PROPOSED IDEA FOR STEGANOGRAPHY ASSIGNMENT

By Farhan Khan

Student ID: g260214

Title of the Proposed Idea:

"Message Concealment Techniques using Image based Steganography"

Proposed Idea:

There are two techniques for message concealment using image based steganography which I want to propose and implement in this assignment:

Use of punctuation marks for message concealment in images:

The idea behind this technique is to utilize the presence of punctuation marks like , ; : " etc. in the text for encoding a secret message. The secret message to be communicated will be hidden in any piece of text through binary encoding of punctuation marks. Two punctuation marks can be used to represent binary data or several punctuation marks can be used to represent binary combinations. The encoded message can then be embedded in an image file (BMP, GIF or grayscale) using any of the popular methods like LSB insertion etc. [1] An additional layer of secrecy can be added by first encrypting the message and then encoding it through the use of punctuation marks before embedding in the cover image file.

Example: Consider the following lines from William Shakespear's renowned tragic play "Hamlet" uttered by the hero of the play Hamlet.

To be, or not to be; that is the question,
Whether 'tis nobler in the mind to suffer;
The slings and arrows of outrageous fortune,
Or to take arms against a sea of troubles,
And by opposing end them? To die, to sleep,
No more, and by a sleep to say we end;
The heart-ache and the thousand natural shocks,
That flesh is heir to, 'tis a consummation,
Devoutly to be wish'd; To die, to sleep;
To sleep, perchance to dream; ay, there's the rub;
For in that sleep of death what dreams may come,
When we have shuffled off this mortal coil,
Must give us pause: there's the respect
That makes calamity of so long life;
For who would bear the whips and scorns of time,
The oppressor's wrong, the proud man's contumely,
The pangs of despised love, the law's delay,
The insolence of office and the spurns
That patient merit of the unworthy takes,
When he himself might his quietus make

With a bare bodkin? who would fardels bear,
To grunt and sweat under a weary life,
But that the dread of something after death,
The undiscover'd country from whose bourn
No traveller returns, puzzles the will
And makes us rather bear those ills we have
Than fly to others that we know not of?
Thus conscience does make cowards of us all;
And thus the native hue of resolution
Is sicklied o'er with the pale cast of thought,
And enterprises of great pith and moment
With this regard their currents turn awry,
And lose the name of action. - Soft you now!
The fair Ophelia! Nymph, in thy orisons
Be all my sins remember'd.

There are a number of punctuation marks in the above lines which can be used to encode a secret message easily. The modified text can then be embedded in an image file. Only the recipient who knows how to interpret the punctuations marks can retrieve the secret message.

Use of Modified Scytale Cipher for message concealment in images:

In cryptography, a scytale (rhymes with Italy, and also transliterated as skytale, in Greek, a baton) is a tool used to perform a transposition cipher, consisting of a cylinder with a strip of leather wound around it on which is written a message. The ancient Greeks and the Spartans in particular, are said to have used this cipher to communicate during military campaigns. The recipient uses a rod of the same diameter on which he wraps the paper to read the message. It has the advantage of being fast and not prone to mistakes, a necessary property when on the battlefield. [3]

Although Scytale cipher is easily broken, it can be used in combination with image steganography to perform message concealment. The idea is to arrange a message on a rectangular grid of some size e.g., 4x16 as shown in the following figure. The remaining cells of the grid can be filled with arbitrary letters or numbers and the row number and column number of the secret message is noted.

a	B	d	g	f	i	a	S	D	A	y	h	o	3	9	7
C	F	3	y	m	h	h	E	O	R	r	j	j	7	R	f
5	H	y	e	i	l	t	N	L	S	u	k	l	9	3	j
D	4	e	5	7	9	u	D	L	.	r	l	t	i	5	h

The next step is to embed this data grid linearly in a cover image file. In order to increase the level of confidentiality the message can be encrypted and the cipher text as well as the key can be arranged in different manner using two different grids. Only the recipient who knows the grid size, row and column number can retrieve the hidden message.

Justification for the proposed idea:

The above proposed two techniques for message concealment are based on the idea of making concealed message discovery more and more difficult.[4] If the steganalysis methods are successful in finding out the presence and content of a hidden message, another level of cryptanalysis would be required to reach the actual content of the hidden message.

Tools Used:

The popular package “S-Tools for Windows”Version 4.0 developed by Andy Brown will be used to carry out the image steganography and data embedding. [5]

Expected Results:

The proposed techniques will be implemented using software packages and BMP, GIF and grayscale images. The input and output text messages and the resulting stegoimages will be compared for checking the level of distortion caused by the steganographic method.

Main Referenced Papers:

1. Kevin Curran, Karen Bailey, “An Evaluation of Image Based Steganography Methods,” *International Journal of Digital Evidence*, Fall 2003 Voulme 2 Issue 2.

2. Neil F. Johnson, Sushil Jajodia, “Exploring Steganography, Seeing the Unseen,” *IEEE Computer Magazine*, 1998.

Summary of Paper "An Evaluation of Image based Steganographic Methods"[1]

In this paper, the authors have analyzed and evaluated different image based steganography methods. Seven steganography methods were implemented and analysed used GIF images namely Stego1Bit, Stego2Bits, Stego3Bits, Stego4Bits, StegoColourCycle, StegoPRNG, StegoFridrich. All of the methods used were based on the manipulation of the least significant bits of pixel values or the rearrangement of colors to create least significant bit or parity bit patterns, which correspond to the message being hidden. The methods were chosen for their different strengths in terms of resistance to different types of steganalysis or their ability to maximize the size of the message they could store. Following is a brief description of the above seven methods.

1. ***Stego1Bit:*** This method involves utilizing a single least significant bit of one of the RGB bytes of a 24-bit image for message concealment. As the color value is not changed much, it will not considerably alter the visual appearance of color and image.
2. ***Stego2Bits****:* This method involves utilizing two least significant bits of one of the RGB bytes of a 24-bit image for message concealment. Although the capacity of data storage is 2 times improved than Stego1Bit, the resulting image is degraded than Stego1Bit.
3. ***Stego3Bits:*** This method involves utilizing three least significant bits of one of the RGB bytes of a 24-bit image for message concealment. Although the capacity of data storage is 3 times improved than Stego1Bit, the resulting image is much degraded than Stego1Bit.
4. ***Stego4Bits:*** This method involves utilizing four least significant bits of one of the RGB bytes of a 24-bit image for message concealment. Although the capacity of data storage is 4 times improved, the resulting image is much degraded than Stego1Bit and color palette is restricted to only 16 variations.
5. ***StegoColourCycle:*** This method involves cycling through the color values in each of the pixels in which to store the data. This means that the same color is not constantly changed e.g., the first data bit could be stored in the LSB of the blue value of the pixel, the second data bit in the red value and the third data bit in the green value.
6. ***Stego1BitPRNG:*** This method involves using a pseudo random number generator to choose random pixels in which to embed the message. This will make the message bits more difficult to find and reduce the existence of patterns in the image.
7. **StegoFridrich:** This method involves searching for the closest color to the color of the pixel which has the correct parity for the bit to be hidden. The message is hidden in the parity bit of the RGB values of close colors. For the color of each pixel into which a message bit is to be embedded the closest colors in the palette are searched until a palette entry is found with the desired parity bit. This technique does not change the palette in any way either by ordering it or by increasing the colors in it.

The above seven methods were evaluated by the authors using the following evaluation methods:

- ***Pattern Analysis of Image Pixels:*** This detection method is based on looking for patterns in the bits that make up the pixel colors. E.g., if methods hide messages in the least significant bits of pixels then looking for patterns in the least significant bits of pixels is an easy way to detect the existence of messages.
- ***Pattern Analysis of Image Palette:*** This detection method is based on looking for patterns in the images palette. For example some steganography methods require an image with a reduced number of colours. The steganography methods then create new colours that are almost identical to the existing ones but have different least significant bits or parities.
- ***Visual Inspection of the Image:*** This analysis method is based on evaluation through visual inspection of the image by independent evaluators. The steganographic methods create a degree of distortion in the image, the visual inspection method checks for tell tale distortion.
- ***Low Level Visual Inspection of Image Pixels:*** This detection method is based on carrying out a detailed inspection of selected sections of an image at a high degree of magnification to determine whether anomalous patterns become apparent.

The conclusion of the authors is that all methods had their own weaknesses as the stegoimage suffered some distortion from the steganography process. In the case of color reduction based techniques (1 to 7), there are strong tell tale signs in the palette as well. Overall the color rearrangement technique (StegoFridrich) appeared to be the most resistant to detection as long as suitable images were chosen. The techniques that try to maximize concealed message size are least resistant to detection.

Summary of Classic Paper "Exploring Steganography: Seeing the Unseen"[2]

In the paper, the authors have introduced basic concept of steganography and how to hide information in image files. The authors have used three popular steganographic software packages for concealing one text message and one image files in two different cover files.

The authors start by first defining steganography as "the art of hiding information in ways that prevent the detection of hidden messages". The structure of image files is explored in order to develop background for image steganography. The concept of lossless and lossy file compression is presented and the choice of BMP, GIF and gray-scale images for steganography is justified.

The authors discuss three popular methods for message concealment in digital images.

1. ***Lease significant bit insertion:*** Least significant bit (LSB) insertion is a simple approach to embedding information in a cover file. It is vulnerable to even a slight image manipulation. Image conversion from a format like GIF or BMP which reconstructs the original message exactly (lossless compression) to a JPEG which does not (lossy compression) and then back could destroy the information hidden in the LSBs. LSB insertion can be performed in 24-bit, 8-bit or gray-scale images.
2. ***Masking and Filtering:*** These techniques, usually restricted to 24-bit and gray-scale images, hide information by marking an image, in a manner similar to paper watermarks. Watermarking techniques may be applied without fear of image destruction due to lossy compression because they are more integrated into the image. Traditional steganography conceals information; watermarks extend information and become an attribute of the cover image. Digital watermarks may include such information as copyright, ownership, or license.
3. ***Algorithms and transformations:*** A number of other techniques like redundant pattern encoding, encrypt and scatter etc. exist which use different approaches for concealing messages.
    a. In redundant pattern encoding, a small message may be painted many times over an image so that if the stegoimage is cropped, there is a high probability that the watermark can still be read.
    b. In *encrypt and scatter* the data are hidden throughout an image. Scattering the message makes it appear more like noise. Proponents of this approach assume that even if the message bits are extracted, they will be useless without the algorithm and stego-key to decode them.

The authors have evaluated three popular steganographic packages namely StegoDoS, White Noise Storm and S-Tools for Windows to conceal one text message and one image file using two different cover files. A brief description of the software packages follows:

- ***StegoDoS:*** It uses LSBs to hide messages, and it is less successful than other tools. It also appends an end-of-file character to the end of the message. But even with the EOF character, the message retrieved from the altered image is very likely to contain garbage at the end.
- ***White Noise Storm:*** It is a very effective steganography application for DOS. White Noise Storm includes an encryption routine to randomize the bits within an image. The software uses the LSB approach and applies this method to IBM Paintbrush (PCX) files. The software extracts the LSBs from the cover image and stores them in a file. The message is encrypted and applied to these bits to create a new set of LSBs. The modified bits are then injected into the cover image to create the new stego-image.
- ***S-Tools for Windows:*** S-Tools applies the LSB method to both images and audio files. It is the most versatile steganography tool. Version 3 includes programs that process GIF and BMP images and audio WAV files. S-Tools will even hide information in the "unused" areas on floppy diskettes. Version 4 incorporates image and sound file processing into a single program. In addition to supporting 24-bit images, S-Tools also includes encryption routines with many options. S-Tools provided the best results for steganography among the tools.

The author has concluded the paper by emphasizing the importance and applications of image steganography for covertly communicating messages.

References:

[1] Kevin Curran, Karen Bailey, “An Evaluation of Image Based Steganography Methods,” *International Journal of Digital Evidence*, Fall 2003 Voulme 2 Issue 2.

[2] Neil F. Johnson, Sushil Jajodia, “Exploring Steganography, Seeing the Unseen,” *IEEE Computer Magazine*, 1998.

[3] Wikipedia, the Free Encyclopedia

[4] Johnson Neil F., Zoran Duric, Sushil Jajodia, “Information Hiding, and Watermarking - Attacks & Countermeasures,” Kluwer 2001.

[5] Andy Brown, S-Tools for Windows, Shareware, 1994
ftp://idea.sec.dsi.unimi.it/pub/security/crypt/code/s-tools3.zip

Instructor Comments:

Both ideas are nice, you are trying to add a security-crypto layer before steganography. This may add some extra confusion to hide data which is needed. However, if you want to sell these ideas, I am not sure how are you going to convince the customer of the benefit and advantage of this idea.

Some specific considerations:
Idea 1: Capacity may be low think if you can make it higher; punctuation may be needed for proper English but you may remove it for stego purposes!!

Idea2: Is scytale secure? I mean can we prove to people that it is beneficial?
What if use a well known secure crypto method such as DES or nawadays AES?

You do not need to change a lot in your work but these may be comments toward improving your work. You can consider or use theses ideas to compare with!!

In your references summaries:
StegoFridrich: It is not clear in your summary how the hidden message is retrieved since the claim is to hide in bits with same value of the cover media!!