On Tardos Fingerprinting and Channel capacities

Dion Boesten

May 11, 2011

Digital fingerprinting

- Prevent illegal distribution of digital content by embedding a unique watermark in each copy
- Watermark consists of two layers:
  - Coding layer: Determines which messages to embed
  - Watermarking layer: Hides the messages in the content
- Until 2003 coding layer was highly deterministic
- Tardos proposed a fully probabilistic approach in 2003

Tardos code construction

- A $n \times m$ code matrix X is generated in two steps:
  1. For each column j a bias $p_j \in [0, 1]$ is generated from a distribution $F(p)$
  2. For each row i a symbol X_{ij} is generated by a coin flip with parameter p_j

$$X = \begin{bmatrix} p_1 & p_2 & p_3 & p_4 & p_5 \\ \hline & & & & \end{bmatrix}$$

Tardos code construction

- A $n \times m$ code matrix X is generated in two steps:
  1. For each column j a bias $p_j \in [0, 1]$ is generated from a distribution $F(p)$
  2. For each row i a symbol X_{ij} is generated by a coin flip with parameter p_j

$$X = \begin{bmatrix} p_1 & p_2 & p_3 & p_4 & p_5 \\ \hline & & & & \end{bmatrix}$$

Tardos code construction

- A $n \times m$ code matrix X is generated in two steps:
  1. For each column j a bias $p_j \in [0, 1]$ is generated from a distribution $F(p)$
  2. For each row i a symbol X_{ij} is generated by a coin flip with parameter p_j

$$X = \left[\begin{array}{|ccccc|} \hline p_1 & p_2 & p_3 & p_4 & p_5 \\ \hline 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ \hline \end{array}\right]$$

Coalition attacks

- A coalition $\mathcal{C}$ of malicious users collaborate
- They produce a forged codeword Y
- The *Marking Assumption* restricts attack options

$$X_{\mathcal{C}} \begin{bmatrix} p_1 & p_2 & p_3 & p_4 & p_5 \\ \hline 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \end{bmatrix}$$

Coalition attacks

- A coalition $\mathcal{C}$ of malicious users collaborate
- They produce a forged codeword Y
- The *Marking Assumption* restricts attack options

$$X_{\mathcal{C}} \begin{bmatrix} p_1 & p_2 & p_3 & p_4 & p_5 \\ \hline 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \end{bmatrix}$$

$$Y = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Coalition attacks

- A coalition $\mathcal{C}$ of malicious users collaborate
- They produce a forged codeword Y
- The *Marking Assumption* restricts attack options

$$X_{\mathcal{C}} \begin{bmatrix} p_1 & p_2 & p_3 & p_4 & p_5 \\ \hline 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & \boxed{1} \\ 0 & 0 & 1 & 1 & \boxed{1} \\ 1 & 1 & 0 & 0 & \boxed{1} \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \end{bmatrix}$$

$$Y = \begin{bmatrix} 1 & 0 & 1 & 0 & \boxed{1} \end{bmatrix}$$

Accusation

- User codewords are compared with the pirated sequence Y
- Users are accused based on accusation scores S_i,
  a user i receives for each column j:
  - A positive amount of accusation $g_1(p_j)$
    if his/her symbol $X_{ij} = Y_j$
  - A negative amount of accusation $g_0(p_j)$
    if his/her symbol $X_{ij} \neq Y_j$

Accusation

- User codewords are compared with the pirated sequence Y
- Users are accused based on accusation scores S_i,
  a user i receives for each column j:
  - A positive amount of accusation $g_1(p_j)$
    if his/her symbol $X_{ij} = Y_j$
  - A negative amount of accusation $g_0(p_j)$
    if his/her symbol $X_{ij} \neq Y_j$

Accusation

- User codewords are compared with the pirated sequence Y
- Users are accused based on accusation scores S_i,
  a user i receives for each column j:
  - A positive amount of accusation $g_1(p_j)$
    if his/her symbol $X_{ij} = Y_j$
  - A negative amount of accusation $g_0(p_j)$
    if his/her symbol $X_{ij} \neq Y_j$

Accusation

- User codewords are compared with the pirated sequence Y
- Users are accused based on accusation scores S_i,
  a user i receives for each column j:
  - A positive amount of accusation $g_1(p_j)$
    if his/her symbol $X_{ij} = Y_j$
  - A negative amount of accusation $g_0(p_j)$
    if his/her symbol $X_{ij} \neq Y_j$

Accusation

- User codewords are compared with the pirated sequence Y
- Users are accused based on accusation scores S_i,
  a user i receives for each column j:
  - A positive amount of accusation $g_1(p_j)$
    if his/her symbol $X_{ij} = Y_j$
  - A negative amount of accusation $g_0(p_j)$
    if his/her symbol $X_{ij} \neq Y_j$
- If $S_i > T$ then user i is considered guilty

Collusion channel

- Pirates employ a probabilistic strategy θ in choosing their output
- Attack is column independent and depends only on Z_j (#1's received in a certain column)
- Interleaving Attack $\bar{\theta}$ is defined as:

$$\bar{\theta}_z \triangleq \frac{z}{c} \qquad , c = |\mathcal{C}|$$

$$\theta_z \triangleq \text{Prob}\left[Y_j = 1 \mid Z_j = z\right]$$

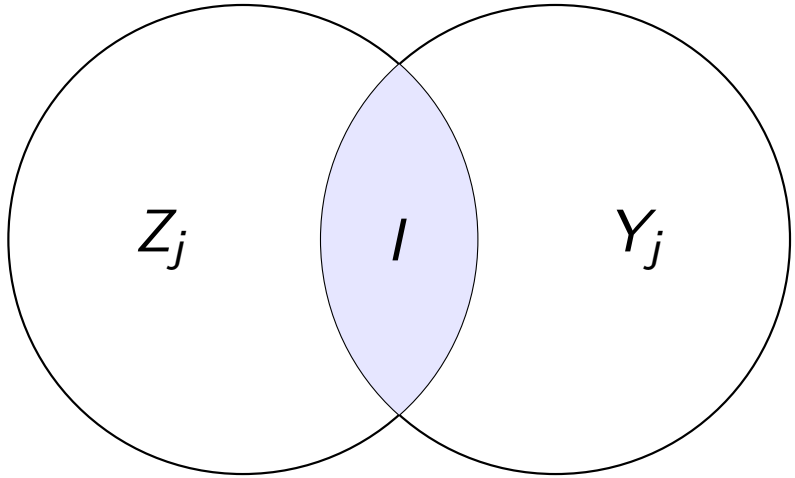
$$X_{\mathcal{C}} = \begin{bmatrix} \boxed{1} & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ \boxed{1} & 1 & 0 & 0 & 1 \end{bmatrix}$$

$$Z_1 = 2$$

Mutual Information

- Mutual Information $I(Y_j; Z_j \mid p_j)$ measures how much we learn about Z_j by knowing Y_j
- The column average $\bar{I}(F, \theta)$ is defined as the average over p_j and per pirate:

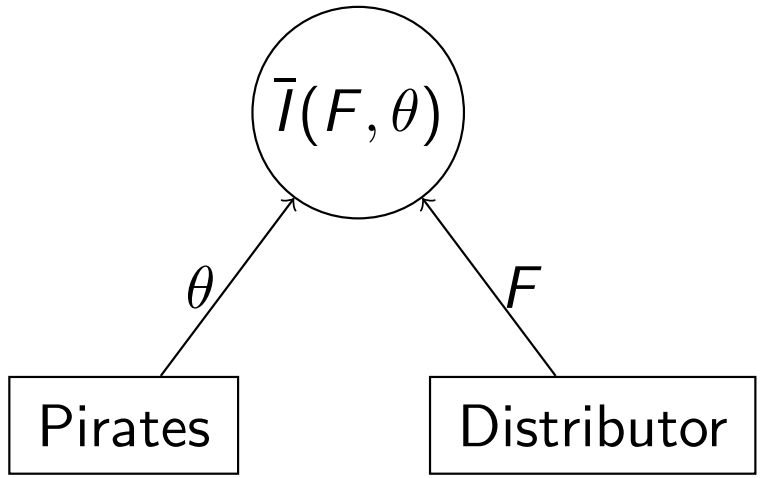
$$\bar{I}(F, \theta) \triangleq \frac{1}{c} \int_0^1 F(p_j) I\left(Y_j; Z_j \mid p_j\right) dp_j$$



Fingerprinting Game

- Distributor wants to maximize $\bar{I}(F, \theta)$ through F
- Pirates want to minimize $\bar{I}(F, \theta)$ through θ
- Fingerprinting Capacity C is defined as the optimal value of the fingerprinting game:

$$C \triangleq \max_{F} \min_{\theta} \bar{I}(F, \theta)$$



Code rates

- Code rate R is defined as:

$$R \triangleq \frac{\log_2 n}{m} \qquad n = \#\text{users}$$

$$m = \#\text{ code length in symbols}$$

- According to *Shannon's Theorem* code can only be reliable if $R < C$
- Code length m then satisfies:

$$m > \frac{\log_2 n}{C}$$

Asymptotic Solution

- Computing C is difficult in general
- We focus on the asymptotic limit $c \to \infty$
  where $c = \#$ pirates
- Solution for binary alphabet was found by Huang and Moulin [2010]
- We solved the non-binary case [2011]

Solution for binary alphabet

Theorem (Huang & Moulin (2010))

The binary asymptotic fingerprinting capacity C is given by:

$$C = \frac{1}{c^2 2 \ln 2} \qquad c \to \infty$$

with optimum strategies:

$$F^*(p) = \frac{1}{\pi} \frac{1}{\sqrt{p(1-p)}} \qquad \textit{(Arcsine distribution)}$$

$$\theta_z^* = \frac{z}{c} \qquad \textit{(Interleaving attack)}$$

Generalization to larger alphabets

- Code entries X_{ij} are from the alphabet $\mathcal{Q} = \{0, 1, 2, \ldots, q-1\}$
- Bias vector $\vec{p} \in [0,1]^q$ per column drawn from $F(\vec{p})$
- Each entry X_{ij} is generated by a dice throw with:

$$\text{Prob}\left[X_{ij} = \alpha \mid \vec{p}^{(j)}\right] = p_\alpha^{(j)}$$

$$X = \begin{bmatrix} \vec{p}^{(1)} & \vec{p}^{(2)} & \vec{p}^{(3)} & \vec{p}^{(4)} \\ \hline 0 & 1 & 2 & 2 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 2 & 1 & 0 & 1 \\ 0 & 1 & 2 & 0 \\ 2 & 0 & 1 & 0 \end{bmatrix}$$

Pirate strategy

- Random variable $\Sigma^{(j)}$ counts # symbols the pirates received in column j
- Pirate strategy θ is now defined by the probabilities:

$$\theta_{y|\vec{\sigma}} \triangleq \text{Prob}\left[Y_j = y \mid \Sigma^{(j)} = \vec{\sigma}\right]$$

- Interleaving attack $\bar{\theta}$ is:

$$\bar{\theta}_{y|\vec{\sigma}} \triangleq \frac{\sigma_y}{c}$$

$$X = \begin{bmatrix} \vec{p}^{(1)} & \vec{p}^{(2)} & \vec{p}^{(3)} & \vec{p}^{(4)} \\ \hline 0 & 1 & \boxed{2} & 2 \\ 1 & 0 & \boxed{1} & 1 \\ 1 & 1 & \boxed{1} & 0 \\ 2 & 1 & \boxed{0} & 1 \\ 0 & 1 & \boxed{2} & 0 \\ 2 & 0 & \boxed{1} & 0 \end{bmatrix}$$

$$\Sigma^{(3)} = (1, 3, 2)$$

Continuum limit of pirate strategy

In the limit of $c \to \infty$ we assume:

- The random variable $\frac{\Sigma^{(j)}}{c}$ becomes continuous in $[0,1]^q$
- The pirate strategy θ satisfies:

Continuous strategy

There exists $\forall y \in \mathcal{Q}$ a continuous and twice differentiable function $g_y : [0,1]^q \to [0,1]$ such that:

$$\theta_{y|\vec{\sigma}} = g_y\left(\frac{\vec{\sigma}}{c}\right) \qquad \forall \vec{\sigma}$$

Asymptotic mutual information game

The q-ary asymptotic fingerprinting capacity C_q can be derived as:

$$C_q = \frac{1}{c^2 2 \ln q} \max_F \min_g \int F(\vec{p}) T_g(\vec{p}) d\vec{p}$$

with

$$T_g(\vec{p}) = \sum_y \frac{1}{g_y(\vec{p})} \sum_{\alpha\beta} K_{\alpha\beta} \frac{\partial g_y(\vec{p})}{\partial p_\alpha} \frac{\partial g_y(\vec{p})}{\partial p_\beta}$$

$$K_{\alpha\beta} \triangleq \frac{1}{c} \mathrm{Cov}\left(\Sigma_\alpha^{(j)}, \Sigma_\beta^{(j)}\right) = \delta_{\alpha\beta} p_\alpha - p_\alpha p_\beta$$

Solving the max-min game

- We have by *Sion's Theorem*:

$$\max_F \min_g \int F(\vec{p}) T_g(\vec{p}) d\vec{p} = \min_g \max_F \int F(\vec{p}) T_g(\vec{p}) d\vec{p}$$
$$= \min_g \max_{\vec{p}} T_g(\vec{p})$$

- We prove $\min_g \max_{\vec{p}} T_g(\vec{p}) = q - 1$ in two steps:
  1. For any allowed strategy g we prove
  $$\max_{\vec{p}} T_g(\vec{p}) \geq q - 1$$
  2. The interleaving attack $\bar{g}$ defined by $\bar{g}_y(\vec{p}) = p_y$ has
  $$T_{\bar{g}}(\vec{p}) = q - 1$$

Final result

Theorem (Boesten & Škorić (2011))

The q-ary asymptotic fingerprinting capacity C_q is given by:

$$C_q = \frac{q-1}{c^2 2 \ln q} \qquad c \to \infty$$

- Our proof technique does not reveal optimal asymptotic strategies

Discussion

- $C_q \sim \frac{q-1}{\ln q}$ is an increasing function of q
- Larger alphabet leads to shorter codes
- Actual implementation of watermarking scheme might not allow larger alphabets
- Future work:
  - Solve the Max-Min game to obtain optimal strategies
  - Solve the game for a different attack model called *Combined Digit Model*