

# Fingerprinting Capacity

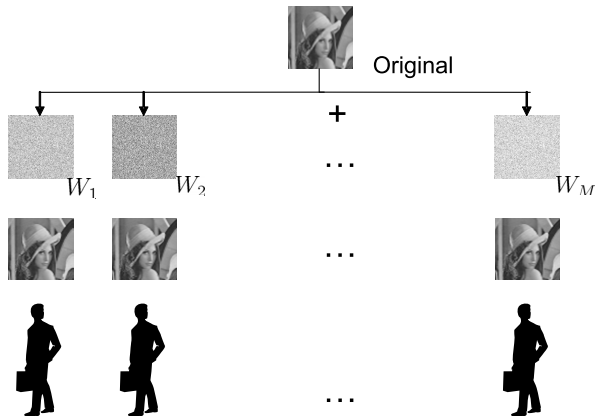
Yen-Wei Huang  
Advisor: Pierre Moulin

University of Illinois at Urbana-Champaign  
Electrical and Computer Engineering

[huang37@uiuc.edu](mailto:huang37@uiuc.edu)

June 5, 2008

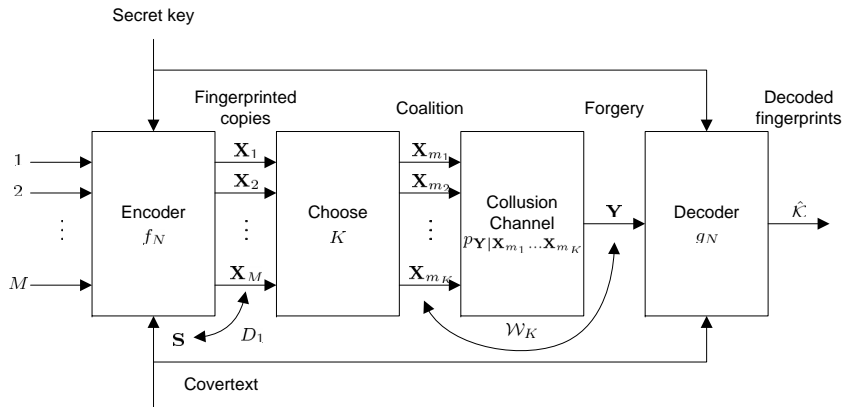
# Fingerprinting



# Setups

- Distortion Constraint
  - ▶ Commonly used in multimedia fingerprinting applications
  - ▶ Restrictions on distortions between:
    - ★ Original data and fingerprinted copies
    - ★ Fingerprinted copies and forgery
- Marking Assumption
  - ▶ Popular model for software fingerprinting
  - ▶ The fingerprint is a set of redundant digits
  - ▶ The coalitions may modify only those positions where they find a difference in their fingerprinted copies

# Model for Fingerprinting Game



# Fingerprinting Capacity

Error probabilities:

- $P_e^{one}(f_N, g_N, p_{\mathbf{Y}|\mathbf{X}_{\mathcal{K}}}) = Pr[\hat{\mathcal{K}} \cap \mathcal{K} = \emptyset]$
- $P_e^{all}(f_N, g_N, p_{\mathbf{Y}|\mathbf{X}_{\mathcal{K}}}) = Pr[\mathcal{K} \not\subseteq \hat{\mathcal{K}}]$
- $P_{FP}(f_N, g_N, p_{\mathbf{Y}|\mathbf{X}_{\mathcal{K}}}) = Pr[\hat{\mathcal{K}} \setminus \mathcal{K} \neq \emptyset]$

## Definition

A rate  $R$  is achievable for embedding distortion  $D_1$ , collusion class  $\mathcal{W}_K$ , and **detect-one** criterion if there exists a sequence of  $(N, \lceil 2^{NR} \rceil)$  randomized codes  $(f_N, g_N)$  with maximum embedding distortion  $D_1$ , such that both  $P_e^{one}(f_N, g_N, \mathcal{W}_K)$  and  $P_{FP}(f_N, g_N, \mathcal{W}_K)$  vanish as  $N \rightarrow \infty$ .

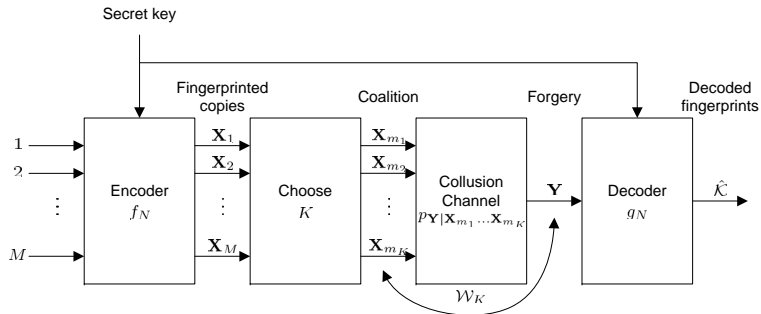
**Detect-all** criterion can be defined analogously.

# Fingerprinting Capacity (cont'd)

## Definition

Fingerprinting capacities  $C^{one}(D_1, \mathcal{W}_K)$  and  $C^{all}(D_1, \mathcal{W}_K)$  are the suprema of all achievable rates with respect to the **detect-one** and **detect-one** criteria, respectively.

# Model for the Marking Assumption



## Fingerprinting Capacity under the Marking Assumption

Consider random variable  $W$  defined over an alphabet  $\mathcal{W} = \{1, 2, \dots, L\}$  and the mutual-information game

$$C_L^{one} = \max_{p_{XW}} \min_{p_{Y|X_K}} \frac{1}{K} I(X_K; Y|W)$$

where  $p_{XW}$  is any p.m.f. over  $\mathcal{X} \times \mathcal{W}$  and the collusion channel  $p_{Y|X_K}$  is subject to the marking assumption:

$$x_1 = \dots = x_K \Rightarrow y = x_1.$$

### Theorem

*Fingerprinting capacity is given by*

$$C^{one} = \lim_{L \rightarrow \infty} C_L^{one}$$

*under the marking assumption and the **detect-one** criterion.*

# Bounds in the Binary Case

Theorem (Tardos, 2003)

$$C_K^{one} \geq \frac{1}{100K^2 \ln 2}$$

Theorem (Anthapadmanabhan et al., 2007)

$$0.25 \leq C_2^{one} \leq 0.322.$$

$$0.083 \leq C_3^{one} \leq 0.199.$$

Theorem (Anthapadmanabhan et al., 2008)

$$O\left(\frac{1}{K^2}\right) \leq C_K^{one} \leq O\left(\frac{1}{K}\right).$$