

Complete characterization of perfectly secure stego-systems with mutually independent embedding operation

Tomáš Filler and Jessica Fridrich

Dept. of Electrical and Computer Engineering
SUNY Binghamton, New York

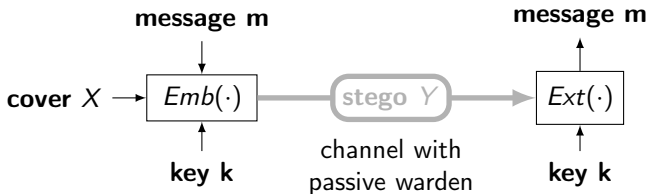
IEEE ICASSP 2009, Taipei, Taiwan



State University of New York

Steganography

Steganography is a mode of covert communication.



X and Y are r.v. on \mathcal{X}^n not necessarily i.i.d.
 $Emb(\cdot)$, $Ext(\cdot)$... embedding, extraction functions

Perfectly secure stegosystem (Cachin):

Cover distribution P and stego distrib. Q satisfy

$$D_{KL}(P||Q) = 0$$

Mutually Independent Embedding Operation

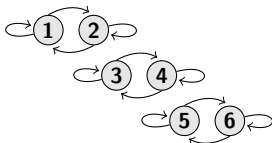
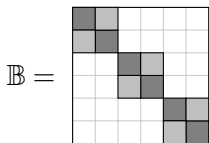
$Emb(\cdot)$ is a probabilistic mapping acting on each cover element (pixel, DCT, ...) independently - **MI embedding**.

$$Pr(Y_l = j | X_l = i) = b_{ij}(\beta)$$

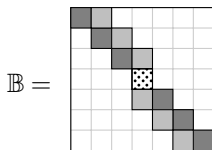
$X_l \dots l$ -th cover element
 $Y_l \dots l$ -th stego element
 $\beta \dots$ change rate (rel. payload)

Matrix $\mathbb{B} = (b_{ij})$ is stochastic (rows are pmfs) for all $\beta \geq 0$.

LSB embedding:



F5:



■ = $1 - \beta$

■ = β

▤ = 1

Perfectly Secure Cover Source

Cover source is
perfectly secure w.r.t. given MI embedding
 \Leftrightarrow
the **resulting stegosystem** is
perfectly secure.

Our Contribution

P ... cover distr. Q_β ... stego distr. with change rate β

Given **specific MI embedding** (matrix \mathbb{B}):

- 1 Complete characterization of perfectly secure cover sources w.r.t. \mathbb{B} .
- 2 Cover source is perfectly secure iff

$$I(0) = \left. \frac{\partial^2 D_{KL}(P||Q_\beta)}{\partial \beta^2} \right|_{\beta=0} = 0.$$

In general

$$D_{KL}(P||Q_\beta) = 0 \Leftrightarrow I(0) = 0$$

(1)

**Complete characterization of perfectly
secure cover distributions**

Perfectly Secure Covers w.r.t. MI embedding

Invariant distributions of MI embedding:

Matrix \mathbb{B} is stochastic \Rightarrow has $k \geq 1$ left eigenvectors

(invariant distributions) $\pi^{(a)}$, $a \in \{1, \dots, k\}$ to 1, $\pi^{(a)}\mathbb{B} = \pi^{(a)}$.

Perfectly Secure Covers w.r.t. MI embedding

Invariant distributions of MI embedding:

Matrix \mathbb{B} is stochastic \Rightarrow has $k \geq 1$ left eigenvectors
(invariant distributions) $\pi^{(a)}$, $a \in \{1, \dots, k\}$ to 1, $\pi^{(a)}\mathbb{B} = \pi^{(a)}$.

Example (perfectly secure cover):

If $P(X_1 = i, X_2 = j) = \pi_i^{(a)} \pi_j^{(a')}$, then P is perfectly secure.

Perfectly Secure Covers w.r.t. MI embedding

Invariant distributions of MI embedding:

Matrix \mathbb{B} is stochastic \Rightarrow has $k \geq 1$ left eigenvectors
(invariant distributions) $\pi^{(a)}$, $a \in \{1, \dots, k\}$ to 1, $\pi^{(a)}\mathbb{B} = \pi^{(a)}$.

Example (perfectly secure cover):

If $P(X_1 = i, X_2 = j) = \pi_i^{(a)} \pi_j^{(a')}$, then P is perfectly secure.

- Elements **distributed independently** with some invariant distribution form perfectly secure cover source.
- Set of all perfectly secure distributions **form convex hull**.
- **We know at least k^n linearly independent** perfectly secure cover sources on n elements.

Perfectly Secure Covers w.r.t. MI embedding

Invariant distributions of MI embedding:

Matrix \mathbb{B} is stochastic \Rightarrow has $k \geq 1$ left eigenvectors
(invariant distributions) $\pi^{(a)}$, $a \in \{1, \dots, k\}$ to 1, $\pi^{(a)}\mathbb{B} = \pi^{(a)}$.

Example (perfectly secure cover):

If $P(X_1 = i, X_2 = j) = \pi_i^{(a)} \pi_j^{(a')}$, then P is perfectly secure.

- Elements **distributed independently** with some invariant distribution form perfectly secure cover source.
- Set of all perfectly secure distributions **form convex hull**.
- **We know at least k^n linearly independent** perfectly secure cover sources on n elements.

Do we know all of them?

Perfectly Secure Covers - Main Result

k ... number of invariant distributions of given MI embedding

Theorem (Mutually independent embedding)

There are exactly k^n linearly independent perfectly secure probability distributions P on n -element covers. Every perfectly secure probability distribution P w.r.t. \mathbb{B} can be obtained by a convex linear combination of k^n linearly independent perfectly secure distributions.

Perfectly Secure Covers - Main Result

k ... number of invariant distributions of given MI embedding

Theorem (Mutually independent embedding)

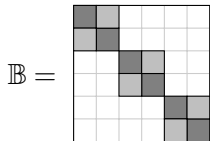
There are *exactly k^n linearly independent* perfectly secure probability distributions P on n -element covers. Every perfectly secure probability distribution P w.r.t. \mathbb{B} can be obtained by a convex linear combination of k^n linearly independent perfectly secure distributions.

Corollary (MI embedding in stationary covers)

There are *exactly k linearly independent* perfectly secure probability distributions P on n -element covers. These sources are i.i.d. with some invariant distribution $\pi^{(a)}$.

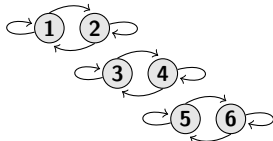
Perfectly Secure Covers - Example

LSB embedding:



■ = $1 - \beta$

■ = β



Left unit eigenvectors of \mathbb{B} (invariant distributions):

$$\pi^{(1)} = \left(\frac{1}{2}, \frac{1}{2}, 0, 0, 0, 0\right), \quad \pi^{(2)} = \left(0, 0, \frac{1}{2}, \frac{1}{2}, 0, 0\right), \quad \pi^{(3)} = \left(0, 0, 0, 0, \frac{1}{2}, \frac{1}{2}\right)$$

$$k = 3 \quad \pi^{(a)} \mathbb{B} = \pi^{(a)}$$

Perfectly secure cover w.r.t. LSB embedding must be independent with evened out histogram bins.

(2)

**Fisher Information and perfectly
secure cover distributions**

Perfect Security and Fisher Information

P ... cover distr. Q_β ... stego distr. with change rate β

Observation: If P is perfectly secure w.r.t. \mathbb{B} , then $I(0) = 0$.

$$D_{KL}(P||Q_\beta) = D_{KL}(Q_0||Q_\beta) = \frac{1}{2}I(0) \cdot \beta^2 + O(\beta^3)$$

Fisher Information (w.r.t. change rate β):

$$I(0) = E_P \left[\frac{\partial}{\partial \beta} \log Q_\beta(Y) \Big|_{\beta=0} \right]^2 = \frac{\partial^2 D_{KL}(P||Q_\beta)}{\partial \beta^2} \Big|_{\beta=0}$$

$I(0)$ is related to quantitative steganalysis (Cramer-Rao LB).

What can we say about security of P w.r.t. \mathbb{B} if $I(0) = 0$?

Perfect Security and Fisher Information

P ... cover distr. Q_β ... stego distr. with change rate β

Observation: If P is perfectly secure w.r.t. \mathbb{B} , then $I(0) = 0$.

$$D_{KL}(P||Q_\beta) = D_{KL}(Q_0||Q_\beta) = \frac{1}{2}I(0) \cdot \beta^2 + O(\beta^3)$$

Fisher Information (w.r.t. change rate β):

$$I(0) = E_P \left[\frac{\partial}{\partial \beta} \log Q_\beta(Y) \Big|_{\beta=0} \right]^2 = \frac{\partial^2 D_{KL}(P||Q_\beta)}{\partial \beta^2} \Big|_{\beta=0}$$

$I(0)$ is related to quantitative steganalysis (Cramer-Rao LB).

What can we say about security of P w.r.t. \mathbb{B} if $I(0) = 0$?

Nothing in general but a lot for MI embedding!

Fisher Information vs. Perfect Security

Theorem (Fisher Information)

- There are *exactly k^n linearly independent* probability distributions P on n -element covers satisfying $I(0) = 0$.
- These distributions are *perfectly secure w.r.t. \mathbb{B}* .
- Every other probability distribution P satisfying $I(0) = 0$ can be obtained by convex linear combination of k^n linearly independent perfectly secure distributions.

Fisher Information vs. Perfect Security

Theorem (Fisher Information)

- There are *exactly k^n linearly independent* probability distributions P on n -element covers satisfying $I(0) = 0$.
- These distributions are *perfectly secure w.r.t. \mathbb{B}* .
- Every other probability distribution P satisfying $I(0) = 0$ can be obtained by convex linear combination of k^n linearly independent perfectly secure distributions.

Corollary (equivalent condition for perfect security)

For arbitrary MI embedding and under no assumption about cover source

$$I(0) = 0 \Leftrightarrow D_{KL}(P||Q_\beta) = 0$$

Application in Determining Steganographic Capacity

Capacity of imperfect stegosystems with MI embedding only increases with the square root of the number of cover elements (pixels).

Square Root Law of IMPERFECT steganography:

- 1 If $\frac{n\beta_n}{\sqrt{n}} \rightarrow 0$ then the stegosyst. are asymptotically secure.
- 2 If $\frac{n\beta_n}{\sqrt{n}} \rightarrow +\infty$ then arbitrarily accurate stego detectors exist.

We used $I(0) = 0$ to exclude all perfectly secure covers.

[Filler, Ker, Fridrich, "The Square Root Law of Steganographic Capacity for Markov Covers", Proc. SPIE, 2009]

Conclusion and Future Directions

Virtually all stegosystems use MI embedding in some appropriate domain (this makes our result relevant to most stegosystems).

Perfectly secure covers form

- convex hull with known basis.

Fisher information w.r.t. change rate

- is an equivalent perfect security descriptor
- is valuable tool for theoretical steganalysis (SRL)

Future work: use Fisher information for benchmarking stegosystems.

Conclusion and Future Directions

Virtually all stegosystems use MI embedding in some appropriate domain (this makes our result relevant to most stegosystems).

Perfectly secure covers form

- convex hull with known basis.

Fisher information w.r.t. change rate

- is an equivalent perfect security descriptor
- is valuable tool for theoretical steganalysis (SRL)

Future work: use Fisher information for benchmarking stegosystems.

Thank you!

tomas.filler@binghamton.edu