# Steganography & Steganalysis

An Overview

Shohini Banerjee
44/MTECHIT/USS/03
SEMINAR IT
Aug-Nov'06

# Objective..

- What is Steganography
  - Concept
  - Methods & Possibilities
  - Applications
    - Terrorist Tool
    - On WAP
    - Digital Watermarking
  - Implementations
    - Embedding data within images
- Steganalysis
- StegoAttacks

# Concept..

Transmission of embedded data that is

- Imperceptible
- Retrievable
- Resistant to degradation, processing
- Difficult to remove, change by unauthorized access
- In the form of innocuous images, audio, video, text or any digitally represented code (bit stream)

# Methods & Possibilities..

- Traditionally
  - Invisible ink (fruit juice, milk)
  - Modulations in layout of documents
  - Minute modulations in handwriting
- More recently
  - Hide info in images
    - LSB method
    - Masking Filtering
    - Transformations like DCT, Fourier, Wavelet

- Hiding info in the file system
  - FAT16 format
  - Hidden partitions
- Internet protocols
  - TCP headers
  - IP headers
- Mimic Functions – obfuscate messages
  - Cant fool a person but can fool the computer performing a search!
- BMP, JPEG, MPEG, TXT, HTML/XML, PDF, PNG, GIF, AU, WAV, MPS, AVI, TIF, TGA, DLL, EXE

# Applications..

- Transfer strategic data & messages
  - Copy right information
    - Digital Watermarking
  - Defence strategies
  - Business plans
  - Private information
  - Illegal content
- Different from Cryptography

# Steganography as a Terrorist Tool

- 9/11 terrorists used the internet-FBI
- Maps, Terrorist Target Photographs, Instructions
- Messages in
  - Mundane emails
  - Website images
    - Pornographic
    - Auctioning
    - 30 billion images,3 billion websites – Keep a watch on all ??
    - Terrorist sympathizer website – image remains visually same, changes statistically every ten minutes
  - Audio – commonly shared, easily carried
- Size of payload (1 bit??)
- Impossible to track

# Steganography on WAP

- Wireless Internet on mobile phones (Wireless Application Protocol)
- Data security/Hidden Communication
- Embed data in WML (Wireless Markup Language)
- Hide data in ID of WML Tags
- Java/J2ME, Nokia 60 series

# Steganography in Digital Watermarking

- Uses
  - Prove ownership
  - Identify misappropriating person
  - Trace dissemination through network
- Various techniques
  - Visible, Invisible, Public, Fragile, Private, Perceptual, Bit stream
- Algorithms
  - NonBlind
  - SemiBlind
  - Blind
- Methods
  - Spatial
  - Frequency

# Implementations

***Cover medium+embedded message+stegokey= stego medium***

- Stego Tools
  - 1 Million tools downloaded from internet website
  - www.stegoarchives.com

# Embedding Data in Images

- Image Domain
  - LSB Insertion
  - Noise Manipulation
  - Simple Systems
  - Tools like StegoDos, STools, Mandelsteg, EzStego etc
- Transform Domain
  - DCT
  - Wavelet Transformation
  - Tools like PictureMarc, SysCop, SureSign etc
  - Much more robust
    - Independent of image format
    - Survive conversion b/w lossless and lossy formats

- JPEG
  - DCT
  - Compressed data stored as integer
  - Calculations in floating point
  - Rounding off errors – lossy compression
  - Hide info – manipulation of rounding values
  - Advantage of DCT – no block like appearance b/w sub images
  - Tools like Jpeg-Jsteg

- Both Image and Transform
  - Patchwork, domain, pattern, block encoding, spread spectrum methods, masking
  - Patchwork – pseudo random technique – select multiple areas called patches for marking
  - Add redundancy
  - Protect against image processing – cropping, rotating

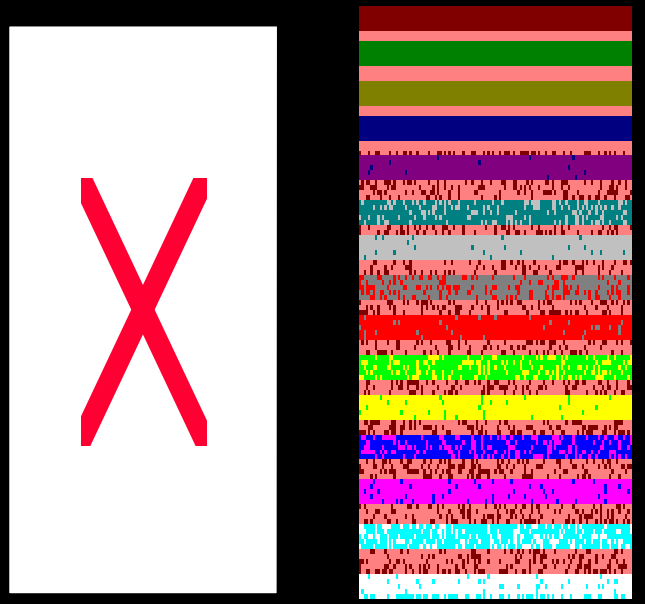
# Detecting Hidden Information

- **Any manipulation introduces some degradation/distortion**
- **Most tools leave signatures**
- **First define a normal/average image**
- **Color composition, pixel relationship, luminance**
- **Eg. Image color palettes – colors arranged from most used to least used**
  - Change is gradual – monochromatic images
  - Change is drastic - hand drawings, fractals, clip art
  - Single outstanding pixel – look here for hidden data!

- Keeping the pallette same
  - **Recognizable as exaggerated noise**
  - 8 bit images without manipulating palette successful if adjacent entries are similar
  - Else noise is obvious
  - Gray scale images are a good medium
- Reordering the palette
  - Sorting may be insufficient
- Creating a new palette
  - Convert 8 to 24 bit
  - Disadvantage- larger size, unsuitable for transmission
  - Poosible soln-convert back to 8 bit

# Looking for signatures

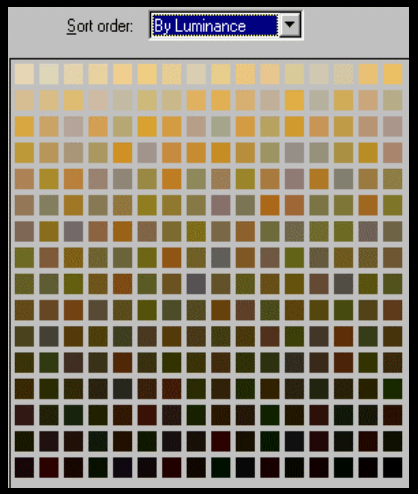
- Repetitive patterns
- Distortions
- Compare cover image with stego image
  - Noise v apparent in JPEG
- Derived/known signatures
- Some tools provide images that look pristine only on paper



Distortion due to contrasting adjacent pallette entries

# Specific Tool signatures

- S-Tools
  - Reduces cover to 32 colors
  - New colors are expanded over several palette entries
  - Sort by luminance – 1 bit changes
  - Not naturally occurring
  - Same for other bit wise and transform tools




Before


After

- SysCop
  - Unique adjacent palette entry pattern
    - 00 00 00, 01 01 00, 01 00 01
  - Buffer 32+ palette entries with black (00 00 00) before raster data begins
  - Normally black has black+near black colors
  - Anomaly – hidden data detected!

# Steganalysis vs Cryptanalysis

- Detect, Extract/Destroy Stego-media
- Cipher text only, known plain text, chosen plain text, chosen cipher text
- Decode Cipher Text
- Stego only, known cover, known message, chosen stego, chosen message

# StegoAttacks

- Detection and Extraction
- Detection and Destruction/Disabling
- Robustness Test
  - Convert b/w lossy and lossless formats, blurring, smoothing, adding noise, sharpening
  - Bit wise tools – less robust
  - Transform Tools
    - Survive minor changes
    - Fail with a combination of image processes
  - If you have original and altered watermark image – recovery possible

# Scope of the Field

- Covert communication would never say die
- Research
  - More robust hiding techniques – steganograpphy
  - More robust revealing/disabling techniques - steganalysists

# References


- ‘Steganalysis: The Investigation of Hidden Images’, Neil F Johnson, Sushil Jajodia
- ‘What You Can’t See Can Hurt You – The Dangers of steganography’, WetStone – Securing Digital Integrity
- ‘Hiding in Plain View – Could steganography be a Terrorist Tool?’, Tom Kellen
- ‘Watermarking in MPEG4 Multimedia Contents’, Chowdhury Vikram
- ‘Steganography in Wireless Application Protocol’, M. Shirali Shareza
- ‘An Information – Theoritic Model for Steganography’, Cachin Christian
- ‘Steganography’, Duric
- http://www.rsac.org
- www.digitaltermpapers.com

THANK YOU!