Steganography & Steganalysis

INSTRUCTOR: JOHN ORTIZ
SENIOR COMPUTER ENGINEER
UTSA
STEGO@SATX.RR.COM

INTRODUCTION TO STEGANOGRAPHY

Overview – Information Hiding

- Steganographic Terms and Definitions

Information Hiding

- Information Hiding is a branch of computer science that deals with concealing the existence of a message
  - It is related to cryptography whose intent is to render messages unreadable, except by the intended recipients
- It employs technologies from numerous science disciplines:
  - Digital Signal Processing (Images, Audio, Video)
  - Cryptography
  - Information Theory\Coding Theory
  - Data Compression
  - Discrete Math
  - Data Networks
  - Human Visual/Auditory perception

Examples of Information Hiding

- A Greek shaved the head of a slave, wrote a message, then waited for the hair to grow back before sending the slave to his destination
- Invisible ink was used by Washington in the Revolutionary War
- Prior to the Civil War, quilts were sewn with special patterns to tell escaping slaves which direction to go and what to do
- During WWI there was a cable that read, "Father is dead." Suspecting a hidden meaning, the censor changed it to "Father is deceased" which caused the reply, "Is Father dead or deceased?"
- During WWII chess by mail was banned, crossword puzzles examined, stamps were removed and replaced by ones of equal value
- In the 1980's, some of Margaret Thatcher's cabinet documents were leaked to the press. She ordered that the word processors being used by government employees, encode their identity in the word spacing of the documents

Information Hiding

- Steganography
- Watermarking
- Covert Channels
- Anonymity

Steganography

- Steganography literally means "Covered Writing"
- Primary goal is not being detected
- Secondary goals are to maximize capacity and make message extraction difficult
- Most frequently applied to images, but nearly all file types can have data embedded
  - Audio
  - Video
  - Text
  - Executable programs

Watermarking

- Primary goal is to prevent extraction or destruction
  - Called Robustness
  - Not being detected and capacity are secondary
- Designed to protect intellectual property rights for images, sounds, and video – prove ownership
  - If it's easily destroyed, those rights cannot be protected
- Even if it's not detectable, an adversary could suspect that a work (of art) could have a watermark and so take steps to destroy it
  - There is a program called StirMark which does just that
- For some applications watermarks may be visible
- May be used to fingerprint a particular file and detect changes
  - Make it tamper proof

CovertChannels

- Covert channels are communication paths that were neither designed nor intended to transfer information
- For example, the telephone was designed to allow voice communication
  - Information could be conveyed via the number of rings
  - Or via the time differences between successive phone calls
- Unused bits in the TCP/IP protocol headers can be used to carry information
- Hiding data in a network timing, order of received data, amount of data, etc., are also covert channels

Anonymity

- Anonymity is about concealing the sender and receiver of messages
  - Tor – Onion routing project
- This is the least studied sub-discipline of information hiding

Goals of Steganography

- Steganography's primary goal is to hide data within some other data such that the hidden data cannot be detected even when it is being sought
- Three measures of a steganographic technique:
  - Security
  - Capacity
  - Robustness

Security

- It is secure if it cannot be detected, even if the attacker has full knowledge of the embedding algorithm
  - Only the knowledge of the secret key should allow the detection
- Can it be seen or heard?
  - Imperceptible to humans
- Can it be detected by statistical analysis?
  - Imperceptible to computers
- Does it leave easily detectable signatures?
  - Such as the software author's name or "secret" online ID

Security

- Levels of Failure:
  - Detection - Proof of existence of message
  - Extraction – removing without destroying the cover
  - Destruction – destroying the message without destroying the cover
- 3 Levels of Perceptibility
  - Indistinguishable from original
    - Comparing side-by-side is ineffective
  - Sense distortion when looking/listening for it
  - Blatantly obvious to the most casual observer

Capacity

- How much data can a cover image hold?
  - Must consider if a change in file size is noticeable
- Maximize amount of hidden data for a given cover file size
- As more data is hidden, the effects tend to become more noticeable
  - Direct tradeoff between capacity and security

Robustness

- How well does the data maintain integrity in the face of modifications?
- Common modifications include the following:
  - Images: blurring, sharpening, scaling, cropping, contrast, gamma, brightness, rotation, skewing, printing/copying/ scanning, etc.
  - Audio: filtering - bass/treble, volume adjustment, stereo to mono, etc.
  - Video: any image/audio hiding, add/delete frames, temporal adjustments, frame swapping, frame averaging
  - Also: lossy compression, A/D and D/A conversion (scan, print, fax), as well as sophisticated attacks

Robustness

- Robustness is achieved through redundant encoding of the message
  - Direct tradeoff between capacity and robustness
  - Redundant bits used for robustness could be used for capacity instead
  - Robustness is primary goal of watermarking

Terminology

- The data to be hidden:
  - Plaintext (from cryptography)
  - Secret message
  - Embedded data
- The data which will have a stego-message embedded in it:
  - Covertext
  - Cover-Object
  - Cover-Image\Cover-Audio\Cover-Video

Terminology

- The key (optional) used to make the stego-message secure
  - Secret Key
  - Key
- The file with the steganography-message embedded
  - Stegotext (ciphertext in cryptography)
  - Stego-Object
  - Stego-Image\Stego-Audio\Stego-Video

Terminology

- Alice and Bob
  - Classical names given to the parties wishing to communicate
- Sometimes, you may have a Carol and a Dave
- Eve, an adversary, can listen to but not modify or forge a message
  - (think passive eavesdropping)
- Wendy the Warden, another adversary, can monitor, modify, or forge a message
  - A passive warden simply listens (like Eve)
  - An active warden may modify a message
  - A malicious warden may forge a fake message

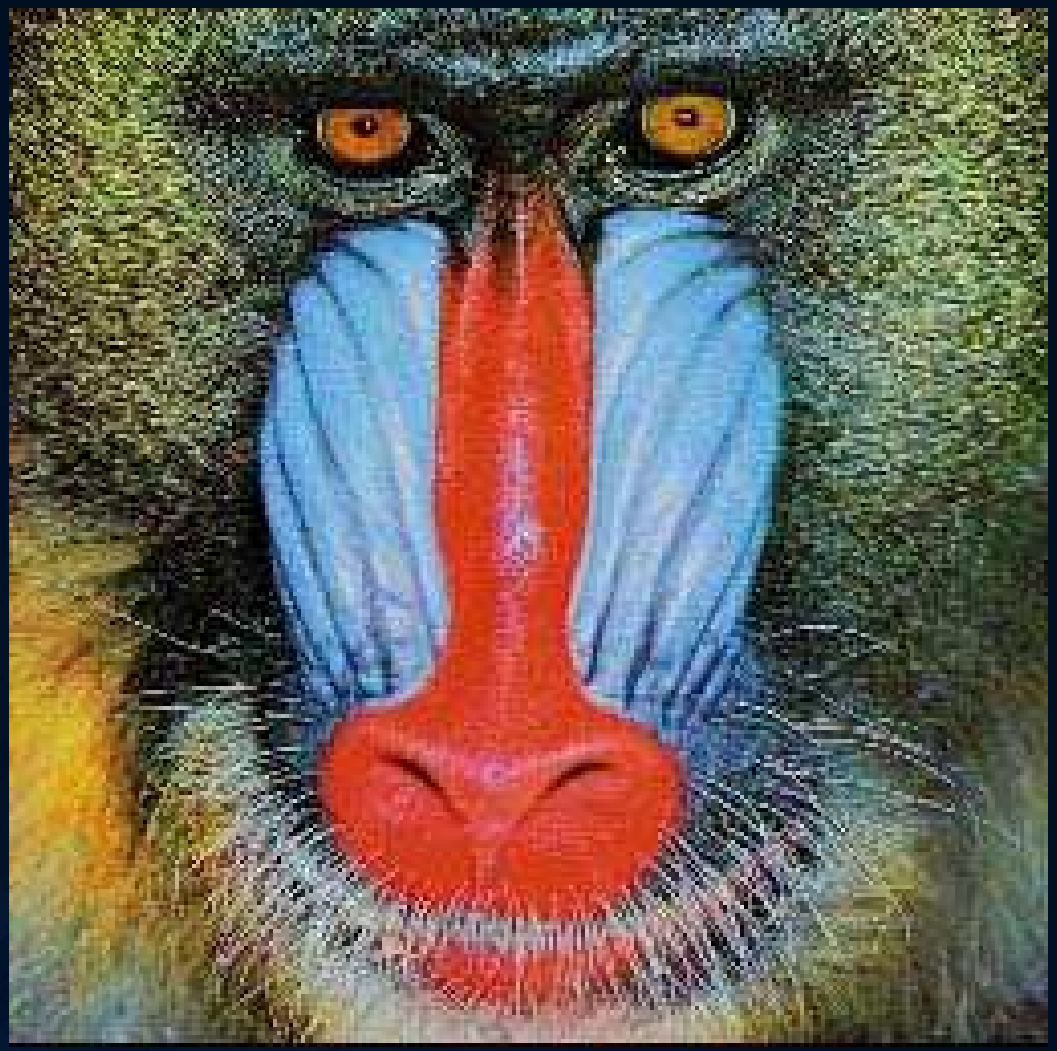
Wisdom from Cryptography

- One of the main principals of cryptography applies to steganography as well
- The premise from which to measure a secure steganographic system is to assume that the opponent knows the system being employed, yet still cannot find any evidence of a hidden message
  - Kerchoff's Principle: the system should not depend on secrecy and should be able to fall into enemy hands without disadvantage
  - Many systems have relied on the "Security by Obscurity" premise and many have failed
    - CSS for DVD, RIAA digital watermarking, Adobe e-books, SDMI

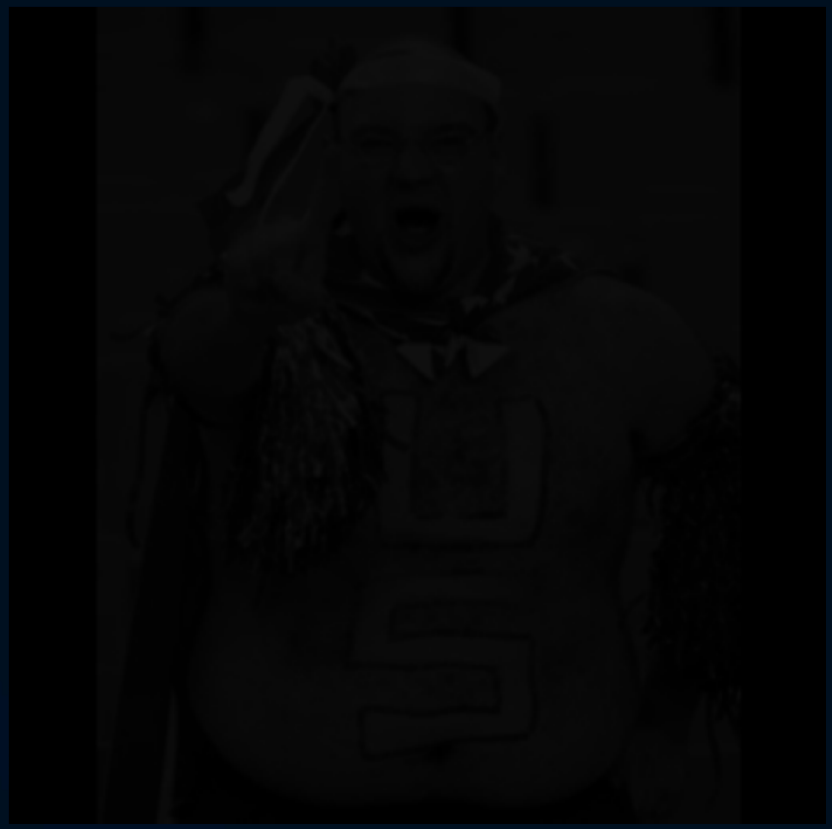
Wisdom from Cryptography

- Often designers think (erroneously) that "They'll never think of this." – yet, the designer did???
  - A criminal would never think to look in a flower pot for the house key
- Equipment may be captured or bought
- If the security depends on the secrecy of the algorithm, once it is compromised, the entire system is compromised - forever
- If a key is compromised, only that message is compromised
- A secure system will not rely on keeping the algorithm secret, just the key

The Cover Object Matters



For Example …



Applications

- Covert military & police communications
  - Criminals can tell police are nearby if they hear encrypted communications
- Digital Rights Management – protecting intellectual property such as images, music, electronic books
- Embedding textual data in medical images would ensure that the picture belongs to a particular patient
- Tamper proofing – ensuring a data file has not been changed
- Communicating in an oppressive country w/o free speech

Applications

- Data hiding has nefarious applications too
  - Money laundering
  - Drug running
  - Child pornography
  - Spying
  - Terrorism
  - Hiding pictures of your ex-girlfriend
- The technology itself isn't bad, but like many things, it can be (and is) abused
- It's like a gun, whether it's good or bad depends on which end is facing you

Questions &Comments