Information Hiding

☞ *Slides adapted from Spring 2011 offering of ENEE 408G and Fall 2013 offering of ENEE 631 in the ECE Department, University of Maryland, College Park by Profs. Min Wu (minwu@umd.edu) and Ray Liu (kjiliu@umd.edu)*

From Fragile/Semi-Fragile to Robust Watermark

- Applications of fragile/semi-fragile watermark
  - Tampering detection
  - Secret communications => "Steganography" (covert writing)
  - Convey side info. seamlessly
- Situations demanding higher robustness
  - Protect ownership (copyright label), prevent leak (digital fingerprint)
  - Desired robustness against compression, filtering, etc.
- How to make it robust?
  - Use "quantization"; Use error correcting coding
  - Borrow theories from signal detection & telecommunications
    - ***"Spread Spectrum Watermark":*** *use "noise" as watermark and add it to the host signal for improved invisibility and robustness*

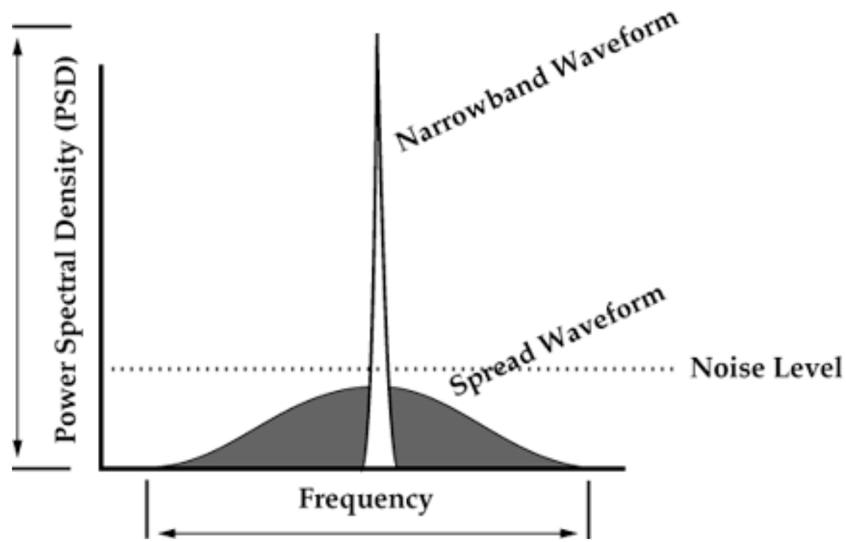
Robust Watermark Design Principles

- Unobtrusiveness
  - Perceptually invisible
- Robustness
  - Common DSP operations (enhancement, compression, etc.)
  - Common geometric distortions (rotation, cropping, scaling)
- Universality
  - Algorithm can work on any image
- Unambiguousness
  - Watermark should be identifiable by owner without any ambiguity

Drexel UNIVERSITY

Spread Spectrum Principle

- Developed to prevent jamming of radio transmissions
- Signal transmitted in one narrow frequency can be easily jammed



- Solution: Spread signal over wide band
  - Difficult to detect (can transmit below noise level)
  - Difficult to jam
- Apply this principle to image watermarking

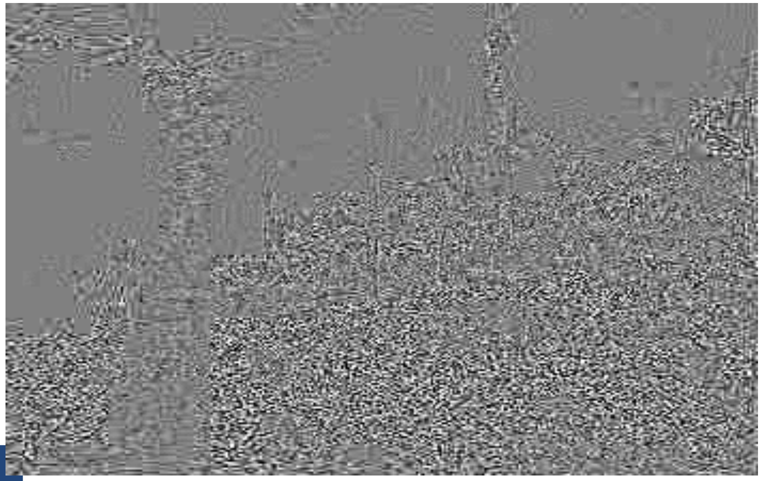
Drexel UNIVERSITY

Spread Spectrum Watermarking

- Communication view of watermarking
  - Image is communication channel
  - Watermark is transmitted signal
  - Attacks & distortion caused by processing are noise
- How to apply spread spectrum to images?
  - Embed in frequency domain by modifying DCT coefficients
  - Spread watermarks throughout the image (not just one spatial location or bit plane)
- Where to embed?

Drexel UNIVERSITY

Example: Robust Watermark via "Noise"



10011010 …

© Copyright …

- *Embedding domain tailored to media characteristics & application requirement*

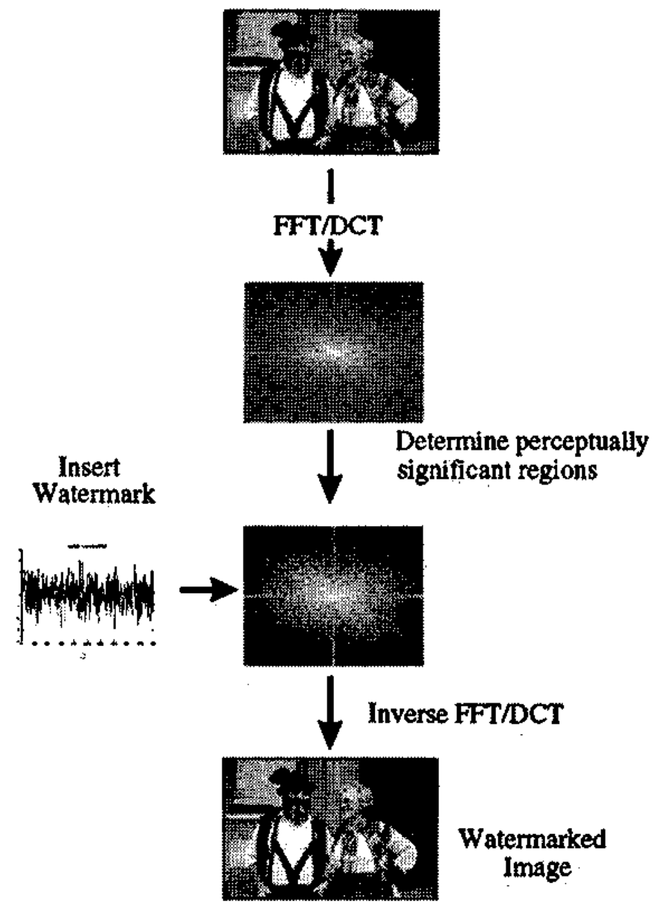
Where to Embed?

- Recall watermark must be both *unobtrusive* and *robust*
- Place watermark in perceptually significant regions
  - Difficult to destroy watermark without severely degrading the image
  - Ensure watermark strength does not perceptually alter content
- Perceptual mask to mark embedding locations
  - Binary mask with “1” corresponding to embedding location
  - Can be secretly chosen to enhance security
- In practice, *N* largest DCT coefficients chosen
  - DC coefficient excluded
  - Typically corresponds to low frequency coefficients

Drexel UNIVERSITY

Embedding Procedure

- Compute DCT of *entire* image
- Determine perceptually significant DCT coefficients suitable for embedding
  - Use N=1000 largest DCT coefficients
- Multiplicatively insert watermark w into selected DCT coefficients v
  - $v'_i = v_i + \alpha v_i w_i = v_i (1+\alpha w_i)$
  - α is embedding strength
  - Typically $\alpha = 0.1$
- Perform IDCT to recover watermarked image

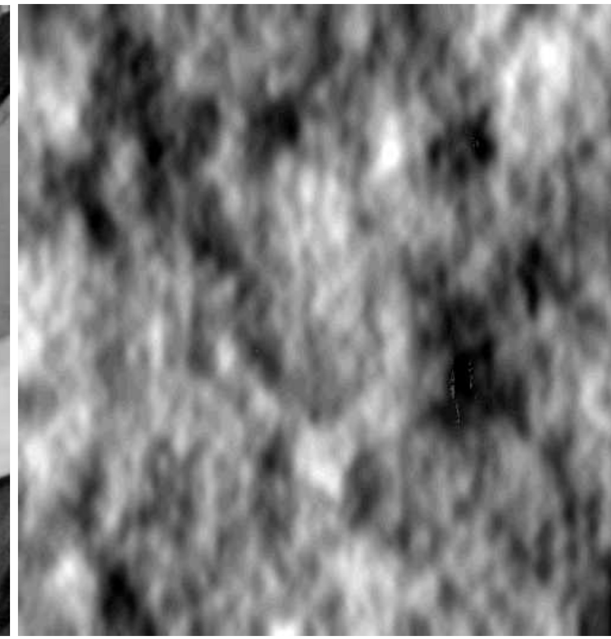


Watermark Design

- Embedding procedure is unobtrusive, universal, and robust
- Watermark must be robust and *unambiguous*
- Use randomly generated watermark
  - Gaussian i.i.d random variable
  - mean = 0 and variance = 1
- Resembles statistical noise
- Statistically independent of other watermarks

Drexel UNIVERSITY

Watermarking Example by Cox et al.



Original

Cox
whole image DCT
Embed in 1000 largest coeff.

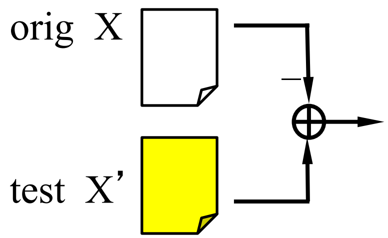
Difference between marked & original

Cox et al's Scheme: Watermark Detection

- Subtract original image from the test one before feeding to detector ("non-blind detection")

X' =X+W+N ?

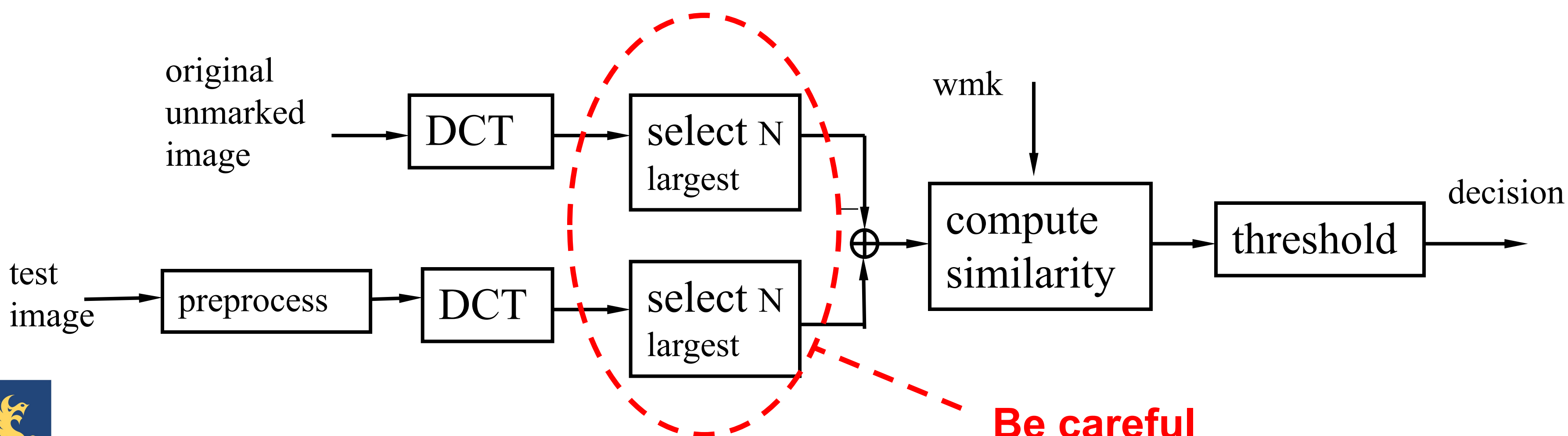
X' =X+N ?



$$Y = X' - X \Rightarrow \begin{cases} H0:\ Y = N & \text{no watermark} \\ H1:\ Y = W + N & \text{watermark} \end{cases}$$

- Correlation-based detection

$$sim(Y,W) = \frac{\langle Y, W \rangle}{\sqrt{\langle Y, Y \rangle}}$$



Performance of Cox et al's Scheme

- Robustness

Distortion	none	scale 25%	JPG 10%	JPG 5%	dither	crop 25%	print-xerox-scan
similarity	32.0	13.4	22.8	13.9	10.5	14.6	7.0

threshold = 6.0 (determined by setting false alarm probability)

  – Claimed to be robust under scaling, JPEG, dithering, cropping, "printing-xeroxing-scanning", multiple watermarking
  – No big surprise with high robustness
    - *equivalent to sending just 1-bit {0,1} with $O(10^3)$ samples*

- Comment
  – Must store orig. unmarked image ⇒ "private wmk", "non-blind" detection
  – Perform image registration if necessary
  – Adjustable parameters: N and α

Improve Invisibility and Robustness on Cox scheme

- Apply better Human Perceptual Model
  - Global scaling factor is not suitable for all coefficients
  - More explicitly compute just-noticeable-difference (JND)
    - *JND ~ max amount each coefficient can be modified invisibly*
    - *Employ human visual model: freq. sensitivity, masking, …*

$$v_i' = v_i + JND_i \cdot w_i$$

  - Use more localized transform => *fine tune wmk for each region*
    - *block-based DCT; wavelet transform*
- Improve robustness: detection performance depends on $||\underline{s}|| / \sigma_d$
    - *Add a watermark as strong as JND allows*
    - *Embed in as many "embeddable" coefficients => improve robustness*
- Block-DCT schemes: Podichuk-Zeng; Swanson-Zhu-Tewfik '97
  - Leverage existing visual model for block DCT from JPEG

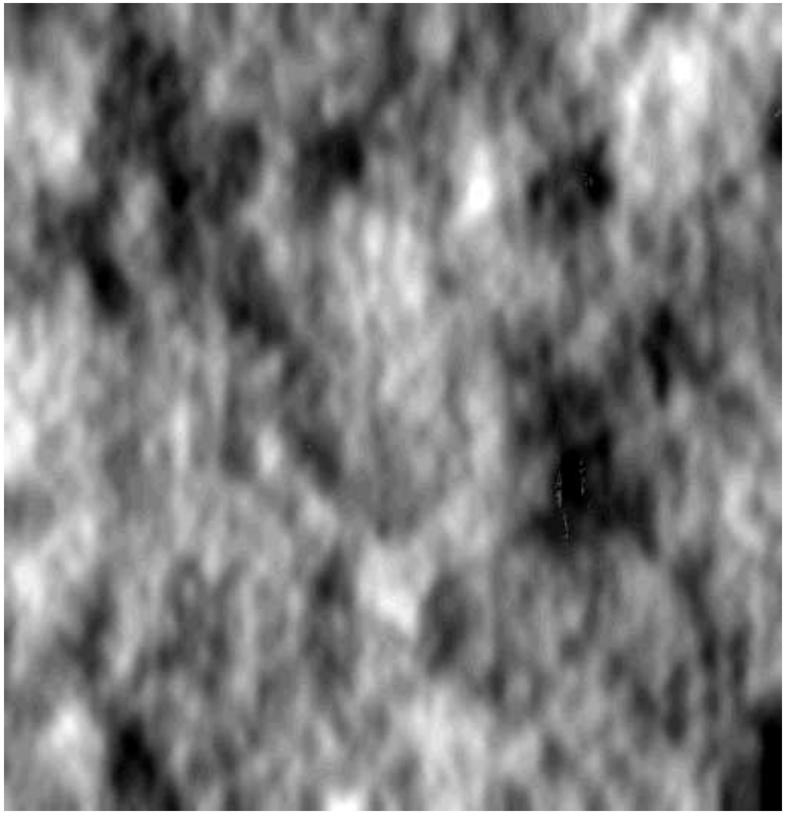
Perceptual Comparison: Cox vs. Podilchuk

Original

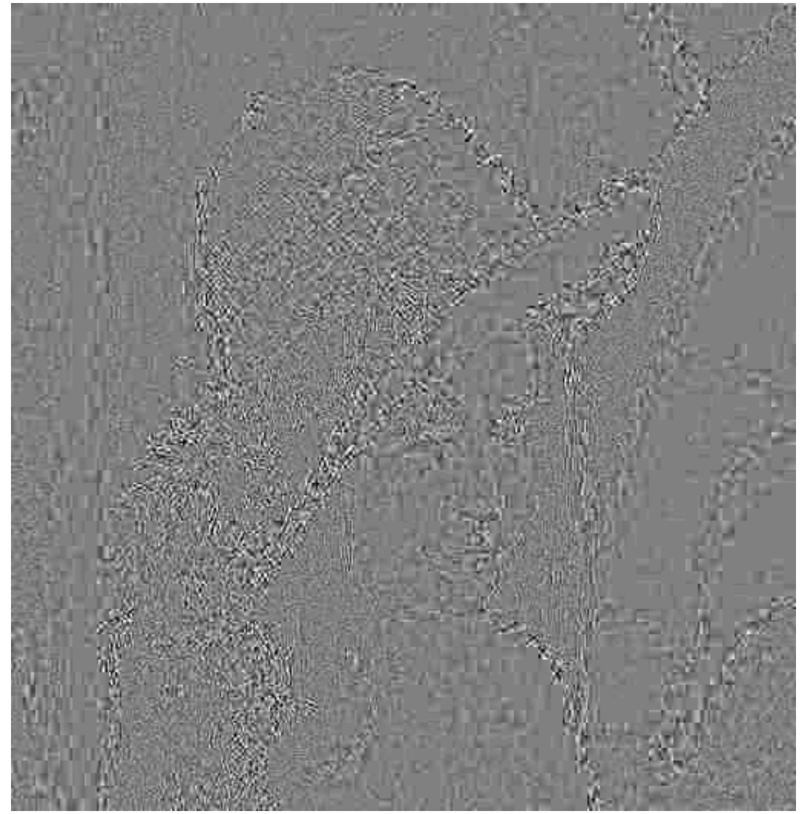
Cox
whole image DCT
Embed in 1000 largest coeff.

Podilchuk
block-DCT
Embed to all "embeddables"

Compare Cox & Podilchuk Schemes (cont'd)



Cox



Podilchuk

Amplified pixel-wise difference between marked and original (gray~0)

Summary: Spread Spectrum Embedding

- Main ideas
  - Place wmk in perceptually significant spectrum (for robustness)
    - *Modify by a small amount below Just-noticeable-difference (JND)*
  - Use long random vector of low power as watermark to avoid artifacts (for imperceptibility, robustness, and security)
- Cox's approach
  - Perform DCT on entire image & embed wmk in large DCT AC coeff.
  - Embedding: $v'_i = v_i + \alpha\, v_i\, w_i = v_i\, (1+\alpha\, w_i)$
  - Detection: subtract original and perform correlation w/ wmk
- Podilchuk's improvement
  - Embed in many "embeddable" coeff. in block-DCT domain
  - Adjust watermark strength by explicitly computing JND