Minimizing Embedding Impact in Steganography using Trellis-Coded Quantization

Tomáš Filler, Jan Judas and Jessica Fridrich

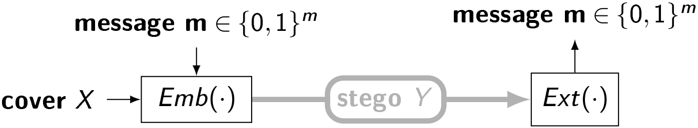
Dept. of Electrical and Computer Engineering
SUNY Binghamton, New York

IS&T / SPIE 2010, San Jose, CA

BINGHAMTON UNIVERSITY
State University of New York

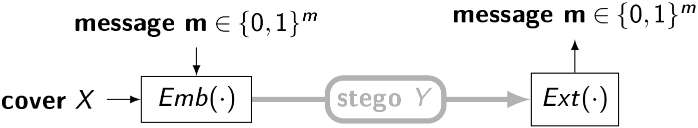
Steganography of Real Digital Media

Cover distribution of real digital media is too complex to be preserved exactly.



Steganography of Real Digital Media

Cover distribution of real digital media is too complex to be preserved exactly.



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

We assume binary embedding operation.

X, $Y \in \{0,1\}^n$ are obtained via mod 2 of cover elements.

Embedding Impact

Total impact of embedding (distortion metric): $x_i, y_i \in \{0, 1\}$

$$D(\mathbf{x}, \mathbf{y}) = \|\mathbf{x} - \mathbf{y}\|_\rho = \sum_{i=1}^{n} \rho_i |x_i - y_i|,$$

$\rho_i \in [0, \infty)$ is a cost of changing ith cover element.
Wet elements ($\rho_i = \infty$) should not be modified at all.

Embedding Impact

Total impact of embedding (distortion metric): $x_i, y_i \in \{0,1\}$

$$D(\mathbf{x},\mathbf{y}) = \|\mathbf{x}-\mathbf{y}\|_\rho = \sum_{i=1}^{n} \rho_i |x_i - y_i|,$$

$\rho_i \in [0,\infty)$ is a cost of changing ith cover element.
Wet elements ($\rho_i = \infty$) should not be modified at all.

Examples of detectability measures:

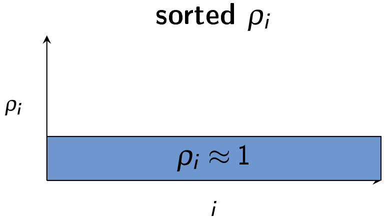
- $\rho_i = 1\ \forall i$ then $D(\mathbf{x},\mathbf{y})$ is total number of emb. changes
- $\rho_i = 1\ i \in Dry$ and $\rho_i = \infty\ i \in Wet \Rightarrow$ Wet Paper Channel
- $\rho_i = Q - 2e_i$ Perturbed Quantization
  Q ... quantization step, $0 \le e_i \le \frac{Q}{2}$ ... quant. error

PROBLEM: create practical algorithm for embedding m bits in n element cover such that $D(\mathbf{x},\mathbf{y})$ is minimal.

Distortion Profiles

Bounded distortion ($\rho_i < \infty$):

- constant profile

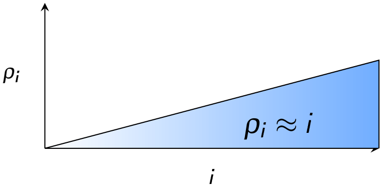


Distortion Profiles

Bounded distortion ($\rho_i < \infty$):

- constant profile
- linear profile

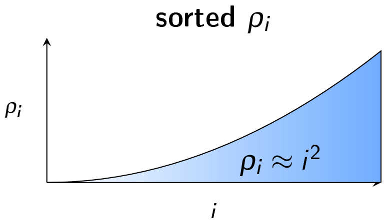
sorted ρ_i



Distortion Profiles

Bounded distortion ($\rho_i < \infty$):

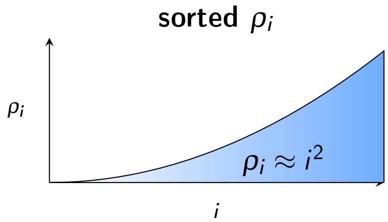
- constant profile
- linear profile
- square profile



Distortion Profiles

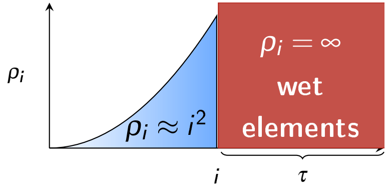
Bounded distortion ($\rho_i < \infty$):

- constant profile
- linear profile
- square profile



Wet Paper Channel (ρ_i may be ∞):

Wet Paper Channel
with square profile
relative wetnes $\tau = 0.5$



Relative Payload & Embedding Efficiency

m ... # of msg bits, k ... # of semi-dry elements ($\rho_i < \infty$)

Relative payload: $\alpha = m/k$

- required to be small to stay undetectable ($\alpha \approx 1/10$)
- has to decrease with increasing cover size **(Square Root Law)**

Relative Payload & Embedding Efficiency

m ... # of msg bits, k ... # of semi-dry elements ($\rho_i < \infty$)

Relative payload: $\alpha = m/k$

- required to be small to stay undetectable ($\alpha \approx 1/10$)
- has to decrease with increasing cover size **(Square Root Law)**

Embedding efficiency: $e = m/D(\mathbf{x}, \mathbf{y})$

Number of bits embedded per unit distortion.

Upper bound:

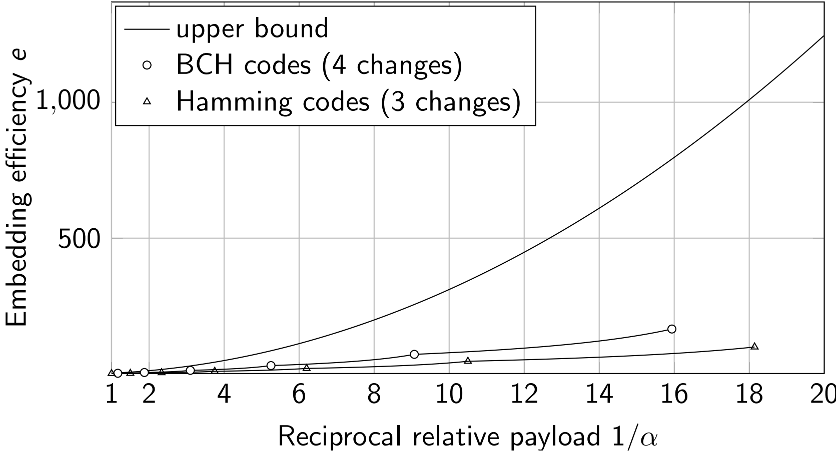
Constant profile ($\rho_i = 1$):

$$e \leq \frac{\alpha}{H^{-1}(\alpha)}$$

Other profiles:

See paper.

State of the Art - Square Profile



Goal: design new algorithms being able to handle arbitrary profile very close to the bound.

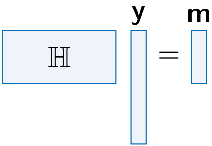
Syndrome Coding Approach

Common tool for constructing steganographic schemes.

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

Extraction function:

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

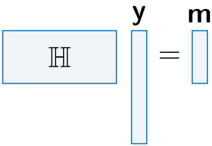


Syndrome Coding Approach

Common tool for constructing steganographic schemes.

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

Extraction function:



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

Embedding function:

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

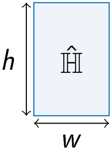
Replace x with y, such that $D(\mathrm{x}, \mathrm{y})$ is minimal and $\mathbb{H}\mathrm{y} = \mathrm{m}$.

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

Syndrome Trellis Codes (1/3)

Parameters: $h \in \{1, \ldots, 15\}$ **... constraint height,** $w = 1/\alpha$

Parity-check matrix $\mathbb{H} \in \{0,1\}^{m \times n}$**:**

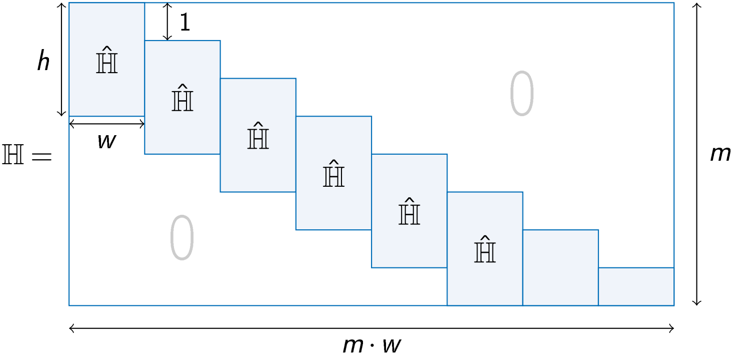


generate $\hat{\mathbb{H}} \in \{0,1\}^{h \times w}$ **pseudo-randomly**

Syndrome Trellis Codes (1/3)

Parameters: $h \in \{1, \ldots, 15\}$ **... constraint height,** $w = 1/\alpha$

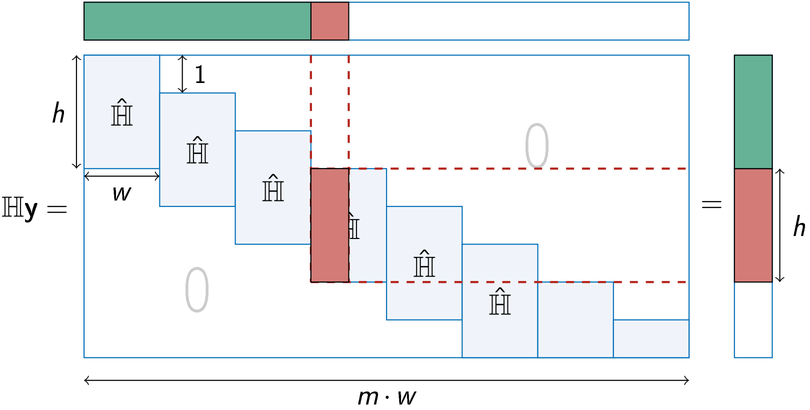
Parity-check matrix $\mathbb{H} \in \{0,1\}^{m \times n}$**:**



Syndrome Trellis Codes (1/3)

Parameters: $h \in \{1, \ldots, 15\}$ **... constraint height,** $w = 1/\alpha$

Parity-check matrix $\mathbb{H} \in \{0,1\}^{m \times n}$:



Syndrome Trellis Codes (2/3)

Syndrome trellis ($h = 2$): $\mathbf{x} = (0, \ldots, 0)$, $\mathbf{m} = (0, 1, \ldots)$

candidates for stego

$\mathbf{y} = (0, 0, ?, \ldots, ?)$

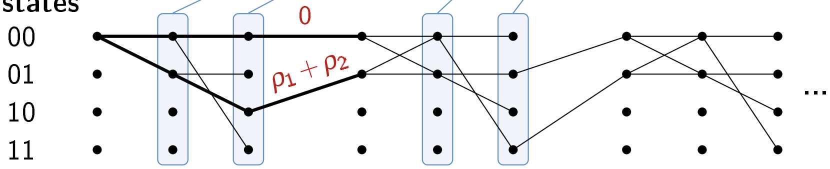
$\mathbf{y} = (\underbrace{1, 1}, ?, \ldots, ?)$

2 elements changed

$\Rightarrow$ **cost** $= \rho_1 + \rho_2$

$$\mathbb{H} = \begin{pmatrix} 1 & 1 & & & & & & \\ 0 & 1 & 1 & 1 & & & & \\ & & 0 & 1 & 1 & 1 & & \\ & & & & 0 & 1 & 1 & 1 \end{pmatrix}$$

2^h states



$\mathbf{m}_1 = 0$ $\mathbf{m}_2 = 1$

Syndrome Trellis Codes (3/3)

Viterbi algorithm (optimal quantizer):

Finds the shortest path (closest stego object)

in the syndrome trellis.

Syndrome Trellis Codes (3/3)

Viterbi algorithm (optimal quantizer):

Finds the shortest path (closest stego object)

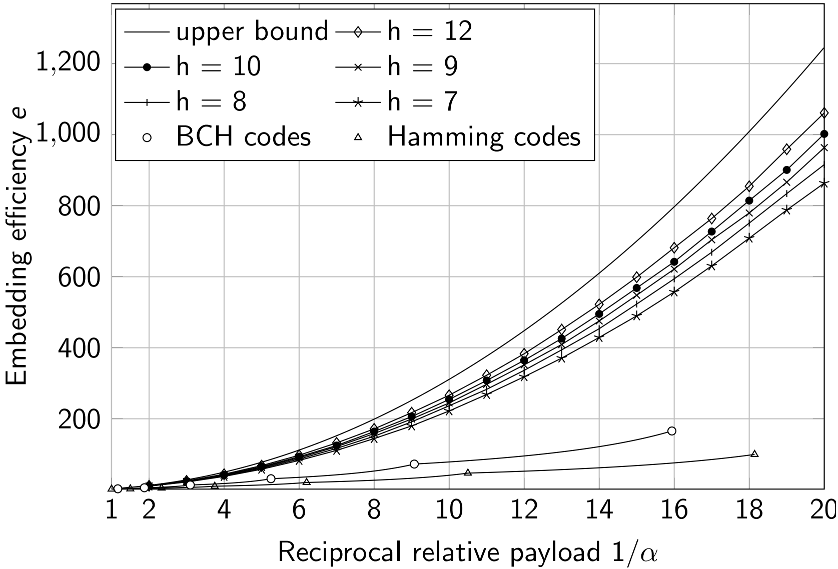
in the syndrome trellis.

Complexity:

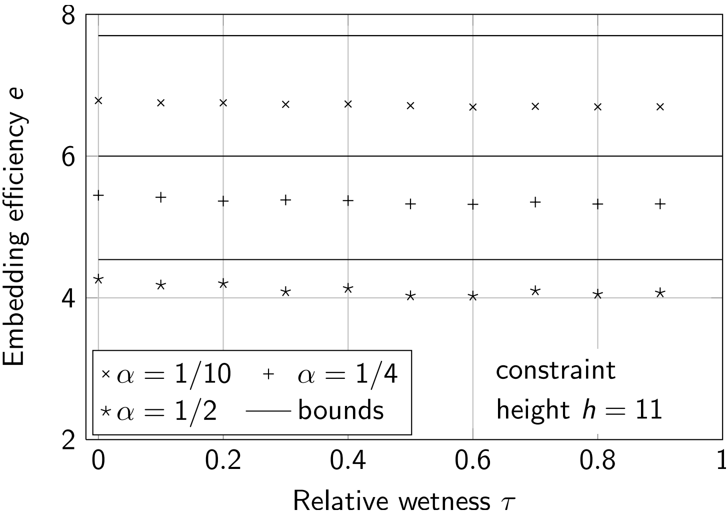
Time and space $\mathcal{O}(2^h n)$.

Whole cover object can be used for embedding.

Results - Square Profile

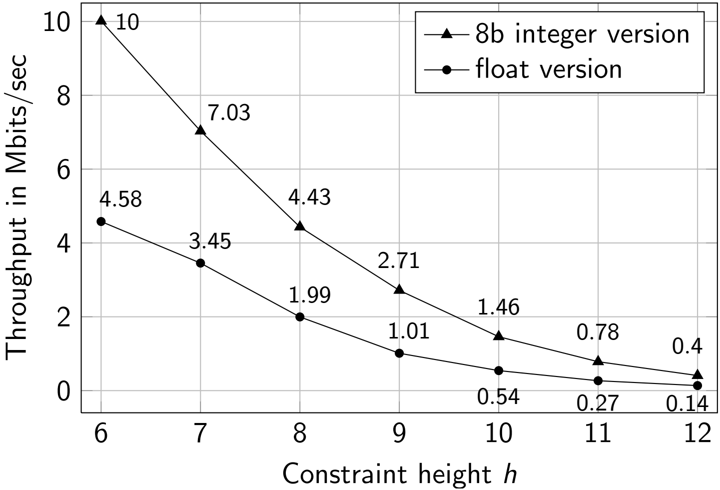


Wet Paper Channel with Constant Profile



No performance drop with wet elements, profile independent!

Results - Speed (independent of α)



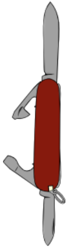
1MPix image embedded in less than 2 seconds!

Conclusion

Principle of minimal embedding impact
is an important design rule for steganography.

Syndrome Trellis Codes
allows to minimize the embedding impact

- for arbitrary profile (even with wet elements)
- for arbitrary rational relative payload $\alpha \leq 1/2$
- with near-optimal embedding efficiency
- where speed can be traded for performance.



Optimized C++ and Matlab code available.

http://dde.binghamton.edu/download

tomas.filler@binghamton.edu

Do you want to join the game?

BOSS

Break Our Steganographic System

Steganalytic chalange is coming up in 2010!
1000 images, 500 with a hidden message
Guess which ones!

`http://boss.gipsa-lab.grenoble-inp.fr`