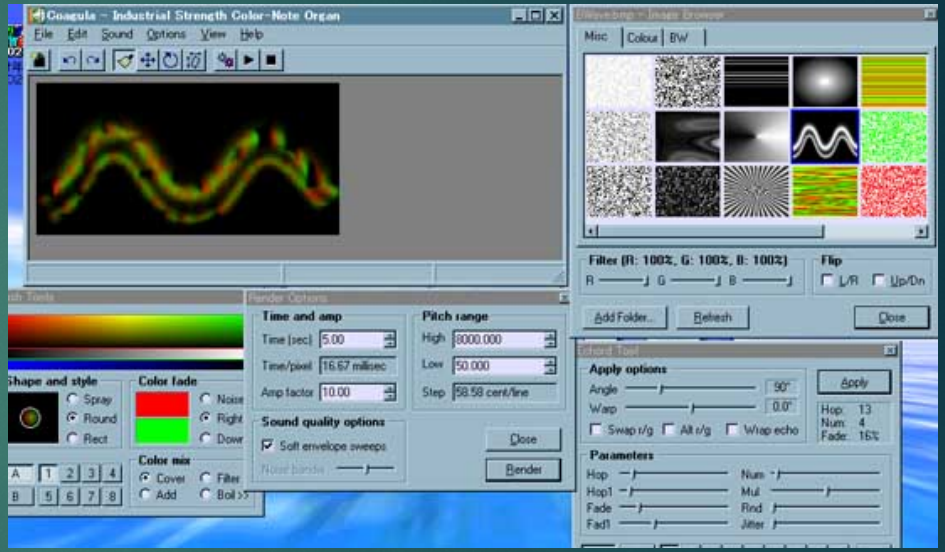
Understanding Covert Channels of Communication

PROF. CLAUDIO CILLI, PH.D., CISA, CISM, CRISC, CGEIT

UNIVERSITY OF ROME, ITALY

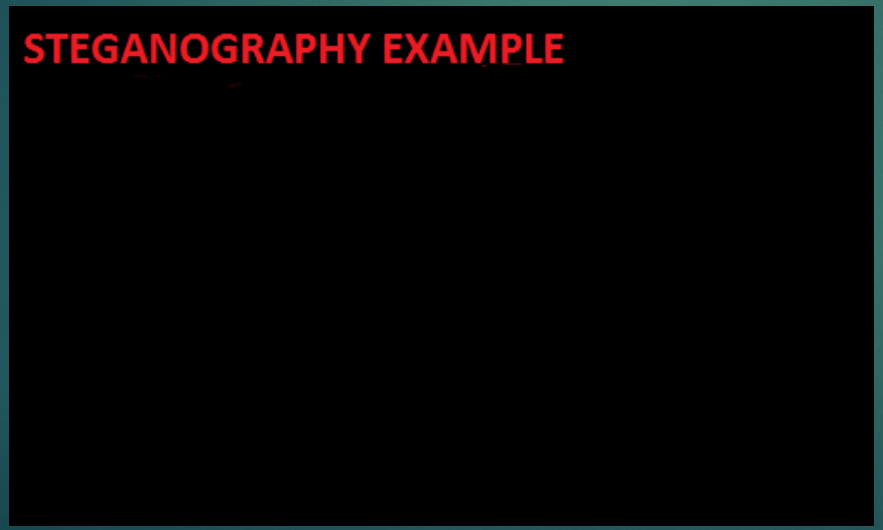
Coagula

- Industrial Strength Color-Note Organ
  - Coagula is an image synth. This means that it is both a simple image editor, and a program for making sound from those images.
  - Coagula uses one sinewave (beep) per image line, one short blip per point (pixel) on the line.
  - Red is left, Green is right, Yellow is green+red, so it's in the middle.
  - Blue makes each sine into a narrow noise-band, so you can create hard noise or organ-like sounds.



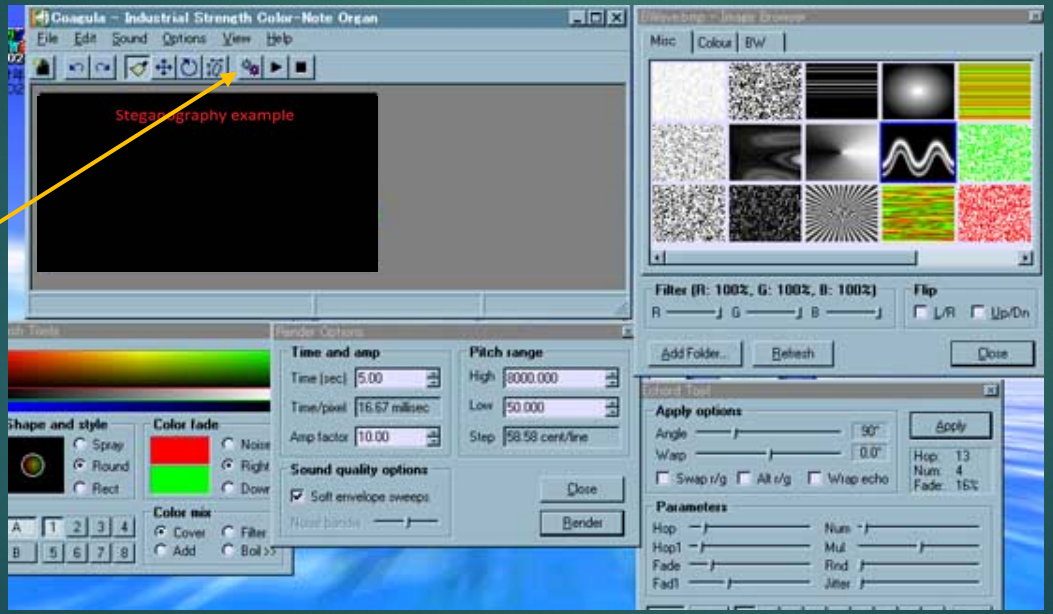
Paint

- Use a simple painting software, like MS Paint, to create a bmp image containing the text to hide. For best results, text should be red with black background



Use Coagula to Render the Text in Music

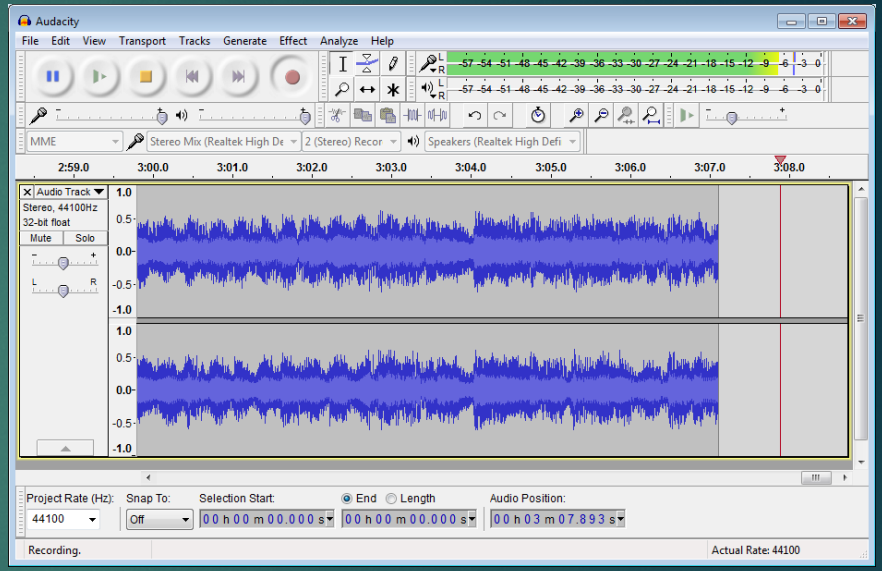
- After loading the text into Coagula, just press the double-wheels button to render the text into a sound and save the file file



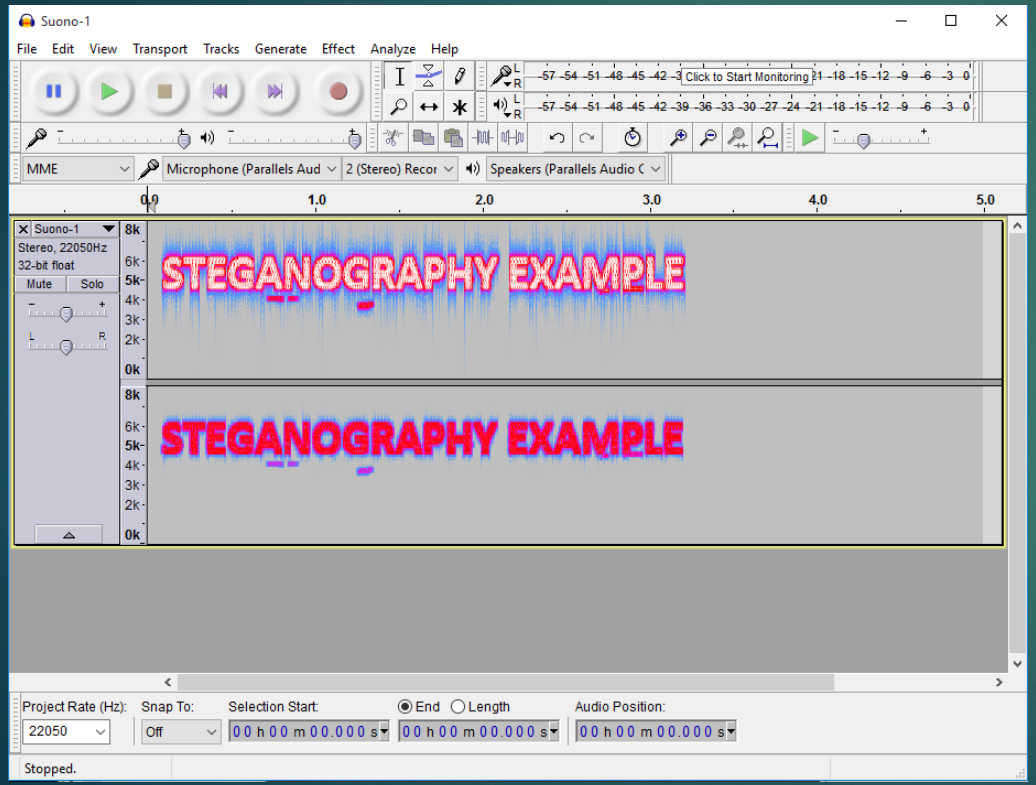
Press to render

Audacity

- The file created with Coagula can be sent as it is or linked to another sound. In this case it can be interpreted as a little noise at the beginning or at the end, and passes unnoticed
- The open-source sound analyzer Audacity shows the file waveform
- ...but what happens when we instruct Audacity to show the Fourier-analysis on the file?!



The Result is...



- Two public domain software apps, not intended for steganography purpose, together did the miracle!

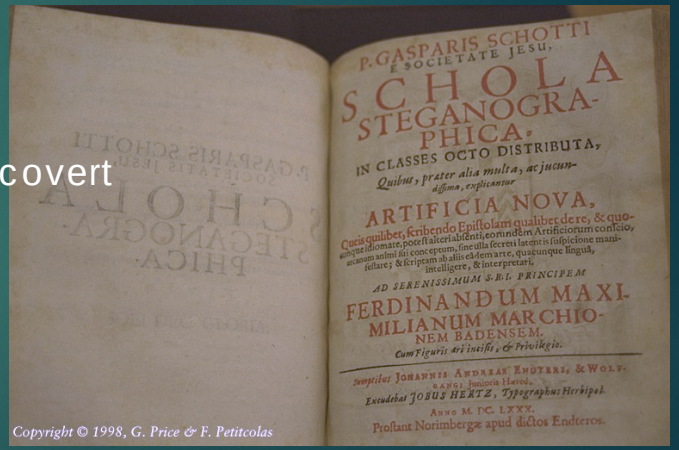
What is Steganography?

- Definition:
  - the art and science of hiding information by embedding it in some other data

- **cryptography** - render message unintelligible
- **steganography** - conceal the existence of the message

Some History

- 400 B.C. – Writings of Herodotus
- 1499 – “Steganographia”, Trithemius - steganography and magic
- 1665 – “Steganographica”, Gaspari Schotti
- 1870 – The Pigeon Post into Paris
- 2001 – A Beautiful Mind
- Steganography is one of the best known methods of covert communication
  - Invisible Ink
  - Wax Tablets
  - Microdots
  - Shaved heads of Slaves
  - Messages hidden in hunted animals



Classes of Information Hiding

- Digital watermarking
- Steganography
- **Covert channels**
  - Anonymous communication
- Protocol obfuscation

To defend against these channels, you must understand how they work

Covert Channels

- Definition: Communicate information between two computer **processes** that are **not allowed** to communicate, by hiding information into **shared resources**
- Steganography: hiding information into **digital media**
- Covert Channels allow multiple parties to communicate ‘unseen’
  - The intent is to hide the fact that communication is even occurring
  - Ensures privacy
- Unlike encryption, where communication is obvious but obscured
  - Encryption is easily identified
  - Clear and visible indications of encryption

Why do they Work?

- Covert Channels work because of human deficiencies
  - Eye sight
  - Hearing
  - Analysis skills
- Lack of Interest
  - It's not really a problem, it doesn't happen
  - "Prove it to me!"
- System Design Discrepancies
  - Components utilized in unintended manner
- **Many covert channels will elude detection simply because most individuals have never considered the possibility**
- Perception overrides reality

Measuring the Threat

- Availability of software tools and applications allow for easy creation of covert channels
  - Graphics editors
  - Audio editors
  - Packet insertion or manipulation libraries
  - Text generators
  - Operating systems (Windows)

- Plethora of web sites that list known applications for creating covert channels and steganography
- 250+ tools available on the Internet
- Good Covert Channels do what they're supposed to do

They hide the fact that communication between two or more individuals is occurring

- Technology has created a large enough haystack within the Internet to hide terabytes of data without detection

Applications

- **Legitimate uses**
  - Individuals or organizations storing sensitive information in steganographic carriers
  - Layered encryption / decoy data
  - Digital watermarking to verify intellectual ownership or authenticity
- **Illegitimate uses**
  - Terrorist Organizations
    - Easy form of covert communication
    - May 16, 2012 – Over 100 Al-Qaeda training manuals and detailed future plots discovered in a porn video found on an operative's flash drive.
  - Stealing/transmitting confidential data or corporate plans
  - Bypass security policy by malicious/compromised computer processes
  - Evade surveillance
  - Bypass communication restrictions

What is the Importance?

- Difficult to detect
- Can operate for a long time and leak a substantial amount of classified data
- Can compromise an otherwise secure system, including one that has been formally verified!

- It seems they should represent the panacea for secure communications, but in the real life things are different…

Covert Channels are Easy?

- Literature is full of articles and examples of covert channels,
- A lot of software for steganography applications exists,

but...

- In the real life things are different
- Using a covert channel is not an easy task: it requires a lot of work and it's risky...

Why Using a Covert Channel

- Covert channels presents several risks for the user should be used only if **ALL** of the following conditions are true:
  - Security is the main issue **AND** we don't want someone knows we're communicating
  - We are targeted **OR** under surveillance
  - We **cannot** establish a direct (encrypted) connection with our partner (prisoner's dilemma)

Why Using a Covert Channel

- Establishing a reliable covert channel requires a lot of work:
- Discover the covert channel inside the environment we and our partners live
- Check if the covert channel is real effective
- Establish a direct connection with our partner informing which kind of hidden communication we're about to use

- This requires a lot of time and the communication is always **SLOW**

Steganography & Cryptography

- Steganography and Cryptography are closely related
- The difference is in their goals...
  - Cryptography: although encrypted and unreadable, the existence of data is not hidden
  - Steganography: no knowledge of the existence of the data
- Steganography and Cryptography can be used together to produce better protection

Digital Watermarking

- Image “painted” with the watermark: “Invisible Man” © 1997, Neil F. Johnson

Digital Watermarking

- Used primarily for identification
- Embedding a unique piece of information within a medium (typically an image) without noticeably altering the medium
- Almost impossible to remove without seriously degrading an image
- Digital Steganography & Watermarking
  - Digital watermarking hides data in a file, and the act of hiding data makes it a form or steganography
  - The key difference is their goals...
    - Steganography: hiding information
    - Watermarking: extending the file with extra information
  - Steganographic information must never be apparent to a viewer unaware of its presence.

Types of Digital Steganography

- **Hiding a Message inside Text**
  - **Partially effective**
  - First-letter algorithm
  - Every n-th character
  - Altering the amount of whitespace
  - Using a publicly available cover source
- **Hiding a Message inside Images**
  - **Most popular technique**
  - Least-significant bit (LSB) modifications
  - 24-bit vs. 8-bit images
  - Tools to implement LSB: EzStego and S-Tools
  - Masking and Filtering
  - Algorithms and Transformations

randoM capitalosis is a rarE disEase ofTen contrAcTed by careless inTernet users. tHis sad illnEss causes the aFfected peRsON To randomly capitalize letters in a bOdy oF texT. Please do not confuse this disease witH a blatant attEmpt aT steganogRAPhy.

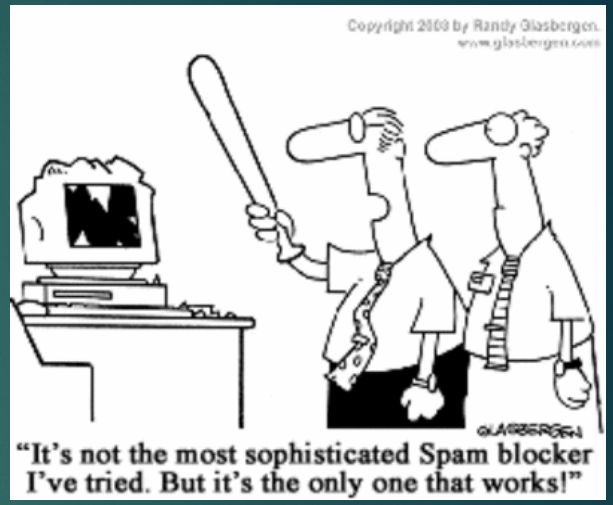
Reveals: MEET AT THE FRONT OF THE TRAP

Types of Digital Steganography

- **Hiding a Message inside Images (cont.)**
  - Removing all but the two least significant bits of each color component produces an almost completely black image. Making that image 85 times brighter produces the hidden image
- **Hiding a Message inside Audio or Videos Files**
  - Advantages
  - Human limitations – 20.000 Hz.
  - Large amount of data that can be hidden inside
  - Hard to recognize because of because of the continuous flow of information (moving stream of images and sound)

“Words, Words, Words”

- Spam is a low intensity, diffuse, and persistent “annoyance”
- We’ve been suffering from spam for thirty years now, and because spammers have only gradually “turned the heat up over time,” we’ve all become accustomed to spam, and we’ve all gradually developed an increasing tolerance for more and more and more of it
- **Most of us don't even believe spam is even a sneaky steganography weapon…**



From www.spammimic.com

Dear Friend , Your email address has been submitted to us indicating your interest in our newsletter . If you no longer wish to receive our publications simply reply with a Subject: of "REMOVE" and you will immediately be removed from our club . This mail is being sent in compliance with Senate bill 2116 , Title 7 , Section 301 ! Do NOT confuse us with Internet scam artists . Why work for somebody else when you can become rich within 13 DAYS ! Have you ever noticed the baby boomers are more demanding than their parents and nobody is getting any younger ! Well, now is your chance to capitalize on this . WE will help YOU process your orders within seconds plus deliver goods right to the customer's doorstep . The best thing about our system is that it is absolutely risk free for you ! But don't believe us ! Mr Ames who resides in Delaware tried us and says "My only problem now is where to park all my cars" ! This offer is 100% legal ! If not for you then for your loved ones act now ! Sign up a friend and you'll get a discount of 50% . Thank-you for your serious consideration of our offer !

Give us an A-

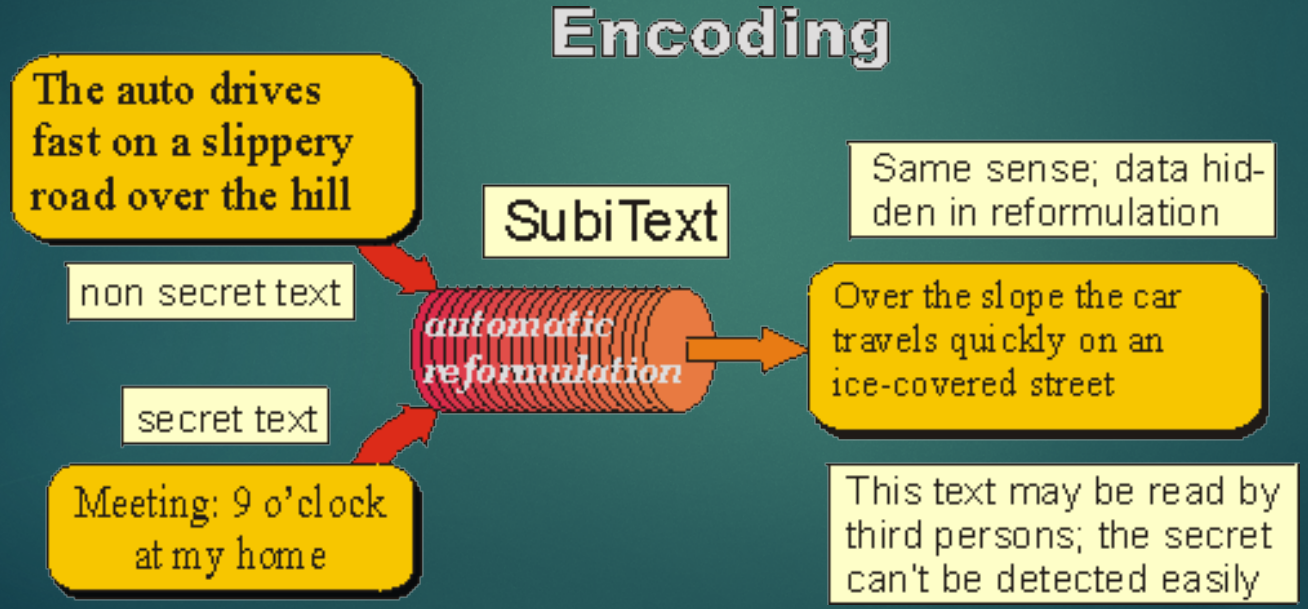
Languages are redundant
Relative message lengths:
Important Message: 13 Bytes
Spam Mail: 1,108 Bytes

Dear Friend , Your email address has been submitted to us indicating your interest in our newsletter . If you no longer wish to receive our publications simply reply with a Subject: of "REMOVE" and you will immediately be removed from our club . This mail is being sent in compliance with Senate bill 2116 , Title 7 , Section 301 ! Do NOT confuse us with Internet scam artists . Why work for somebody else when you can become rich within 13 DAYS ! Have you ever noticed the baby boomers are more demanding than their parents and nobody is getting any younger ! Well, now is your chance to capitalize on this . WE will help YOU process your orders within seconds plus deliver goods right to the customer's doorstep . The best thing about our system is that it is absolutely risk free for you ! But don't believe us ! Mr Ames who resides in Delaware tried us and says "My only problem now is where to park all my cars" ! This offer is 100% legal ! If not for you then for your LOVED ONES act now ! Sign up a friend and you'll get a discount of 50% . Thank-you for your serious consideration of our offer !

Give us an A+

From www.texthide.com

TextHide hides information in texts: the secret text "Meeting: 9 o'clock at my home" is to be hidden. A non-secret text – from the provided collection of texts – is "the auto drives fast on a slippery road over the hill". The secret text controls the rephrasing of this text and returns for instance: "Over the slope the car travels quickly on an ice-covered street."

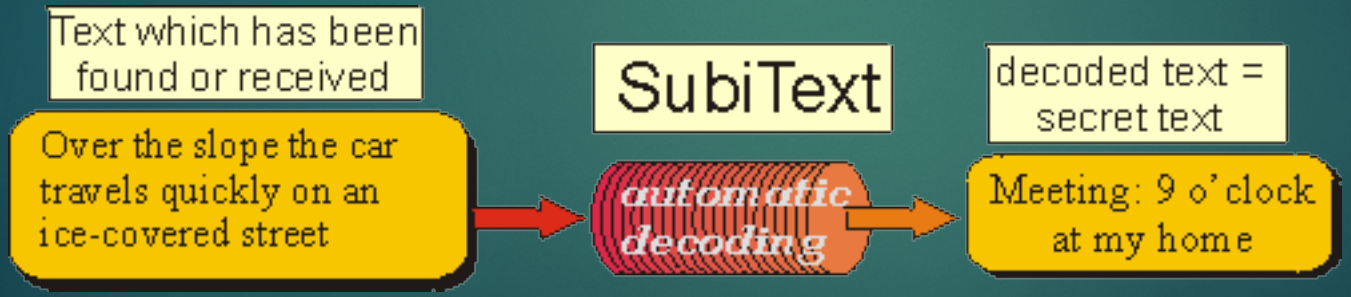


The sense of the sentence was preserved. Through the fact that exactly this one out of numerous possibilities for rephrasing was selected, the secret data is stored.

From www.texthide.com

Hiding

- By directly reformulating text data (text, binary data, ...) can be hidden in text. Everyone is able to decode something from the text, but if the text to be hidden was encrypted before, it cannot be seen whether the data decoded is relevant.



Ones and Zeros (1's and 0's)

- Commas in lists
  - Guns, butter, and brownies
  - Guns, butter and brownies
- Carriage return vs. Line feed (newline)
  - Carriage return: ASCII 015
  - Line feed: ASCII 012
    - ASCII 015 = 1 & ASCII 012 = 0

Spy Game

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

Spy Game

- The following message was actually sent by a German Spy in WWII

p
h
g
l
o m
j
i

s

Spy Game

- In 2006 during an routine investigation two CDs taped under coffee can were found:
  - One CD contained Cloak v7.0a
    - Very strong encryption option
  - Other CD contained
    - 41 files between ~12.5Mb and ~23Mb
    - Carrier file was only 263Kb

Carrier file

A Picture Joke

What's lurking behind this pretty face?

A Picture Joke

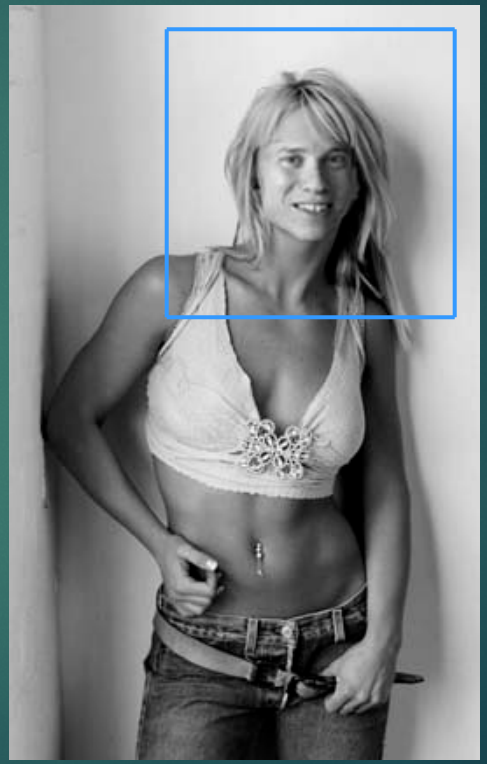
Another pretty face

(and quite a body)

A Picture Joke

Another pretty face

(and quite a body)



A Picture Joke

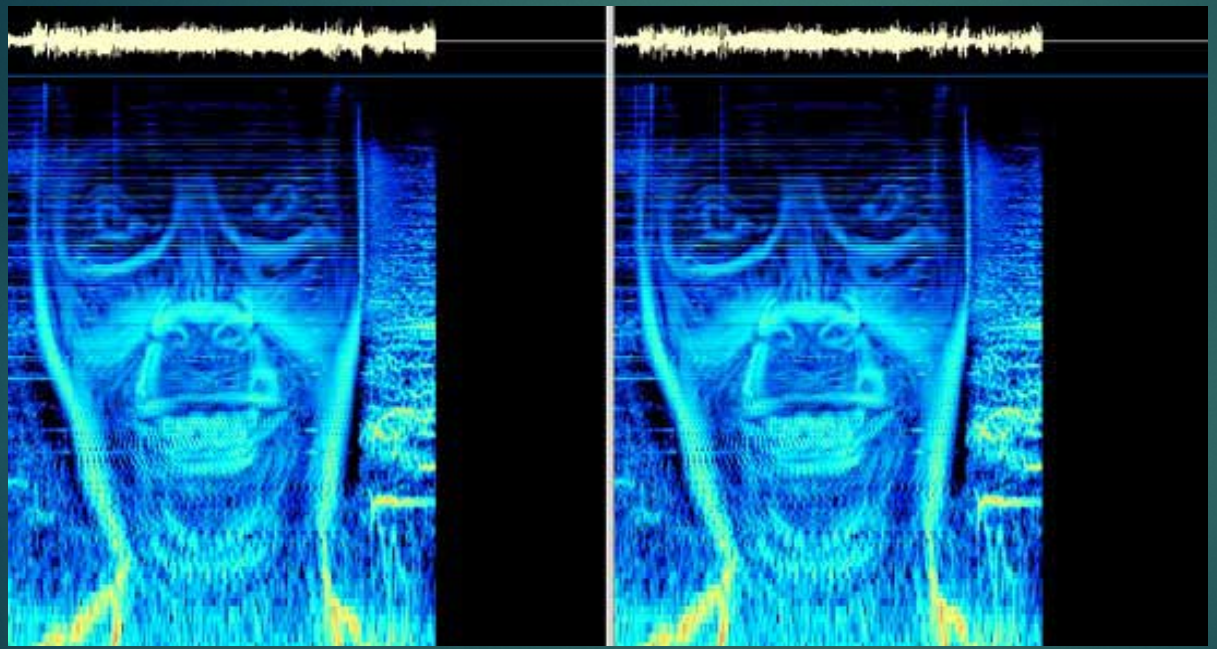
Images have a lot of data:
- Spam Mail: 1,108 Bytes
- Picture of Dave: 152 KB

Ways to hide information
- Least significant bit (BMP)
- Palette Shifts (GIF)
- Discrete Cosine Transforms (JPG)

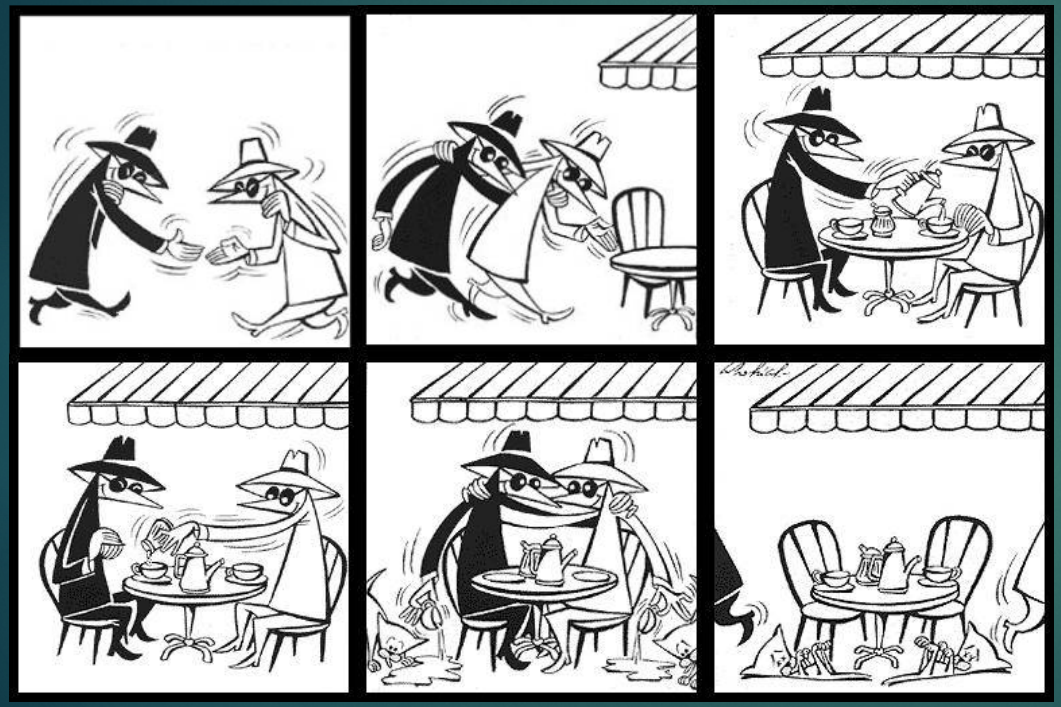
Steganography in Audio

- Audio files contain even more data:
  - Spam Mail: 1,108 Bytes
  - Picture of Dave: 152 KB
  - Aphex Twin: 2,769 KB
- Least significant bit (RAW)
- Echo hiding
  - We cannot perceive short echoes (millisecond short)
  - Introduce two types of short echo with different delays to encode zeros and ones
- Example program: MP3Stego
  - Information hidden during compression process

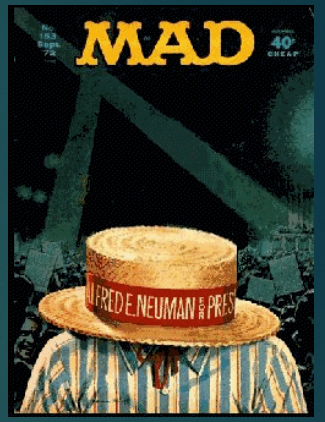
Aphex Twin



Spy Vs. Spy

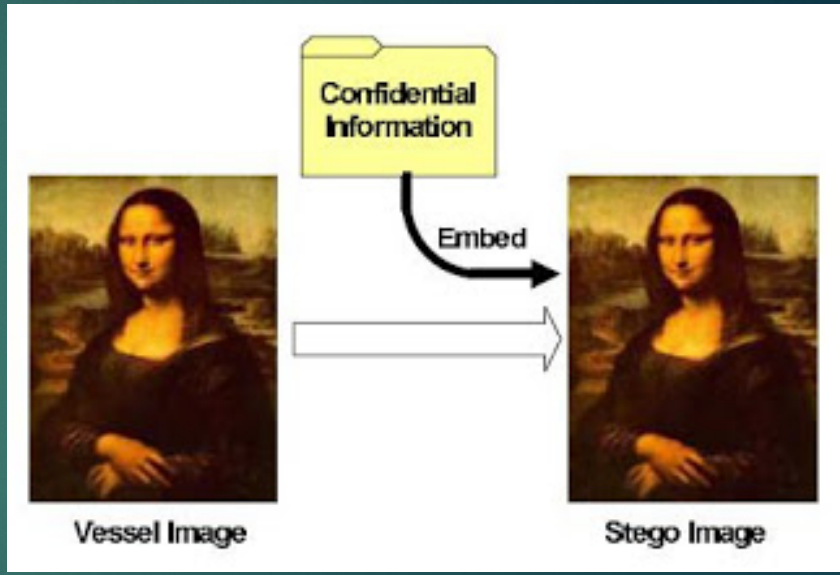


by Antonio Prohias
from MAD Magazine



Digital Steganography

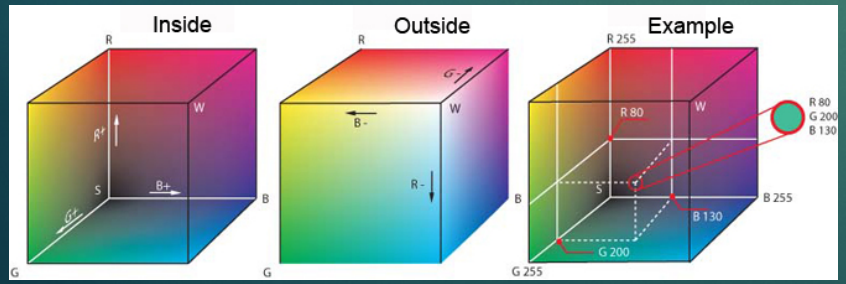
- *"Any sufficiently advanced technology is indistinguishable from magic."*, Sir Arthur Charles Clarke
- The art of hiding data in a file so that only the sender and intended recipient suspect the presence of hidden data
  - A form of security through obscurity
  - Very easy to accomplish
  - Harder to detect and decrypt
  - BMP, JPG, TXT, HTML/XML, PDF, PNG, GIF, AU, WAV, MP3, AVI, TIF, TGA, DLL, EXE



LSB Method

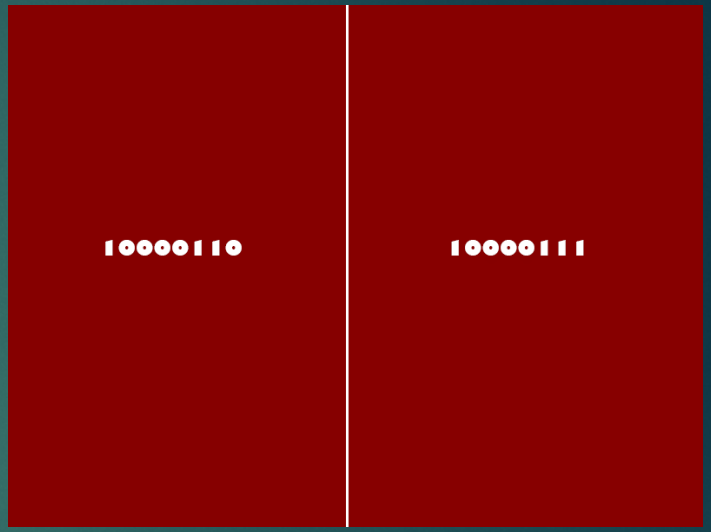
- Most common form of digital steganography
- In a RGB image, Information is hidden in the LSB[s] of the RGB values of each pixel
- In a 24-bit bitmap, each pixel represented by 3 bytes.
  - 8 bits representing red value = 2^8 = 256 shades of **RED**
  - 8 bits representing green value = 2^8 = 256 shades of **GREEN**
  - 8 bits representing blue value = 2^8 = 256 shades of **BLUE**

16,777,216 possible colors



Color Perception

- Changing the LSB of the Red value by 1 (in 24-bit color depth) is undetectable by the human eye
- Using the three color channels (RGB) we have 3 bit for hiding information
- Nokia 808 PureView:
  - 41 megapixel camera phone
  - 41 megapixels / (3 pixels/byte) = 13.66MB of data can be hidden in a single image



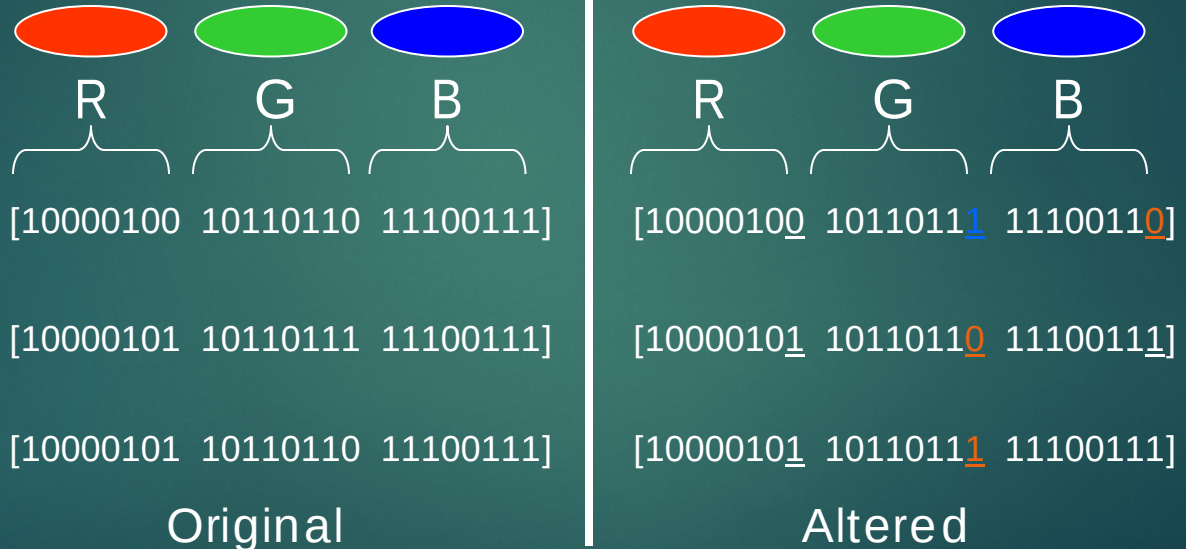
A Typical Example

Carrier Image

Pixels not to scale

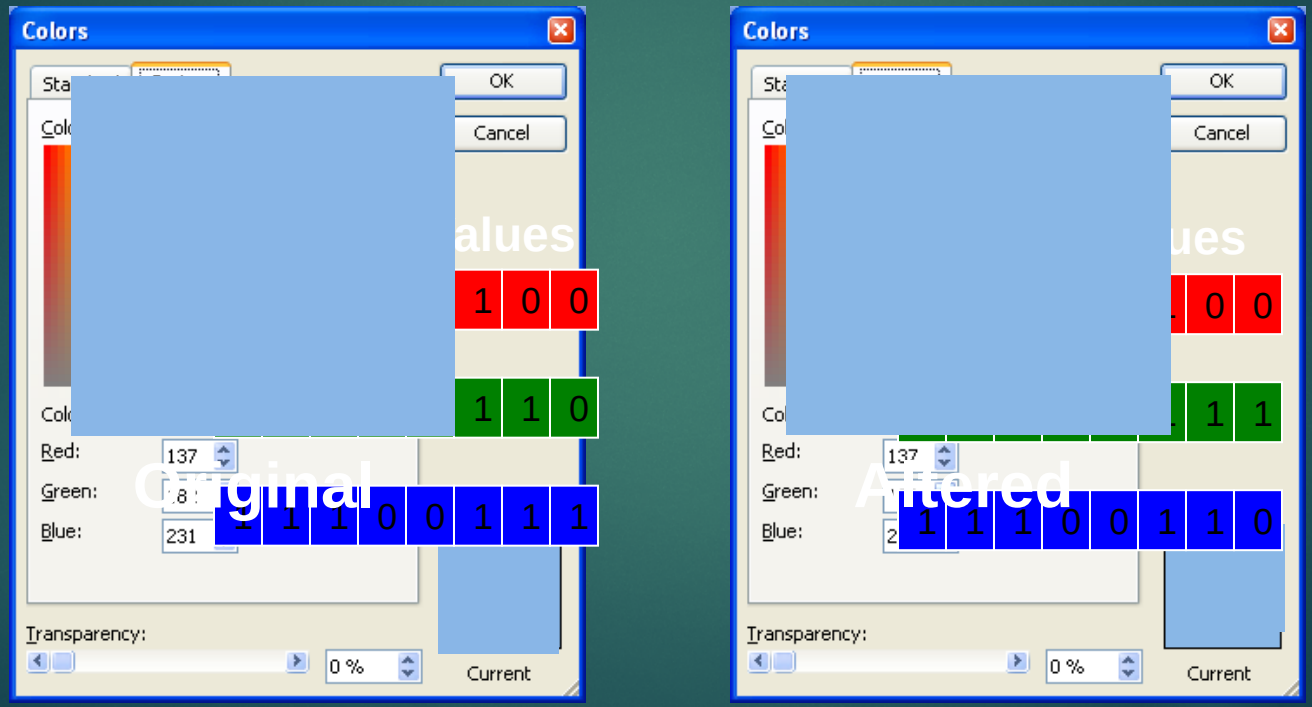
A Typical Example

Add the letter “W” to a 24-bit image file: W = 01010111 (ASCII)



A Typical Example

- Effect of change on first pixel:



A Typical Example

Carrier Image

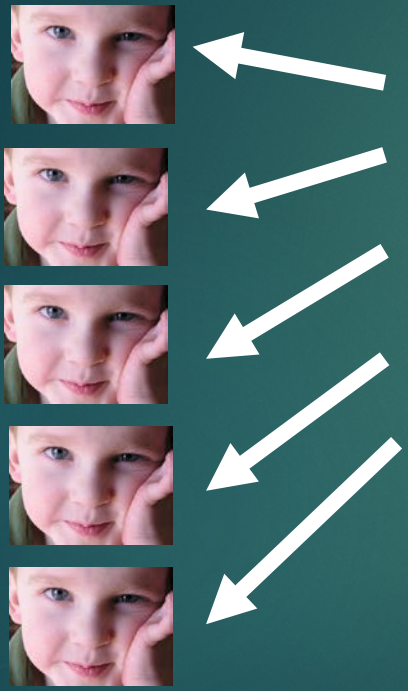
Altered Image

Altered image contains full text of Martin Luther King's I have a dream speech, 1963 *(With room for another 285,915 characters!)*

Image Size (768 X 1,024) = 786,432 pixels
= 2,359,296 bytes
= 294,912 characters

Document Size = 1,651 words
= 8,997 characters (w/spaces)

Carrier Group Concept



Multiple carriers
400k in size

Payload File
100k max

Carrier group

Traditional carrier

Single carrier file
400k in size

Payload File
100k max

Network Steganography

- Modifying network packet's header or payload
  - In TCP/IP networks, unused bits in the IP and TCP header may be used
- Packet based length steganography
  - Manipulation of the MTU (Maximum Transmission Unit)
- VoIP - Lost Audio Packets Steganographic Method (LACK)
  - Transmitter intentionally delays packets by an "excessive" amount of time.
  - Payload of these lost packets contains the secret information

Covert Network Channels

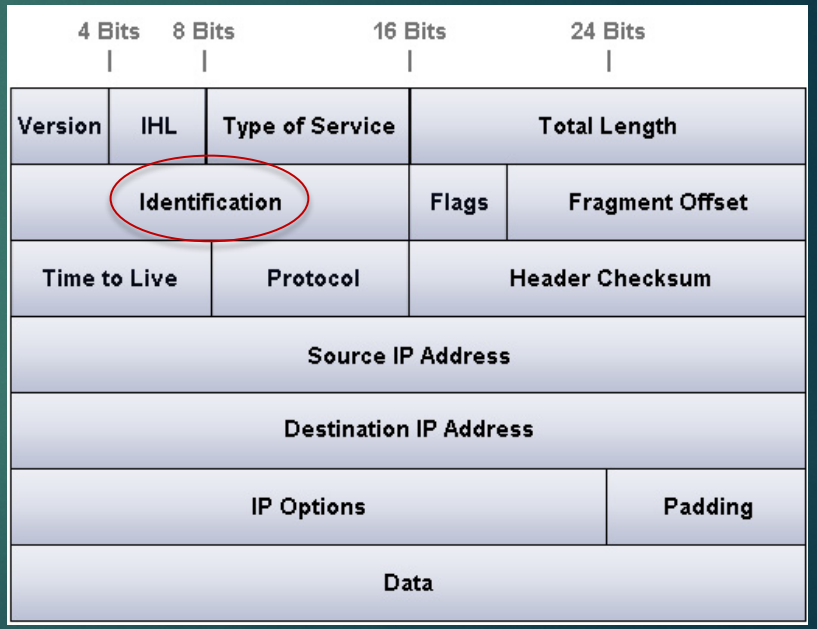
- All network protocols contain headers
- Each header contains areas that could be used to store or transmit data
- Many of these areas are never used for normal network transmission
- The most useful fields to store data in are those considered mandatory
  - *Less likelihood of being stripped off at a router*

Covert Network Channels

ID field (IPv4 Header):

- Can transmit one ASCII character per packet
- Represented by unsigned integer
  - We take the ASCII number for each character and multiply by 256 to give a realistic integer for this field and avoid suspicion:
    - “H” = ASCII 72 = 18432
    - “Hello” = 18432 / 17664 / 19456 / 19456 / 20224
    - Divide each by 256 to get the ASCII character number
- Plus other possibilities…

Standard IPv4 Header

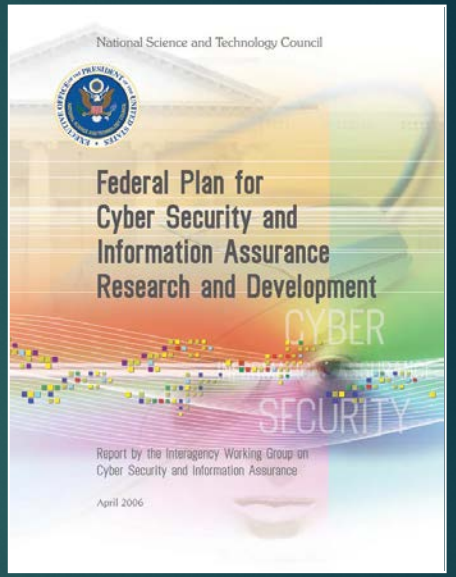


Stego Noise and Stego Bot Concepts

- Stego Noise
  - The stego noise concept was introduced 1997 by Fabian Hansmann, author of Steganos
  - Creating a benign worm written to take advantage of vulnerabilities on computer systems around the world. As the worm located systems with the vulnerabilities it was looking for, it would infect every image on each system it had access to with a benign form of steganography
  - The worm was programmed to insert random information into each image, creating useless steganography, or stegonoise, within the image. When law enforcement officials attempted to scan a computer system or the Internet for images with potential hostile or hidden content, eventually they would be inundated with large numbers of images appearing to have steganography within them
- The idea of the Stegobot takes the Stego Noise concept one step further
  - Sites with vulnerabilities can be infected with the stego noise virus
  - Infected files then pass on to the visitors of the site.
  - E.g. The slammer worm hit critical mass in just 3 minutes

Is Steganography a Threat?

- "The threat posed by steganography has been documented in numerous intelligence reports."
- "International interest in R&D for steganographic technologies and their commercialization and application has exploded in recent years."
- In describing threat and vulnerability trends … **insiders are at the top of the list!**



Not detected by firewalls!
Not detected by IDS/IPS!
Not detected by content filters!

Insider Use of Steganography

- A serious and growing threat
  - Conceal illegal images
    - Child pornography
  - Conceal unauthorized images
    - Adult pornography
  - Conceal evidence of criminal activity
- ***Not detected by firewalls!***
- ***Not detected by IDS/IPS!***
- ***Not detected by content filters!***

Insiders Surrounded by Sensitive Information

Insiders Surrounded by Sensitive Information

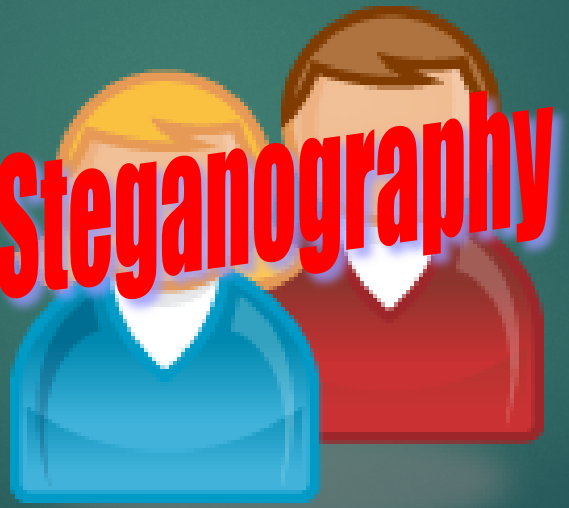
Portable Electronic Devices (PDA/iPod/etc)

E-mail

Telephone

E-mail attachments

Cell/Camera phones



3.5” Floppies

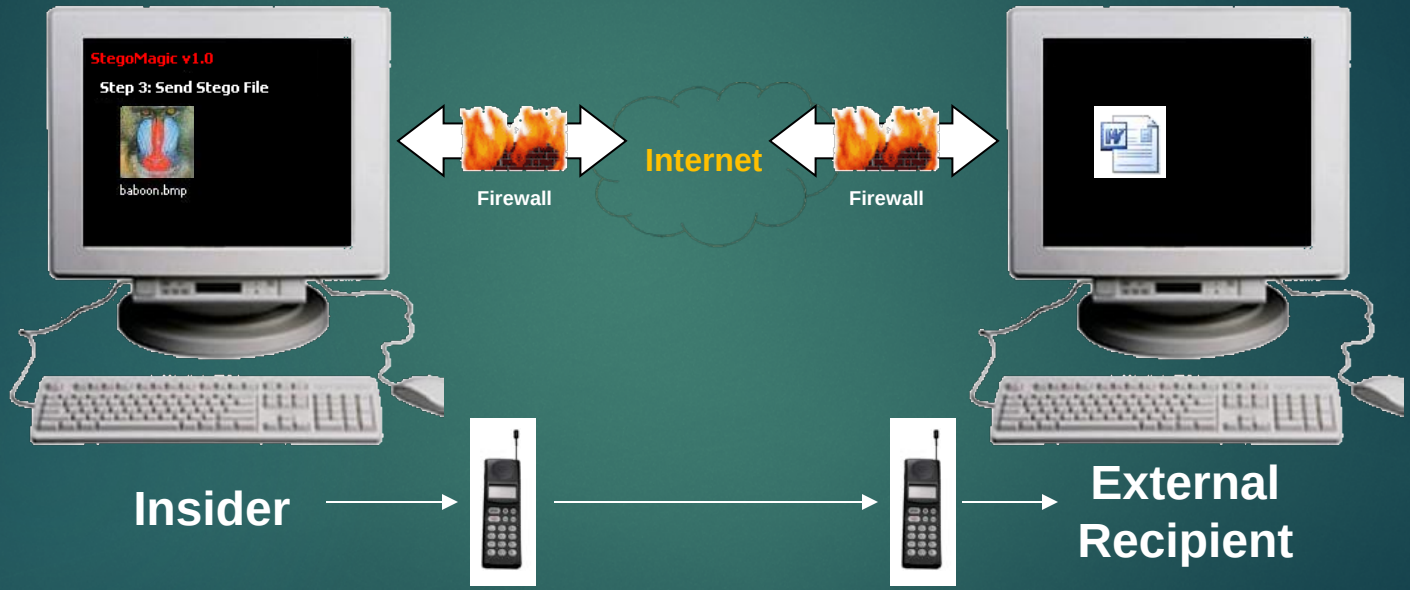
Printed listings

Portable storage media

CDs/DVDs

Jane and John Insider

Insider Use of Steganography – Email Scenario



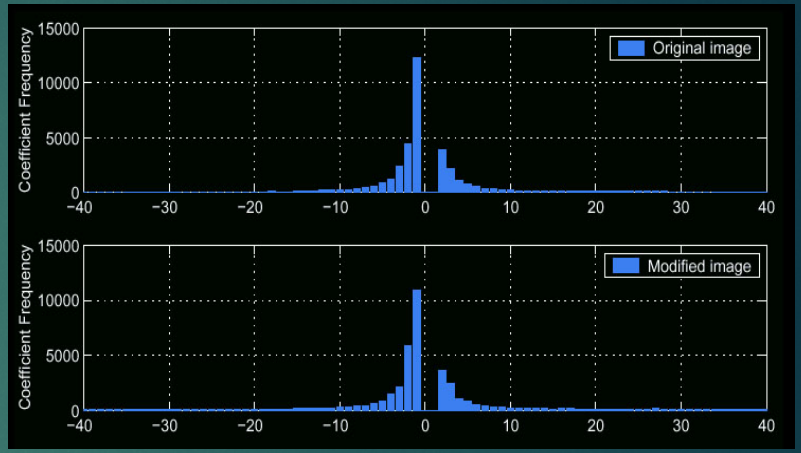
You **must** inform the recipient about **which** stego software you're been using and **when** data are transmitted

Insider Use of Steganography – Web Site Scenario

You **must** inform the recipient about **which** stego software you're been using and **when** data are posted on the web

Detecting Steganography

- Statistical properties of
  - Text
  - Music
  - Images
  - Videos
- Stego detection industry is still very young
- Few detection tools are available
- Few detection tools that work reliability
- Too many false positives
  - Difficult to detect covert channels
  - Can't detect minute amounts of data in large files
- Very few decryption or brute force options



Problems with Detecting Steganography

- Impractical to actively scan all internet content for steganography
- Data is likely encrypted
- Data can be hidden in certain parts of image or scattered based on a random seed
- Messages can be hidden in chains of files
  - Can be hidden in several files using different techniques for each
- Time consuming

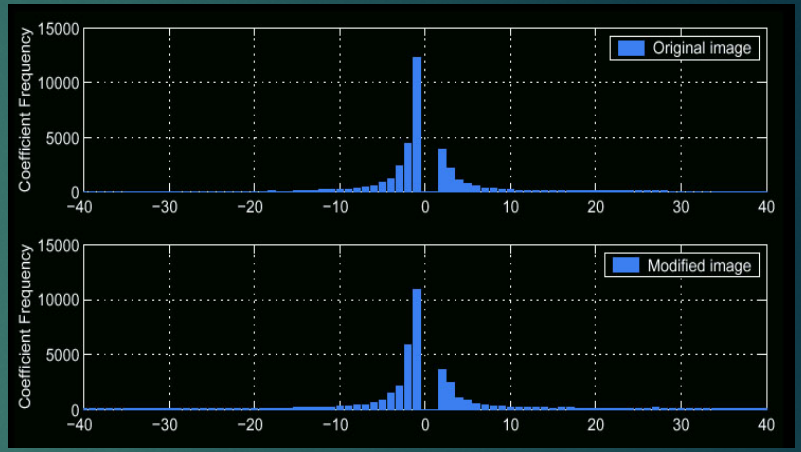
Original Image (cover)

Stego Image (with hidden data)

Can you see the difference?

Steganalysis

- Analyzing images for possible hidden data
- Many algorithms perform a statistical analysis to detect anomalies in the cover object
  - E.g. repetitive patterns could indicate use of a steganography tool or hidden message
- Investigating pixel “neighborhoods” to find inconsistencies with ways files are compressed.



Detecting Steganography

- Traditional approach
  - Blind detection
    - Visual attack
    - Structural attack
    - Statistical attack
  - Result expressed as probability
    - No extraction capability
- New approach
  - Analytical detection
    - Detect “fingerprints”
    - Detect “signatures”
  - Accurately identify application used
    - Provide extraction capability

Detecting Steganography

Detecting "fingerprints" of file artifacts

- *Artifact Detection*

A539F21BCA458D2EFFD4

Hash Value

Detecting "signatures"

- *Signature Detection*

Hexadecimal Byte Pattern

Detecting Steganography

- Difference is *subtle* but *very* *significant*
  - Artifact detection
    - Detecting hash values of files associated with steganography applications
      - Application ***might*** ***be*** ***used*** to hide something
  - Signature detection
    - Detecting hexadecimal byte patterns associated with steganography applications in carrier files
      - Application ***has*** ***been*** ***used*** to hide something

Detecting Steganography

File Associated With Steganography Application

```
3E 25 9F AD 2E E4 48
01 92 B3 21 00 00 62
FF 01 23 54 21 01 34
E4 AA 02 75 1E BC 42
00 DC 04 67 E8 A1 B3
44 02 34 53 47 85 4E
73 E6 FF 32 D2 21 03
24 45 A0 21 BB C4 34
67 F5 E2 DD 34 58 EF
```

A539F21BCA458D2EFFD4

Result is "hash value" or "*fingerprint*" of the file *artifact* associated with a steganography application

Any File

```
E3 52 F9 DA E2 4E 84
10 29 3B 12 00 00 26
FF 10 32 45 12 10 43
4E AA 20 57 E1 CB 24
00 CD 40 76 8E 1A 3B
44 20 43 35 74 58 E4
37 6E FF 23 2D 12 30
42 54 0A 12 BB 4C 43
76 5F 2E DD 43 85 FE
```

2E DD 43

Result is "hexadecimal byte pattern" or "*signature*" left in carrier file by the steganography application

Conclusion

- You can **only** combat covert channels if you understand how it works
- Insider use of steganography is serious and growing threat
- Will **never** be detected if no one ever **looks for it**
- Steganalysis should be conducted as routine aspect of computer forensic examinations
- Using covert channels and steganography implies a **direct contact** between parties (prisoner's dilemma)
- This is the **only weakness** of the chain which allows (sometimes) to detect its use

Thanks for your attention!

Questions?