Using Pixel Indicator Technique in Images for Better Steganography

Abdul-Rahman Shaheen, Mahmoud Ankeer, Muhammed Abu Ghalioun.

Introduction

Steganography is the art of hiding information in ways that prevent the detection of hidden messages. Steganography, derived from Greek, literally means “covered writing.” it includes a vast array of secret communication methods that conceal the message’s very existence. These methods include invisible inks, microdots, character arrangement, digital signatures, covered channels, and spread spectrum communications.

To a computer an image is an array of numbers that represent light intensities at various points (pixels) these pixels makeup the image’s raster data. Digital images are typically stored in either 24-bit (RGB) or 8-bit (Grayscale) files.

A 24-bit image provides the most space for hiding information; however it can be quite large (with the exception of JPEG images). All color variations for the pixels are derived from three primary colors: red, green, and blue. Each primary color is represented by one byte.

Embedding data, which is to be hidden into an image, requires two files. The first is the image that will hold the hidden information, called the cover image. The second file is the message- the information to be hidden. When combined the cover image and the embedded message make a stego-image or stego-file.

Many Steganography techniques, using the image as a cover media, were proposed and implemented; the most common one is the LSB algorithm where the information is hidden in sequential fashion. Hence the risk of information being uncovered is relatively high as such approach is susceptible to all ‘sequential scanning’ based techniques. The random pixel manipulation technique attempts at overcoming this problem, where pixels are chosen in a random fashion based on a stego-key instead of a sequential one.

Our work is to improve the random selection of pixels without a stego-key. In the next section we are proposing and describing our new technique.

The Proposed Idea

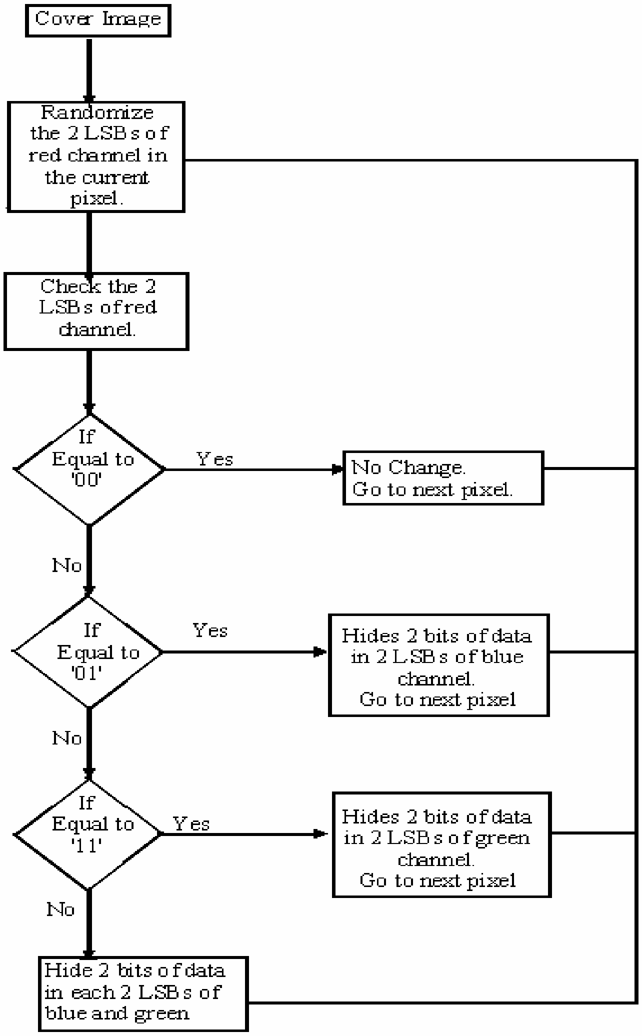
In the random pixel manipulation technique a stego-key is chosen. The stego-key provides a seed value that will be used to generate a repeated sequence of unique pseudo random number. This random sequence is then used to scramble the hidden data. At the receiving end the stego-key is used to uncover the data again by giving the receiver the ability to know which pixels are hold data.

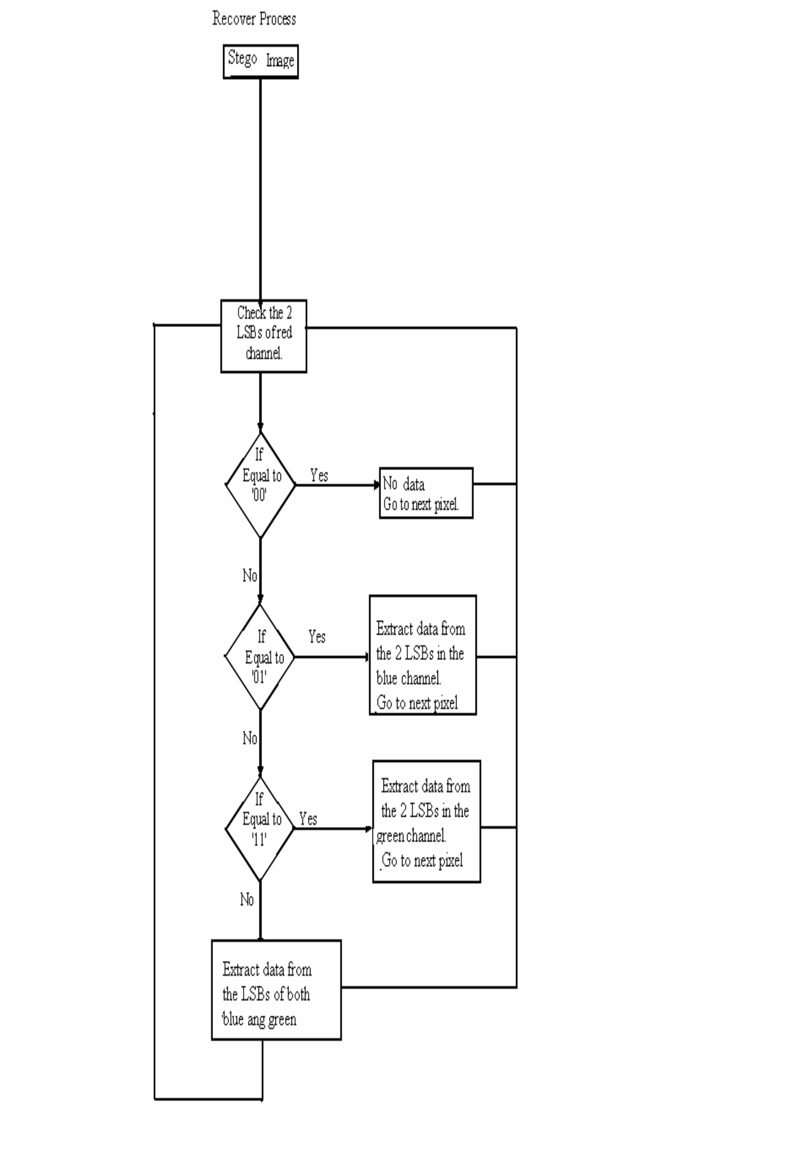
Our technique is based on RGB images. The two least significant bits of the red channel will be used as an indication to the existence of hidden data in green and blue channels as follow:

2 LSBs of red	2 LSBs of green	2 LSBs of blue
00	No hidden data	No hidden data
01	No hidden data	Contains hidden data
10	Contains hidden data	No hidden data
11	Contains hidden data	Contains hidden data

The least two significant bits of the red channels will be selected in a random fashion. The proposed technique attempts to overcome the problem of the sequential fashion and the use of stego-key to select the pixels.

Hiding Process


Cover Image
Randomize the 2 LSBs of red channel in the current pixel.
Check the 2 LSBs of red channel.
If Equal to '00'
Yes
No Change. Go to next pixel.
No
If Equal to '01'
Yes
Hides 2 bits of data in 2 LSBs of blue channel. Go to next pixel
No
If Equal to '11'
Yes
Hides 2 bits of data in 2 LSBs of green channel. Go to next pixel
No
Hide 2 bits of data in each 2 LSBs of blue and green


Recover Process
Stego Image
Check the 2 LSBs of red channel.
If Equal to '00'
Yes
No data Go to next pixel.
No
If Equal to '01'
Yes
Extract data from the 2 LSBs in the blue channel. Go to next pixel
No
If Equal to '11'
Yes
Extract data from the 2 LSBs in the green channel. Go to next pixel
No
Extract data from the LSBs of both blue ang green

Justification of Our Work

Our work tries to randomize the selection of pixels that will carry part of the data to be hidden. The idea will try to overcome the problem of sequential scanning and the use of stego-key to select the pixels. In the random pixel manipulation technique described above, the key should be shared by the sender and the receiver which put more overhead in the system due to the key transfer or synchronization between the two ends of communication.

Our algorithm will not require a key, since the key (indicator) will be a part of the stego-image. Also, any unauthorized try to recover the data will have to resolve the following issue:

- It should distinguish between the indicator and the data, since all of them are part of the same pixel.
- Not all pixels will carry data. Also, if a pixel does, it should identify whether the data is in B or G channels or in both of them.

Another improvement to our method is to change the indicator each time you move to a new pixel, that is, in the first pixel R will be used as an indicator while in the second pixel G will be used and in the third pixel B will be used. This process will be repeated until all data to be hidden are embedded in the cover image.

Because some of the pixels will not have data hidden in them, and this in turn will affect the capacity, RGB will be used due its large capacity.

Methods and Tools

To implement the mentioned algorithm we will use the MATLAB.

Expected Results

We expect to get better algorithm in term of security since we don't use a seed key to select the pixels that will hide the data; rather the pixels are selected in random fashion.

In comparison with random pixel manipulation algorithm we expect that the capacity of our algorithm will be better since the probability that the pixel will not hold any data is 1/4 and a pixel can hold up to max of four bits of the secret message.

References

1. Venkatraman.S , Ajith Abraham+, Marcin Paprzycki, "Significance of Steganography on Data Security" IEEE Computer Society, 2004.
2. Kathryn, Hempstalk, " Hiding Behind Corners: Using Edges in Images for Better Steganography", 2006.
3. Neil F. Johnson. Sushil Jajodia, "Exploring Steganography: Seeing the Unseen", IEEE computer, 1998.
4. Gary C. Kessler, "An Overview of Steganography for the Computer Forensics Examiner", 2004.
5. Donovan Artz • Los Alamos National Laboratory, “Digital Steganography: Hiding Data within Data”,2001

Appendix

- ## Significance of Steganography on Data Security

As a result of the improvement of data communication and data storage, The Information security becomes a wide area for research and development, Cryptography the art of secret writing means how to scramble your message so that it cannot be understood, On the other hand, Steganography the art of covered and hidden writing means how to hide the existence of data in any cover medium.

Different types of steganographic techniques employ color composition, luminance, unusual sorting of color palettes, exaggerated noise, relationship between color indices etc. the main objectives of the steganographic algorithms and techniques are confidentiality, data integrity and authentication.

Steganographic algorithms have many considerations, Perceptual transparency, Information capacity, and Tamper proof. Since we hide the secret message in a cover medium such as an image or audio file, the steganographic algorithm should perform its operation without raising any suspicion of the eavesdropper, the noise or any modulation induced by the originator should not change the characteristics of the cover medium. The amount of information that can be embedded without modifying the medium is another important factor for the hiding algorithm. Finally tamper proofing indicates that the host signal has been modified from its authored state.

The most common steganography method in audio and image files employs some type of least significant bit substitution or overwriting, LSB is the algorithm that hides the secret message in the least significant bit, LSB hides data in sequential manner, an improvement to the LSB is Random pixel manipulation technique which uses a stego-key to hide the secret message, the key used as a seed value for the randomization algorithm that will selects the pixels which will hide the secret message randomly, the receiver will use the same stego-key to recover the pixels that hide the data in the randomized pixels, the stego-key works like a password in this algorithm.

- ## Hiding Behind Corners: Using Edges in Images for Better Steganography

Steganography is the art of hiding information in ways that prevent the detection of the hidden messages. Embedding a data, which is to be hidden, requires two files: a cover image and the secret message. The resulted image called the stego-object or stego-image.

One of the easiest ways to hide information is to use lossless images and replace the *x* least significant bits in each pixel by the binary data. However this way is not secure, since it is susceptible to all "sequential scanning" based techniques. Another modern method is called the "*Hide Seek*" method. It attempts to overcome the previous method by randomly distributing the message across the image. It uses a random seed (stego-key) to select the order of pixels to be used for hiding the message.

However, the noise created by the previous 2 algorithms is noticeable to the naked eye in large blocks of color- where a single modified pixel stands out amongst its uniform neighbors. This is expressed explicitly by the Laplace formula. The Laplace formula simply measures the difference between a pixel and its four touching neighbors.

The new algorithm, called *filter first*, uses the Laplace formula to find the pixels that are least like their neighbors, then uses *x* least significant bits to hide the data. However this algorithm is also, weak since it has the problem of the first way described above.

New improved one is to combine the *filter first* and *Hide Seek* algorithm. In this algorithm, Laplace formula is used to find the proper pixels. Then Hide Seek will be used to select random pixels. If the random selected pixel match any of those selected by the Laplace formula, then we have a hit. A hit means data can be stored in this pixel.

- Digital Steganography: Hiding Data within Data

Digital steganography is the art of inconspicuously hiding data within data. Steganography's goal in general is to hide data well enough that unintended recipients do not suspect the steganographic medium of containing hidden data.

Governments, businesses and normal users can take benefit from steganography

Encryption and Steganography achieve separate goals. Encryption encodes data such that an unintended recipient cannot determine its intended meaning. Steganography, in contrast, does not alter data to make it unusable to an unintended recipient. Instead, the steganographer attempts to prevent an unintended recipient from suspecting that the data is there.

Steganography has many constraints one of them that the intended recipient must have prior knowledge of steganography presence and algorithm. Also, the amount of data that can be effectively hidden in a given medium tends to be restricted by the size of the medium itself and the integrity of the medium.

The digital image steganography can be categorized into two types based on effecting original image: steganography effects original image like changing cosine coefficients in JPEG and LSB in RGB and grayscale images and one that does not affect original image like changing order of colors in color map in GIF. In audio steganography, LSB can be altered to represent data. Also, ordering data that does not have an ordering constraint is often an effective method of steganography.

Steganalysis, the official countermeasure to steganography, is the art of detecting and often decoding hidden data within a given medium.

Two major tools in steganalysis, information theory and statistical analysis, reveal in clear terms the tremendous potential for hidden information in Internet data. However, there is no guarantee that the message is exist.

Instructor Comments:
Your idea will reduce the capacity, but it is very interesting.
How did you choose the indicator?
You can run a test to see which one of RGB would lead to the best capacity. Then, compare with your idea of mixing or rotating the indicator.
To increase capacity, you can try to hid info in the least 3 bits, which will make the pixel hold two bits in the indicator and up to 6 bits of hidden data. This can be compared with your idea of hiding two bits only. The comparison can be in terms of security as well as capacity.