STEGANOGRAPHY: HIDDEN IN PLAIN SIGHT

BY: KEVIN R. MEDINA SANTIAGO
COMPUTER FORENSICS

• Investigation of information found in computers and digital storage media

• Focuses on:
  • Identifying
  • Preserving
  • Recovering
  • Analyzing
WHAT IS STEGANOGRAPHY?

S
Covered, concealed, protected

GRAPHEIN
Writing
Histiaeus  Herodotus  Revolution Histories against the Persians 440 A.C.
PHYSICAL STEGANOGRAPHY

• Invisible Ink
  ISEC
• Message under a postage stamp
  InfoSecurity
• Knitting a message in on clothing
  Tour
• Blinking in Morse code
  2018
DIGITAL STEGANOGRAPHY

• 1975, Personal Computers

• 1985, Barrie Morgan and Mike Barney, Datotek, M2B2

• Steganography tools surfacing
  • Slow at first, followed by a rapid spike
CURRENT STEGANOGRAPHY TOOLS

• TOO MANY TO LIST!!!
• Here are a few:
  • ImageHide
  • Hide in Picture
  • BDV DataHider
WHAT DO THEY DO?

• Hide stuff
  • Images, videos, audio files, documents, text

• Inside other stuff
  • Images, videos, audio files, documents, executables, folders
ENCRYPTION (WHY NOT?)

• Advanced Encryption Standard
• Data Encryption Standard
• Message Digest 5
• Secure Hashing Algorithm
IMAGE STEGANOGRAPHY

Is EHILOORESU FRUWEOERU
DIGITAL WATERMARKING

• Visible Watermarking
  • A logo or text that denotes the owner

• Invisible Watermarking
  • Data embedded into file
    • Invisible and inaudible
STEGANOGRAPHY METHODS
LEAST SIGNIFICANT BIT (LSB)

Data to be hidden:

101101

10000010
01101101
10101001
**DISCRETE COSINE TRANSFORM (DCT)**

- Technique used to compress JPEG, MJPEG, MPEG

<table>
<thead>
<tr>
<th></th>
<th>-23</th>
<th>-2</th>
<th>0</th>
<th>0</th>
<th>0</th>
<th>0</th>
<th>0</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>-21</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>-1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
STEGANALYSIS

• Stego-Only attacks – Stego object available
• Known Cover Attack – Original and Carrier available
• Chosen Stego Attack – Programs used, patterns compared
• Known Stego Attack – Everything is available
HOW TO DETECT?

- EnCase, Guidance Software Inc.
- Ilook Investigator
- StegDetect
- Forensic Toolkit, AccessData
NETWORK STEGANOGRAPHY

- Coined in 2003, Krzysztof Szczypiorski
- Communication Protocols
  - Protocol Logic Manipulation
- Deliberate Packet Delays
- Much harder to detect!
CRYPTOGRAPHY V.S. STEGANOGRAPHY

- Known message passing
- Common technology
- Most algorithms known to governments
- Current algorithms resistant to BFA, but strength reduces while technology increases

- Unknown message passing
- Little Known Technology
- Technology still being developed for certain formats
- Once detected message is known
WHY IS THIS SCARY?

• Mostly used maliciously:
  • Terrorism
  • Hide stolen data
  • Hide illegal videos/images

• Research and Development must go on!
CONCLUSION

• Still being investigated
• Difficult to notice
• Can hide large amounts of data
• Various types of uses, including commercial
REFERENCES

• Funds for foreign cryptology support, 10 USC §412


REFERENCES


This material is based upon work supported by, or in part by the National Science Foundation Scholarship for Service (NSF-SFS) award under contract award #1563978.