Steganography

Steganography

- In Greek
  - Steganos = covered
  - Graphein = to write
- Cryptography and steganography are cousins in the spycraft family.
- Cryptography scrambles a message so it cannot be understood.
- Steganography hides the message so it cannot be seen.

- Historically, secret messages were often hidden (or memorized)
- Today, steganography is used primarily to protect digital rights
  - “watermarking” copyright notices
  - “fingerprinting” a serial ID

Who wants it?

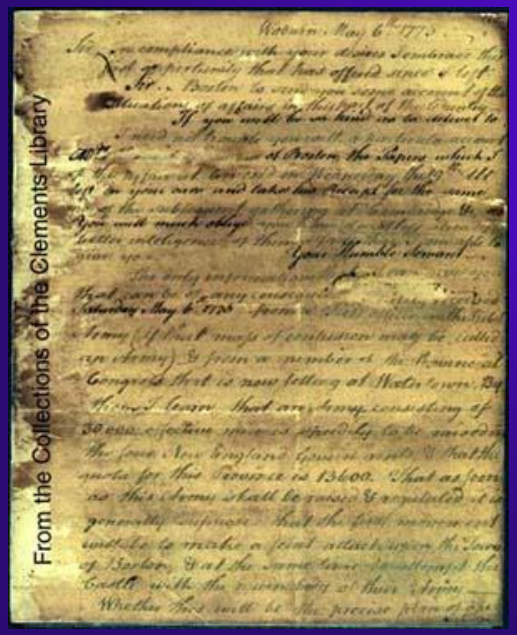
- Evil doers. If evil messages can't be seen by good people, evil will triumph. *Osama bin Laden?*
- Good doers. If the good guys can communicate in secret, then good
  will triumph. *U.S. forces*
- Content owners and copyright czars. Hidden messages can carry information about rights to view, copy, share, listen, understand, etc.
- Software Developers. "Hidden" channels can be added to data structures without crashing previous versions. Steganography can fight bit rot.

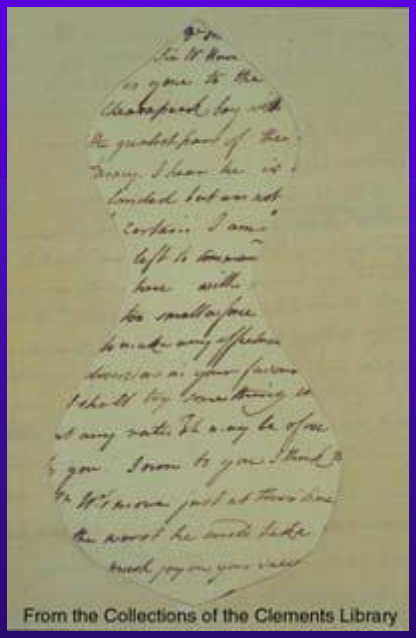
History of Steganography

- Memorizing messengers used for communication
  - Sometimes killed after delivering the message
- Greek Histaiaeus encouraged Aristagoras of Miletus to revolt against the Persian King.
  - Writes message on the shaved head of the messenger, and sends him after his hair grew
- Chinese silk balls
  - Message is written on silk, turned into wax-covered ball that was swallowed by the messenger…

History of Steganography (cont.)

- Invisible Ink





History of Steganography (cont.)

- Microdots
  - In WWII, Germans used “microdots” - documents shrunk to the size of a dot, and embedded within innocent letters
- Easter eggs
  - Programmers often embed Easter eggs in their software (http://www.eeggs.com)
  - Eg. =rand() in MS word; Ctrl+Alt+Shift, ? !
  - It is claimed that The Beatles have embedded secret messages in their music
    - e.g., about Paul McCartney’s death

Modern Steganography

- Hiding one message within another (“container”)
- Most containers are rich media
  - Images, audio, video – very redundant, can be tweaked without affecting human eye/ear
  - US argued that Bin Laden implanted instructions within taped interviews
- Copyright notices embedded in digital art
  - Prove ownership
  - Serial number embedded to prevent replication
  - Seek infringements on the web using spiders

Hiding a message within a text

- An actual message from a German spy

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

Hiding a message within a text

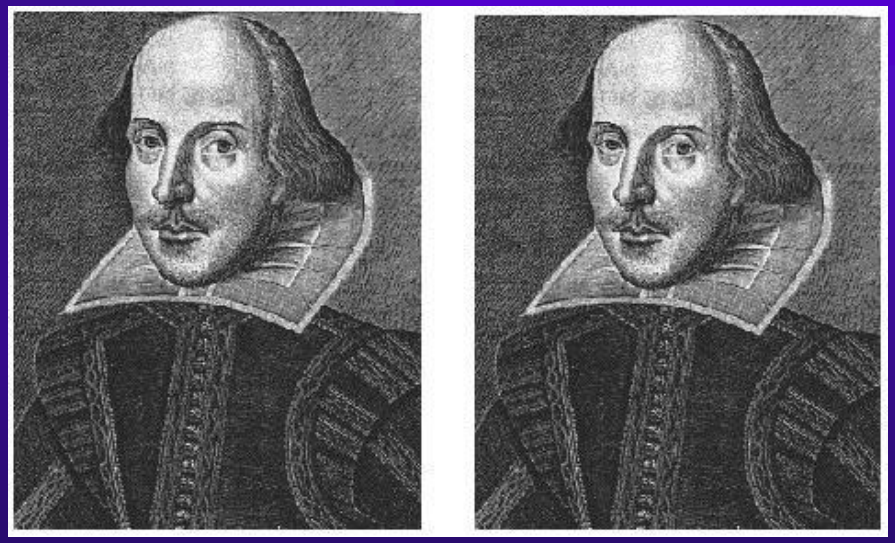
- read second letter in each word

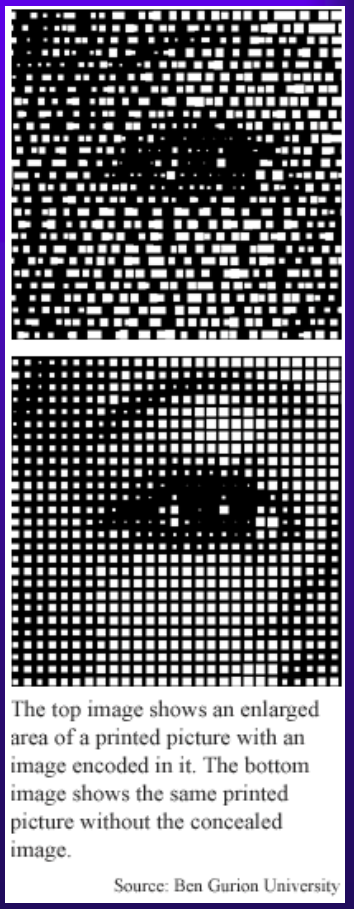
"Apparently, neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affect pretext for embargo on by products, ejecting suets and vegetable oils."

"Pershing Sails from NY June 1"

Hiding a Message in an Image

- Example: use 1-2 Least Significant Bits (LSB) in each pixel
  - human eye wont notice the difference
  - message can be compressed to reduce number of bits needed
  - only half the bits are likely to change on average
  - prefer “containers” with a lot of variations





The top image shows an enlarged area of a printed picture with an image encoded in it. The bottom image shows the same printed picture without the concealed image.

Source: Ben Gurion University

- Check out Steganos (www.steganos.com), Digimarc (www.digimarc.com)

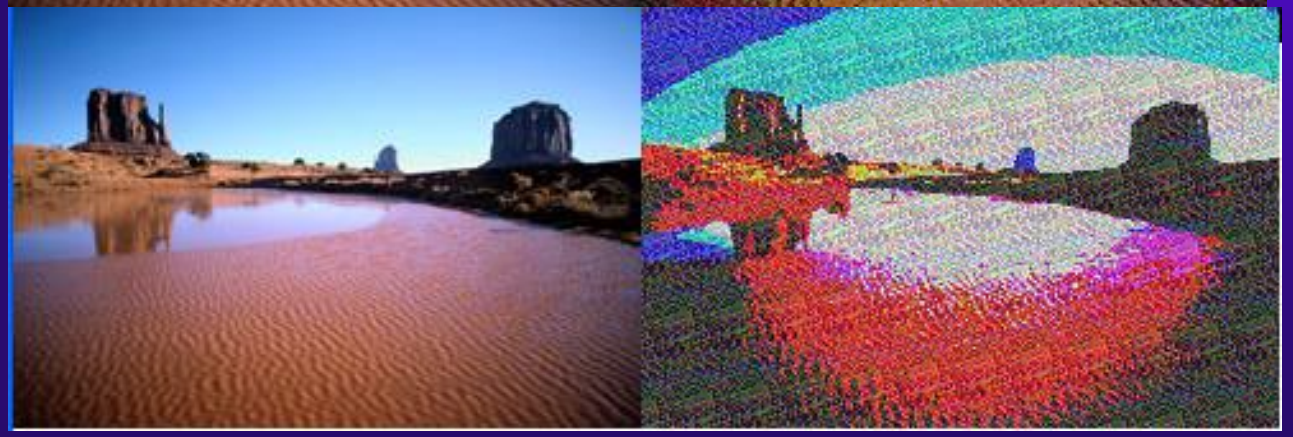
LSB Modification

- Side Effects:
  - The data may not have the same statistical pattern as the least significant bits being replaced.
- Add a lot of noise, and it's obvious

4 LSB modified produces banding

More LSB Modification

6 bits



7 bits

Mesh Watermarking

- Robust mesh watermarking, Emil Praun, Hugues Hoppe, Adam Finkelstein, **July 1999** *Proceedings of the 26th annual conference on Computer graphics and interactive techniques*

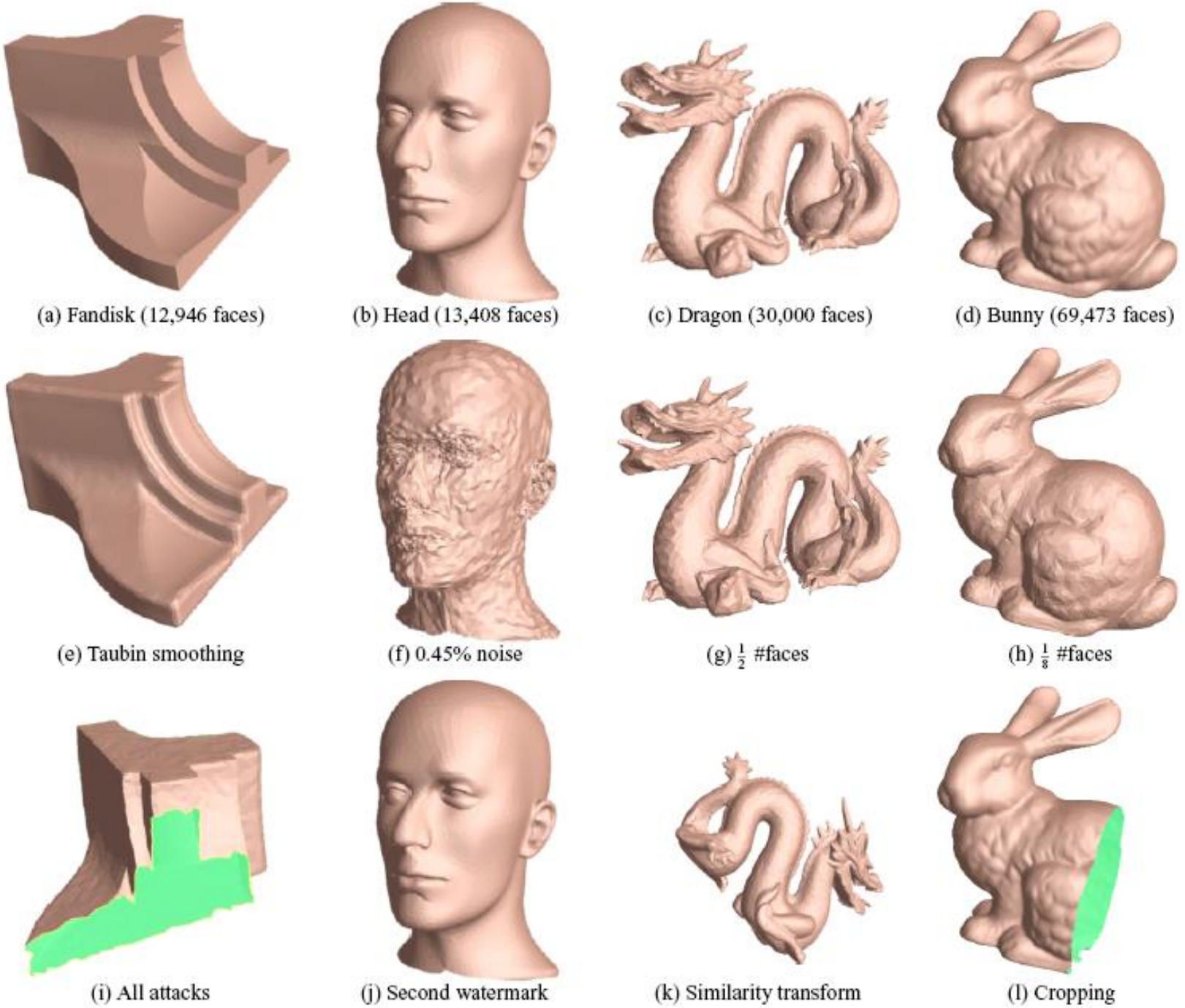
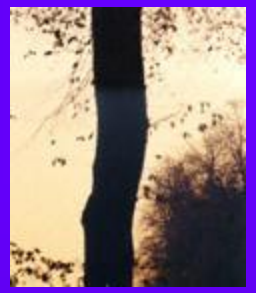


Figure 4: Watermarked models (top row) and various attacks.

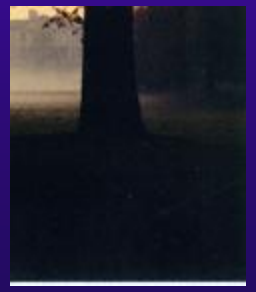
Issues to evaluate

- "Capability"
  - Payload carrying ability
  - Detectability
  - Robustness
- *Securing information: Capacity is the wrong paradigm*, Ira S. Moskowitz, LiWu Chang, Richard E. Newman , **September 2002** Proceedings of the 2002 workshop on New security paradigms



- “Mosaïc attack”: Defeat an embedded watermark by chopping up image and serving it in pieces

```
<nobr>
 <img SRC="kings_chapel_wmk1.jpg’ BORDER="0’ ALT="1/6’ width="116’ height="140">
 <img SRC="kings_chapel_wmk2.jpg’ BORDER="0’ ALT="2/6’ width="116’ height="140">
 <img SRC="kings_chapel_wmk3.jpg’ BORDER="0’ ALT="3/6’ width="118’ height="140">
 </nobr>  <br>
 <nobr>
 <img SRC="kings_chapel_wmk4.jpg’ BORDER="0’ ALT="4/6’ width="116’ height="140">
 <img SRC="kings_chapel_wmk5.jpg’ BORDER="0’ ALT="5/6’ width="116’ height="140">
 <img SRC="kings_chapel_wmk6.jpg’ BORDER="0’ ALT="6/6’ width="118’ height="140">
 </nobr>
```



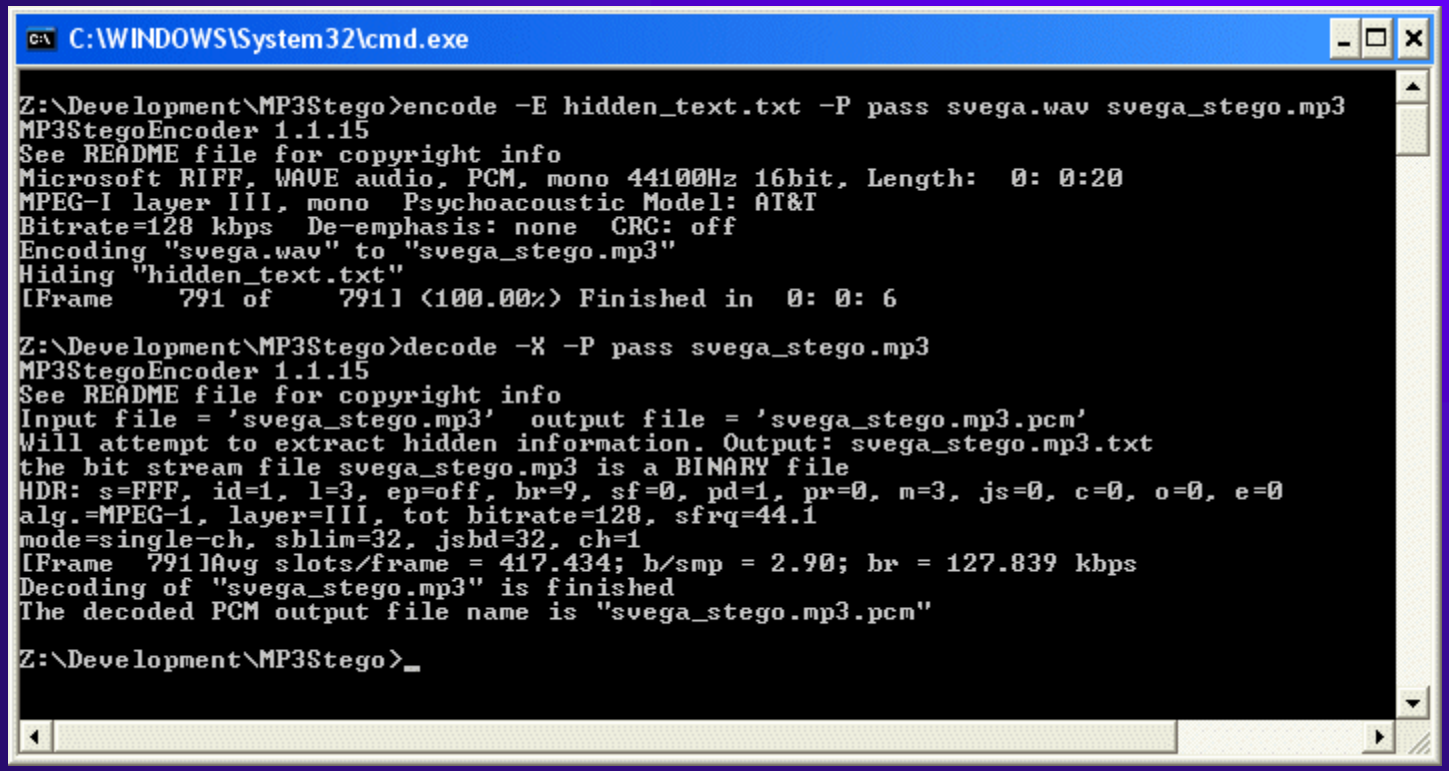
Mosaïc assembled

- Some websites use mosaics to deter casual copying!

MP3Stego

- Hides information in MP3 files during the compression process
- Takes advantage of the fact that MP3 provides high-quality compression of 11:1
  - Plenty of room for information hiding!
  - Randomly chooses which parts of the Layer III inner loop to modify; makes sure modifications don’t exceed threshold defined by the psycho acoustic model.
- Defeat by decompressing & recompressing

MP3Stego in action



http://www.petitcolas.net/fabien/steganography/mp3stego/index.html

Steganalysis

- Goals
  - Detect steganography containers (yes/no)
  - Recover and decode the hidden message (actual steganalysis)
- Detection
  - Develop signatures for known steganographic tools, e.g. in LSB method, many pixels in same neighborhood differ in 1 bit
  - When content is encrypted, the message should have a high entropy (“white noise”)
  - Promising results: high detection vis-à-vis normal images
- Decoding
  - No significant work in this area !
- Destruction
  - Most steganographic algorithms not robust to image alterations
  - Short messages (e.g. copyright), can be encoded thousands of times in an image, and it is enough that some survive

Steganography (Summary)

- Steganography is arguably weaker than cryptography because the information is revealed once the message is intercepted
- However, steganography can be used in conjunction with cryptography

Tools and References

- Fabien a. p. penticolas
  - http://www.petitcolas.net/fabien/steganography/
- Digimarc
- http://theargon.com/archivess/steganography/
- **Hiding Secrets with Steganography**
  - http://www.onlamp.com/pub/a/bsd/2003/12/04/FreeBSD_Basics.html
- http://www.outguess.org