Image Steganography

Student: Kewen Meng
Advisor: Jun Li

University of Oregon
Any obvious visual difference?
What is steganography

- **Concealing** important data within the carrier medium (video, audio, image, etc.)

- It is to *prevent* others from *thinking* there is secret data hidden in the carrier
Project Goals

• Store more information
• Reuse the image (support multi-user)
• More secure
Design

Let's start from image
Design

Assign different layers to different users

- Support multiple users (up to 3)
- Avoid conflicts
- Reuse image
Design

Minimize the changes

pick one pixel

e.g. 150

0b10010110

Least Significant Bit
Design

• Every input character will be coded as 12 bits

• Layer available indicator 30 bits
  101100111100011111000011111100000

• Length of input will be coded as 20 bits embedded into image as well
Design

More secure

- Input message will be encrypted by RSA
- RSA Keys given by user (doesn’t store any key)
- Length of the input will also be encrypted
Design

Message Embedding

- Start
- parameter empty?
  - Yes → Notify user
  - No → Layer available?
    - Yes → Length over image size?
      - Yes → Encrypt input
        - Embed to image
        - End
      - No → Layer available?
        - No → End
    - No → Notify user

Message Extraction

- Start
- parameter empty?
  - Yes → Notify user
  - No → Layer unused?
    - Yes → Extract & Decryption
      - Key correct?
        - Yes → Output
        - No → Notify user
    - No → Notify user
In this project, I will focus my research on image steganography, which is used to hide important data in the carrier medium to avoid detection from attackers while exchanging messages. Unlike encryption, steganography is not designed to keep others from knowing the hidden data, instead it is to prevent others from thinking there is secret data hidden in the carrier medium. That is to say, the goal of steganography is to store private data in images and at the same time bring minimum changes to the carrier medium itself in order to lower the possibility of being suspected. It is an important technology for message exchange, and really interesting to me.

The existing steganography method can be categorized into two directions: spatial domain and frequency domain. For spatial domain methods, people directly manipulate the value of pixels to hide additional data. For example, we can hide secret messages into the least significant bits (LSB) of a pixel which is usually the last bit of the pixel. Because the changes of least significant bits would bring small impact on the entire image. It is difficult for people to tell the difference visually. In frequency domain based steganography methods, researchers decomposed carrier image by DCT (Discrete Cosine Transform) into several blocks and then insert secret data into the coefficients' insignificant bits (based on LSB). The frequency domain methods are very effective for carriers like compressed audio or compressed image such as JPEG format. Due to the compression algorithm, minor changes to the carrier will cause obvious impact on carriers, being easy to detect. Researchers also introduced FFT (Fast Fourier Transform) and DWT (Discrete Wavelet Transform) into frequency domain methods to achieve better performance.

Since our application will allow one user or multiple users to hide information, therefore one problem need to be considered is how to avoid conflicts and guarantee that the information is retrievable. For instance, user B's hidden message cannot overwrite that of previous user A. One approach came to me is that we could take the advantage of structure of color image to solve this problem. In color image, one pixel can be represented in various ways. Two common representations are HSL (hue-saturation-lightness) and HSV (hue-saturation-value) which provides us three layers to store data separately. Therefore, our application will support up to three users to hide data into the same image and guarantee no conflicts among users. Regardless of multiple users, single user could hide up to three different encrypted messages into the same image. Furthermore, before hiding data into image, our application will encrypt the message in the first place to improve information security. Even if the messages are exposed, attackers still have to decrypt to obtain plaintext.

Reference

[1] Boneh D. Twenty years of attacks on the RSA cryptosystem[J]. Notices of the AMS, 1999, 46(2): 203-213.
[2] Provos N, Honeyman P. Hide and seek: An introduction to steganography[J]. Security and Privacy, IEEE, 2003, 1(3): 32-44.
[3] Wu H C, Wu N I, Tsai C S, et al. An Image Steganographic Scheme Based on Pixel-Value Differencing and LSB Replacement Methods[J]. 2004.
[4] Artz D. Digital steganography: hiding data within data[J]. internet computing, IEEE, 2001, 5(3): 75-80.
[5] Chandramouli R, Memon N. Analysis of LSB based image steganography techniques[C]. Image Processing, 2001. Proceedings. 2001 International Conference on. IEEE, 2001, 3: 1019-1022.
[6] Fridrich J, Goljan M, Du R. Reliable detection of LSB steganography in color and grayscale images[C]/ Proceedings of the 2001 workshop on Multimedia and security: new challenges. ACM, 2001: 27-30.
[7] Zhang T, Ping X. Reliable detection of LSB steganography based on the difference image histogram[C] Acoustics, Speech, and Signal Processing, 2003. Proceedings.(ICASSP’03). 2003 IEEE International Conference on. IEEE, 2003, 3: III-545-8 vol. 3.
Thank you!