Computer Security

CS 727/827, 2020 Spring

Dongpeng Xu

Week 7

Information Hiding

- Digital Watermarks
  - Example: Add “invisible” info to data
  - Defense against music/software piracy
- Steganography
  - “Secret” communication channel
  - Similar to a covert channel
- Example: Hide data in an image file

Steganography

- According to Herodotus (Greece 440 BC)
  - Shaved slave’s head
  - Wrote message on head
  - Let hair grow back
  - Send slave to deliver message
  - Shave slave’s head to expose a message warning of Persian invasion
- Historically, steganography used by military more often than cryptography

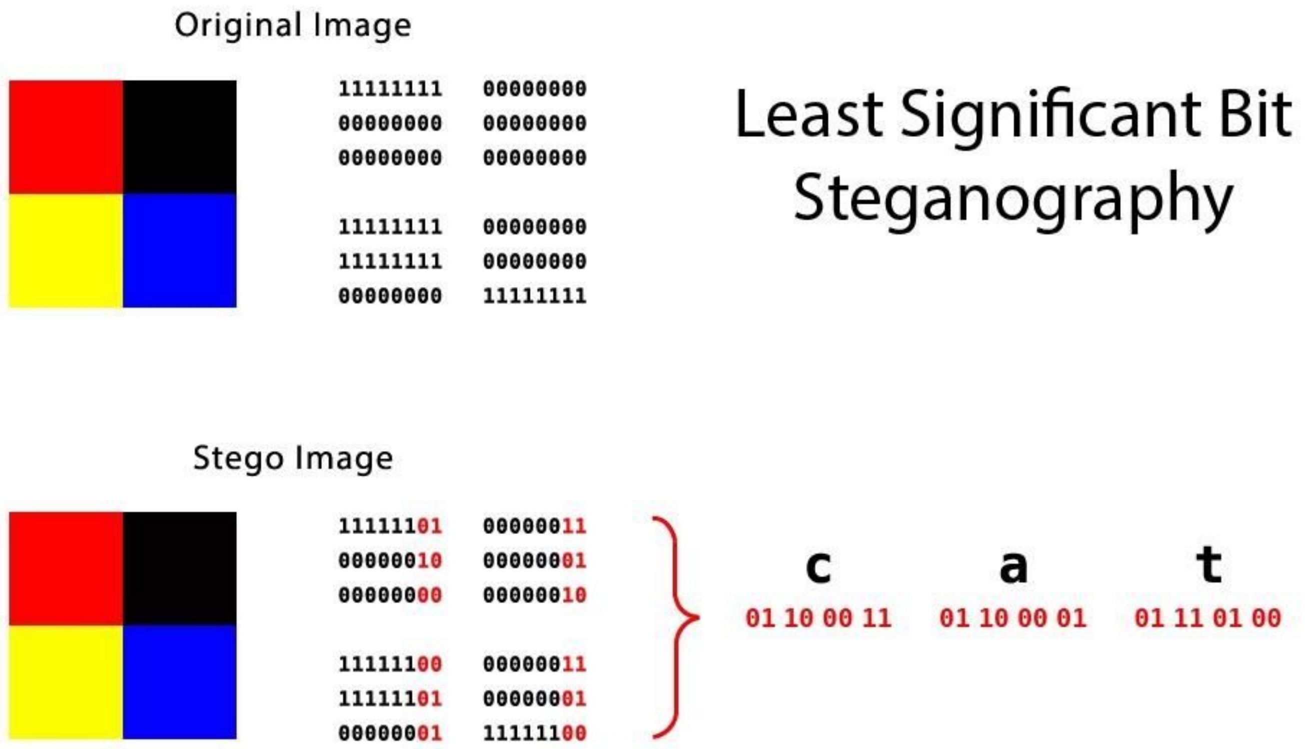
Images and Steganography

- Images use 24 bits for color: **RGB**
  - 8 bits for **red**, 8 for **green**, 8 for **blue**
- For example
  - **0x7E 0x52 0x90** is **this color**
  - **0xFE 0x52 0x90** is **this color**
- While
  - **0xAB 0x33 0xF0** is **this color**
  - **0xAB 0x33 0xF1** is **this color**
- Low-order bits don’t matter…

Images and Steganography

- Given an uncompressed image file…
  - For example, BMP format
- …we can insert information into low-order RGB bits
- Since low-order RGB bits don’t matter, changes will be “invisible” to human eye
  - But, computer program can “see” the bits

Images and Steganography



Original Image

```
11111111   00000000
00000000   00000000
00000000   00000000

11111111   00000000
11111111   00000000
00000000   11111111
```

Least Significant Bit Steganography

Stego Image

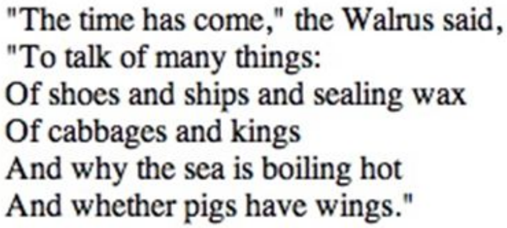
```
11111101   00000011
00000010   00000001
00000000   00000010

11111100   00000011
11111101   00000001
00000001   11111100
```

```
     c              a              t
01 10 00 11    01 10 00 01    01 11 01 00
```

HTML Steganography

- Walrus.html in web browser



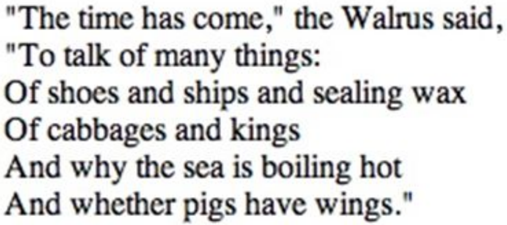
"The time has come," the Walrus said,
"To talk of many things:
Of shoes and ships and sealing wax
Of cabbages and kings
And why the sea is boiling hot
And whether pigs have wings."

- Walrus.html in “View Source”

```
<font color=#000000>"The time has come," the Walrus said,</font><br>
<font color=#000000>"To talk of many things: </font><br>
<font color=#000000>Of shoes and ships and sealing wax </font><br>
<font color=#000000>Of cabbages and kings </font><br>
<font color=#000000>And why the sea is boiling hot </font><br>
<font color=#000000>And whether pigs have wings." </font><br>
```

HTML Steganography

- stegoWalrus.html in web browser



"The time has come," the Walrus said,
"To talk of many things:
Of shoes and ships and sealing wax
Of cabbages and kings
And why the sea is boiling hot
And whether pigs have wings."

- stegoWalrus.html in “View Source”

```
<font color=#000101>"The time has come," the Walrus said,</font><br>
<font color=#000100>"To talk of many things: </font><br>
<font color=#010000>Of shoes and ships and sealing wax </font><br>
<font color=#010000>Of cabbages and kings </font><br>
<font color=#000000>And why the sea is boiling hot </font><br>
<font color=#010001>And whether pigs have wings." </font><br>
```

- “Hidden” message: 011 010 100 100 000 101

Steganography

- Some formats (e.g., image files) are more difficult than html for humans to read
  - But easy for computer programs to read…
- Easy to hide info in **unimportant bits**
- Easy to damage info in unimportant bits
- To be robust, must use important bits
  - But stored info must not damage data
  - Collusion attacks are also a concern
- Robust steganography is tricky!

Information Hiding

- Not-so-easy to hide digital information
    - “Obvious” approach is not robust
    - **Stirmark**: tool to make most watermarks in images unreadable without damaging the image
    - Stego/watermarking are active research topics
- If information hiding is suspected
    - Attacker may be able to make information/watermark unreadable
    - Attacker may be able to read the information, given the original document (image, audio, etc.)

Lab 1

- Download `alice.bmp`
- Hide your name inside `alice.bmp`
- Generate hash digest using SHA-256
- Create a RSA public and private key pairs (2048 bit)
- Generate a SHA-256 digest signed by the private key
- Implement TEA and encrypt `alice-new.bmp`
- (BONUS) Implement CBC mode TEA

Questions?

dongpeng.xu@unh.edu