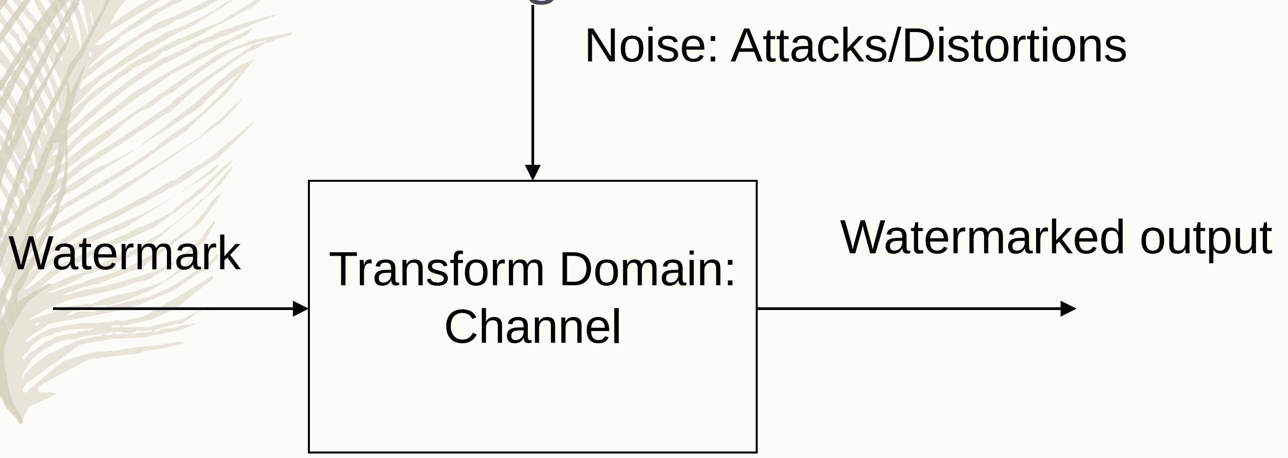
Lecture 6: How to Design a Good Digital Watermark?

Multimedia Security

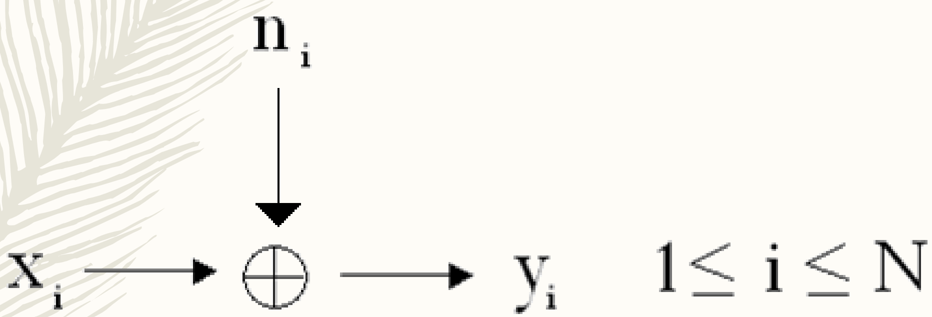
- **The watermark should be placed on the most perceptually significant components of an image (Psychovisual Effect)**
  - **Against lossy data compression**
- **The watermark should resemble the image it is designed to protect**
  - **Any operation that is intentionally performed to damage the watermark will also damage the image.**

- The frequency domain of the image or sound is viewed as a Communication Channel, and correspondingly, the Watermark is viewed as a Signal that is transmitted through it.
- Attacks and unintentional signal distortions are treated as Noise that immersed signal must be immune to.



Information Theoretic Point of View

– **Reliable communication**



– x_i : one element of a watermark vector of length N

– n_i : an element of a noise vector due to image processing operation

– y_i : an element of a watermark distorted by noise n_i

Assumptions & Conceptions

– (Gaussian channel) Discrete-time channel with input X_i , noise Z_i , and output Y_i at time i. This is

$$Y_i = X_i + Z_i ,$$

where the noise Z_i is drawn i.i.d. from N (0, N) and assumed to be independent of the signal X_i .

- The noise is additive, white, stationary and Gaussian
- The n_i are uncorrelated

$$p(y_i \mid x_i) = p(n_i) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left[-\frac{(y_i - x_i)^2}{2\sigma^2} \right]$$

$$p(y_1, y_2, \ldots, y_n, \mid x_1, x_2, \ldots, x_n) = \prod_{i=1}^{N} p(y_1 \mid x_1)$$

$$I(X;Y) = H(X) - H(X|Y)$$

Where

$I(X;Y)$ **:Mutual Information between X and Y**

Trans-information

$$H(X) = -\sum_i p(x_i)\log p(x_i)$$ **:Entropy of X**

Then

$$C = \max_{p(x)} I(X;Y)$$ **:Channel capacity**

C is the maximal achievable information transfer rate for the specific probability density function *p(x)*

– **For continuous data source X, the capacity is maximized with respect to the distribution p(x) if**

$$p(x_i) = \frac{1}{\sqrt{2\pi\gamma^2}} \exp\left[-\frac{x_i^{\,2}}{2\gamma^2} \right]$$

which is a Zero Mean Gaussian density with

variance γ^2 ---- (Gaussian distribution watermark)

In this case,

$$C = I_{\max} = \frac{1}{2} N \log\left[1 + \frac{\gamma^2}{\sigma^2} \right] = \frac{N}{2\ln 2} \ln\left(1 + \frac{\gamma^2}{\sigma^2} \right)$$

For the ease of watermark extraction, we need

$$\underset{\text{signal power}}{\gamma^2} >> \underset{\text{noise power}}{\sigma^2}$$

then

$$\ln\left(1+\frac{\gamma^2}{\sigma^2}\right) \approx \ln\frac{\gamma^2}{\sigma^2}$$ **(signal-to-noise power ratio)**

For a reliable communication, the real information rate *J* must be

$$J < I_{\max} \cong \frac{N}{2\ln 2}\ln\frac{\gamma^2}{\sigma^2}$$

– **That is,**

$$\ln\frac{\gamma^2}{\sigma^2} > (2\ln 2)\frac{J}{N} \quad \text{.........(1)}$$

frequency bands if the channel is in the transform domain

N: the number of sites used to hide watermark information bits

Imperceptible watermark : γ^2 **the smaller the better**

$\Rightarrow$ $\frac{\gamma^2}{\sigma^2}$ is severely limited

$\Rightarrow$ For fixed *J*, "*N*" should be as large as possible: Spread Spectrum Communications

Where the watermark should be placed?

- Assume the image may be considered as a collection of paralleled uncorrelated Gaussian channels which satisfy

$$x_i + n_i = y_i, \quad 1 \le i \le N$$

- Imperceptible watermarking requires that

$$\sum_{i=1}^{N} \gamma_i^2 \le E \text{ ....(2)}$$

E= Energy

Assuming additive, white, stationary Gaussian noise and the noise variances are not necessarily the same in each channel, the channel capacity can be represented by a more general formula as:

$$C = \frac{1}{2}\sum_{i=1}^{N}\log_2\left(1+\frac{\gamma_i^2}{\sigma_i^2}\right)$$

where σ_i^2 is the variance of the noise corrupting the watermark and γ_i^2 is the average power of the watermark signal in the *i*-th channel.

– **Capacity is achieved when**

$$\begin{cases} \gamma_i^2 + \sigma_i^2 = Th, & if \;\; \sigma_i^2 < Th \\ \gamma_i^2 = 0, & if \;\; \sigma_i^2 > Th \end{cases}$$

Watermark Embedding

Where the threshold *Th* is chosen to maximize the sum on the left-hand side of eqn.(2) and thus maximize the energy of the watermark.

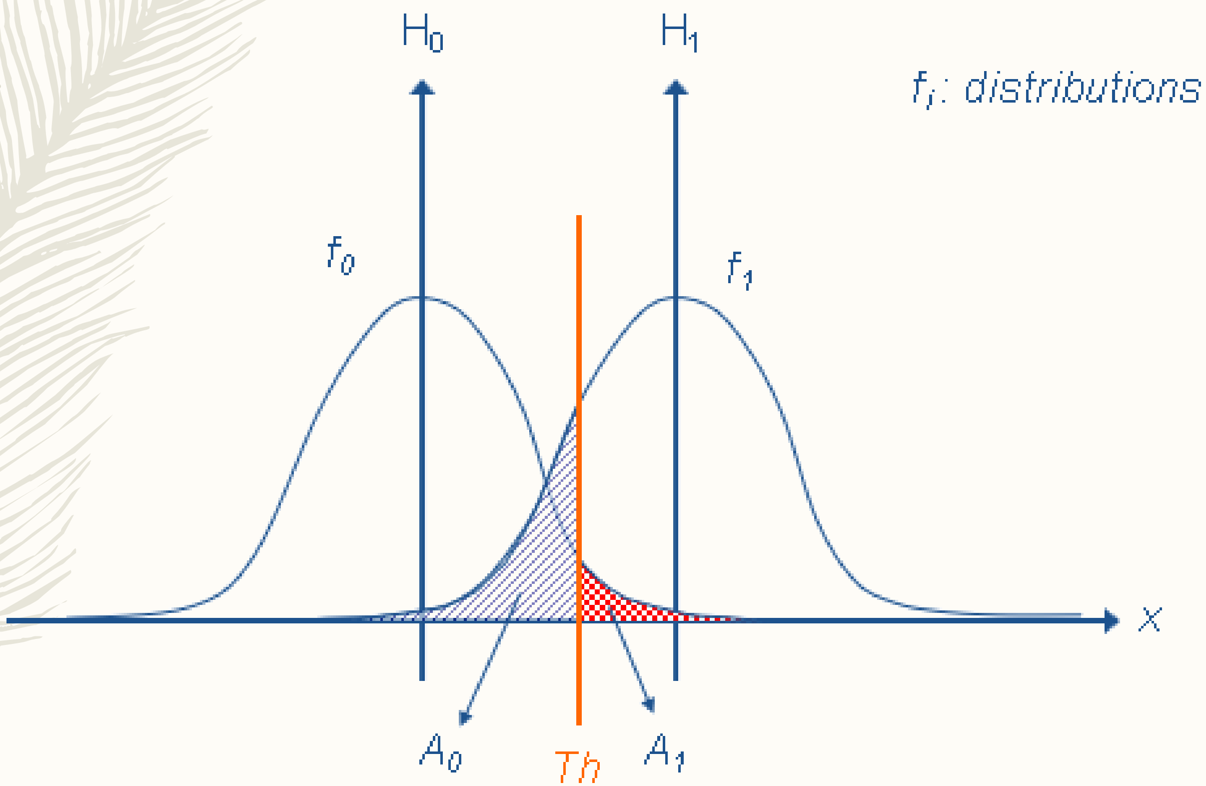
Conclusion

- The watermark should be placed in those areas where the local noise variance σ_i^2 is smaller than threshold *Th* and not at all in those areas where the local noise variance exceeds the threshold.
- Remarks:
  1. Gaussian noise assumption : Conservative but tractable.
  2. Synthesis-by-Analysis approach.

     :content–dependent / content-aware approach.

Watermark Extraction

Hypothesis Testing



$$if\ \sigma_i^{\ 2} < Th, \quad y_i^{\ 2} = \sigma_i^{\ 2} + \gamma_i^{\ 2}$$

$$\Rightarrow Exp(y_i) = Exp(\gamma_i)$$

$$if\ \sigma_i^{\ 2} > Th, \quad y_i^{\ 2} = \sigma_i^{\ 2}$$

$$\Rightarrow Exp(y_i) = 0$$

$$Area(A_0) = p(y_0 \mid H_1) = \int_{-\infty}^{Th} f_1(x)dx = p(miss)$$

$$Area(A_1) = p(y_1 \mid H_0) = \int_{Th}^{\infty} f_0(x)dx = p(false\ alarm)$$