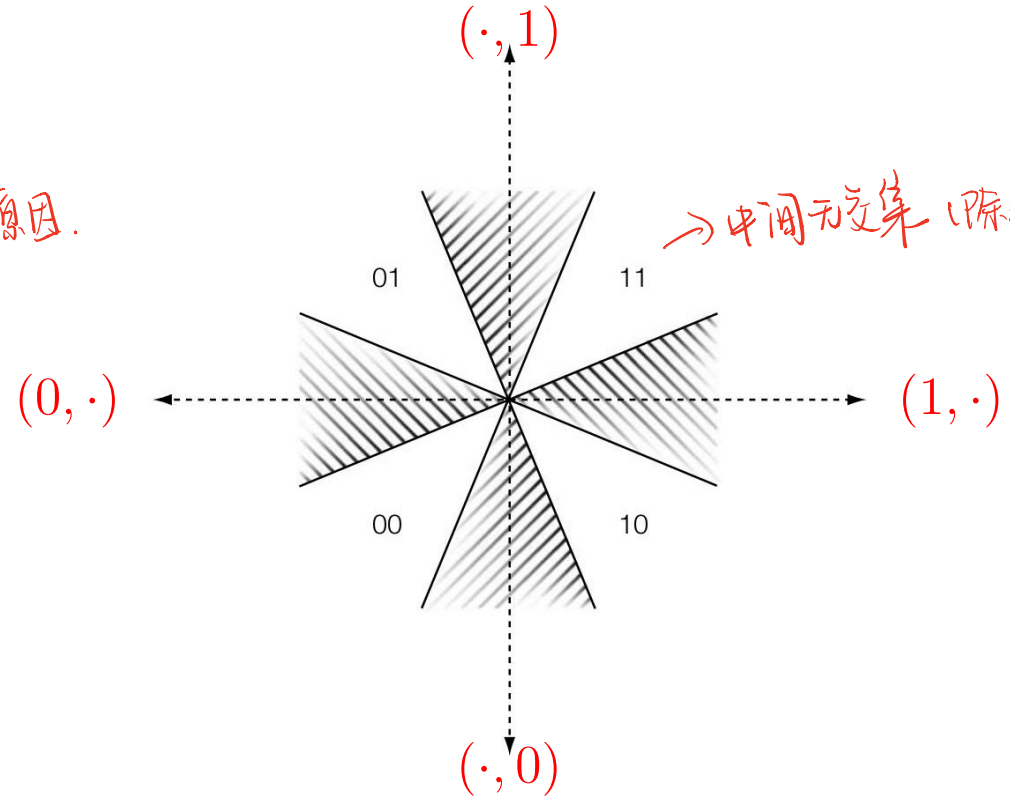
Less distinguishable.

- Large threshold: none is correlated enough, no symbol found.
- Small threshold: High false positive probability.

Geometric Interpretation

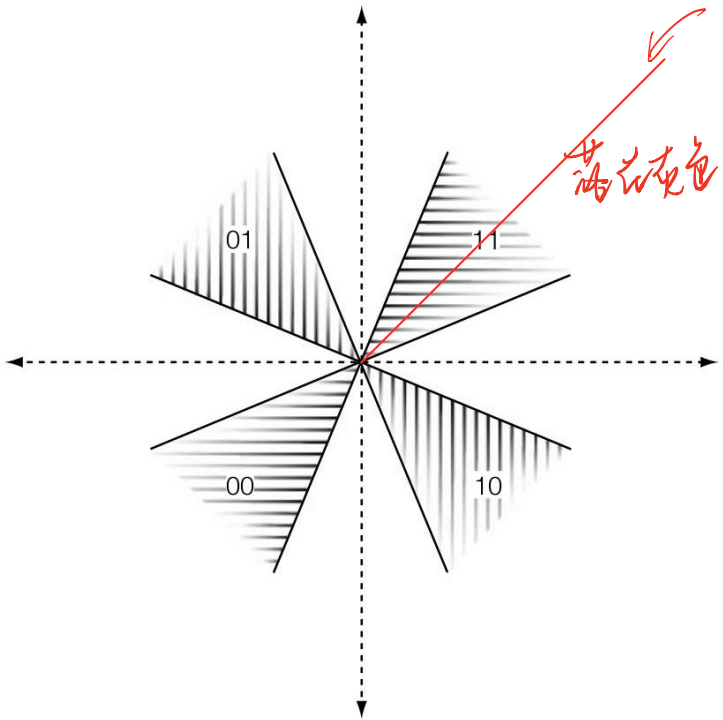
Large threshold: no overlap for the cones.

- No detectable 2-bit message.



Reencode

1. Extract message m.
2. Reencode m into mark $\mathbf{v}_m$.
3. Test the presence of $\mathbf{v}_m$



False Positive Probability

When the detection regions for the different messages do not overlap,

$$P_{fp} = |\mathcal{M}| P_{fp0}.$$

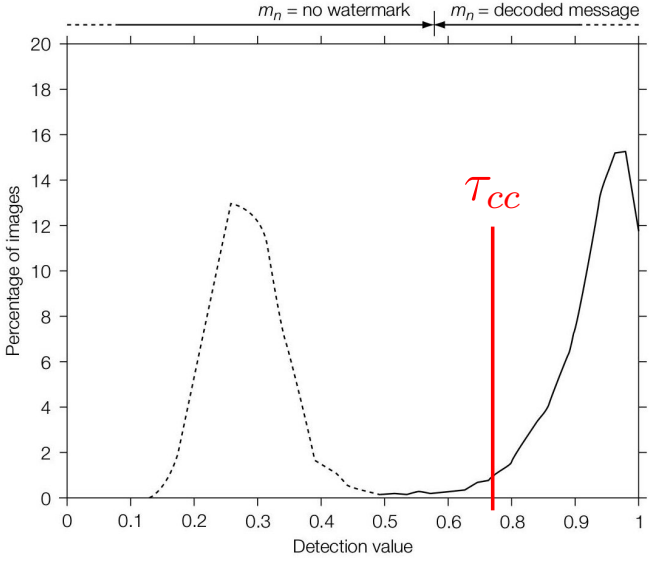
E_BLK_8/D_BLK_8

8-bit message:

- Trellis code with two padding 0 at the end.
  - A sequence of 10 symbols drawn from a 16-symbol alphabet.
- Reference marks:
  - 8×8 (block): low dimensional mark space.
    - So choose seed to reduce max correlation (0.73).
- Embedding strength $\alpha = 2$.
- $\tau_{cc} = 0.65$: false positive probability 10^{-6}.

Performance

- 2000 unwatermarked images (dashed line).
  - No false positive found.
- 12000 watermarked images (solid line).
  - 6 messages $\times 2000$ images.
  - 109 fail: effectiveness 99%.



Project: System 6

E_BLK_8/D_BLK_8

- Marking space: 8×8 block.
- 8-bit message.
- ECC: hamming or optional.
- Reencode check.
- z_{cc}.

Presentation: 7.6 Analysis of Normalized Correlation

Approximate Gaussian Method

- False Positive Analysis
- False Negative Analysis