Lecture 13-Digital Watermarking

Yuyao Zhang, Xiran Cai PhD
zhangyy8@shanghaitech.edu.cn caixr@shanghaitech.edu.cn
SIST Building 2 302-F/302-C
Course piazza link：
piazza.com/shanghaitech.edu.cn/spring2021/cs270spring2021

上海科技大学
ShanghaiTech University

Watermarking

We all like watermarks，so charming…

Purpose of Digital Watermarking

- **Anti-counterfeiting（防伪）：**

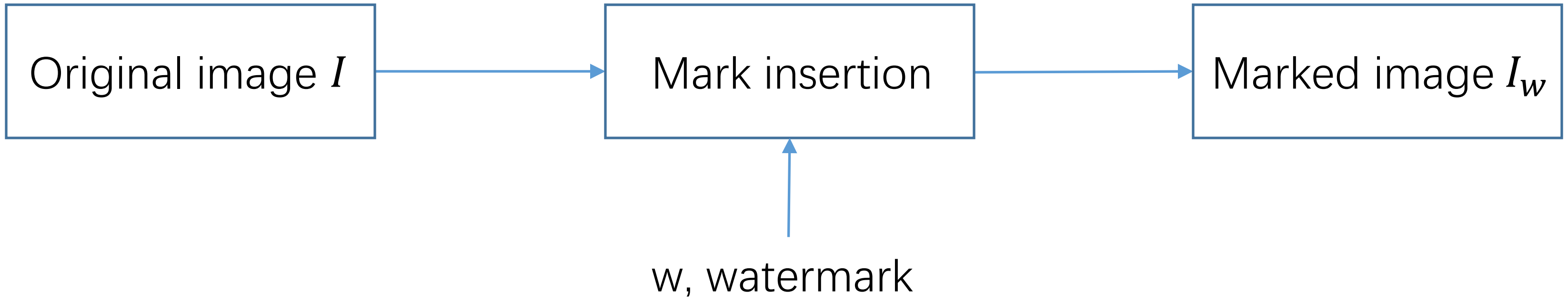
Embedding information into an image, so that:

- Image seems unchanged
- Watermark can be extracted even after processing.
- Removing watermark should destroy the image.

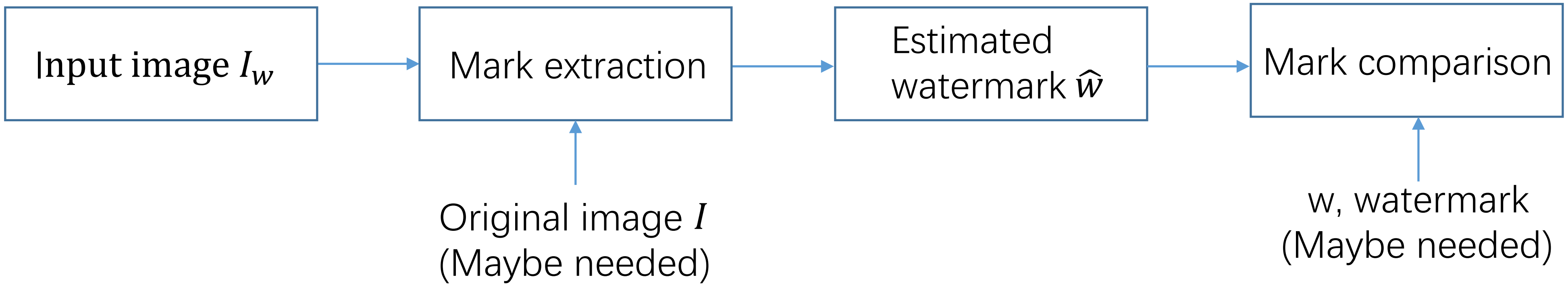
Anti-counterfeiting

Insertion and detection of watermarks

- **Insertion/ embedding:**



- **Detection:**



Spatial watermarking

- Idea: mark less significant bits.

w is a 2-bit image; I is a 8-bits image.

$$I_w = \left\lfloor \frac{I}{4} \right\rfloor * 4 + \frac{w}{64}$$

Take the floor
6-bits approx + 2 bits’ s of w

- Easy to remove.

- Not robust at all to all kinds of noise.

Spatial watermarking

Anti-counterfeiting

Spatial watermarking 2-Pseudo random noise pattern

- Embedding:
  - ✓ Split image into blocks.
  - ✓ Define pseudo-random noise patters, $w_1, w_2, w_3, \cdots, w_K$ same size as image blocks.
  - ✓ To decode:

$$I_w(block\ k) = I(block\ k) + \alpha w_K$$

- Decoding:
  - ✓ Split image into blocks.
  - ✓ Correlate each block with $w_1, w_2, w_3, \cdots, w_K$, extract watermark correspond to high correlation.
  - ✓ Not robust to crop resizing.

Robust watermarking in frequency domain 1

- **Idea: hide information in visually important frequency bands.**
- Embedding:
  - Compute DCT of the entire image.
  - Find K largest magnitude coefficients $\boldsymbol{c_1}, \boldsymbol{c_2}, \boldsymbol{c_3}, \cdots, \boldsymbol{c_K}$ (not included DC).
  - Watermark is a K-length random vector or a logo image: $\boldsymbol{w_1}$, $\boldsymbol{w_2}, \boldsymbol{w_3}, \cdots, \boldsymbol{w_K}$.
  - Embed the watermark: $\boldsymbol{c'_i} = \boldsymbol{c_i}\,(\mathbf{1} + \boldsymbol{\alpha w}_{\mathrm{i}})$ (α>0) .
  - Replace $\boldsymbol{c_i}$ with $\boldsymbol{c'_i}$, and take the inverse DCT.

Robust watermarking in frequency domain 1

- **Idea: hide information in visually important frequency bands.**
- Embedding:
  - Compute DCT of the entire image.
  - Find K largest magnitude coefficients $\boldsymbol{c_1}, \boldsymbol{c_2}, \boldsymbol{c_3}, \cdots, \boldsymbol{c_K}$ (not included DC).
  - Watermark is a K-length random vector or a logo image: $\boldsymbol{w_1}, \boldsymbol{w_2}, \boldsymbol{w_3}, \cdots, \boldsymbol{w_K}$.
  - Embed the watermark: $\boldsymbol{c'_i} = \boldsymbol{c_i}\,(\mathbf{1} + \boldsymbol{\alpha w_{\mathrm{i}}})$ (α>0) .
  - Replace $\boldsymbol{c_i}$ with $\boldsymbol{c'_i}$, and take the inverse DCT.

Robust watermarking in frequency domain 1

➢ **Decoding:**

- Compute DCT of the image.
- Extract K coefficient in known locations (side information, may differ from original case).
- Compute $\widehat{w'}_i = (\frac{c'_i}{c_i} - 1)/\alpha$
- Find information in $\widehat{w'}_i$.

上海科技大学 ShanghaiTech University

Robust watermarking in frequency domain 2

- Idea: hide binary information in comparable values.
- Simple frequency-flipping method: (block-based)
- Compute DCT of cropped blocks.

```
Y_Table=[ 16  11  10  16  24  40  51  61 ; ...
          12  12  14  19  26  58  60  55 ; ...
          14  13  16  24  40  57  69  56 ; ...
          14  17  22  29  51  87  80  62 ; ...
          18  22  37  56  68 109 103  77 ; ...
          24  35  55  64  81 104 113  92 ; ...
          49  64  78  87 103 121 120 101 ; ...
          72  92  95  98 112 100 103  99 ];
```

- Choose 2 DCT coefficients location that are expected to have comparable average values/range.

  N(4,1) = N(2,3) = 14;

- Per 8X8 block, compute DCT c(u,v);

  c(4,1) > c(2,3) then bit 0;   c(4,1) > c(2,3) then bit 1;

- If coefficients don’ t already match w, flip them.

Take home message

- **Desirable properties for digital watermark**
  - Visual imperceptible
  - Statistically imperceptible
  - Robust to inadvertent or intentional attacks.
    - Cropping resizing, compression, enhancement, rotation.
    - Print image/rescan, collusion.
  - Alternative: fragile watermark breaks as soon as image is modified.
  - High capacity.
  - Speed of embedding and detection.