Approach 1 - EzStego

- Use cover image with similar colors
- Experts recommend gray-scale images
- Arrange palette so adjacent colors are similar

Approach 2 – S-Tools

- Use only x bits for unique color information.
- 8 – x bits are for secret message
- Example (x = 7):
- Can only have 128 unique colors
- For each unique color, there’re two similar colors xxxx xxx0 & xxxx xxx1

LSB – Analysis – The Good

- Simple to implement
- Allows for large payload
- Max. payload = b * p where;
- b = number of bytes per pixel
- p = number of pixels of cover image

LSB – Analysis – The Bad

- Easy for attacker to figure out message if he knows the mes sage is there
- But the images look the same, so can't tell it's a stego-imag e… right?
- Human vision can't tell but vulnerable to statistical analysis

LSB – Analysis – The Ugly

- It’s even easier if the attacker just wants to corrupt the mes sage.
- Just randomize the lsbs himself
- Even vulnerable to unintentional corruption: image croppin g, conversion to jpeg and back, etc.
- Integrity is extremely frail

LSB – Analysis – The Conclusion

- Good for cases where only low security is desired, but not n ecessary.
- Added security when coupled with cryptography
- Foundation for many variations, which are more secure e.g. not vulnerable to statistical analysis attacks.

Audio Steganography

- It is a technique used to transmit hidden information by modifying an audio signal in an imperceptible manner.
- It is the science of hiding some secret text or audio information in a host message.
- The host message before steganography and stego message after steganography have the same characteristics.

Audio Steganography- CONT.

- Advantages:
  - No one suspects existence of message
  - Highly secure
- Disadvantages:
  - It requires a lot of overhead to hide a relatively few bits of information

WILL BE CONTINUE IN THIS SUBJECT IN NEXT LECTURE, INSHALLAH.

Steganography V.s Cryptography

Steganography	Cryptography
Unknown message passing	Known message passing
Steganography prevents discovery of the very existence of communication	Encryption prevents an unauthorized party from discovering the contents of a communication
Little known technology	Common technology
Technology still being develop for certain formats	Most of algorithm known by all
Once detected message is known	Strong current algorithm are resistant to attacks ,larger expensive computing power is required for cracking
Steganography does not alter the structure of the secret message	Cryptography alter the structure of the secret message


Q&A