

SAND2013-4217P

# Steganography and Steganalysis in Digital Media

Tu-Thach Quach

Sandia National Laboratories

July 9, 2013



Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.



Cover image from BOSSbase 0.92 image database.

# Introduction

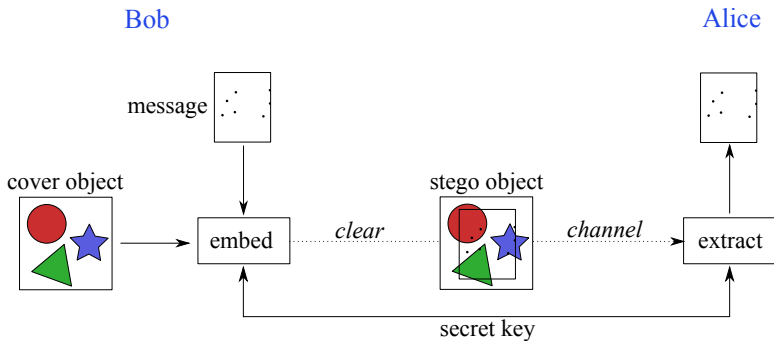
## ① Steganography

- Classical Hiding Techniques
- Techniques in Digital Media
- Square Root Law of Steganographic Capacity

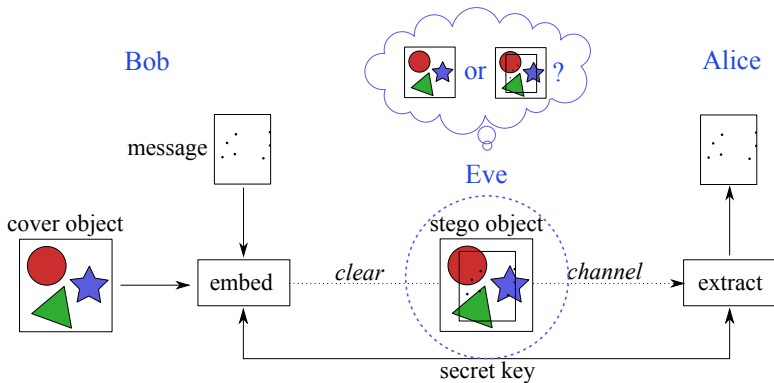
## ② Steganalysis

- Approach and Challenges
- Payload Location

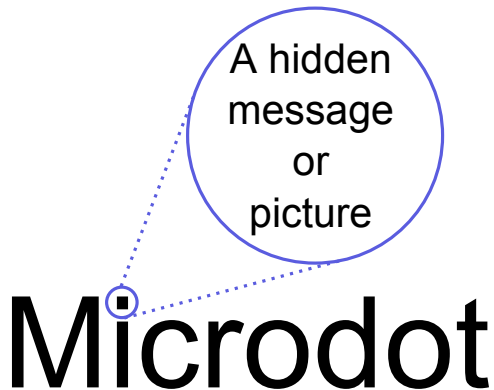
# Steganography



# Steganography



# Microdot



Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils.

Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils.

Pershing sails from NY June 1

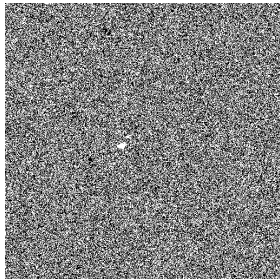
## Others

- Shave head and tattoo.
- Wax tablet.
- Invisible ink.
- Postage stamp with message on back.
- Musical notes.

## Hiding in Digital Images

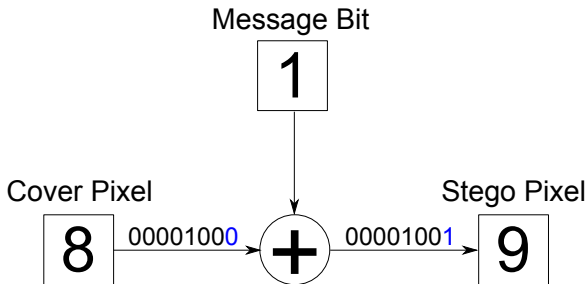


Cover image



Least significant bit

# LSB Replacement Steganography



# Group-Parity Steganography

Use multiple pixels to embed a single bit (2 pixels, 1 bit):

$$m_1 = c_1 \oplus c_2, \text{ no change}$$

$$m_1 \neq c_1 \oplus c_2, \text{ change } c_1 \text{ or } c_2$$

# Matrix Embedding

Use multiple pixels to embed several bits (3 pixels, 2 bits):

$$m_1 = c_1 \oplus c_3, \quad m_2 = c_2 \oplus c_3, \quad \text{no change}$$

$$m_1 \neq c_1 \oplus c_3, \quad m_2 = c_2 \oplus c_3, \quad \text{change } c_1$$

$$m_1 = c_1 \oplus c_3, \quad m_2 \neq c_2 \oplus c_3, \quad \text{change } c_2$$

$$m_1 \neq c_1 \oplus c_3, \quad m_2 \neq c_2 \oplus c_3, \quad \text{change } c_3$$

# General Framework

Find  $\mathbf{e}$  such that  $\mathbf{e}^T \mathbf{d}$  is minimized subject to

$$\mathbf{A}(\mathbf{c} + \mathbf{e}) = \mathbf{m}. \quad (1)$$

# Capacity

**Capacity:** how much should be hidden?

**Perfect** steganography: distribution of cover objects and stego objects are identical.

- Undetectable/Secure.
- Capacity is linear with data sent.

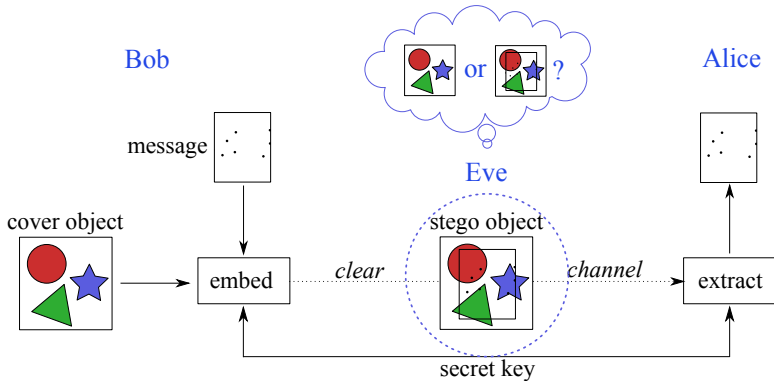
**Imperfect** steganography: embedding changes cover object

- More practical.
- Square root law [Ker].

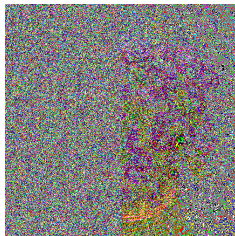
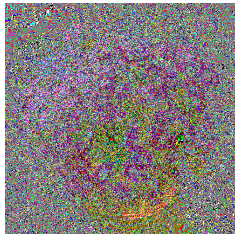
# Square Root Law

The amount of information that can be securely hidden is asymptotically proportional to the square root of the size of the cover object  $[Ker]$ .

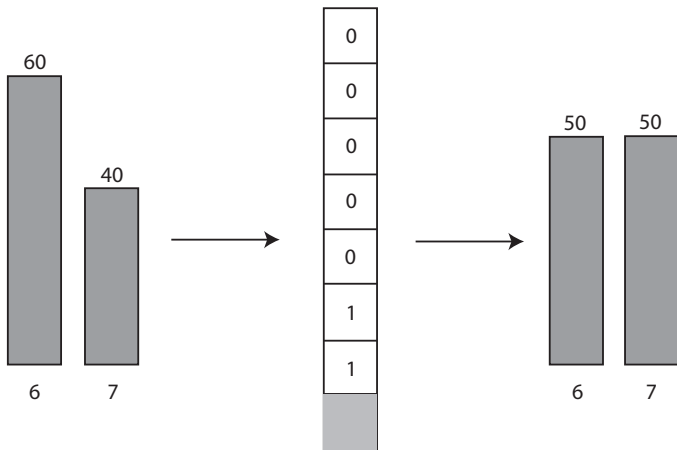
# Steganalysis



# Visual Inspection



## Structural Analysis



Half will be 0 and half will be 1 after LSB embedding

# Current Techniques

## Current Approach:

- Extract features (histograms, high-order models, etc.).
- Apply pattern classification algorithms (SVM, etc.).

## Challenges:

- High dimensional feature space (50,000 features).
- Few training samples.
- Too many training samples (months training with SVM).

# Payload Location

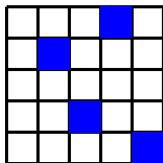
## Goal:

- Identify message bits, but not necessarily their logical order.

## Approach:

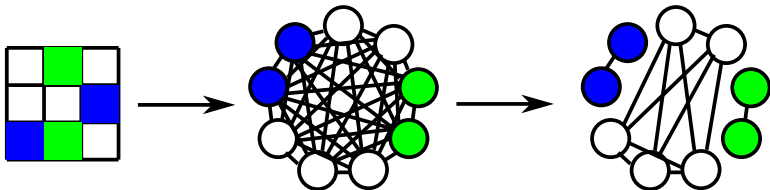
- Use a number of stego images.
- Payload in each image is determined by same set of pixels.

## Payload Location: Simple LSB



Known cover images:  $\log_2 m$  image pairs to locate payload.

## Payload Location: Group-Parity



Known cover images:  $8k^2 \log(km)$  image pairs to locate payload.

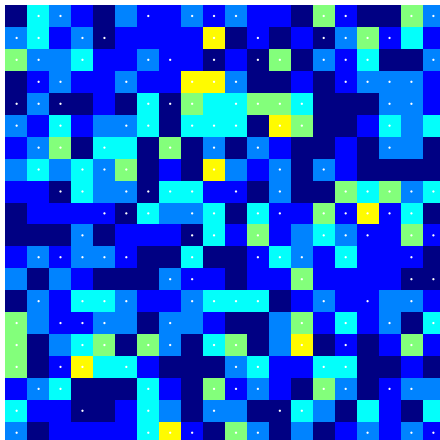
## Cover Estimation

Given stego image  $\mathbf{s}$ , estimate cover image:

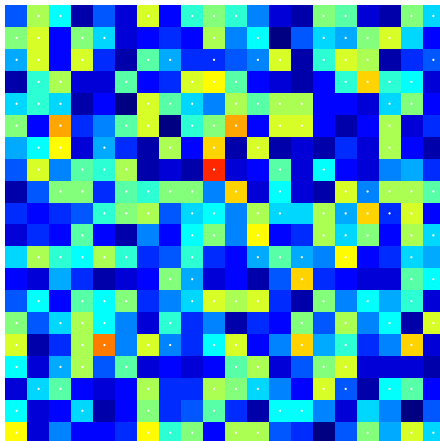
$$\hat{\mathbf{c}} = \arg \max_{\mathbf{c}} p(\mathbf{c}|\mathbf{s}). \quad (2)$$

- MAP estimators:  $\rightarrow, \leftarrow, \uparrow, \downarrow, \nearrow, \searrow, \nwarrow, \swarrow$ .
- Markov Random Field: captures two-dimensional constraints in images.

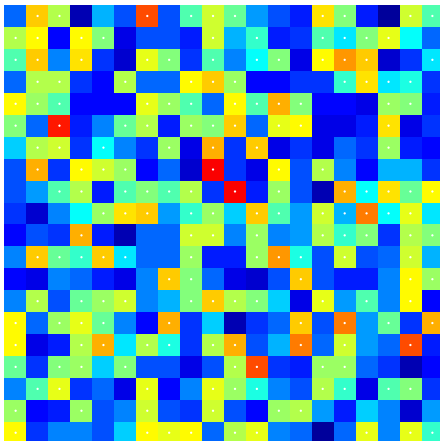
# 10 Images



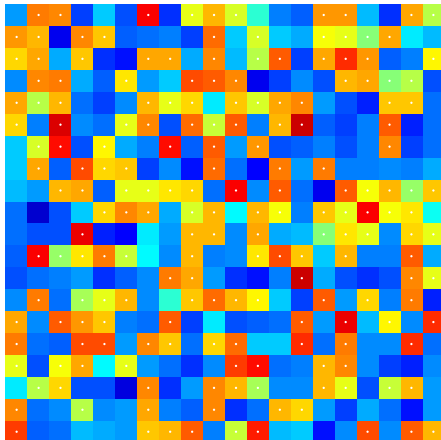
# 50 Images



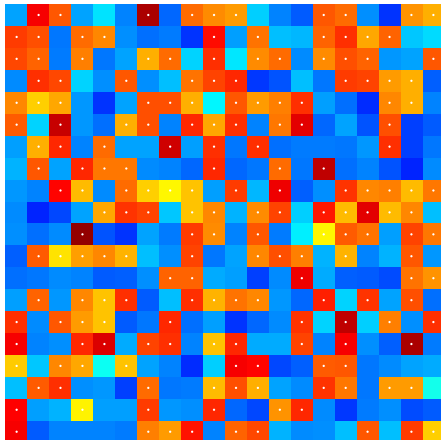
# 100 Images



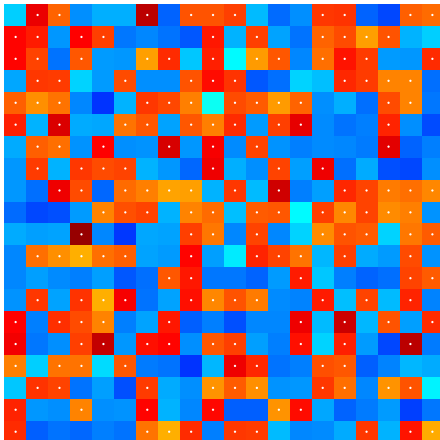
## 200 Images



# 500 Images



# 1000 Images



# Perfect Cover Estimator

Payload location accuracy depends on good cover estimators.

- Perfect estimator not likely.
- Accuracy can be improved using several estimators:  
Locatability Theorem.

# Locatability Theorem

Given a single stego image, all modified pixels can be located using a sufficiently large number of independent modified pixel detectors where each detector performs better than guessing [Quach].

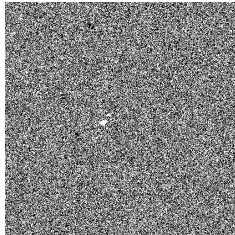
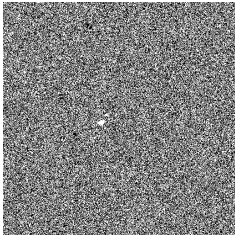
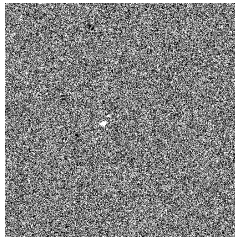
## Conclusions

- Embedding techniques are sophisticated and rapidly approaching theoretical limits.
- Capacity of imperfect steganography follows square root law.
- Ensemble classification and online learning for steganalysis.
- Detecting stego content is hard, extracting hidden message is even more challenging.
- There is more interesting work to do in payload location.



Cover image from BOSSbase 0.92 image database.

Did u  
guess  
right ?



Thank You

tong@sandia.gov