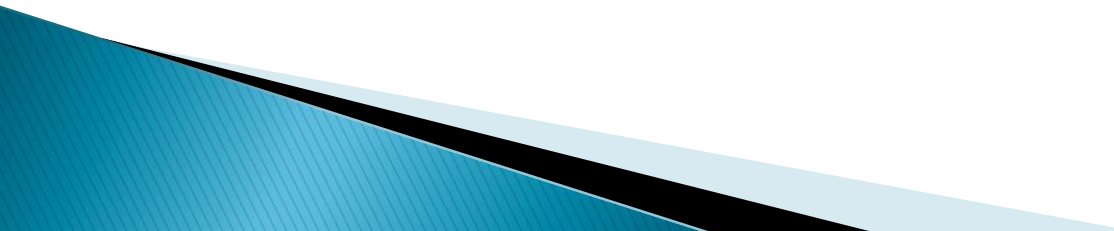


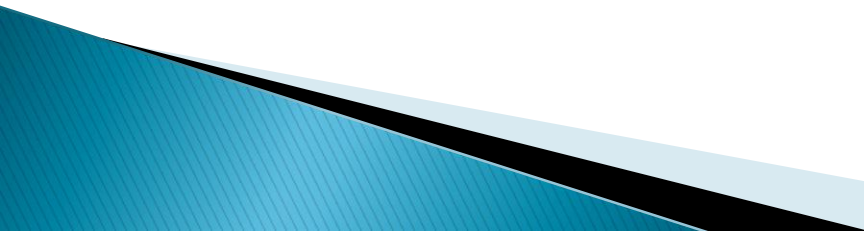
Steganography

- ▶ **Steganography** refers to any methodology used to hide a message (including text, sound, or picture) in a separate file. Most commonly text or an image is inserted into another image. However there are permutations where video is hidden in another video, or sound in sound or even sound in video. The image/sound/video that the underlying message is hidden in is referred to as a carrier or cover file or signal.
- ▶ The most common implementation of steganography utilizes the least significant bits in a file in order to store data. By altering the least significant bit one can hide additional data without altering the original file in any noticeable way.

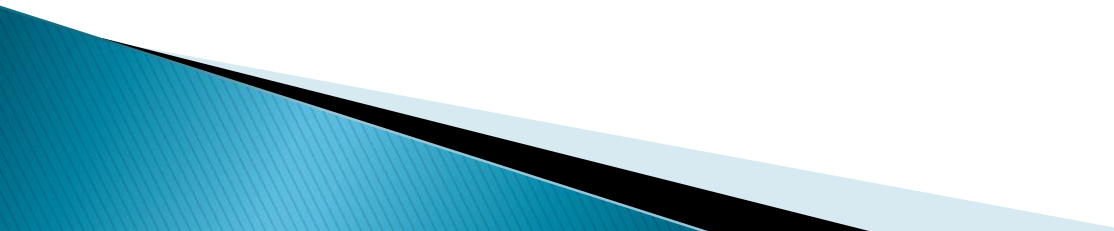
Historical Steganography

- ▶ The ancient Chinese wrapped notes in wax and swallowed them for transport.
 - ▶ In ancient Greece a messenger's head might be shaved, a message written on his head, then his hair was allowed to grow back.
 - ▶ In 1518 Johannes Trithmeus wrote a book on cryptography and described a technique where a message was hidden by having each letter taken as a word from a specific column.
- 

Historical Steganography – Continued

- ▶ During WW II the French Resistance sent messages written on the backs of couriers using invisible ink
 - ▶ Microdots are images/undeveloped film the size of a typewriter period, embedded on an innocuous documents. These were said to be used by spy's during the Cold War.
- 

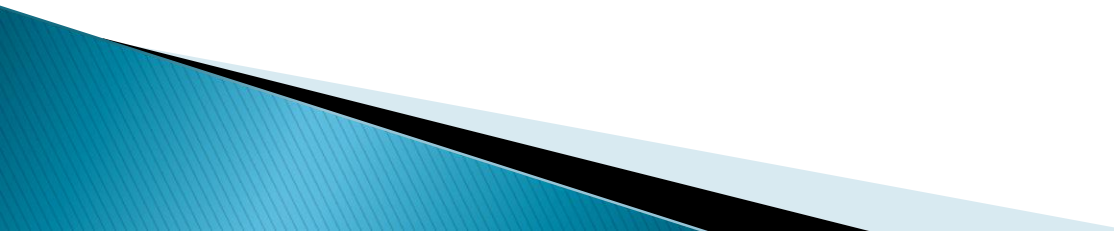
Steganography Terms

- ▶ Steganophony – the concealment of messages in Voice-over-IP conversations.
 - ▶ Payload is the data to be covertly communicated.
 - ▶ The carrier is the signal, stream, or data file into which the payload is hidden. This is also sometimes called the cover object.
 - ▶ The channel is the type of medium used.
- 

Steganography details

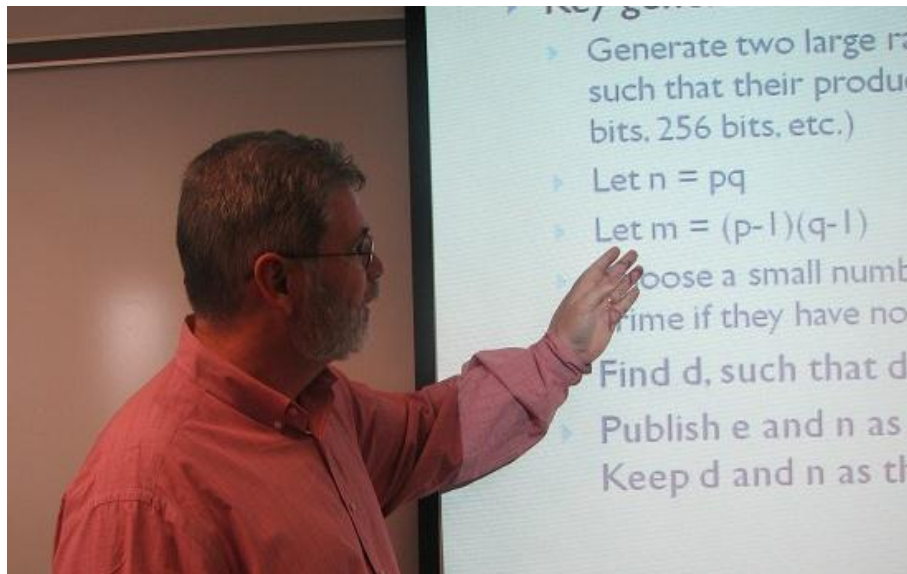
- ▶ With least significant bit (lsb) replacement, certain bits in the carrier file are replaced.

Other forms of Steganography

- ▶ Echo Hiding: This method adds extra sound to an echo inside an audio file, that extra sound conceals information.
 - ▶ Discrete Cosine Transform is often used for Video steganography. This method alters values of certain parts of the individual frames. The usual method is to round up the values.
- 

Demonstration

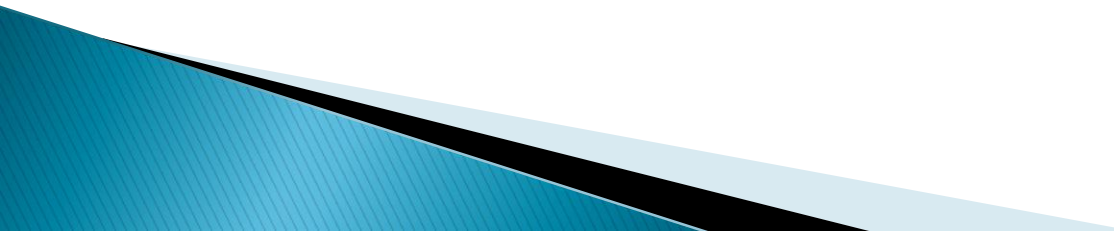
- ▶ I began with an image, a jpeg that was 68.3 K in size.



Demonstration Continued

- ▶ I took a text document that was 3,741 words / 26 KB and hid it in this image using various tools.
 - Using Invisible Secrets the resulting image was 77.4 KB, an increase of 9.1 KB.
 - Using QuickStego the resulting image was a 520 KB bitmap, a more than 7 fold increase.

Steganography Implementations

- ▶ QuickStego – very easy to use but very limited.
 - ▶ Invisible Secrets – much more robust with both a free and commercial version.
 - ▶ MP3Stego – specifically for hiding payload in MP3 files.
 - ▶ Snow – hides data in whitespace.
 - ▶ StegVideo – hides data in a video sequence.
- 

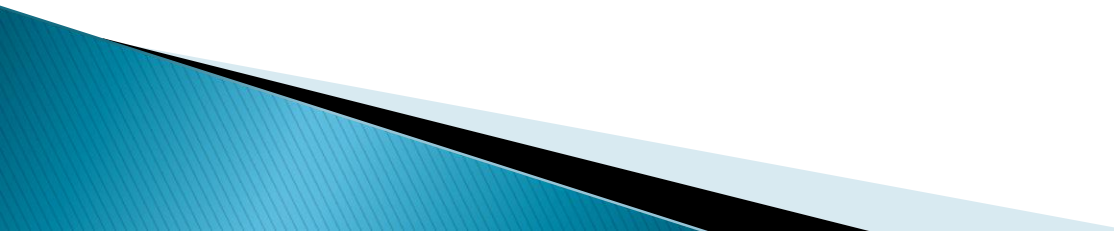
Steganalysis

- ▶ By analyzing changes in an image's close color pairs, the steganalyst can determine if LSB substitution was used. Close color pairs consist of two colors whose binary values differ only in the LSB.

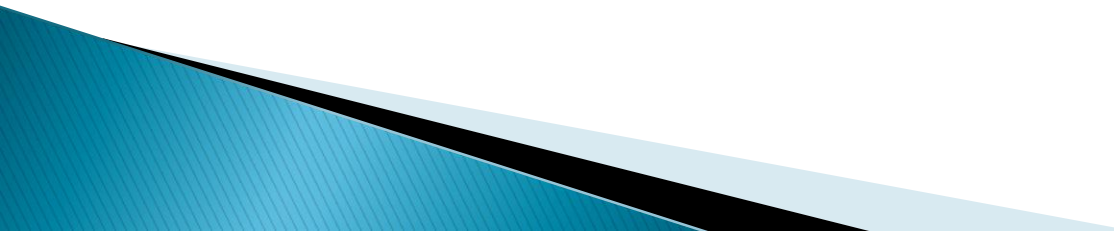
Steganalysis – RQP

- ▶ The Raw Quick Pair method
 - Based on statistics of the numbers of unique colors and close-color pairs in a 24-bit image.
 - Analyzes the pairs of colors created by LSB embedding
 - Countermeasure – Maintaining the color palette without creating new colors

Steganalysis – Chi-Square Analysis

- ▶ Chi-Square Analysis calculates the average LSB and builds a table of frequencies and Pair of Values.
 - ▶ Then it performs a chi-square test on these two tables.
 - ▶ Essentially it measures the theoretical vs. calculated population difference
- 

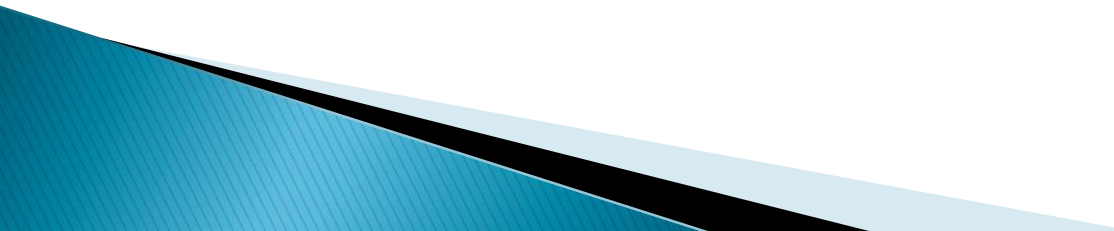
Steganalysis – Audio Steganalysis

- ▶ Examine noise distortion in the carrier file.
 - ▶ Noise distortion could indicate the presence of a hidden signal.
- 

Steganography Detection Tools

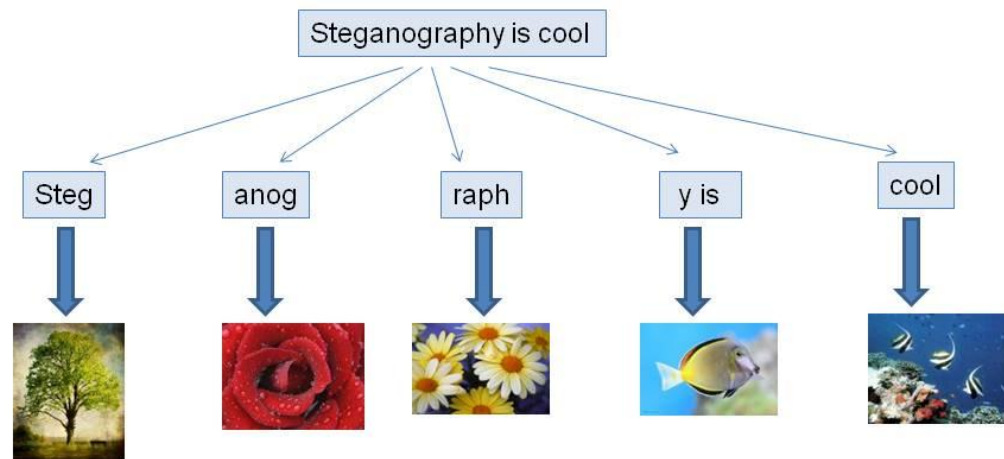
- ▶ Outguess's StegDetect is an easy to use but limited tool
<http://www.outguess.org/detection.php>
- ▶ StegSpy has fewer limitations than StegDetect
<http://www.spy-hunter.com/stegspydownload.htm>
- ▶ AccessData's Forensic Toolkit and Guidance Software's Encase can detect steganography.

Detection Demo

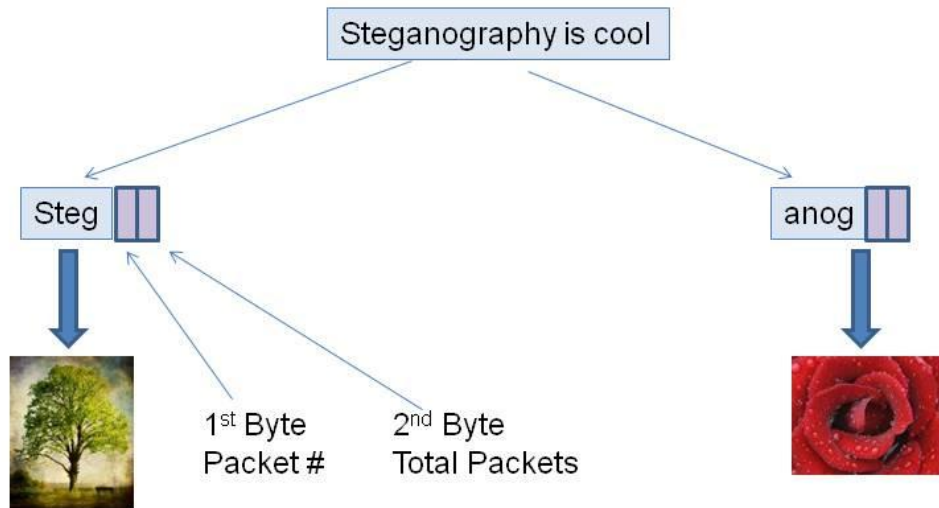
- ▶ I used StegDetect on both files. It errored out on the jpeg and could not read the bitmap.
 - ▶ I used StegSpy and it discovered the bitmap stegonography but not the jpeg.
- 

Distributed Steganography

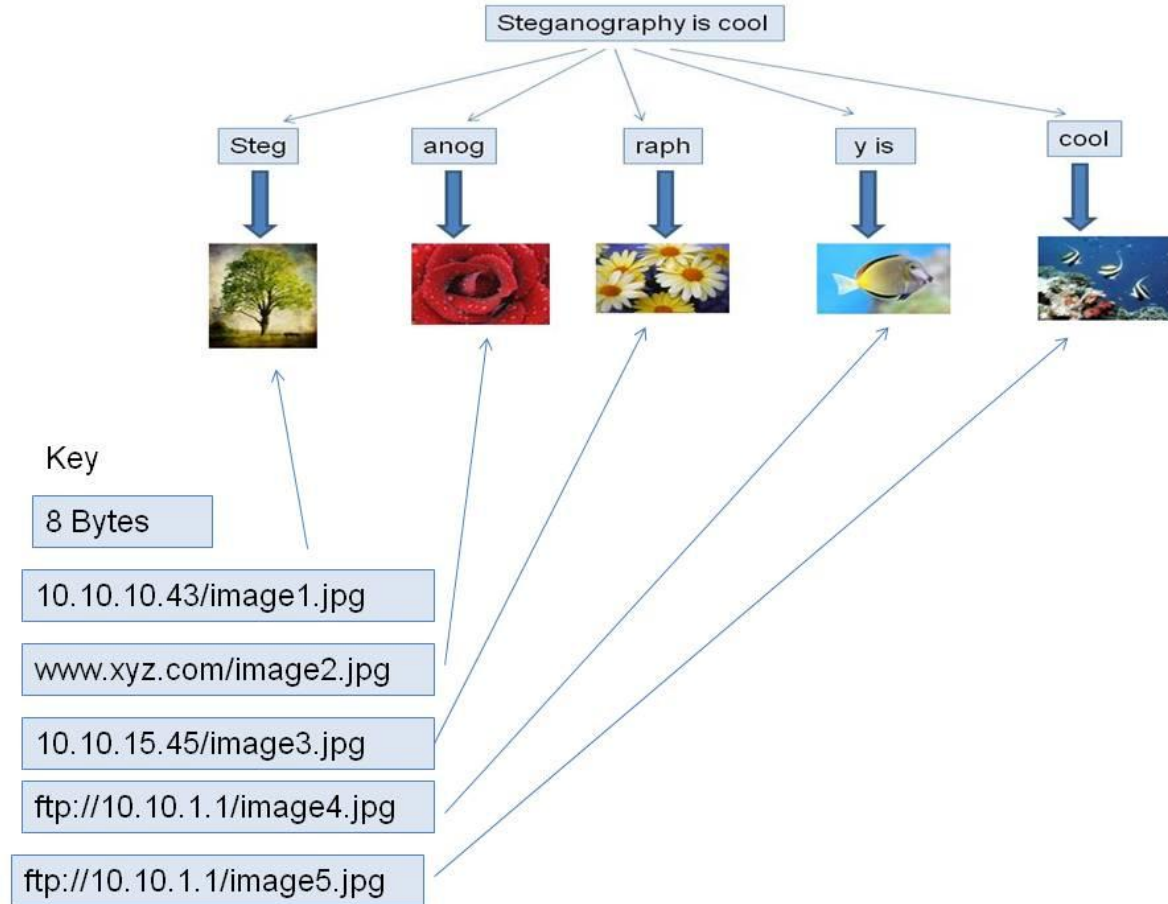
Provisional Patent 61/379,087 <http://ip.com/IPCOM/000204600>



Distributed Steganography (Continued)



Distributed Steganography (Continued)



Additional Resources

- ▶ A white paper on a steganographic method
<http://www.scribd.com/doc/3367439/Steganography>
- ▶ ABC story on steganography
<http://www.abc.net.au/catalyst/stories/s1320215.htm>
- ▶ Technical paper on steganography <http://www.jjtc.com/stegdoc/>
- ▶ ComputerWorld article on steganography
http://www.computerworld.com/s/article/71726/Steganography_Hidden_Data
- ▶ RQP Paper –
http://www.ws.binghamton.edu/fridrich/Research/acm_2001_03.pdf
- ▶ Detection of LSB steganography
<http://www.cecs.uci.edu/~papers/icme06/pdfs/0001377.pdf>
- ▶ Detection of audio steganography
http://www.ece.ucdavis.edu/~yliu/pub/papers/Tracy_ISC08.pdf