The Use of Steganography and Steganalysis Trends in Computer Forensics

Dinesh Reddy

Assistant Professor of Cybersecurity

Our Lady of the Lake University

Agenda

- History of Data Hiding

- Use of Steganography Methods in Computer Forensics
  - Image: LSB Method, Masking and filtering, Transformations
  - Text: Line-Shift Coding, Word-Shift Coding
  - Audio: LSB coding, Echo Hiding
  - Video steganography

- Use of Steganalysis in Computer Forensics
 - Invisible Secrets, S-Tools

History of Data Hiding

- Ancient Chinese wrapped notes in wax and swallowed them for transport

- In ancient Greece, message written on slave's shaved head, then hair allowed to grow back

- During World War II, French Resistance sent messages written on the backs of couriers using invisible ink

Steganography

- The art and science of writing hidden messages

- Goal is to hide information so that even if it is intercepted, it is not clear that information is hidden there

- Most common method is to hide messages in pictures using the least significant bit (LSB) method

Steganography Vs Encryption

Steganography

Message hidden | **Message present but obfuscated**

Encryption/Cryptography

5
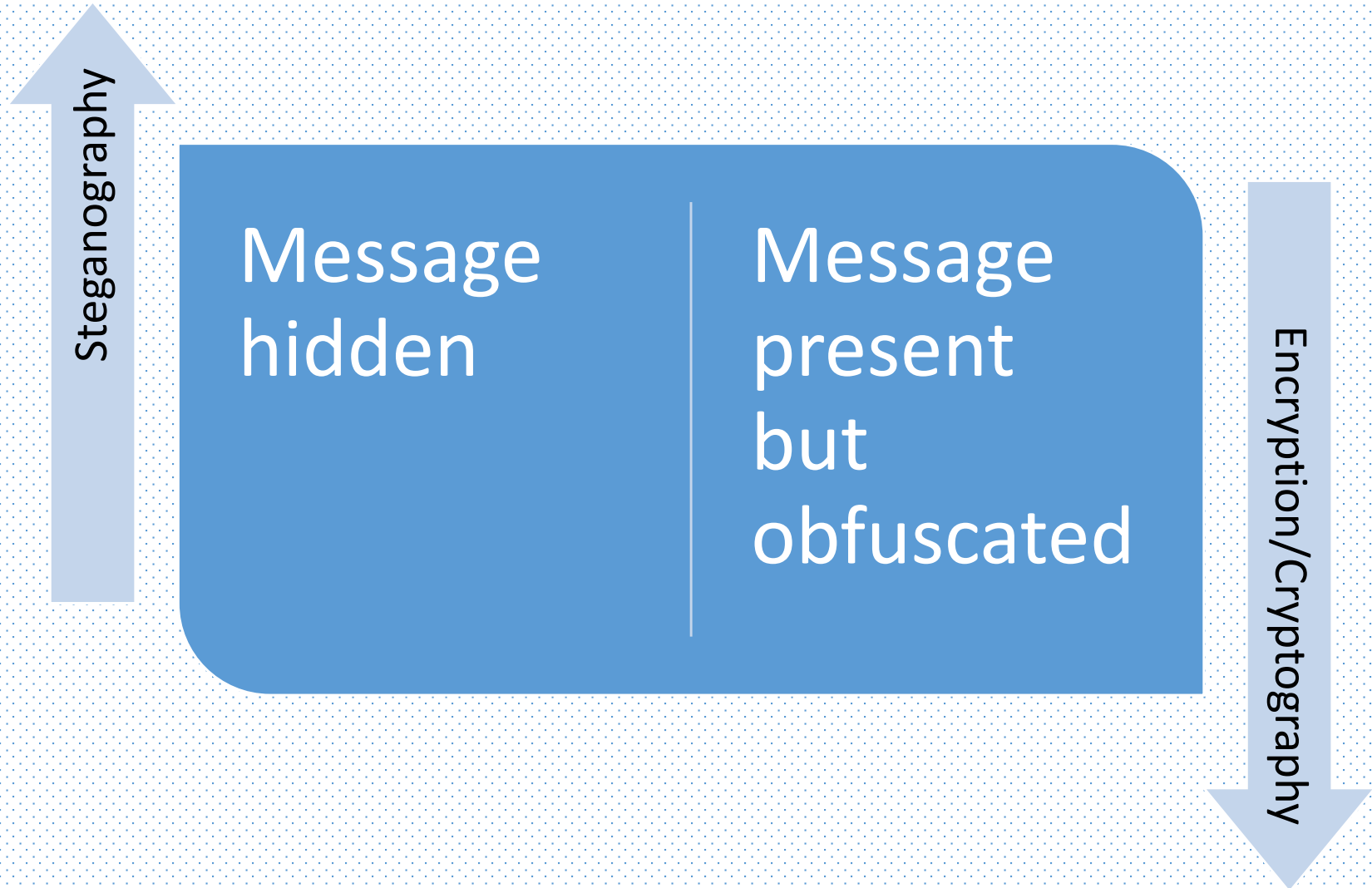
Basic Steganography Terms

Payload

Carrier

Channel

LSB Method

- The LSB method depends on the fact that computers store things in bits and bytes.

- Colored pixels in a computer stored in bits

- Consider 11111111 = 255 in decimal
- Change last digit to 0
- 11111110 = 254 in decimal (Minimal deviation as compared to original value which was 255)

- So, the last bit or least significant bit is used to hide data

LSB Method

- MSB ………LSB

- 11111111 = 255
- 11111110 = 254
- 01111111 = **128 (Changing MSB will significantly change the image revealing that image is modified)**

- Decimal equivalent conversion of binary number 11111111

  $1 \times 2^7 + 1 \times 2^6 + \ldots + 1 \times 2^2 + 1 \times 2^1 + 1 \times 2^0 = 255$

LSB Method
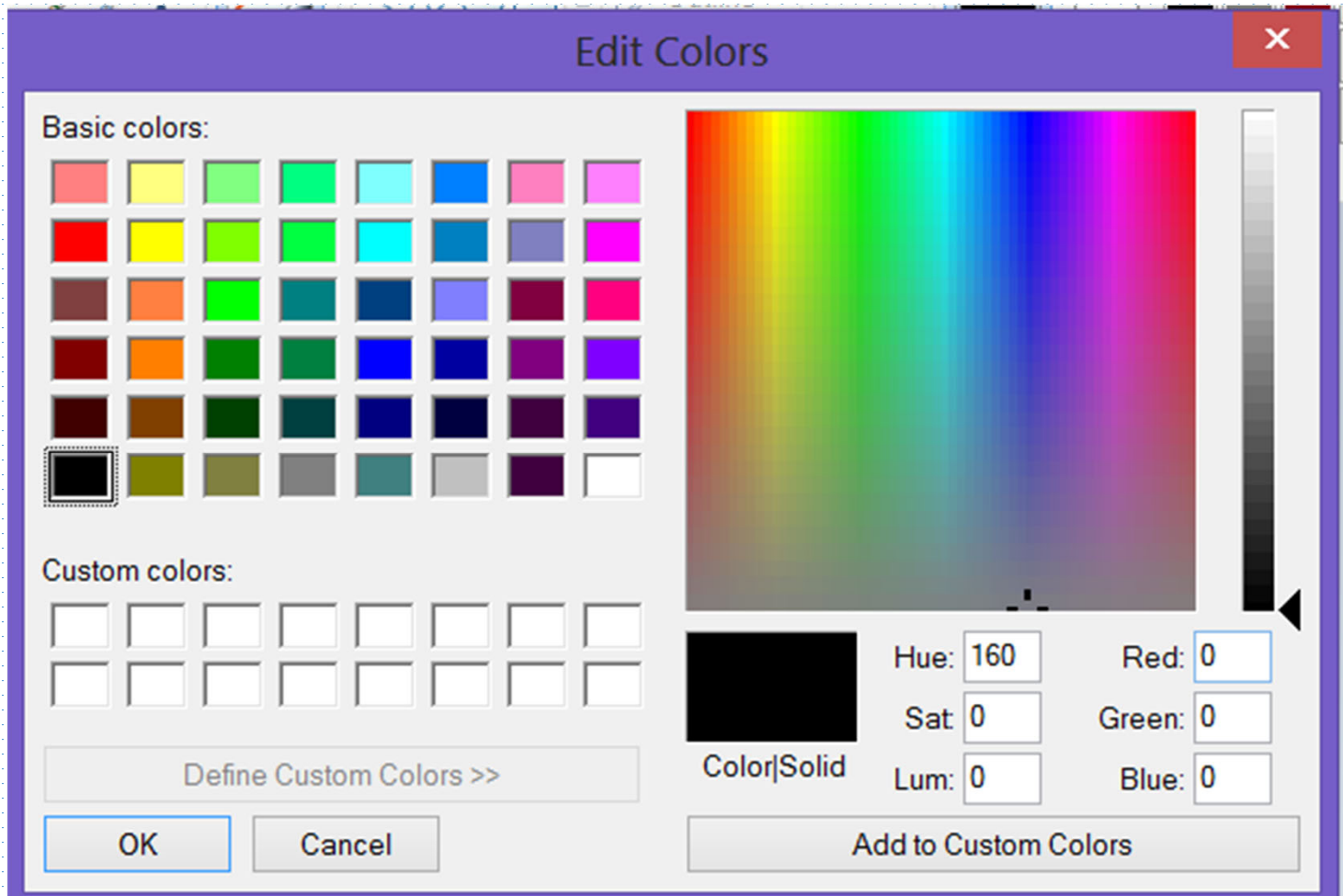
LSB Method

LSB Method

- E.g. 3 pixels of a 24-bit color image, uses 9 bytes:

  (00100111 11101001 11001000)

  (00100111 11001000 11101001)

  (11001000 00100111 11101001)

- After hiding A (binary 10000001):

  (00100111 11101000 11001000)

  (00100110 11001000 11101000)

  (11001000 00100111 11101001)

- Only three bits were sufficient to hide A

Other Image Steganography Methods

- Masking and filtering
  - Hide information by modifying the luminance to create a marking on an image (similar to watermarks)
  - Restricted to 24 bits

- Transformations
  - Hide information by modifying discrete cosine transformations (DCT)
  - DCT is performed by an image compression algorithm to reduce the size of an image for efficiency

Text Steganography

- Hide information by modifying textual characters, page layouts and other similar textual content and formatting items in a text file.

- Line-Shift Coding
  - Vertically shifting the location of text lines to hide new information.

- Word-Shift Coding
  - Horizontally shifting the location of words within text lines to hide new information.

Other Forms of Steganography

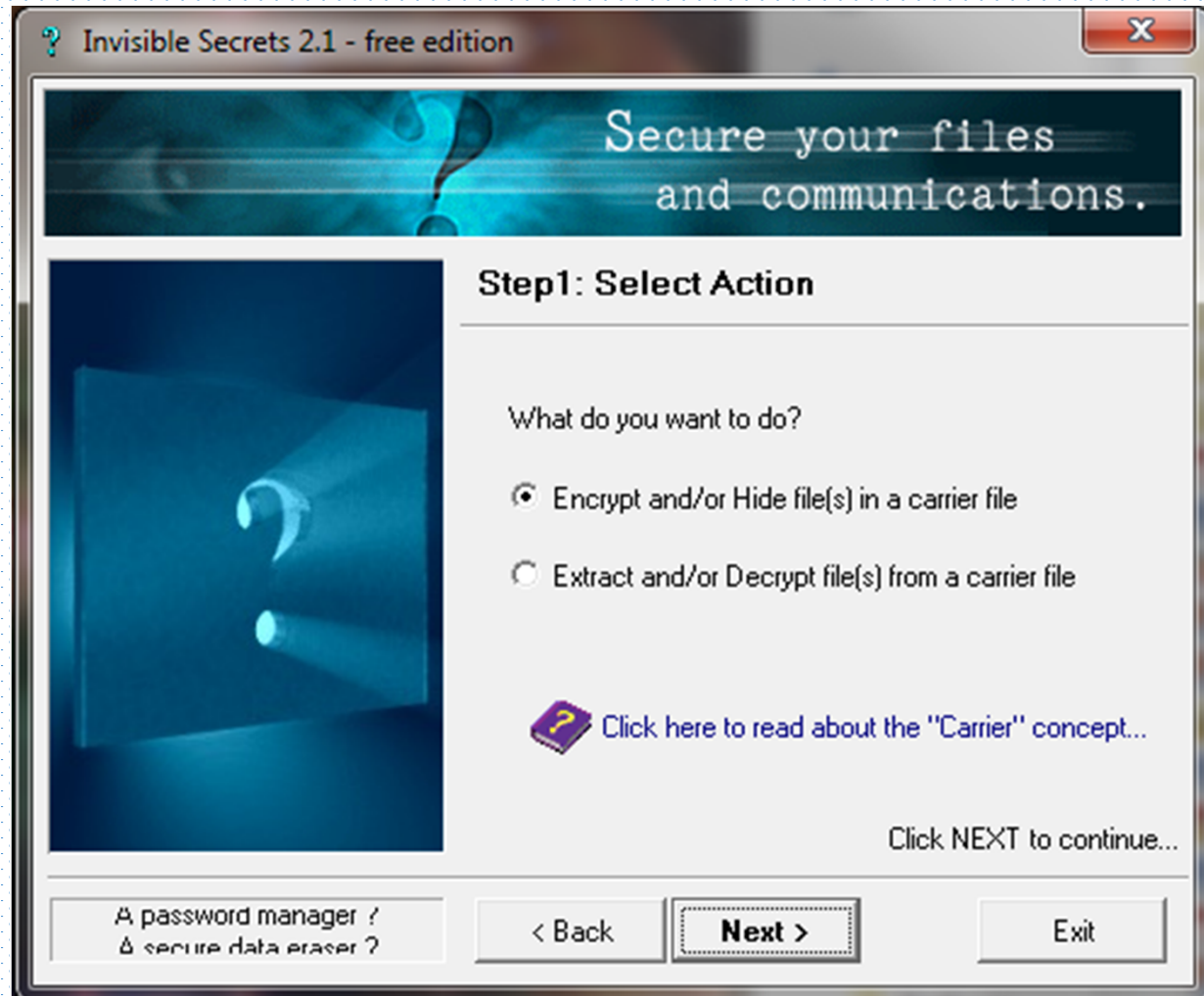| Steganophony	• Hiding messages in sound files
Video steganography	• Hiding information in video files • Combination of image and audio

Audio steganography

- LSB coding
  - LSB are modified after analog voice signal is converted to digital voice signal.

- Echo Hiding
  - Hide information by adding an echo to the audio signal
  - Intensity of echo is kept below the threshold of human auditory system
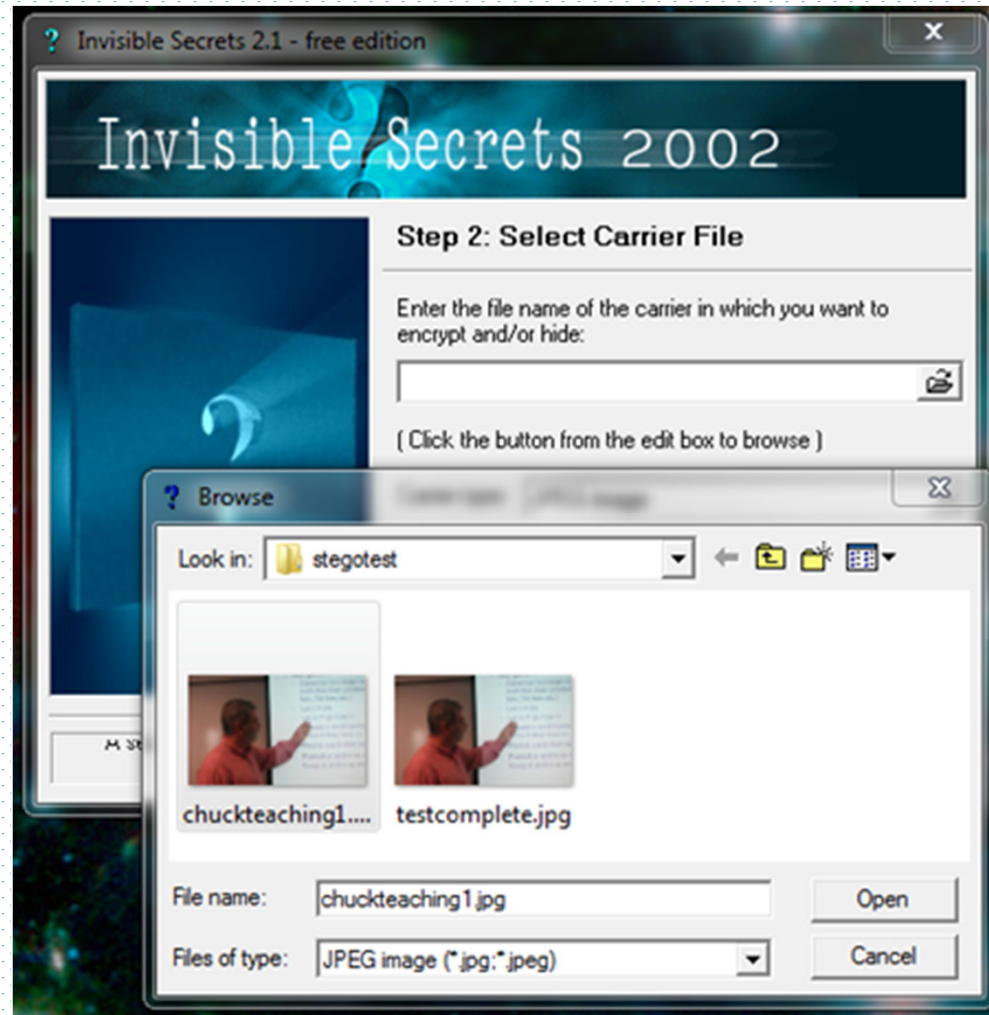
Steganalysis

- The process of analyzing a file or files for hidden content

- Can show a likelihood that a given file has additional information hidden in it

- Common method for detecting LSB steganography is to examine close-color pairs (created by LSB embedding)
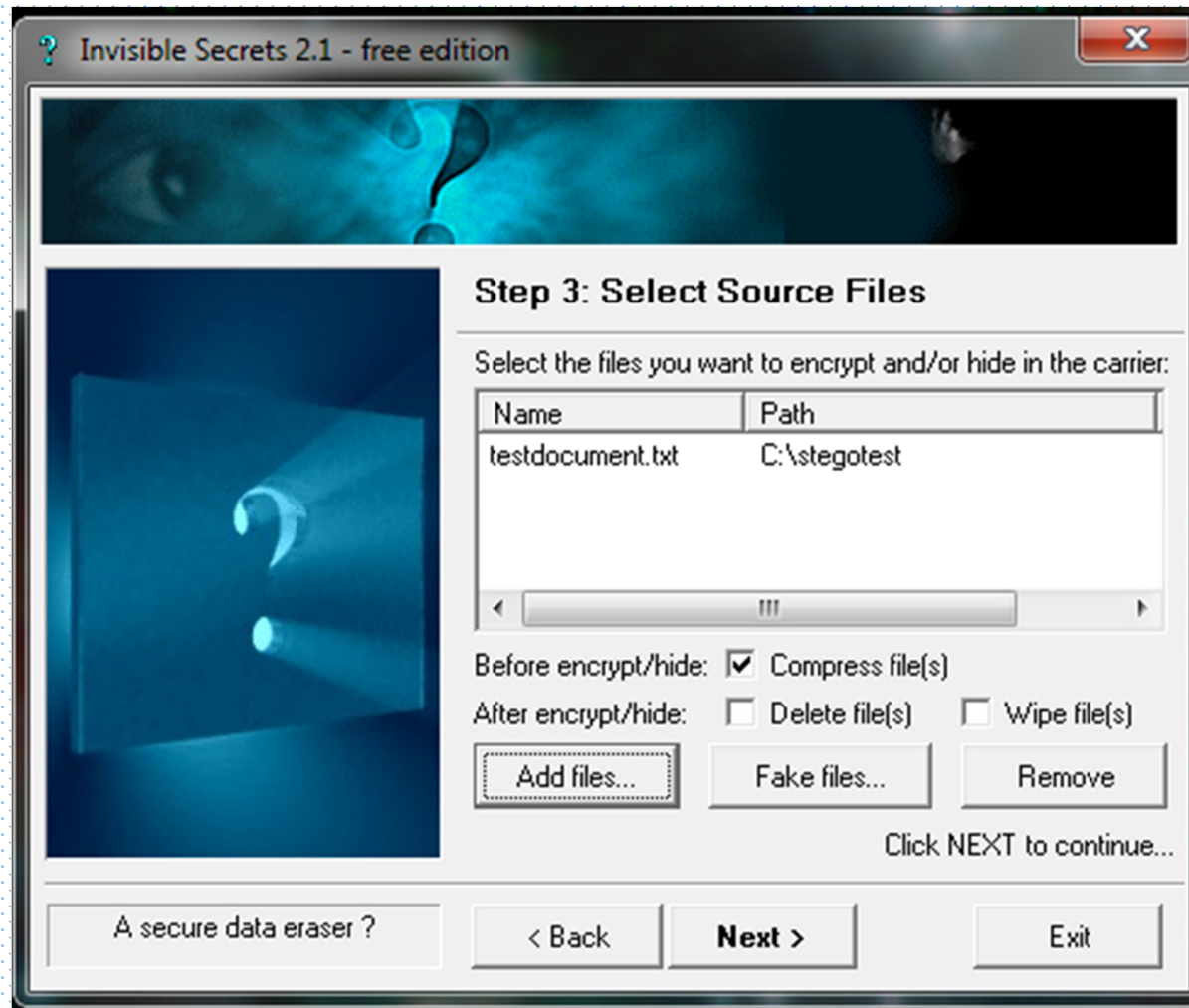
- S-Tools, Invisible Secrets

Invisible Secrets

Invisible Secrets

Invisible Secrets

Invisible Secrets

Invisible Secrets

Thank You