THE UNIVERSITY OF RHODE ISLAND

Steganalysis

Problem

- Hidden Evidence
  - Innocuous Files hide:
    - Stolen Credit Card numbers
    - Foreign Intel. (SVR in *USA vs Metsos et al)*
    - Trade secrets
- Free, easy programs
- More than encryption
  - How to determine hidden evidence is there?

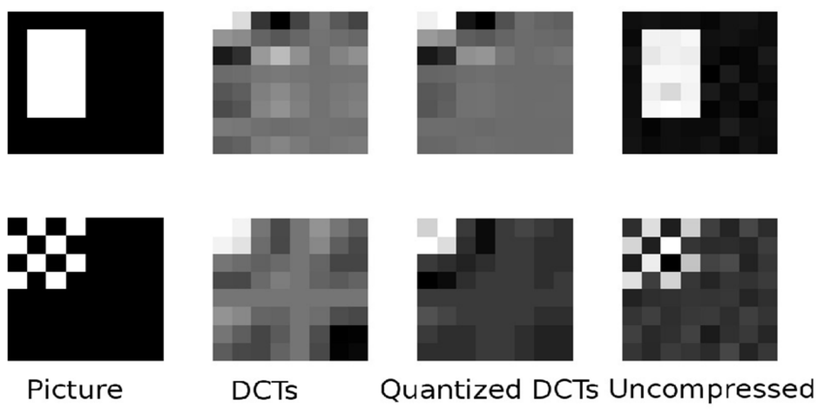
How it works

1. Take any image
2. Software encodes data to embed
3. Makes subtle changes to image that represent that data
4. Send/post new file


Image Compression

- Frequency Domain
  - Removes high frequency information, because human eyes do not notice subtle changes
  - Different Qualities yield different amount of removal

Sample image blocks, at 90% and 70% quality



-12	4	0	0	0	0	0	0	-8	-4	4	-1	0	0	0	0
18	-2	0	1	-2	0	0	0	12	4	-1	1	0	0	0	0
0	-4	-2	-2	0	0	0	0	5	-3	-1	0	0	0	0	0
-3	0	1	1	0	0	0	0	-4	0	1	1	1	0	0	0
-2	2	0	0	0	0	0	0	-3	3	0	0	-1	0	0	0
2	0	-2	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	-1	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
-41	0	0	-2	0	0	0	0	-38	-8	3	1	-1	1	0	0
4	1	0	-1	0	0	0	0	13	-7	1	1	-2	0	0	0
2	1	0	-2	0	0	0	0	5	-2	-1	1	-2	0	0	0
2	1	0	0	0	0	0	0	-2	3	-2	0	0	0	0	0
0	1	0	0	0	0	0	0	-1	3	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

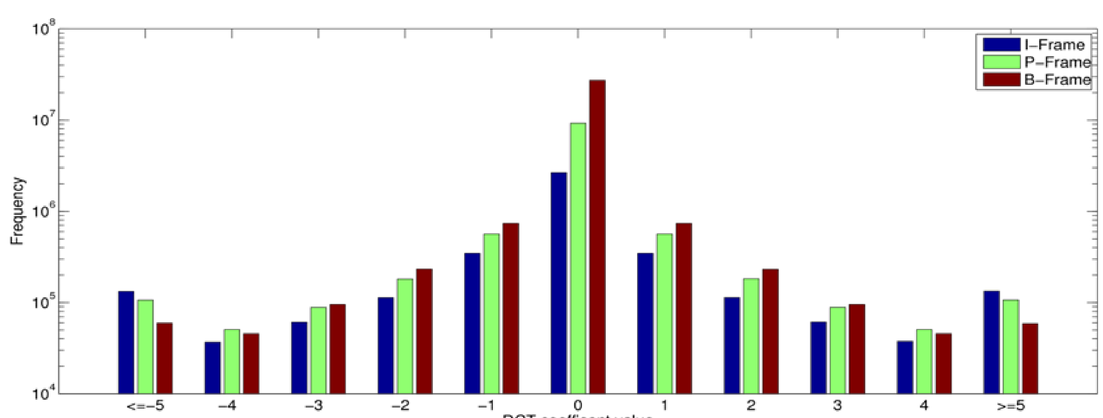
Image Steganalysis

- DCT value statistics indicate steg
  - Compare DCT Coefficients between blocks and throughout the image
  - Look for changes at block boundaries
  - Use Statistical models, such as Linear Discriminant Analysis

Functional	Dimensionality
Global histogram $\mathbf{H}_I$	11
5 AC histograms $\mathbf{h}_I^{ij}$	5×11
11 Dual histograms $\mathbf{g}_{ij}^{d}$	11×9
Variation V	1
2 Blockiness B_α	2
Co-occurrence matrix $\mathbf{C}_{st}$	25

Video Steganalysis

- Works similar to Image Steganalysis
- For compression, not all frames are stored using the same range of DCT values
- Different statistical models must be made for the different types of frames to maintain accuracy



Impact

- Detect steg with >95% accuracy down to 20% embedding rate
- Commercial transition of JPG and MP3 detection engine to Wetstone Technology's StegoSuite product

THINK BIG WE DO

Digital Forensics Center

Research sponsored by the National Institute of Justice