Minimizing Additive Distortion Functions with Non-binary Embedding Operation in Steganography

Tomáš Filler and Jessica Fridrich

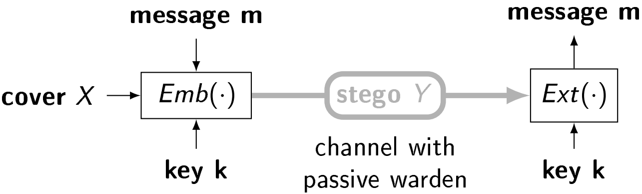
Dept. of Electrical and Computer Engineering
SUNY Binghamton, New York

Second IEEE International Workshop on
Information Forensics and Security
December 15, 2010

BINGHAMTON UNIVERSITY
State University of New York

Steganography

Steganography is a mode of covert communication.



X and Y are r.v. on $\mathscr{X}^n$ — digital images for example

$Emb(\cdot)$, $Ext(\cdot)$ ... embedding, extraction functions

Perfectly secure steganography:

Probability distribution of X and Y are exactly the same.

No statistical test (warden) can detect steganography.

Can we construct perfectly secure stegosystems?

Yes, but ...
only for artificial cover sources for which we know the exact probability distribution (Gaussian).

No perfectly secure stegosystem exists for real digital media.

Can we construct perfectly secure stegosystems?

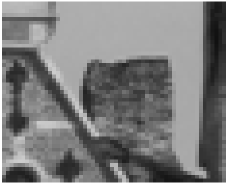
Yes, but ...
only for artificial cover sources for which we know the exact probability distribution (Gaussian).

No perfectly secure stegosystem exists for real digital media.
In practice, we have to do...

Steganography by cover modification:
Stego object Y is produced by slightly modifying some of the elements (pixels, DCT coefficients, ...) in X.

Which pixels can be changed?

Pixels in hard-to-model content.



Do not change saturated pixels!

Minimal-distortion Embedding

Pixels in textured areas can be changed more frequently than those in smooth areas.

Embedding operation $\mathscr{I}_i \subset \mathscr{I}$:
Set of stego pixels into which ith cover pixel can be changed.
Binary if $|\mathscr{I}_i| = 2$ for all pixels.

Additive distortion funct.: $\rho_i(y_i, x)$ = cost of changing $x_i \rightarrow y_i$

cost of changing cover x to stego y $\longrightarrow$ $D(x,y) = \sum_{i=1}^{n} \rho_i(y_i, x)$

Example:

- $\rho_i(x_i, x) = 0$ and $\rho_i(x_i - 1, x) = \rho_i(x_i + 1, x) = 1$ # of changes
- $\rho_i(y_i, x) \gg 1$ if y_i should almost never be used for pixel i

Problem Fomulation & Optimal Solution

THEORY

Embedding algorithm for FIXED cover x:
Select stego y with probability $Pr(y|x) = \pi(y|x)$.

What is the best distribution π?

Payload-limited sender: choose π such that

minimize expected distortion while Entropy$[\pi] = m$ bits

Solution: $\pi(y|x) \propto \exp(-\lambda D(x,y))$ and λ solves payl. constr.

Problem Fomulation & Optimal Solution

THEORY

Embedding algorithm for FIXED cover x:
Select stego y with probability $Pr(y|x) = \pi(y|x)$.

What is the best distribution π?

Payload-limited sender: choose π such that

minimize expected distortion while Entropy$[\pi] = m$ bits

Solution: $\pi(y|x) \propto \exp(-\lambda D(x,y))$ and λ solves payl. constr.

PRACTICE:
Send m bits in stego y with $D(x,y)$ as small as possible.
Receiver does not know cover x and costs ρ_i, just msg. size!

Problem bares strong relationship with the
"source coding with a fidelity criterion" (Shannon 1959).

Problem Fomulation & Optimal Solution

THEORY

Embedding algorithm for FIXED cover x:
Select stego y with probability $Pr(y|x) = \pi(y|x)$.

What is the best distribution π?

Payload-limited sender: choose π such that

minimize expected distortion while Entropy$[\pi] = m$ bits

Solution: $\pi(y|x) \propto \exp(-\lambda D(x,y))$ and λ solves payl. constr.

PRACTICE:
Send m bits in stego y with $D(x,y)$ as small as possible.
Receiver does not know cover x and costs ρ_i, just msg. size!

MAIN CONTRIBUTION: practical and near-optimal approach for solving non-binary embedding problem.

(1)

Binary embedding operation.

Cover and stego pixels $\in \{0,1\}$

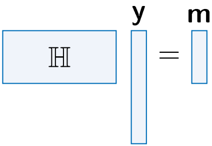
Review of known facts and algorithms.

Syndrome Coding

Common tool for solving the source-coding problem.

$\mathbb{H} \in \{0,1\}^{m \times n}$ ... shared parity-check matrix

Extraction function:



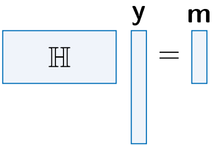
$$\mathbf{m} = Ext(\mathbf{y}) = \mathbb{H}\mathbf{y}$$

Syndrome Coding

Common tool for solving the source-coding problem.

$\mathbb{H} \in \{0,1\}^{m \times n}$ ... shared parity-check matrix

Extraction function:



$$\mathbf{m} = Ext(\mathbf{y}) = \mathbb{H}\mathbf{y}$$

Embedding function:

$$\mathbf{y} = Emb(\mathbf{x}, \mathbf{m}) = \arg \min_{\mathbb{H}\mathbf{y}=\mathbf{m}} D(\mathbf{x}, \mathbf{y})$$

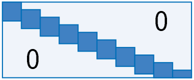
Replace x with y, such that $D(\mathrm{x}, \mathrm{y})$ is minimal and $\mathbb{H}\mathrm{y} = \mathrm{m}$.

Embedding is NP hard problem for general parity-check matrix $\Rightarrow$ we need some structure in $\mathbb{H}$.

Syndrome-Trellis Codes (SPIE 2010)

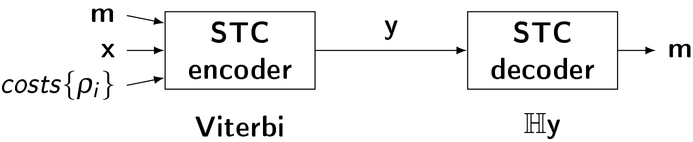
Practical and very versatile class of linear codes.

Parity-check matrix: **banded matrix**

$\mathbb{H} =$ 

$\Rightarrow$ **efficient graphical representation**

Embedding $\arg\min_{\mathbb{H}\mathbf{y}=\mathbf{m}} D(\mathbf{x},\mathbf{y})$ **is realized by the Viterbi alg.**



(2)

Non-binary embedding operation.

Main contribution of the paper.

Multi-layered Construction (1/2)

Example (quaternary embedding operation):
Pixels $x_i, y_i \in \{0,1,2,3\}$ can be represented as $\underbrace{(MSB, LSB)}_{2\,\text{bits}}$.

Problem:
Embed m bits into cover x such that $D(x,y)$ is minimal.
Optimal coding scheme sends ith stego pixel according to

$$Pr(y_i|x) \propto \exp(-\lambda \rho_i(y_i, x)).$$

Use "product rule" $Pr(MSB, LSB) = Pr(MSB) \cdot Pr(LSB|MSB)$.

$$\text{Entropy}[MSB, LSB] = \underbrace{\text{Entropy}[MSB]}_{\text{1st layer of MSBs}} + \underbrace{\text{Entropy}[LSB|MSB]}_{\text{2nd layer of LSBs}}$$

How to implement this using STCs in practice?

Multi-layered Construction (2/2)

$$\text{Entropy}[MSB, LSB] = \underbrace{\text{Entropy}[MSB]}_{\text{1st layer of MSBs}} + \underbrace{\text{Entropy}[LSB|MSB]}_{\text{2nd layer of LSBs}}$$

1st layer of MSBs:
Embed Entropy[MSB] bits into MSBs by minimizing costs

$$\rho_i(MSB = 0) = \rho_i(0, x) + \rho_i(1, x)$$

$$\rho_i(MSB = 1) = \rho_i(2, x) + \rho_i(3, x)$$

2nd layer of LSBs:
Embed Entropy[$LSB|MSB$] bits into LSBs with costs

$$MSB = 0 \Rightarrow \begin{array}{l} \rho_i(LSB = 0) = \rho_i(0, x) \\ \rho_i(LSB = 1) = \rho_i(1, x) \end{array}$$

$$MSB = 1 \Rightarrow \begin{array}{l} \rho_i(LSB = 0) = \rho_i(2, x) \\ \rho_i(LSB = 1) = \rho_i(3, x) \end{array}$$

This is optimal if we know how to solve the binary problems.

Practical Issues

THEORY:

Order in which layers are processed does not matter.

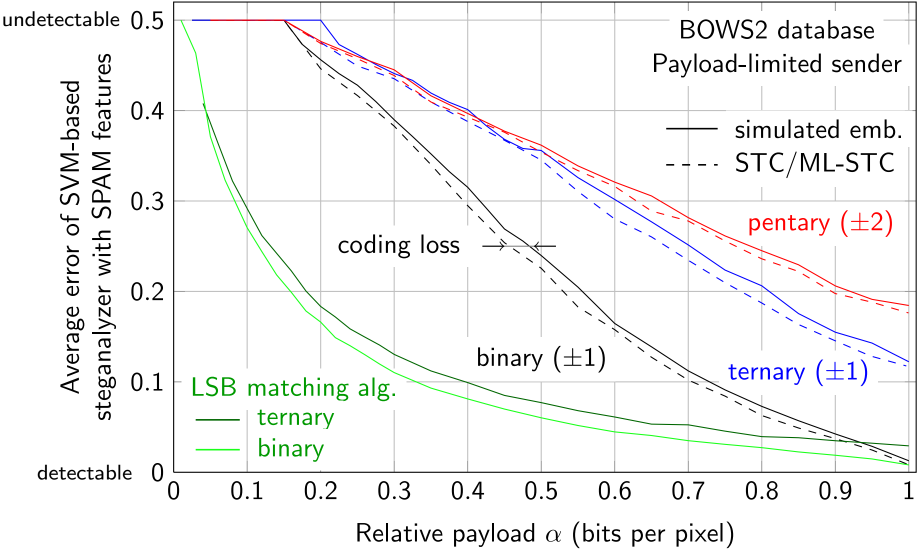
$$\text{Entropy}[MSB, LSB] = \underbrace{\text{Entropy}[MSB]}_{\text{MSBs first}} + \underbrace{\text{Entropy}[LSB|MSB]}_{\text{then LSBs}}$$
$$= \underbrace{\text{Entropy}[LSB]}_{\text{LSBs first}} + \underbrace{\text{Entropy}[MSB|LSB]}_{\text{then MSBs}}$$

PRACTICE:

Order in which layers are processed DOES play a role.

Different expansions lead to different costs assignments for which the practical codes (STCs) may fail.

Application to Spatial-Domain Digital Images



Conclusion

Proposed Multi-layered construction allows

- implementing the minimal-distortion embedding paradigm with non-binary embedding operation.
- Optimal if optimal binary source-coding exist.
- Near-optimal when realized with Syndrome-Trellis Codes
- No need to share the costs with the receiver.

Future directions:

- Can we minimize statistical detectability by learning costs $\rho_i(y_i, x)$? $\Rightarrow$ SPIE 2011.

C++ and Matlab implementation available.

Information Hiding 2011, May 18-20, Prague

www.ihconference.org

Submission deadline: January 17 (extension possible)
IEEE ICASSP is also in Prague May 22-27.

See you in Prague.