3.4 Geometric Models of Watermarking

Points in Space

- Media space 点 ⟺ work
  - A point corresponds to a work.
- Marking space
  - Projections or distortions of media space.
    - histogram etc.

Regions and Distributions

- Distribution of unwatermarked works
- Region of acceptable fidelity
- Detection region
- Embedding distribution (embedding region)
- Distortion distribution

Distributions and Regions

像素数量，位深

N dimensional space for **EACH** work.

- Monochrome images with N pixels: N.
- 24bit RGB images with N pixels: $24N$.
- N frames video clip: $N \times \ldots$
- ...

Assume to be continuous.

Distribution of Unwatermarked Works

- Very different statistical distributions
  - Audio: song, nature, speech ...
  - Images: X-ray, photo, cartoon ...
  - Video: scene, sports, movie ...
- Useful for false positive rate ← 定义边界.（做不到的）
  - A priori of content: it is not likely a watermark.
- Statistical Models:
  - Elliptical Gaussian
  - Laplacian or generalized Gaussian
  - Random, parametric processes

Region of Acceptable Fidelity

Is the modified work still like the original one?

- Depends on human perception
  - Difficult to accurate model.
  - Just noticeable difference (JND).
- Approximate by mean squared error (MSE)

$$D_{\textsf{mse}}(\mathbf{c}_1, \mathbf{c}_2) = \frac{1}{N}\|\mathbf{c}_1 - \mathbf{c}_2\|^2.$$

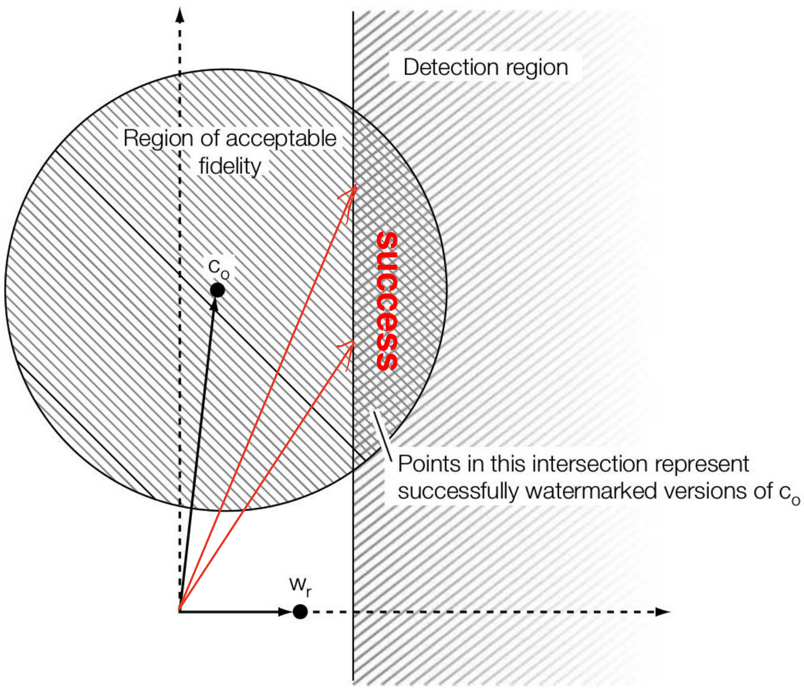
$$D_{\textsf{snr}}(\mathbf{c}_1, \mathbf{c}_2) = \frac{\|\mathbf{c}_1 - \mathbf{c}_2\|^2}{\|\mathbf{c}_1\|^2}.$$

A ball around the original point.

Detection Region

From the view point of detector

- Works containing the watermark
- For D_LC: $\tau_{lc} < |z_{lc}(\mathbf{c}, \mathbf{w}_r)| = |\mathbf{c} \cdot \mathbf{w}_r|/N$.



Embedding Distribution or Region

The region (probability) of watermark embedder output for all the unwatermarked works (according to the distribution).

- Every point is possible: E_BLIND.
  - Even those outside the detection region.
- Only in detection region: E_FIXED_LC.

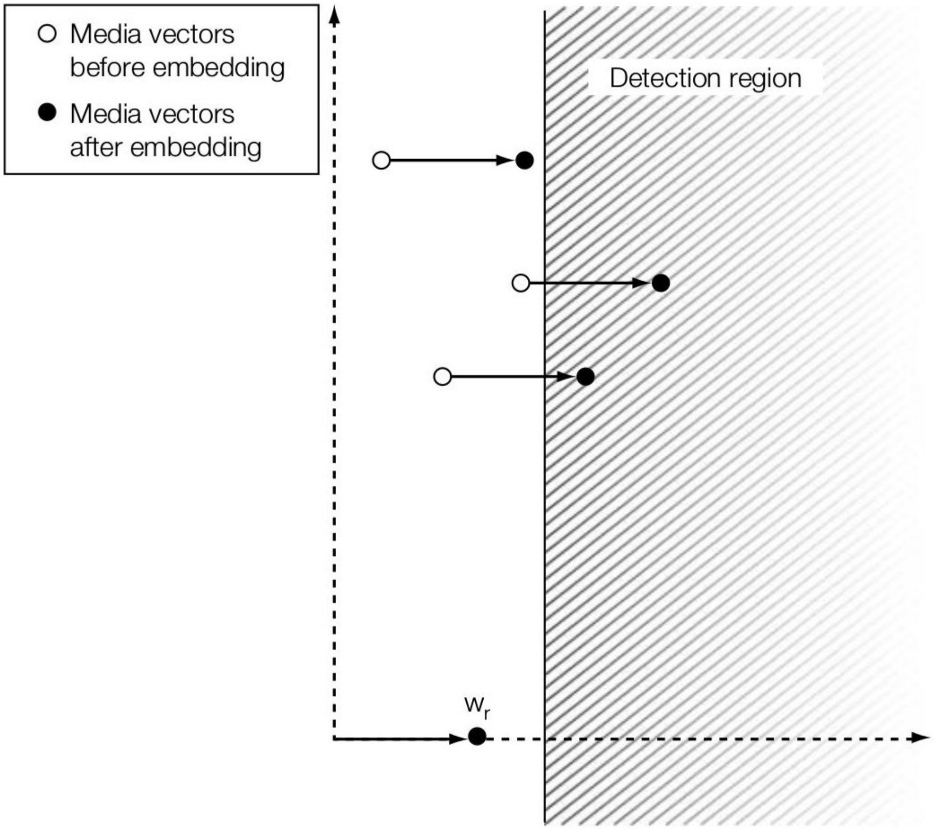
100% effectiveness

$\Longleftrightarrow$

embedding region $\subset$ detection region.

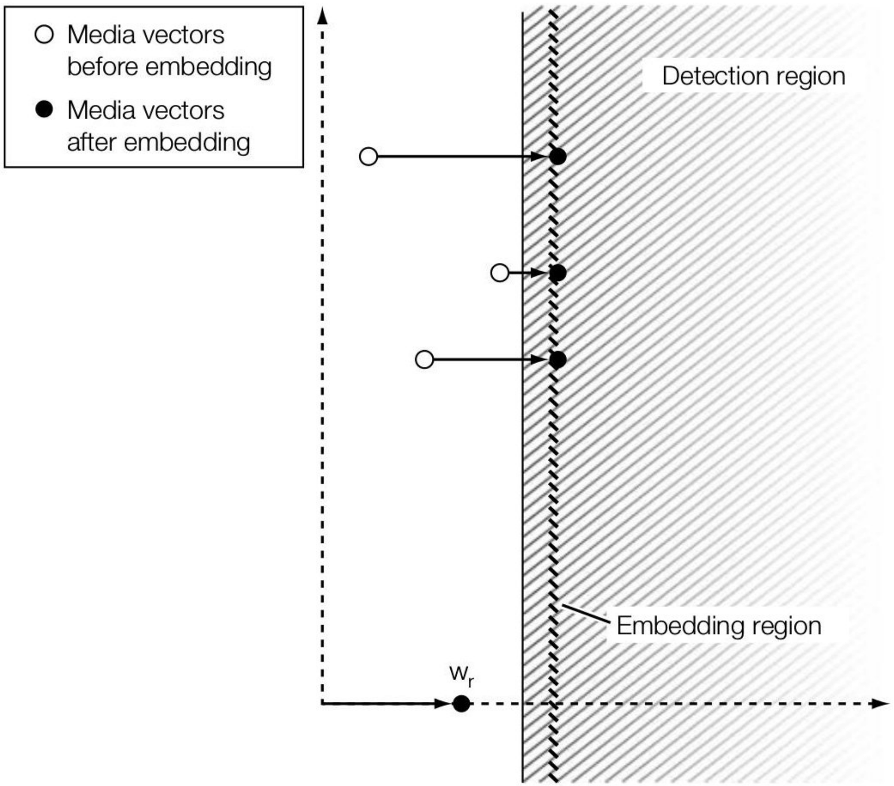
embeding region $\cap$ unwatermark regin $\Rightarrow$ fpr

E_BLIND



Media vectors before embedding
Media vectors after embedding
Detection region
w_r

E_FIXED_LC


Media vectors before embedding
Media vectors after embedding
Detection region
Embedding region
w_r

Distortion Distribution

The region of $\mathbf{c}_{wn}$ from $\mathbf{c}_m$: Effect of noise, attack ...

- Additive Gaussian noise:
  - Too simple, sometimes naive.
- Usually depends on content:
  - Lossy compression, filtering, noise reduction, and temporal or geometric distortions.
- Can be complex:
  - Not continuous, multimodal,
    - Interpolate the original image and a cropped one?

Marking Spaces

相较于 media 更低维.

Transform the work before embedding.

- Direct embedding in media space

$$\mathbf{c}_w = f(\mathbf{c}, \mathbf{w}(m)).$$

加水印

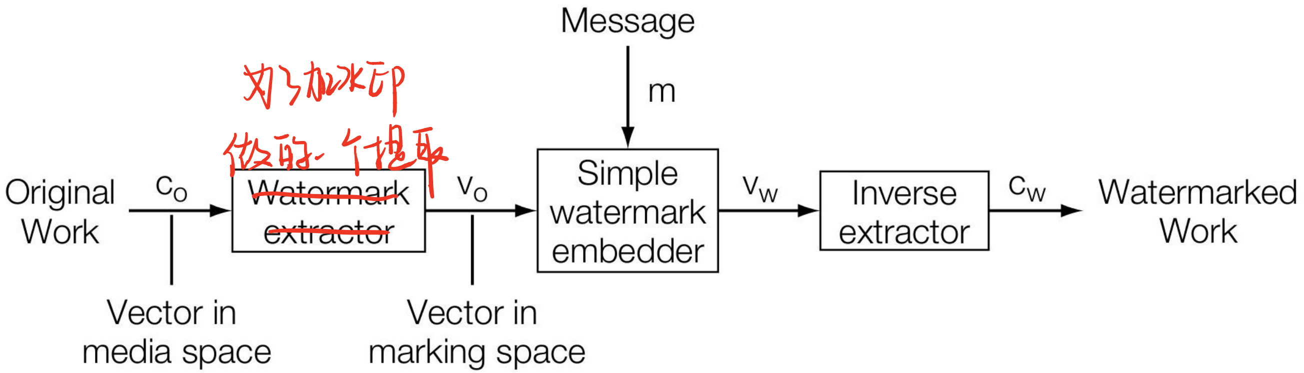
- Embedding in marking space

$$\mathbf{v} = \mathcal{T}(\mathbf{c}),\ \mathbf{v}_w = g(\mathbf{v}, \mathbf{w}(m)),\ \mathbf{c}_w = \mathcal{T}^{-1}(\mathbf{v}_w, \mathbf{c}).$$

- If $\mathcal{T} = \mathrm{Id}$ ...
- g can be simpler than f.

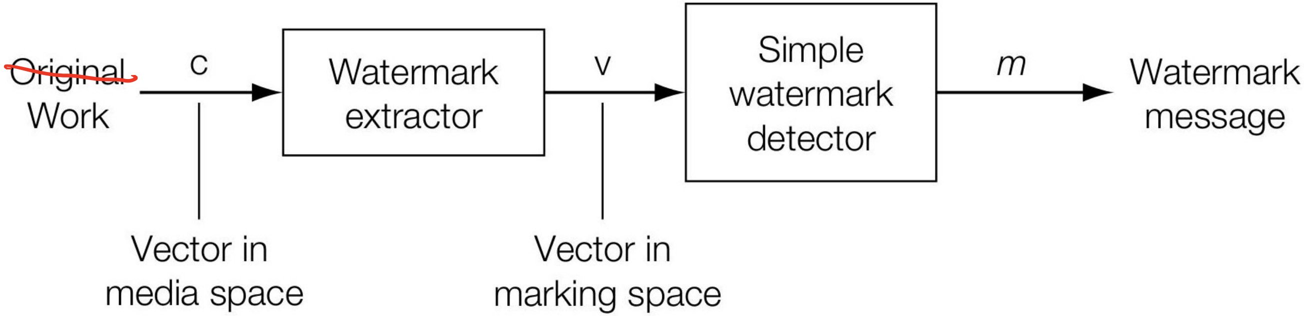
Embedder

$$\mathcal{T}(\mathbf{c}) \rightarrow \mathbf{v}, g(\mathbf{v}, \mathbf{w}(m)) \rightarrow \mathbf{v}_w, \mathcal{T}^{-1}(\mathbf{v}_w, \mathbf{c}) \rightarrow \mathbf{c}_w.$$



Detector

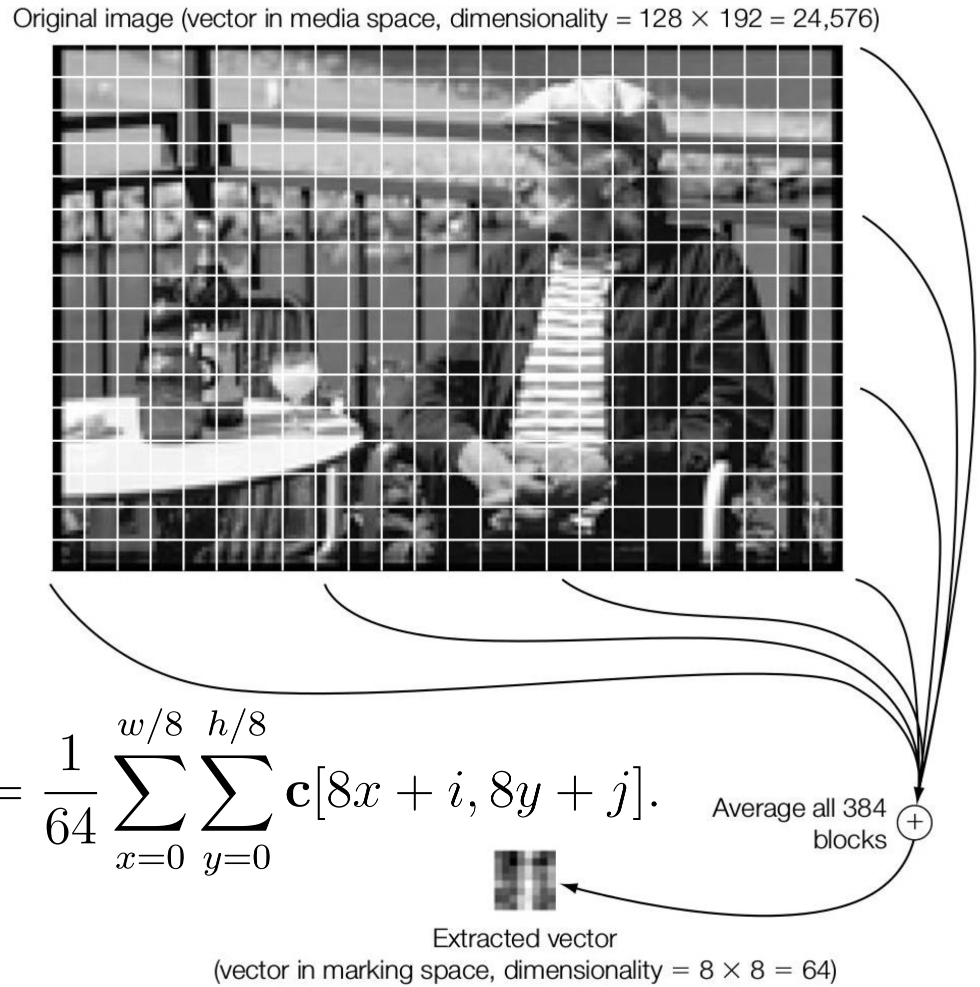
$$\mathcal{T}(\mathbf{c}_w) \to \mathbf{v}_w, \quad \mathrm{Cor}_g(\mathbf{v}_w, \mathbf{w}(m)) \to m.$$



Purposes

- Low cost of embedding and detection
  - Lower dimension for $\mathbf{v}$.
- Simpler distribution
  - Average blocks: more closely Gaussian.
  - Fourier: acceptable fidelity is more closely spherical.
  - Normalization: cancel out geometric and temporal distortions.
    - Not multimodal

Block Average as $\mathcal{T}$



$$\mathbf{v}[i,j] = \frac{1}{64}\sum_{x=0}^{w/8}\sum_{y=0}^{h/8}\mathbf{c}[8x+i, 8y+j].$$

Detector

- D_LC: Linear correlation.
  - Can be used.
- D_CC: Correlation coefficient.
  - Better (will show later).
  - Normalize (mean and variance) $\mathbf{v} \to \mathbf{v}'$: 均值为0，方差为1

0 1

sum($\tilde{\mathbf{v}}$)=0

抵抗提亮等…

使图像更鲁棒

$$\tilde{\mathbf{v}} = \mathbf{v} - \mu_{\mathbf{v}} \mathbf{1} \triangleq \mathbf{v} - \bar{\mathbf{v}},$$
$$\mathbf{v}' = \tilde{\mathbf{v}} / \|\tilde{\mathbf{v}}\|.$$

平均值.

对比度.

  - Correlation:

长度都为1

$$-1 \leq z_{cc}(\mathbf{v}, \mathbf{w}_r) = \mathbf{v}' \cdot \mathbf{w}_r' \leq 1.$$

Embedder

- E_FIXED_LC: adaptive weight α.
  - Complicated for D_CC.
- E_BLIND: $\alpha = 1 \Rightarrow \mathbf{v}_w = \mathbf{v}_o + \mathbf{w}_m$.
- $\mathbf{c}_w = \mathcal{T}^{-1}(\mathbf{v}_w, \mathbf{c}_o)$:
  - Changes on mark $\mathbf{v}$:

$$\Delta_w = \mathbf{v}_w - \mathbf{v}_o = \mathbf{w}_m.$$

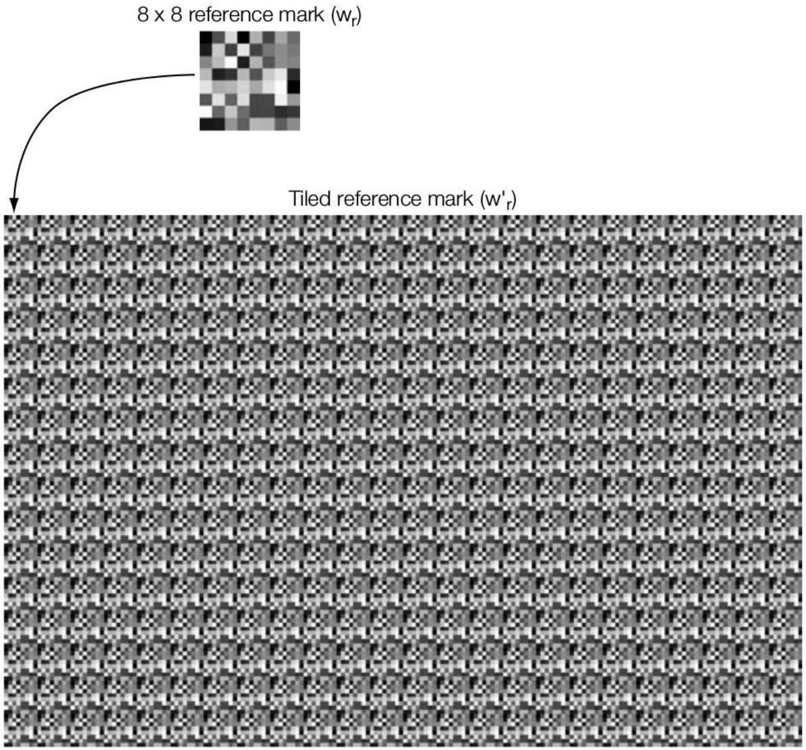
  - Add to cover c:

$$\mathbf{c}_w[x, y] = \mathbf{c}_o[x, y] + \Delta_w[x \bmod 8, y \bmod 8].$$

Performance 1

If using D_LC: Identical!

- Special reference pattern (key).



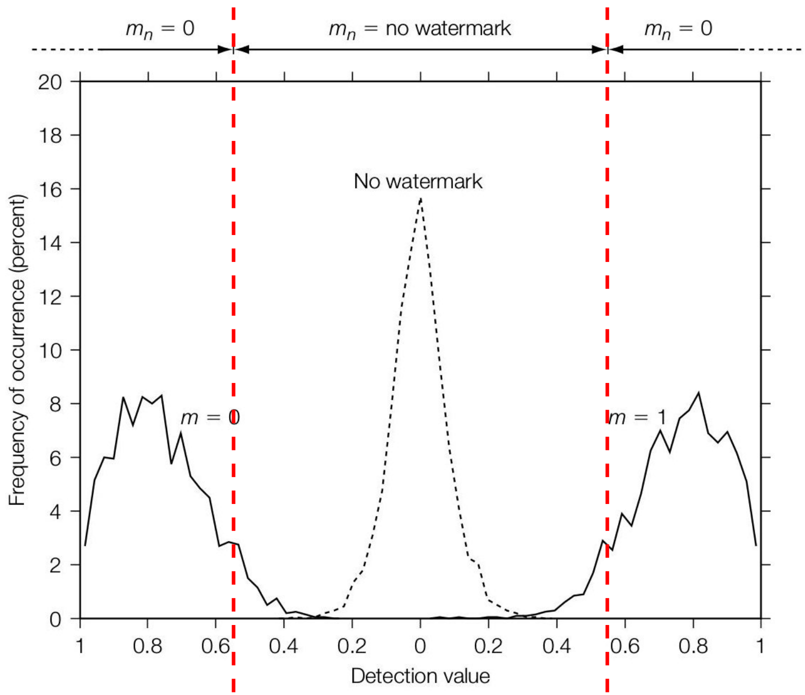
Performance 2

- Faster
- But smaller keyspace.

Performance 3

E_BLK_BLIND/D_BLK_CC: $\tau_{cc} = 0.55$.

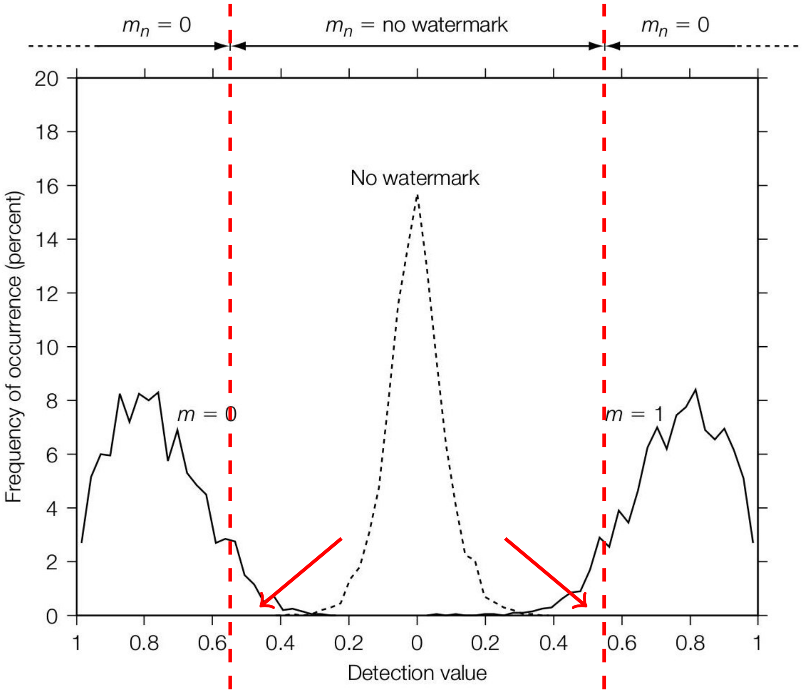
- False positive probability: 10^{-6}.
- Effectiveness: 92%.



Performance 3

E_BLK_BLIND/D_BLK_CC: $\tau_{cc} = 0.55$.

- False positive probability: 10^{-6}.
- Effectiveness: 92%.



3.5 Modeling Watermark Detection by Correlation

Correlation based

- Linear correlation
- Normalized correlation 只改变长度，不变均值（不能抵抗加噪，但可以抵抗乘法）
- Correlation coefficient

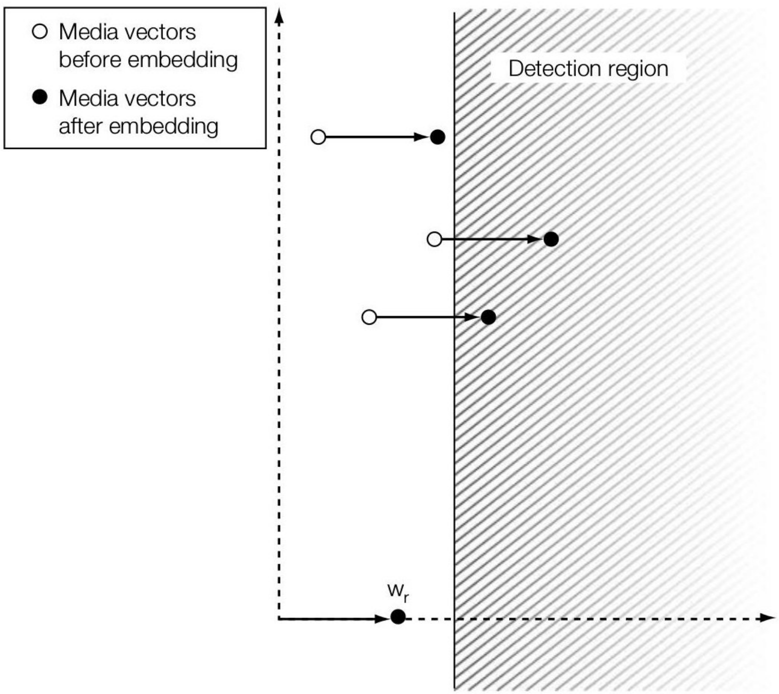
Feature based *read Chapter 9.*

- Corners ... 边角上也没动
- Lines ...

Linear Correlation

Project $\mathbf{v}$ onto $\mathbf{w}_r$

$$z_{lc}(\mathbf{v}, \mathbf{w}_r) = \frac{1}{N} \sum_i \mathbf{v}[i]\mathbf{w}_r[i] = \frac{1}{N}\mathbf{v} \cdot \mathbf{w}_r.$$



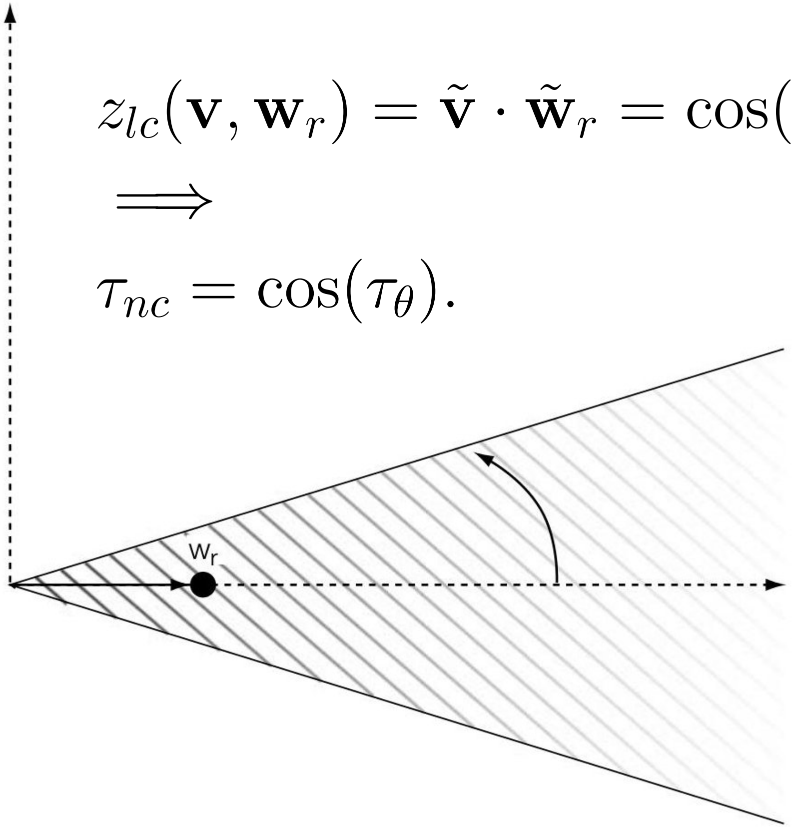
Normalized Correlation

Normalize length of $\tilde{\mathbf{v}} = \mathbf{v}/\|\mathbf{v}\|, \tilde{\mathbf{w}}_r = \mathbf{w}_r/\|\mathbf{w}_r\|$.

$$z_{lc}(\mathbf{v}, \mathbf{w}_r) = \tilde{\mathbf{v}} \cdot \tilde{\mathbf{w}}_r = \cos(\theta)$$

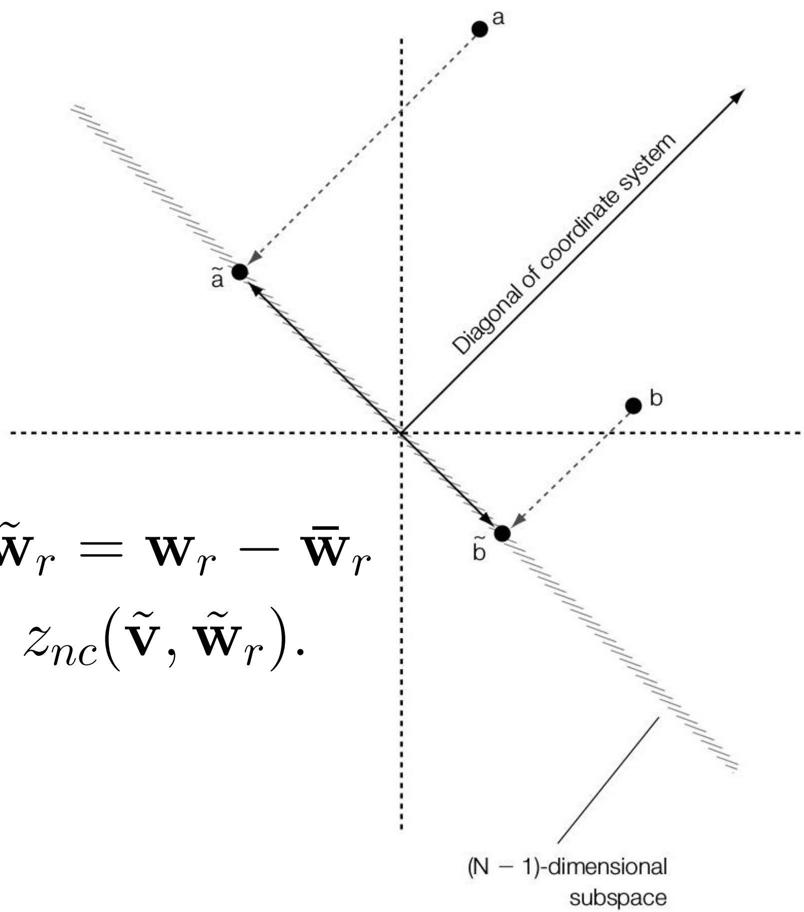
$$\Longrightarrow$$

$$\tau_{nc} = \cos(\tau_\theta).$$



Correlation Coefficient

Centered and normalized:



$$\tilde{\mathbf{v}} = \mathbf{v} - \bar{\mathbf{v}}, \tilde{\mathbf{w}}_r = \mathbf{w}_r - \bar{\mathbf{w}}_r$$

$$z_{cc}(\mathbf{v}, \mathbf{w}_r) = z_{nc}(\tilde{\mathbf{v}}, \tilde{\mathbf{w}}_r).$$

One Less Dimension

N-space to $(N-1)$-space:

$$\begin{aligned}\tilde{\mathbf{v}} &= \mathbf{v} - \bar{\mathbf{v}} \\ &= \mathbf{v} - \mathbf{1}_{N\times 1}\,\mu_{\mathbf{v}} \\ &= \mathbf{v} - \mathbf{1}_{N\times 1}\,\frac{\mathbf{1}_{1\times N}\,\mathbf{v}}{N} \\ &= \left(\mathrm{Id} - \frac{\mathbf{1}_{N\times N}}{N}\right)\mathbf{v}.\end{aligned}$$

Rank of $T = \left(\mathrm{Id} - \frac{\mathbf{1}_{N\times N}}{N}\right)$ is ....

One Less Dimension

N-space to $(N-1)$-space:

$$\begin{aligned}\tilde{\mathbf{v}} &= \mathbf{v} - \bar{\mathbf{v}} \\ &= \mathbf{v} - \mathbf{1}_{N\times 1}\,\mu_{\mathbf{v}} \\ &= \mathbf{v} - \mathbf{1}_{N\times 1}\,\frac{\mathbf{1}_{1\times N}\,\mathbf{v}}{N} \\ &= \left(\mathrm{Id} - \frac{\mathbf{1}_{N\times N}}{N}\right)\mathbf{v}.\end{aligned}$$

Rank of $T = \left(\mathrm{Id} - \frac{\mathbf{1}_{N\times N}}{N}\right)$ is ....

- $T\,\mathbf{1}_{N\times 1} = 0$.

Equivalent to

Normalizing by standard deviation:

$$z_2(\mathbf{v}, \mathbf{w}_r) = \frac{\mathbf{v} \cdot \mathbf{w}_r}{s_v} = \sqrt{N} \frac{\mathbf{v}}{\|\tilde{\mathbf{v}}\|} \cdot \mathbf{w}_r.$$

If w_r

- Zero mean.
- Unit length.

Presentation: 7.5

- The Effect of Whitening on Error Rates
  - http://en.wikipedia.org/wiki/Whitening_transformation
  - Just a linear transformation
  - How to construct the transformation.
  - What is the effect.
  - http://ufldl.stanford.edu/wiki/index.php/Exercise:PCA_and_Whitening