13.1.1

STEGANOGRAPHY

(Hide)

Laboratory Overview

Objective

At the end of this lab students will be able to hide and retrieve data in .bmp bitmap image file using a Steganography program written for the Windows Win32 platform.

Information for Laboratory

Students will utilize Hide in picture v2.1 to hide and retrieve data in a bitmap graphic file

Student Preparation

The student will have completed requisite reading. The student will require paper for notes and should be prepared to discuss the exercises upon completion.

Student computers should have Windows XP, have a .jpg viewer (Windows picture and fax viewer), and access to windows notepad.

Hide in picture v2.1 is available at http://www16.brinkster.com/davitf/hip/

Estimated Completion Time

60 Minutes

Steganography

Steganography is the Art of Hidden Writing. The word *steganography* literally means *covered writing* as derived from Greek. It includes a vast array of methods of secret communications that conceal the very existence of the message. Throughout history, a multitude of methods and variations have been used to hide information. Today, with computers everywhere, and access to a global network like the Internet, these methods have gone digital. Steganography has been used since ancient Greece, extensively during World War 2, and still exists today.

On Feb. 5, 2001, USA Today reported that the United States FBI had proof the Osama bin Laden and his associates were hiding maps, photographs of terrorist targets, and instructions for terrorist activities in web pages on the Internet using Steganography techniques.

An example of Steganography

The following message was sent by a German Spy in WWII:

Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by products, ejecting suets and vegetable oils.

Taking the second letter in each word the following message emerges:

Pershing sails from NY June 1.

Steganography Software

There are several different programs, both commercial and shareware/freeware that incorporate the many different Steganography techniques on the market today. Some of which are written for Unix/Linux and or the Windows platform. Hide in picture v2.1, is a freeware windows based program that is simple to use, works well, and easily shows how steganography cab be used. Hide in picture v2.1 is capable is hiding plain text files, or even executable files inside images.

How it works - Bitmaps

A bitmap picture is simply a series of numbers representing color intensities, one color for each pixel (point) of the picture. Hide in picture hides a file inside a picture by placing its bits in the least-significant bits of each color in the picture. The lest significant bits, or LSB, being the rightmost bit of the byte. The lowest binary value of 0 or 1, therefore it is the least significant bit.

Suppose you have a picture containing the following bytes:

200 53 2 195 54 69 191 56

The binary values of these numbers are:

11001000 00110101 00000010 11000011 00110110 01000101 10111111 00111000

To hide the character 109 (in binary 01101101), the least-significant bit of each byte would be replaced by a bit of the character. The result would be:

11001000 00110101 00000011 11000010 00110111 01000101 10111110 00111001

Which corresponds to:

200 53 3 194 55 69 190 57

The difference between the new values and the old ones is very small, so it is difficult, if not impossible, for the human eye to identify any difference from the original picture. If the hidden file is large, it may be necessary to modify more than a single bit from each byte of the picture, which can make this difference more visible.

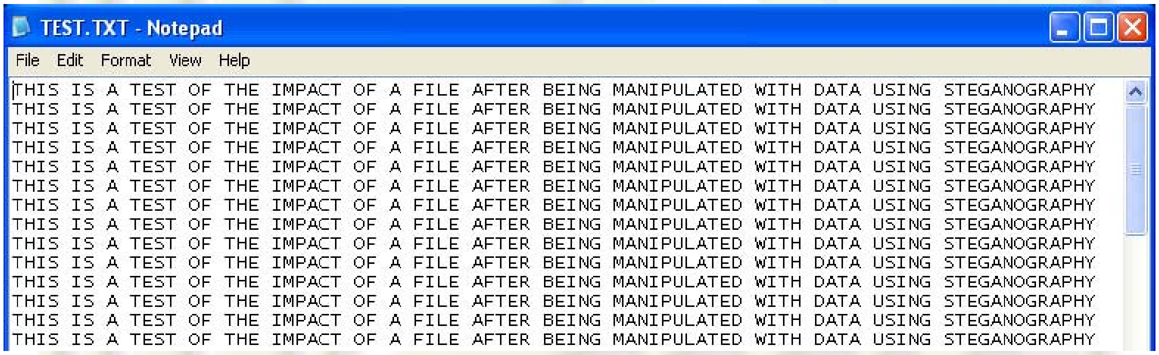
Step I: Verify data files

Open the test graphic file, stegan-org.bmp with your image viewer, and make sure it looks like this.

Steganography
Steganography
The art of hiding

Step 2: Verify data files

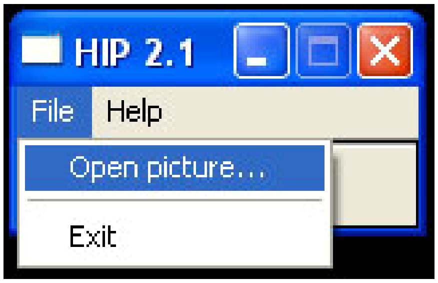
Open test.txt and verify the data before we start. This is the text file that we will be hiding and retrieving from our image file. Your file should look like just like this.



```
THIS IS A TEST OF THE IMPACT OF A FILE AFTER BEING MANIPULATED WITH DATA USING STEGANOGRAPHY
THIS IS A TEST OF THE IMPACT OF A FILE AFTER BEING MANIPULATED WITH DATA USING STEGANOGRAPHY
THIS IS A TEST OF THE IMPACT OF A FILE AFTER BEING MANIPULATED WITH DATA USING STEGANOGRAPHY
THIS IS A TEST OF THE IMPACT OF A FILE AFTER BEING MANIPULATED WITH DATA USING STEGANOGRAPHY
THIS IS A TEST OF THE IMPACT OF A FILE AFTER BEING MANIPULATED WITH DATA USING STEGANOGRAPHY
THIS IS A TEST OF THE IMPACT OF A FILE AFTER BEING MANIPULATED WITH DATA USING STEGANOGRAPHY
THIS IS A TEST OF THE IMPACT OF A FILE AFTER BEING MANIPULATED WITH DATA USING STEGANOGRAPHY
THIS IS A TEST OF THE IMPACT OF A FILE AFTER BEING MANIPULATED WITH DATA USING STEGANOGRAPHY
THIS IS A TEST OF THE IMPACT OF A FILE AFTER BEING MANIPULATED WITH DATA USING STEGANOGRAPHY
THIS IS A TEST OF THE IMPACT OF A FILE AFTER BEING MANIPULATED WITH DATA USING STEGANOGRAPHY
THIS IS A TEST OF THE IMPACT OF A FILE AFTER BEING MANIPULATED WITH DATA USING STEGANOGRAPHY
THIS IS A TEST OF THE IMPACT OF A FILE AFTER BEING MANIPULATED WITH DATA USING STEGANOGRAPHY
THIS IS A TEST OF THE IMPACT OF A FILE AFTER BEING MANIPULATED WITH DATA USING STEGANOGRAPHY
THIS IS A TEST OF THE IMPACT OF A FILE AFTER BEING MANIPULATED WITH DATA USING STEGANOGRAPHY
```

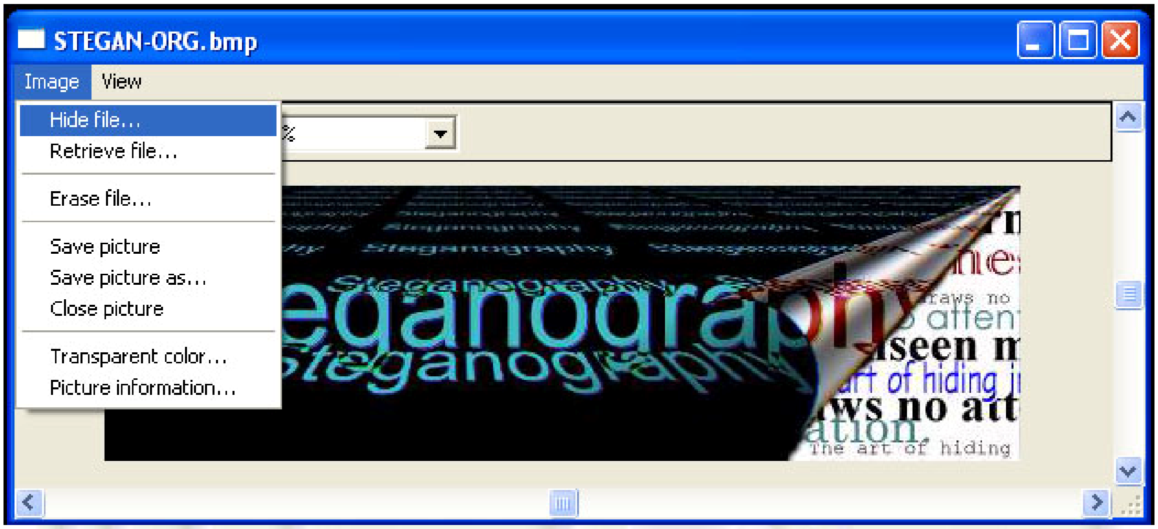
Step 3: Open Hide in Picture 2.1

Open the program Hide in Picture. Click File, then click Open picture, and select the graphic to open, stegan-org.bmp



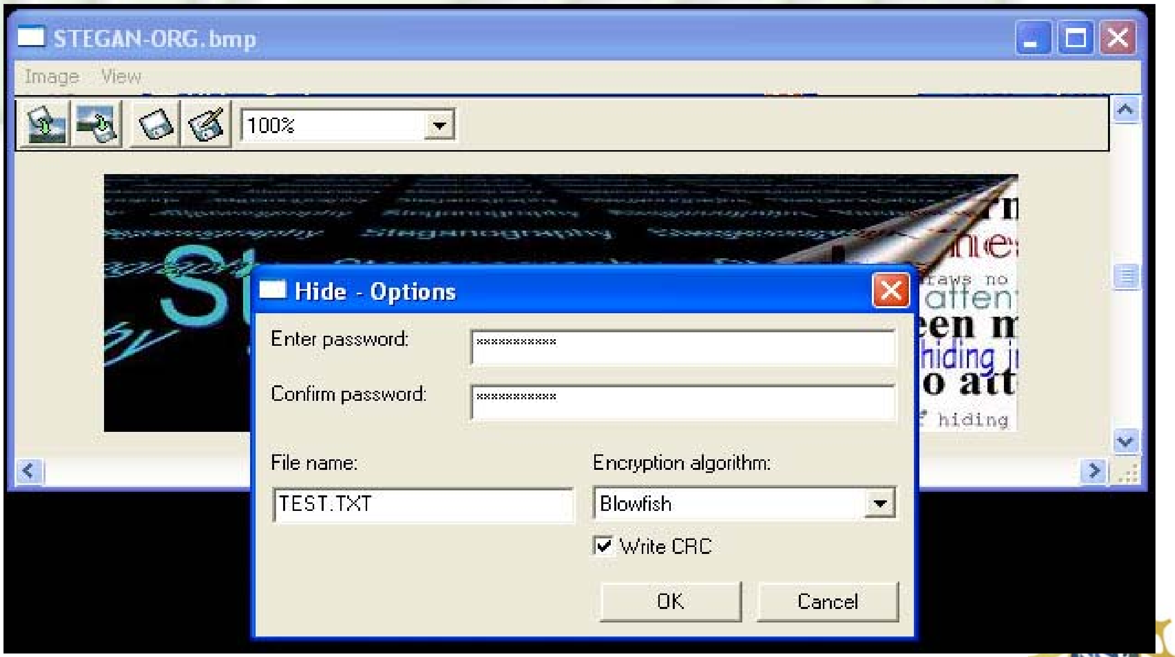
Step 4: Hiding the data text file

Once the picture is opened, Click Image, then click Hide file, and select the test.txt data file to hide.



Step 5: Hide – Options

After selecting your file, Hide in picture prompts you for a password, and Encryption algorithm. Enter and confirm your password, and select Blowfish Encryption, and then click OK.



Enter password: ************

Confirm password: ************

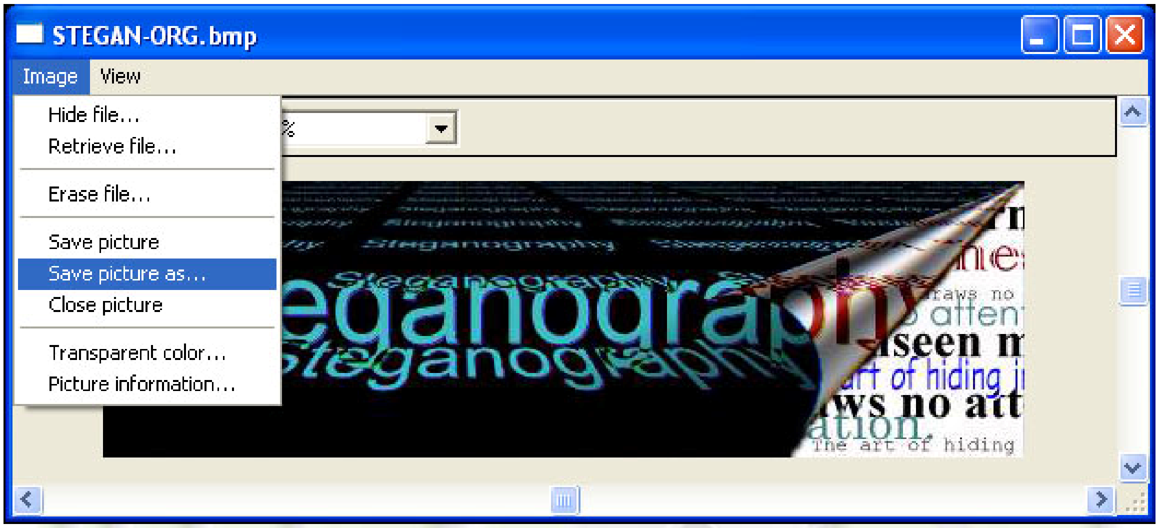
File name: TEST.TXT

Encryption algorithm: Blowfish

☑ Write CRC

Step 6: Save the new image file with the hidden data

Click Image, Save picture as, and save the picture with a different file name, stegan-hidden.bmp. Once the new image stegan-hidden.bmp is saved, close the program Hide in picture. You now have two different image files, the original graphic, and the modified graphic with the hidden text file in it.

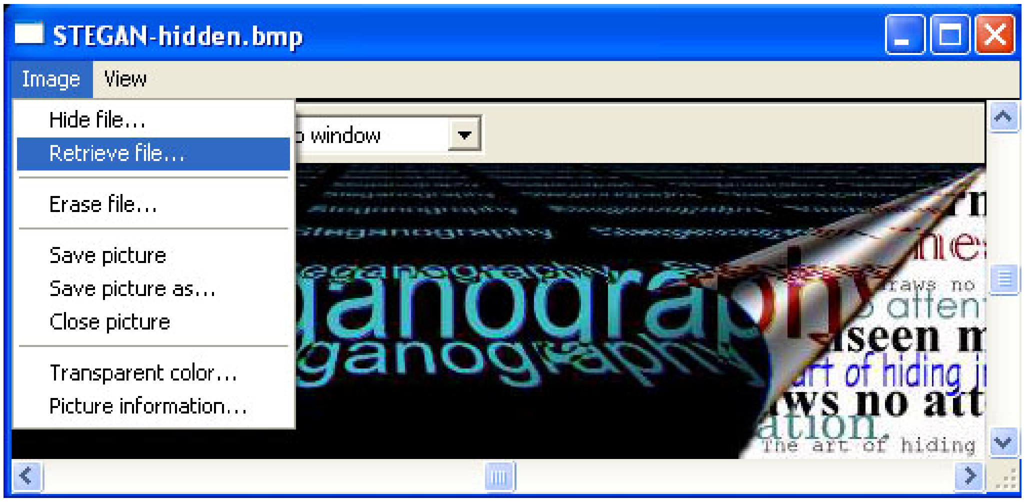


Step 7: Verify data and Image quality

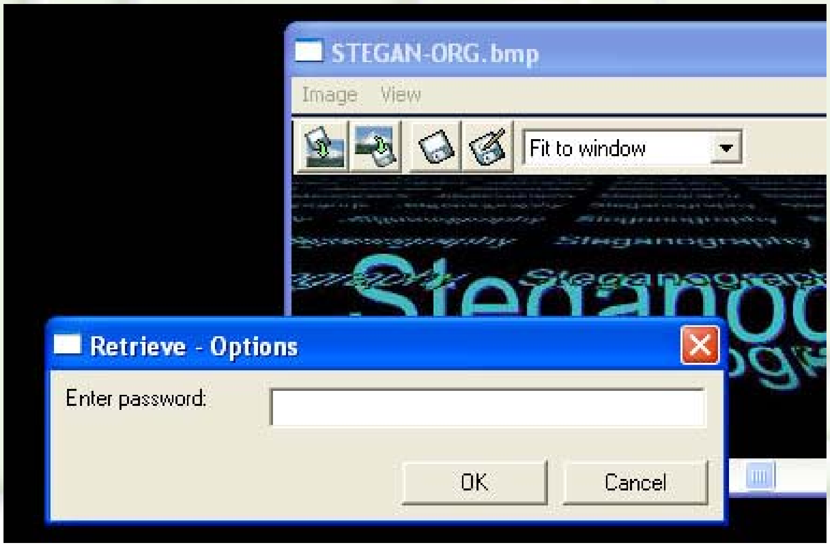
Open both the graphic files stegan-org.bmp, and stegan-hidden.bmp. Do both files open ok? Do you see any difference in image quality?

Step 8: Retrieving the hidden data

Open Hide in picture, Click File, then click Open picture, and open the image stegan-hidden.bmp. Once the file is open, Click Image, then click Retrieve file.



You will be prompted for your password in order to retrieve the data file, enter it the password box.



Enter password:

Step 9: Saving the hidden data

After entering your password, you will be prompted for a file name to save your data file. Name the file test-retrieved.txt and click save.

Step 10: Verify the hidden data.

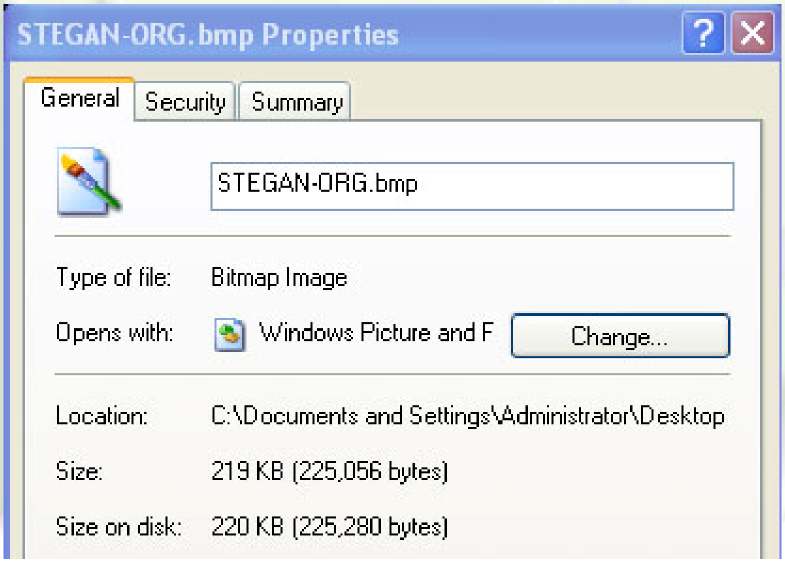
Locate both the test.txt and the test-retrieved.txt data files. Open both data files in notepad, and compare. Are the contents of both files the same?

Step 11: Analysis - Advanced verification of all data.

Locate all 4 files used.

stegan-org.bmp
stengan-hidden.bmp
test.txt
test-retrieved.txt.

Right click, and go to properties of each file.



STEGAN-ORG.bmp Properties

STEGAN-ORG.bmp

Type of file: Bitmap Image

Opens with: Windows Picture and F

Location: C:\Documents and Settings\Administrator\Desktop

Size: 219 KB (225,056 bytes)

Size on disk: 220 KB (225,280 bytes)

Compare the file sizes of stegan-org.bmp the original image file to stegan-hidden.bmp the image file with the hidden data. Is there a difference in file size?

Compare the file sizes of the two text data files, test.txt and test-retrieved.txt. Is there a difference in the file size?

STEP 12: Hiding an executable file

Repeat steps 4 - 11 again, but this time use the given file pathping.exe to hide, instead of the previously used text file test.txt.

After hiding and then retrieving the executable file from the image file, try to execute the retrieved file pathping.exe. Did the program launch successfully?

Summary Discussion

This lab proves that steganography uses the least significant bits of an image and replaces them with hidden data.

Since the original text file hidden was 50KB, and it was hidden inside a 219K image file, the image file should have grown by 50K. But since we removed the LSB's and replaced them with our hidden data, we were able to hide 50K of data inside the image file without affecting the file size.

Want To Learn More about Steganography

http://www.jjtc.com/stegdoc/steg1995.html

http://www.stegoarchive.com/

Appendix:

This lab was developed using Hide in Picture Version 2.1, which can be obtained from:

www16.brinkster.com/davitf/hip/

(As of this writing, neotrace was a product of Neoworx, Inc., which was owned by McAfee Systems).

The OS environment for this lab was Windows XP Professional, Version 2002, Service Pack 2 (8/04).