Dr. R. Beezer
Practicum #1
Steganography

Math 133
Fall 2003

Steganography is the practice of hiding a message within another one. Here we will hide a text message in an image. This exercise will get you started with command-line tools, electronic mail, passwords and a specialized steganography tool. Links are available on the course page.

Procedure

1. If you do not have it already, pick up and install the evaluation version of the WinZip program for compressing and decompressing files, it is available at `www.winzip.com`. This tool will be necessary for the next step, and could be useful later in the semester.

2. Pick up the Windows versions of the JPEG Hide/Seek programs from Allan Latham at `linux01.gwdg.de/~alatham/stego.html`.

3. Use WinZip to extract the files from `jphs_05.zip` into a directory like `c:\jphs`. Use a command like `c:\> mkdir jphs` at a "Command Prompt" to make a directory. You will need to unzip an inner file of the archive — we will explain later about the included signature file.

4. Grab an image in JPEG format off the Internet, these usually end with the suffix `.jpg`. An easy place to go is Google (`www.google.com`) and click on the Images tab. Save the image into `c:\jphs`, perhaps by left-clicking on it to initiate the saving procedure. We'll assume here that this file is called `goldengate.jpg`.

5. Create a small text file with a message in it, using a program like Notepad, available at `Start>Programs>Accessories`. Do not use Word or your file may end up being too huge. Write just a sentence or two, then save the file as `message.txt`.

6. Run `jphide.exe` within `c:\jphs` as follows:

   ```
   jphide  goldengate.jpg  goldengatehide.jpg  message.txt
   ```

   and supply the class passphrase when prompted. This will create the new JPEG image `goldengatehide.jpg` which will contain the image and the contents of the message file, encrypted.

7. View both JPEG files with a viewer (MS Photo Editor, your browser, email,. . .) and see if you can discern any differences in the image.

8. To test all of the above, run `jpseek.exe` within `c:\jphs` as follows:

   ```
   jpseek  goldengatehide.jpg  messageout.txt
   ```

supplying the same password as above (but just once). This should create a new file called `messageout.txt` with your original message in it. Open `messageout.txt` in Notepad (or use the `type` command at a prompt) to see if your original message survived. If it did, you are essentially done, see the steps below for how to turn in your work.

Grading

1. Send an email message to everyone in your discussion group, containing the image with the message (`goldengatehide.jpg` in this example), and be sure to also include me on the message.

2. Decode the messages you receive from others in your group. Send me an email with just text, containing your message, AND the messages you received from the others in your group.

3. If you successfully decode other's messages, and they are able to decode yours, you will earn a Pass on this practicum.

Notes

1. The message file should not be too large relative to the size of the image,and since some JPEG's are very compressed, you need to be careful about this.

2. It would be interesting to try hiding very big files and watch the image quality degrade, but these programs prevent that. There is a link to a "Stego Bit Twiddler" that demonstrates what happens when you try to pack too much information into an image.

3. Any file could be hidden this way, it even could be another image.

4. For a larger message file, it could be compressed with WinZip first, making it smaller and further disguising its use.

5. You should destroy the original image file after use, since if the secret police obtain it then also it might tip them off to your use of steganography. For this reason, you really should not use publicly available images, but should instead use travel photos from your own digital camera.