Digital Watermarking

Multimedia Security
What is the Watermark?

- **Paper Watermark**
  - the technique of impressing into the paper a form, image, or text
  - to make forgery more difficult
  - to record the manufacturer’s trademark
**Digital Watermark**

- **A digital watermark**
  - a digital signal or pattern imposed on a digital document (text, graphics, multimedia presentations)

- **visible watermark**
  - the more obvious means of discouraging unauthorized use by reducing the commercial value of a document

- **invisible watermark**
  - the watermark is imperceptible to the human eye
  - when the ownership of data is in question, the watermark will then be extracted to characterize the ownership
Visible Watermarking

Motivation
- The distribution of digital media is becoming faster, easier and requiring less effort to make exact copies
  - How to protect the intellectual property?

Conventional approaches
- In analog world
  - signature, steel seal, embossed portrait, copyright label...
- In digital world: cryptology

\[
E \rightarrow D
\]

encryption key

decryption key
Cryptology vs. Watermarking

- **Cryptology**
  - Once the data is decrypted, subsequent retransmission or dissemination is **not** encrypted

- **Watermarking**
  - Copyright information is hidden into digital data itself
  - Not restrict to access the data
  - Its objective is to **permanently** and **unalterably** reside in the data
Watermarking Requirements

- Imperceptible
- Undeletable
- Statistically undetectable
- Robustness
  - resistant to lossy data compression
  - resistant to signal manipulation and processing operation
- Unambiguous
Watermarked Image

Transmission

Lossy Compression
Geometric Distortions
Signal Processing
D/A - A/D Conversion

Typical Distortions or Intentional Tampering

Transmission

Corrupted Watermarked Image
Watermark Embedding

- **Making the watermark robustness is not trivial**
  - with complete knowledge
    - any watermark can theoretically be removed
  - with partial knowledge
    - the removal may interfere with the viewing of the data
    - the effort of removal is greater than the value of the data

- **Challenges from data compression**
  - Whatever hole one may find to fill with watermark is likely to be eliminated by data compression
Watermarking for Text

- Line-Shift Coding
- Word-Shift Coding


- Feature Coding

```
:5 AND 1 Incremental Mod
```

```
:5 AND 1 Incremental Mod
```
Watermarking for Images & Videos

• Watermarking in \{ spatial domain, transform domain \}

• Watermarking in \{ raw data, compressed data \}

• Watermarking with \{ random number, visually recognizable pattern \}

• Detection/extraction \{ with, without \} the original data
LSB Flipping Method


- Generate the random walk sequence for each watermark (e.g., 0011₂)
- Force the LSB to match the watermark bit

œ This works will not survive any modification
Spread Spectrum Method


**Spread spectrum coding of a watermark**

- frequency domain of the image ➔ communication channel
- watermark ➔ the signal transmitted through the channel

The watermark $W = w_1, \ldots, w_n$

- each $w_i$ is chosen according to zero-mean Gaussian Distribution
- the image $X$ is transform by full-frame DCT

$n$ highest magnitude coefficients (except DC) are chosen: $y_1, \ldots, y_n$

**Embedding:** $y'_i = y_i + \alpha w_i$

**Extracting:** $w_i = (y_i^* - y_i) / \alpha$

similarity = correlation $(W, W^*)$
Spread Spectrum Method (cont.)

1. Original Image (IFT/DCT)
2. Determine Perceptually Significant Regions
3. Watermarked Image (IFT/DCT)
4. Received Image
5. Original Watermark
6. Extracted Watermark
7. Similar
• Watermark detector

Watermark detector response to 1000 randomly generated watermarks
Perceptually Masking Method


Detection

\[ H_0 : X = F^* - F = N \]
\[ H_1 : X = F^* - F = W^* + N \]

the hypothesis decision is obtained by

similarity = correlation \((X,W)\)
Perceptually Masking Method (cont.)

- Frame from “pingpong”

- The watermark

![Similarity value graph](image)
Digimarc Watermarking

- A commercial watermarking software
  - http://www.digimarc.com
Watermarking for Audio

- **Phase Coding**
  - Inserting the watermark by modifying the phase of each frequency component

- **Spread Spectrum Method**
  - The watermark code is spread over the available frequency band, and then attenuated and added as additive random noise

- **Perceptual Method**
  - The watermark is generated by filtering a PN-sequence with a filter that approximates the frequency masking characteristics of HAS
  - Weighting the watermark in the time domain to account for temporal masking

- Watermark generator
• Watermark detection
Watermarking for Polygonal Models


- 3D models watermarking
  - vertex coordinates
  - vertex topology (connectivity)

Embedded pattern  Simplified polygonal
Limitations of Watermarking

- Basic watermarking steps

Limitations of Watermarking (cont.)

• Counterfeit

Watermarked image $I'$ $\rightarrow$ $D_{inv}$ $\rightarrow$ Counterfeit image $I^*$

$W^*$

$I'$ $\rightarrow$ $D$ $\rightarrow$ $W$ $\rightarrow$ $C$ $\rightarrow$ y/n ?

$I$ Watermark $W$

$I'$ $\rightarrow$ $D$ $\rightarrow$ $W^*$ $\rightarrow$ $C$ $\rightarrow$ y/n ?

$I^*$ Watermark $W^*$
Digital watermark

Visible watermark  Invisible watermark

Random sequence watermark  Visually recognizable watermark

Watermark:
ID number (random number)

Verification:
Quantitative measurement of the detection

Visually recognizable pattern
Extracted pattern & Quantitative measurement