Information Coding 2013/14

Work2 – Steganography

Goal

As you know Steganography is the science of writing hidden messages in such a way that no one apart from the sender and intended recipient even realizes there is a hidden message. In digital steganography, electronic communications may include steganography coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganography transmission because of their large size. For example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it [1].

The main goal of this work is the implementation a program that enables hiding a secret message (text file) in an image file and also recovers the hidden data.

Implementation

Implement a program that based on the selected option (h or u), performs the operation of hide or recover a secret message. The secret message is a text file and the cover is an image file.

- In case of option hiding (h)

  ```
  ➢ stego h <secret_msg_file> <image_file> <new_image_file>
  ```

  The secret message file (<secret_msg_file>) will be hidden in the image file and a new image file will be generated with the specified name (<new_image_file>). The new file will also be a ppm image file format.

- In case of option hiding (u)

  ```
  ➢ stego u <image_file> <recovered_secret_msg_file>
  ```

  Obviously, the recovered message file (<recovered_msg_file>) must be exactly equal to the original secret message file.

Consider that your program only work with ppm images format (portable pixmap file format). See lab class 4 for details concerning the ppm file format. The secret file is a text file (use juliuscaeser.txt) and use as cover image file the taz.ppm file and the duende.ppm file.

[1] http://en.wikipedia.org/wiki/Steganography

Information Coding 2013/14

Work2 – Steganography

The most common and popular method of modern day steganography is to make use of the LSB of a picture's pixel information. Thus the overall image distortion is kept to a minimum while the message is spaced out over the pixels in the images (this technique works best when the image file is larger then the message file).

Your program (stego) should work by changing the value of some pixels in the original image, where some bits of the image pixels are selected to "hide" the secret message file. Note that the changes in the values of the pixels should not cause any visible changes in the initial image, so you must carefully chose which pixels and bits to select. In class 11 a very simple "hiding" pattern was presented, however in this work is intended that you propose and implement a concealment scheme that best fits the provided files.

As an improvement of your work you may choose to "encode" your secret data in order to compress the secret file and obtain a "better" result.

To be delivered

1. Your code file, properly commented.
2. A brief report:
   - Explaining and justifying the assumptions you made and why you chose that concealment scheme.
   - Explaining and justifying most relevant code options.

The code file(s) and report should be sent by email to cpm@fct.unl.pt until 16 of December. Discussion of works will take place on December 17.

Do not forget to put in the email subject **CI - delivery work2**, and indicate in the email your **names** and **numbers**.