Image Processing and Visual Communications

Watermarking and Security in Visual Communications

Zhou Wang

Dept. of Electrical and Computer Engineering
University of Waterloo

Outline

- **Digital Multimedia Security and Digital Watermarking**
  - Security issues in multimedia communications
  - Digital watermarking
- **Image Watermarking**
  - Design considerations
  - Least significant bit embedding
  - Spread spectrum embedding
  - Quantization index modulation embedding
- **Discussions about Watermarking**

Security Issues in Multimedia Communications

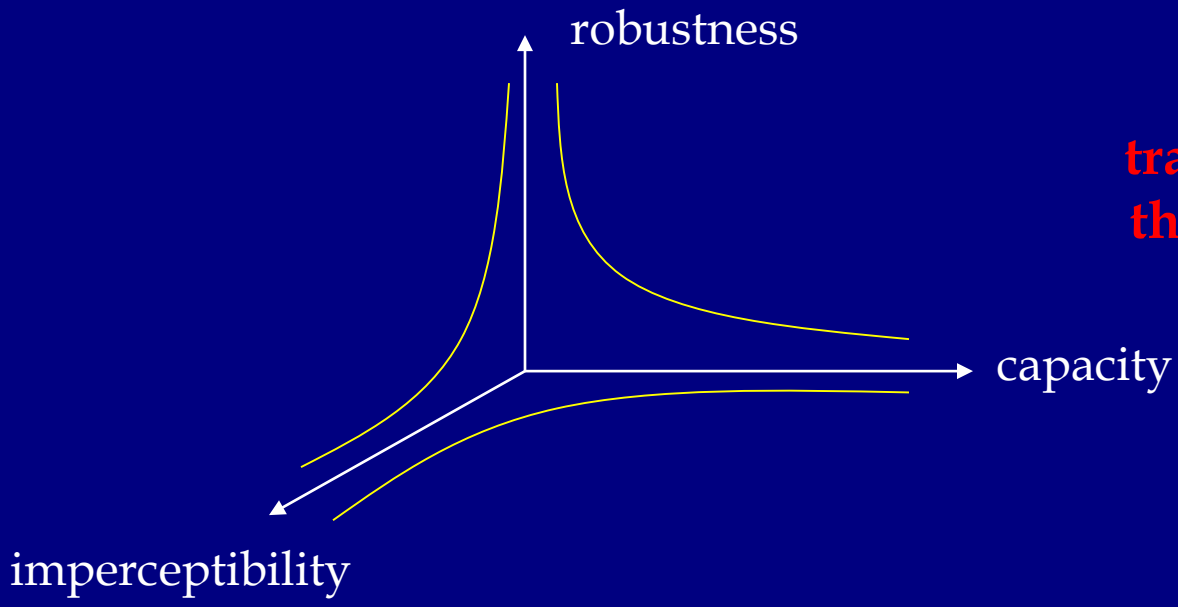
- **Copyright Protection**
  - To prevent others from claiming copyright of multimedia content
- **Copy Protection**
  - To prevent unauthorized copying of multimedia content
- **Data Authentication**
  - To prevent modifications to multimedia content
- **Broadcast Monitoring**
  - To verify whether multimedia content was broadcasted as agreed
- **Techniques**
  - Cryptography: to prevent unauthorized decoding of the content
  - Data hiding/digital watermarking
    protection even after the content has been decoded

Digital Watermarking

- **A Multidisciplinary Field**
  - Multimedia signal processing
  - Human perceptual systems
  - Information and communication theories
  - Networking system protocols
  - Law and consumer psychology
- **Classification Method 1**
  - Robust watermark: copyright protection
  - Fragile watermark: digital signature
  - Semi-fragile watermark: data authentication
- **Classifications Method 2**
  - Blind watermark: does not need the original signal for detection
  - Informed (non-blind) watermark: original signal needed

Image Watermarking: Design Considerations

- **Imperceptibility**
  - Original and watermarked images look the same
- **Robustness**
  - Watermarks survive after image distortions
- **Capacity**
  - Maximum amount of information that can be embedded



Need a good tradeoff between the three factors!

Method 1: Least Significant Bit Embedding

- **Methods**
  - Replace LSB with the information to be embedded
- **Properties**
  - Easy embedding
  - Easy detection
  - Large capacity
  - Poor robustness - fragile with minimum distortions
  - Easy removal (if the watermarking method is known to attacker)
- **Usage**
  - Steganography: hide a large amount of information
  - Tempering detection: use the fragility property

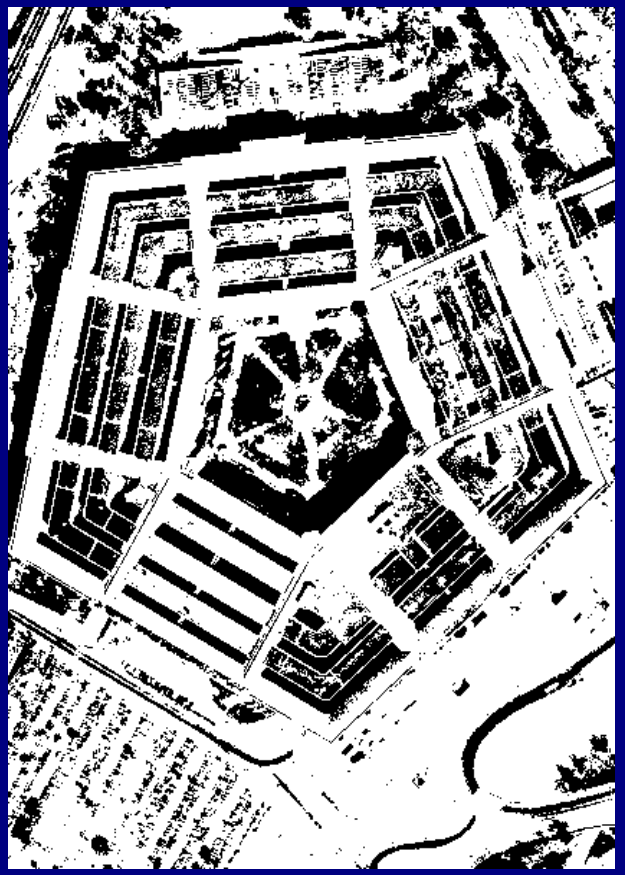
Method 1: Least Significant Bit Embedding

Sources: *http://www.cl.cam.ac.uk/~fapp2/steganography/image_downgrading/*
Digital Image Processing Notes by Prof. Min Wu

Method 1: Least Significant Bit Embedding

original image

watermarked image



watermark

Watermark embedding: Replace LSB with Pentagon's MSB

Source: Digital Image Processing Notes by Prof. Min Wu

Method 1: Least Significant Bit Embedding

original image

watermarked image

watermark

Watermark embedding: Replace 6 LSB's with Pentagon's 6 MSB's

Source: Digital Image Processing Notes by Prof. Min Wu

Method 2: Spread Spectrum

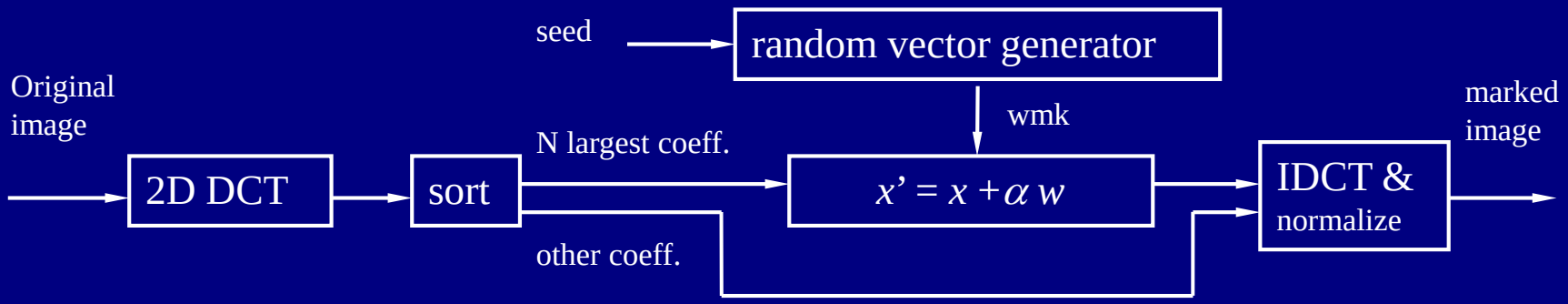
- **Idea**
  - Spread watermark to multiple frequency coefficients (broadband)
  - To improve robustness: use significant (large) coefficients only

- **Watermark Embedding**

  $x'_i = x_i + \alpha w_i$ (there are other embedding schemes also)

  x_i : original coefficient; x'_i : marked coefficient;

  α : small constant (e.g., 0.1); w_i : zero-mean "random"



Source: [Cox *et al.*, *IEEE Trans. IP*, Dec. '97] and Digital Image Processing Notes by Prof. Min Wu

Method 2: Spread Spectrum

- **Watermark Detection**
  - Coefficients of received test image:

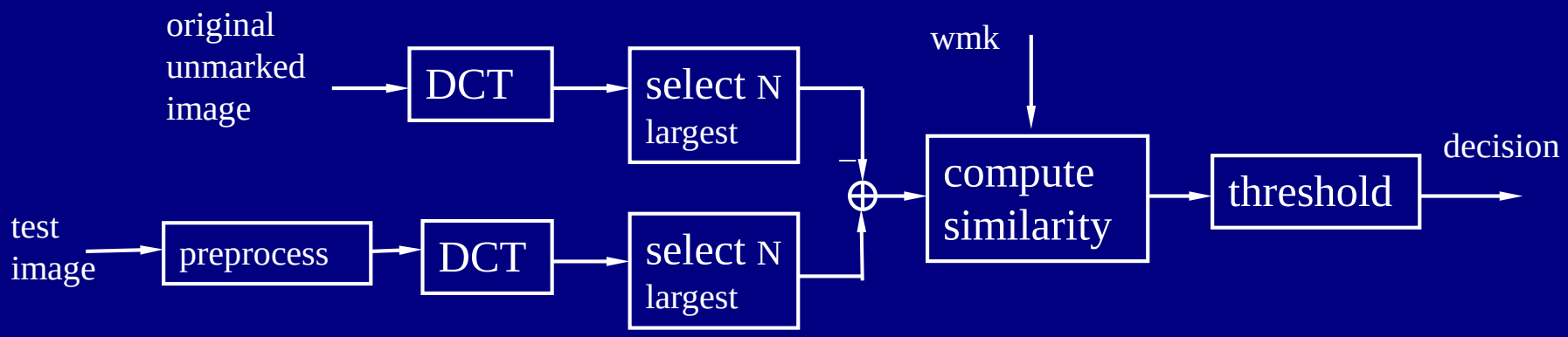
    w/o watermark: $y_i = x_i + N$

    w/ watermark: $y_i = x'_i + N = x_i + \alpha w_i + N$
  - Correlation detector:

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

Close to 0, if w/o watermark

Close to 1, if w/ watermark

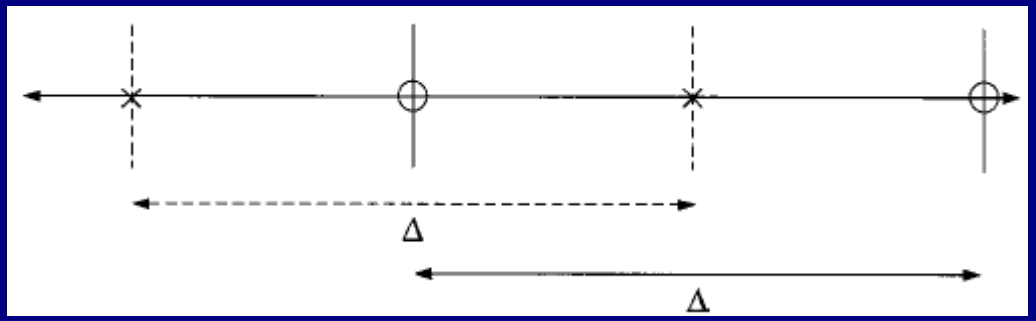


Source: [Cox *et al.*, *IEEE Trans. IP*, Dec. '97] and Digital Image Processing Notes by Prof. Min Wu

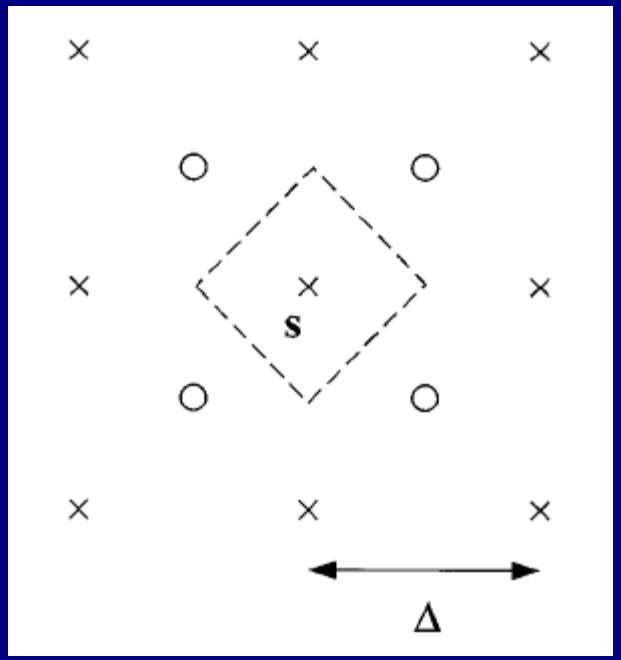
Method 3: Quantization Index Modulation

- **Watermark Embedding**
  - Design two sets of quantization grids, and quantize the signal using one of the two sets, depending on the bit to be embedded

scalar case



vector case



- **Watermark Detection**
  - Closest neighborhood criterion
- **Advantages:**
  - blind detection; good balance between capacity and robustness

[Chen & Wornell, *IEEE Trans. Info. Theory*, May 2001]

Discussions about Watermarking

- **Attacks by Regular Distortions**
  - Additive and multiplicative noise
  - Image enhancement and filtering
  - Lossy image coding and transcoding
  - Editing (geometrical distortions, cropping …)
  - D/A and A/D conversion (e.g., printing + scanning)
- **Malicious Attacks**
  - Remove a watermark
  - Make watermarks undetectable
  - Forge a watermark
  - Insert additional watermarks
- **Attacks in Real World Applications**
  - A critical issue, especially for copyright protection

Discussions about Watermarking

- **Controversial Arguments**
  - Watermarks themselves will never be secure!?
    can be easily removed if the watermarking method is known
  - Contradiction between the goals of compression and watermarking
    watermarking: exploit perceptual redundancy
    compression: remove perceptual redundancy
- **Future of Watermarking?**
  - Applications where robustness to malicious attacks is not critical
  - Non-security applications: binding data with images

data authentication?

- **Relevant Readings**

- C. Herley, "Why watermarking is nonsense?" *IEEE SP Magazine*, Sep. 2002
- P. Moulin, "Comments on 'Why watermarking is nonsense?'" *IEEE SP Magazine*, Nov. 2003
- M. Barni *et al.*, "What is the future for watermarking?" *IEEE SP Magazine*, Oct. & Nov. 2003