

Image Forensics and Steganalysis

(Hans) Georg Schaathun

Department of Computing
University of Surrey

26 June 2009



- 1 Examples
 - Tampering
 - Different Security Scenarios
- 2 Steganography and Steganalysis
 - Steganography
 - JPEG and F5
 - The Markov Based Model
 - Double Compression
 - Conditional Probability Features
- 3 Our group
- 4 Conclusion



How worrying is the Iranian weaponry?



- Picture from AFP.
- One of the rockets really fired
- Some rockets are the product of PhotoShop...
- The image was retracted after publication



Crime Scene Photography



- What did the crime scene look like?
 - Photography is vital evidence
- Photography can be altered...
 - What can we prove?



Who were actually there?



- Former Culture Secretary James Purnell
- Late for the meeting.
 - Arrived after three other MPs had to leave.
- James Purnell was added to the picture
- (BBC News - 28 September 2007)

Is the photo real?

- Does it show reality?
- Or has its author exercises artistic licence?
 - tampering with evidence
 - adding grandeur to a story
 - computer generated images
- For example
 - Merging images
 - Erasing details or objects

Where does the photo come from?

- Objective: add credibility to claims
- All information about the image is potentially useful...
- Which camera took the image?
- Time of day, time of year, etc.
- Subsequent image processing
 - contrast, compression, brightness, etc.

Is there more than meets the eye?

- Additional information hidden in the image?
 - known as *steganography*

Three important questions

- 1 Is the photo real?
- 2 Where does the photo come from?
- 3 Is there more than meets the eye?



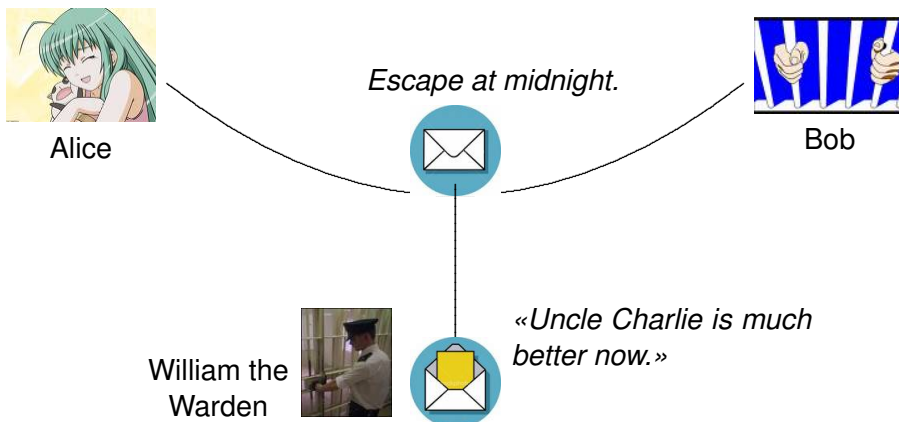
User scenarios

- News agency, news paper, etc.
 - can we trust images from the public?
 - they can get thousands of images in a day
- Forensics and Court of Law
 - what can we prove?
 - what is the truth?
 - is the image real or synthetic?
- Intelligence services
 - is there secret communications hidden in the image?



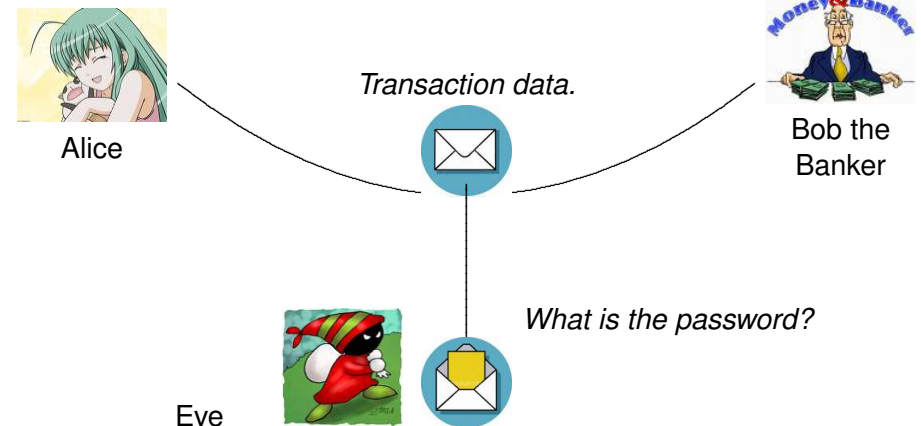
The basic problem

Simmons Crypto'83



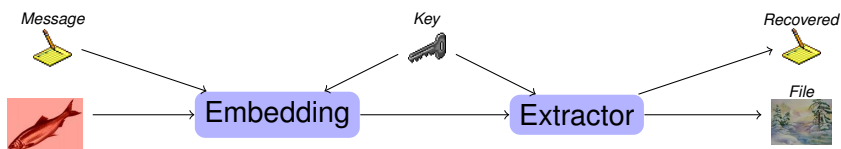
The basic crypto-problem

Encryption



The data hiding system

Watermarking System



- Security depends on the confidentiality of the algorithm.



Definitions

The tools

Definition (Stego-system)

A system which allows Alice and Bob to communicate secretly without Eve **knowing that** any secret communication is taking place.

Definition (Steganography)

The study of (and art of developing) stego-systems.

Definition (Steganalysis)

The art of detecting whether secret communications is taking place or not.



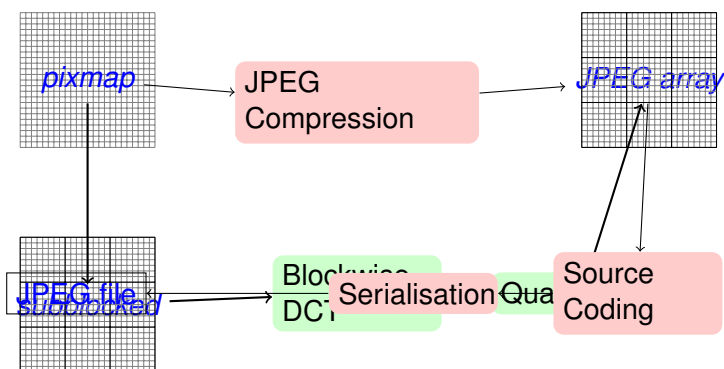
Steganalysis

Using Machine Learning

- Most recent steganalysis systems use Machine Learning
 - or related statistical techniques
 - Most often a two-class SVM is used (natural vs. steganogram)
- 1 Extract features (statistics) from the image
 - Multi-dimensional floating point vector
 - 2 Train the system
 - Input two ensembles of feature vectors
 - The system will estimate a model
 - 3 Testing
 - Input the estimated model + Images from each class
 - Output classification decisions – Estimate accuracy
 - 4 Real use
 - Input: model; feature vector from a suspicious image



JPEG images



JPEG Steganography

- Many stego-algorithms work on the JPEG Array
 - Integer matrix
- E.g. Jsteg
 - Ignore +1 and 0 coefficients
 - Embed in the least significant bit of each coefficient
 - Extract by taking $c \bmod 2$



The F5 Algorithm

by Andrea Westfeld

- Better preservation of image statistics
- JPEG coefficient magnitudes are always decreased
- Matrix coding (source coding) is used
 - coding to match the cover
 - minimise the number of modifications



Typical JPEG Steganography

- Modulate information on the cover
 - ± 1 changes to coefficients
- Independent modifications
 - Independence of the cover
 - Independence of individual coefficients
- This is the problem of steganography
 - Image coefficients are *not* independent
 - The modifications become detectable noise



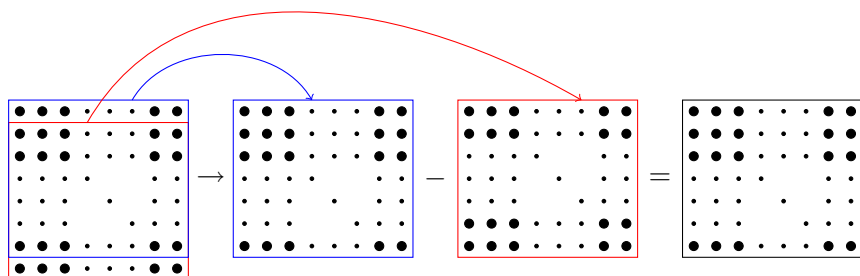
The Markov Based Model – Overview

Yun Q Shi *et al*

- Consider the absolute value of the JPEG array
- Difference matrix – differences between adjacent coefficients
- Model the difference matrix
 - First-order Markov model
- Estimate a Transition Probability Matrix
 - which forms our features



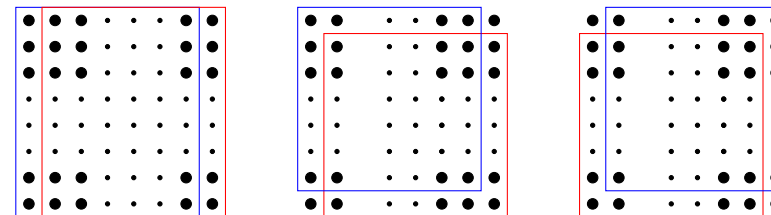
The difference array



- $F_v(i, j) = |J_{i,j}| - |F_{i+1,j}|$
- To reduce complexity, the difference array is capped at $\pm T$
 - Large (small) values are reduced (increased) to the capping value.



The other three difference arrays



- Horizontal, and major and minor diagonal



Transition Probability Matrix

- For $s, t \in \{-T, -T + 1, \dots, T - 1, T\}$, we estimate
 - $M_{s,t}^v = P(F_v(i + 1, j) = s | F_v(i, j))$
 - $M_{s,t}^h = P(F_h(i, j + 1) = s | F_h(i, j))$
 - $M_{s,t}^d = P(F_d(i + 1, j + 1) = s | F_d(i, j))$
 - $M_{s,t}^m = P(F_m(i, j + 1) = s | F_m(i + 1, j))$
- This gives four matrices
 - $M^x = [M_{s,t}^x]$
- $4(2T + 1)^2$ features
 - Shi *et al* suggested $T = 4$ for 323 features
- Performance around 90%–98% accuracy



The F5 implementation

- JPEG based stego-algorithms should work on the JPEG array
- This is what F5 (and Jsteg) Software actually do:
 - 1 Load and Decompress the Image
 - Internal Spatial Representation
 - Compression Parameters are discarded
 - 2 Compression and Embedding as an integrated process
 - Compression implemented by tweaking existing compression routines
 - Usually using default parameters
 - 3 Save the compressed image



Double Compression

- The F5 software recompresses the image
 - Usually using a different compression factor
 - Known as *Double Compression*
- This normally causes artifacts
- Typical Steganalysis classifiers
 - Compare Clean images against F5 processed images
 - What is detected?
 - Double Compression or Steganography?



Alternative Experiment

- New training set
 - 1 Steganograms from F5 (with a hidden message)
 - 2 Cover images processed by F5 without a message
- Thus both of classes are doubly compressed
- Our classifier will have to work on the embedding only



1st vs. 2nd Order Markov Models

Performance

- Ignoring Double Compression

	Message length (bytes)		
	618	1848	4096
1st Order	89.5%	93.5%	98.0%
2nd Order	99.1%	99.1%	98.6%

- F5 vs. doubly compressed (clean) images

	Message length (bytes)		
	618	1848	4096
1st Order	50.2%	84.3%	97.9%
2nd Order	50.0%	55.6%	70.6%



Complexity

- Shi *et al*'s technique uses 323 features
- Computationally costly, to extract and to train
- We have proposed a simpler set
 - achieving similar performance



Basic ideas

- 1 The Markov Model is flawed
 - probability distribution of each coefficient is
 - determined by preceding coefficients
 - independent of position
 - it should depend on the frequency (position in a subblock)
- 2 The transition probability matrix is too fine-grained
 - too many features to compute



The coefficients considered

	x_h	y_h	z_h				
x_v	x_d						
y_v		y_d					
z_v			z_d				



The CP Features

Definitions

- Triplet (x, y, z) as in figure
- Three posterior events
 - $A_1 : y > z$; $A_2 : y = z$; $A_3 : y < z$
- Three prior events
 - $B_1 : x > y$; $B_2 : x = y$; $B_3 : x < y$
- Nine features per triplet (x, y, z)
 - $P(A_i|B_j)$ fro $i, j = 1, 2, 3$
- 27 features in total
 - A 54-feature variant (six triplets) was less effective



Performance

CP Features

- Computation – Markov Model based technique in parenthesis
 - Training 770ms (150ms) on 2480 images
 - Classification 0.2ms (same) per image
 - **Feature Extraction 114ms (13s) per image**
- Accuracy (large message, 4kB)
 - 97.2% for both CP and Markov Model
 - 95% confidence interval is (95.3%, 99.2%)



Steganalysis and Image Forensics

and Machine Learning

- Steganalysis
 - Development of Scientific Methodology
 - New feature sets
- sister team on Image Forensics
- sister group in Biologically Inspired Methods



Information Security

- Security in Contact-Less Payment Systems
 - are they sufficiently secure
- sister group in E-voting



Coding Theory

Applications in Data Hiding

- Deletion/Insertion Correction
 - for use in Watermarking
 - Geometric Distortions
- Wet Paper and Dirty Paper Coding
 - Distortion Minimisation in Watermarking and Steganography
- Construction/Non-Existence of Codes



Next project

- Information Forensics is a booming area
 - Image Forensics in particular
 - The methods and methodology are largely shared with Steganalysis
- Is there room for collaboration?
 - Machine Learning
 - Sound methodology

