Capacity and Random-Coding Error Exponent for Public Fingerprinting Game

Ying Wang and Pierre Moulin
University of Illinois at Urbana-Champaign
Electrical and Computer Engineering

ISIT, Seattle
July 11, 2006
Information Hiding

- Hide data in cover object $S$ such as image, video, audio, or text.

- Applications:
  - Covert communications (steganography)
  - Copyright protection (watermarking)
  - Traitor tracing (fingerprinting)
    - Fingerprinting is a multiuser access problem.
  - etc.
Fingerprinting may be viewed as a problem of communication with side information at the encoder and/or decoder.

- Cover object $S$ is viewed as side information
- *Private* fingerprinting: $S$ known to encoder & decoder
  - Somekh-Baruch and Merhav (2005): Capacity and error exponent
- *Public* fingerprinting: $S$ known to encoder only
  - *This paper*: capacity and random coding error exponent
Public Fingerprinting

- $S \in S^N$: covertext available to the encoder only
- $M = 2^{NR}$ messages, each corresponding to a user
- $X_m = f_N(S, m)$: fingerprinted copy for the $m^{th}$ user
- Additive distortion function: $d^N(S, X) = \frac{1}{N} \sum_{i=1}^{N} d(S_i, X_i)$
- Distortion constraint: $d^N(S, X_m) \leq D_1$ almost surely
• **L-user coalition:** \( \{ X_{c1}, X_{c1}, \ldots, X_{cL} \} \)

• **Collusion attack:** \( p_{Y|X_{c1},X_{c2},\ldots,X_{cL}} \) to generate a forgery \( Y \)

• **Fairness constraint:** \( p_{Y|X_{c1},X_{c2},\ldots,X_{cL}} = p_{Y|X_{c2},X_{c1},\ldots,X_{cL}} = \cdots \)

• **Distortion constraint:** \( Ed^N(Y, X_{c,l}) \leq D_2, 1 \leq l \leq L \)
Public Fingerprinting

- Detect all coalition members: \( g_n(Y) = (\hat{m}_{c1}, \ldots, \hat{m}_{cL}) \)
- Error if \( g_n(Y) \neq (m_{c1}, \ldots, m_{cL}) \)
Capacity and Reliability Function

- Minmax probability of error:
  \[ P_{e,N} = \min_{f_N, g_N} \max_{p_Y|X_{c1}\cdots X_{cL}} P_e(f_N, g_N, p_Y|X_{c1}\cdots X_{cL}), \]
  where
  \[ P_e(f_N, g_N, p_Y|X_{c1}\cdots X_{cL}) = \Pr[g_N(Y) \neq (m_{c1}, \ldots, m_{cL})|f_N, g_N, p_Y|X_{c1}\cdots X_{cL}] \]

- A rate \( R \) is said to be achievable if \( P_{e,N} \to 0 \) as \( N \to \infty \).
- The capacity \( C \) is the supremum of all achievable rates.
- The reliability function is defined as
  \[ E(R) = \lim \inf_{N \to \infty} \left[ -\frac{1}{N} \log P_{e,N} \right] \]
A Few Definitions

• Consider two colluders with $X_1$ and $X_2$, i.e., $L = 2$

• Feasible discrete memoryless collusion channel (DMCC)

$$p_{Y|X_1X_2} \in \mathcal{P}_{Y|X_1X_2}(D_2)$$

$$p_{Y|X_1X_2}(y|x_1,x_2) = \prod_{i=1}^{N} p_{Y|X_1X_2}(y_i|x_{1,i},x_{2,i}),$$

$$p_{Y|X_1X_2} = p_{Y|X_2X_1}, \text{ and}$$

$$\sum_{x_1,x_2,y} p_{X_1,X_2}(x_1,x_2)p_{Y|X_1X_2}(y|x_1,x_2)d(x_i,y) \leq D_2, \ i = 1, 2.$$ 

• Feasible transmit channel $p_{XU|S}(x,u|s) \in \mathcal{P}_{XU|S}(D_1)$

$$\sum_{x,u,s} p_{XU|S}(x,u|s)p_{S}(s)d(s,x) \leq D_1$$

where $U \in \mathcal{U}$ is an arbitrary auxiliary random variable.
Capacity

- Capacity: 

\[ C(D_1, D_2) = \sup_U \max_{p_{XU|S} \in \mathcal{P}_{XU|S}(D_1)} \min_{p_{Y|X_1X_2} \in \mathcal{P}_{Y|X_1X_2}(D_2)} \min \left\{ I(U_1; Y|U_2) - I(U_1; S|U_2), I(U_2; Y|U_1) - I(U_2; S|U_1), \frac{1}{2} [I(U_1, U_2; Y) - I(U_1, U_2; S)] \right\}, \]

where \( U_1 \in \mathcal{U}, U_2 \in \mathcal{U} \), and \( p_{X_1U_1|S} = p_{X_2U_2|S} = p_{XU|S} \).

- Capacity \( C(D_1, D_2) \) is the value of a game between the encoder and decoder and the colluders.

- Converse part of proof: an extension of Gel’fand and Pinsker’s proof for channel coding with random parameters (1980).
Random Coding Error Exponent

• The reliability function $E(R)$ is lower-bounded by

$$
E_r^{DMCC}(R) = \min_{\tilde{p}_S \in \mathcal{P}_S} \sup_{U} \min_{\tilde{p}_{X_2U_2|X_1U_1S}} \max_{p_{X_1U_1|S=p_{X_2U_2|S}}} \left( \min_{\tilde{p}_Y|X_1X_2U_1U_2S} \min_{p_{Y|X_1X_2} \in \mathcal{P}_{Y|X_1X_2}(D_2)} \left[ D(\tilde{p}_{S|X_1X_2U_1U_2Y},|p_{S|p_{X_1U_1|S}p_{X_2U_2|S}p_{Y|X_1X_2}}) + J(\tilde{p}_S, p_{X_1U_1|S}, \tilde{p}_{X_2U_2|X_1U_1S}, \tilde{p}_Y|X_1X_2U_1U_2S) \right] \right)
$$

for all $R \leq C$, where $U_1 \in \mathcal{U}$, $U_2 \in \mathcal{U}$,

$$
\sum_{X_1,U_1} \tilde{p}_{X_2U_2|X_1U_1S} \cdot p_{X_1U_1|S} = p_{X_2U_2|S},
$$
and

\[ J(\tilde{p}_S, p_{X_1 U_1 | S}, \tilde{p}_{X_2 U_2 | X_1 U_1 S}, \tilde{p}_Y | X_1 X_2 U_1 U_2 S) = \]

\[ \left| \min \left\{ I(U_1; Y | U_2) - I(U_1; S | U_2) + I(U_1; U_2 | S) - R, \right. \]

\[ I(U_2; Y | U_1) - I(U_2; S | U_1) + I(U_1; U_2 | S) - R, \]

\[ I(U_1, U_2; Y) - I(U_1, U_2; S) + I(U_1; U_2 | S) - 2R \right\} \right|^+. \]

- \( E_{rDMCC}^D(R) \) is the value of a game between the encoder and decoder and the colluders.

- \( E_{rDMCC}^D(R) \) is strictly positive at all rates below capacity.
Stacked Random Binning Scheme

- Method of types, constant composition codes

- *Stacked binning* scheme (Moulin and Wang, 2004): for each state sequence type $p_s$, the codebook $C(p_s) = \{u(m, k, p_s)\}$ is a $2^{NR}$ by $2^{N\rho(p_s)}$ array

- Encoding rule: given $(s, m)$, find $u(m, k, p_s)$ such that $(s, u) \in T^*(p_s)$; encoding error if no such $u$ is found.
Stacked Random Binning Scheme (Cont’d)

• **Maximum penalized mutual information** decoder:

\[
(\hat{m}_1, \hat{m}_2) = \arg \max_{m_1, m_2} \left\{ \max_{p_s} \left[ I(u_1 u_2; y) - 2\rho(p_s) + I(u_1; u_2) \right] \right\},
\]

where \( u_1 = u(m_1, k_1, p_s) \) and \( u_2 = u(m_2, k_2, p_s) \).

• \( \rho(p_s) = \tilde{I}_{U;S}(p_s, p_{u|s}) + \epsilon \) is the optimal fine-tuning parameter for the tradeoff between the encoding and decoding error probabilities.
Conclusion

• Stacked binning scheme strikes an optimal balance between the encoding and decoding error probabilities

• Future work:
  – An upper bound on reliability function
  – The stacked binning technique for fingerprinting can be applied to multi-access communication with side information too.