International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Implementing Random Encoding for Image Steganography

Venus[1], Rachna[2]

[1]Department of Computer Science, Gateway Institute of Engineering & Technology (GIET), Deenbandhu Chhotu Ram University of Science & Technology (DCRUST), Sonepat

[2]Department of Computer Science, Gateway Institute of Engineering & Technology (GIET), Deenbandhu Chhotu Ram University of Science & Technology (DCRUST), Sonepat

Abstract: ***Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. Steganography works by replacing bits of useless or unused data in regular computer files (such as graphics, sound, text, HTML, or even video) with bits of different, invisible information. This hidden information can be plain text, cipher text, or even images. Most of the steganographic techniques use sequential encoding and decoding for hiding text or image in a canvas image file. In this paper, we propose a new random encoding technique for image steganography. In this technique a user can hide text or image randomly across pixels in a canvas image file. The final output is an image file that contains the message protected by encryption and encoding. Therefore hidden message is difficult to detect and recover.***

Keywords: Image Steganography, Sequential Encoding, Random Encoding, LSB

1. Introduction

The term Steganography [1, 2] is adapted from the Greek word *steganographia,* meaning "covered writing" and is taken in its modern form to mean the hiding of information inside other information. Steganography is a form of science that deals with cryptic information. It is the art of writing in cryptic text that is unrecognizable to a person who doesn't hold the key to decrypt it. In contemporary terms, steganography has evolved into a digital strategy of hiding a file in any form of multimedia such as an image, an audio file or even a video file.

In order for a data hiding technique to be successful it must adhere to two rules [3]:

- The embedded data must be undetectable within its carrier medium (the audio or image file used). The carrier should display no properties that flag it as suspicious, whether it is to the human visual/auditory system or in increased file size for the carrier file.
- The embedded data must maintain its integrity within the carrier and should be easily removable, under the right circumstances, by the receiving party.

Before going deep into the steganographic process, first and foremost, we need to understand the various components of a steganographic message. The below list covers all the possible components that will be present in the steganographic message [4].

- Secret message
- Cover data or object
- Stego message or object

The *secret message* refers to the part of the message which is intended to be hidden. This message will later be encrypted to make it even more difficult for anyone who tries to break the security to get hold of the hidden informatics message. This is the crucial component in a steganographic message.

Next part is the *cover data* component. This component refers to the container in which the secret message is hidden. This cover data component can be anything like digital photos, digital videos, audio files and text files. A *stego* object is one which looks exactly same as the cover object but it contains hidden information. To add more security, the data to be hidden is encrypted with a key before embedding. To extract the hidden information one should have this key.

The final component is the *stego message* which is as crucial as the *secret message*. The *stego message* component refers to the final product.

2. Image Steganography Approaches

Images are used as the popular cover medium for steganography. A message is embedded in a digital image using an embedding algorithm, using the secret key. The resulting stego-image is send to the receiver. On the other side, it is processed by the extraction algorithm using the same key. During the transmission of stego- image unauthenticated persons can only notice the transmission of an image but cannot see the existence of the hidden message. For embedding a message in an image, a different set of techniques such as least-significant bit insertion, masking and filtering, and subtle transformation of the image are used. These techniques or transformations do not cause any visible changes in the cover image when viewed [6].

Steganography in images is mainly classified into:

- Least significant bit (LSB) insertion method.
- Masking and filtering.
- Algorithms and transformation.

Licensed Under Creative Commons Attribution CC BY

Least significant bit insertion method
Least significant bit insertion method is the most common method used. In this type, the data to be hidden is inserted into the least significant bits of the pixel information. In digital format the images are represented with numerical values of each pixel where the value represents the color and intensity of the pixel.

Images are mainly of two types:
• 24-bit images • 8-bit images

24-bit images: These images have 24 bit value for each pixel in which each 8 bit value refers to the colors red blue and green. We can embed 3 bits of information in each pixel, one in each LSB position of the three 8 bit values in 24 bit value. Increase or decrease of value by changing the least significant bit doesn't change the appearance of the image, such that the resulted stego image looks exactly same as the cover image.

8-bit images: In these images 1 bit of information can be hidden in each pixel. As in 8-bit images maximum number of colors that can be present are only 256 colors, the color variation may occur and therefore, care should be taken in considering the cover image.

Advantages:
- There is less chance for degradation of the original image.
- More information can be stored in an image (hiding capacity is more).

Disadvantages:
- Less robust, the hidden data can be lost with image manipulation.
- Hidden data can be easily destroyed by simple attacks.

Masking and Filtering
Masking refers to covering a signal by a different signal in such a way that the first signal is not apparent. This is based on the human visual acuity which cannot detect slight changes. Masking is mainly used in watermarking techniques. This is not pure steganography as here we extend the image information as well as other attributes of the image. Since much of the data is integrated into the image, the data won't be lost even if the image manipulation is done like compression, cropping etc.

Advantages:
This method is much more robust than LSB replacement with respect to compression.

Disadvantages:
Techniques can be applied only to gray scale images and restricted to 24 bits.

Algorithms and Transformations
Data is embedded into the cover image by changing the coefficients of transformation of an image, such as discrete cosine transform coefficients. If we embed information in spatial domain, it may be subjected to the losses if the image undergoes any image processing technique like compression, cropping etc. To overcome this problem we embed the information to be hidden in frequency domain. As the digital data is not continuous, to analyze the data of the image, we apply transformations to the image. We embed the data to be hidden by changing the values of the transformation coefficients accordingly.

There are mainly three transformation techniques:
1) Fast Fourier transformation technique (FFT)
2) Discrete cosine transformation technique (DCT).
3) Discrete Wavelet transformation technique (DWT).

3. Proposed Work

In this paper we purpose an image based steganography that Least Significant Bits (LSB) techniques and random encoding technique on images to enhance the security of the communication. In the LSB approach, the basic idea is to replace the Least Significant Bits (LSB) of the cover image with the Bits of the messages to be hidden without destroying the property of the cover image significantly. The LSB-based technique is the most challenging one as it is difficult to differentiate between the cover-object and stego-object if few LSB bits of the cover object are replaced. In Random Encoding technique, a random-key is used as seed for the Random Number Generator is needed in the embedding process [7]. Both the techniques used a stego-key while embedding messages inside the cover image. By using the key, the chance of getting attacked by the attacker is reduced.

3.1 Least-Significant Bit (LSB) Technique

The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message. Digital images are mainly of two types (i) 24 bit images and (ii) 8 bit images. In 24 bit images we can embed three bits of information in each pixel, one in each LSB position of the three eight bit values. Increasing or decreasing the value by changing the LSB does not change the appearance of the image; much so the resultant stego image looks almost same as the cover image. In 8 bit images, one bit of information can be hidden.

The following figure 1 & 2 shows the mechanism of LSB technique

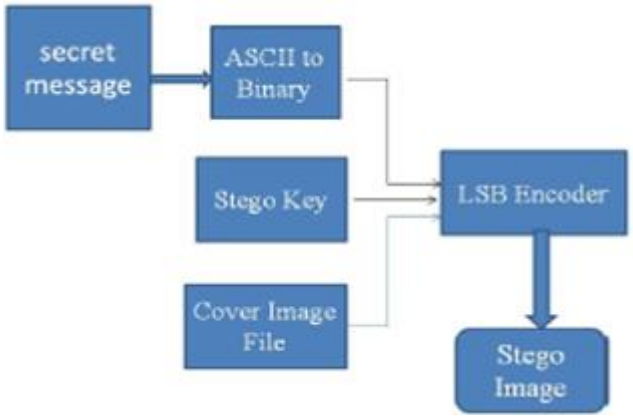

Figure 1: LSB insertion Mechanism

Licensed Under Creative Commons Attribution CC BY

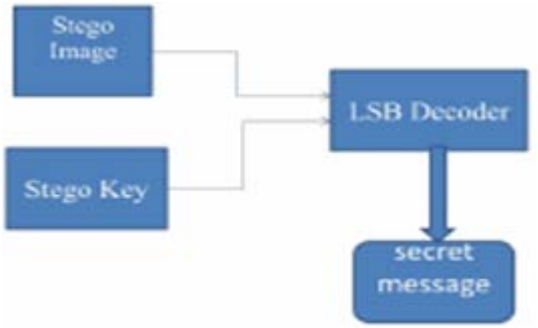

Figure 2: LSB extraction Mechanism

2.1.1 Data Embedding

The embedding process is as follows.
Inputs: Cover image, stego-key and the text file
Output: stego image
Step 1: Extract the pixels of the cover image.
Step 2: Extract the characters of the text file.
Step 3: Extract the characters from the Stego key.
Step 4: Choose first pixel and pick characters of the Stego key and place it in first component of pixel.
Step 5: Place some terminating symbol to indicate end of the key. 0 has been used as a terminating symbol in this algorithm.
Step 6: Insert characters of text file in each first component of next pixels by replacing it.
Step 7: Repeat step 6 till all the characters has been embedded.
Step 8: Again place some terminating symbol to indicate end of data.
Step 9: Obtained stego image. [8]

2.2.2 Data Extraction

The extraction process is as follows.
Inputs: Stego-image file, stego-key
Output: Secret text message.

Step 1: Extract the pixels of the stego image.
Step 2: Now, start from first pixel and extract stego key characters from first component of the pixels. Follow Step3 up to terminating symbol, otherwise follow step 4.
Step 4: If this extracted key matches with the key entered by the receiver, then follow Step 5, otherwise terminate the program.
Step 5: If the key is correct, then go to next pixels and extract secret message characters from first component of next pixels. Follow Step 5 till up to terminating symbol, otherwise follow step 6.
Step 6: Extract secret message [9].

2.2.3 Image Encoding Algorithm

Inputs: Image file, stego key and image file
Output: Stego image.

1) The cover and secret images are read and converted into the unit8 type.
2) The numbers in secret image matrix are conveyed to 8-bit binary. Then the matrix is reshaped to a new matrix a.
3) The matrix of the cover image is also reshaped to matrix b
4) Perform the LSB technique described above
5) The stego-image, which is very similar to the original cover image, is achieved by reshaping matrix b.
6) While extracting the data, the LSB of the stego image is collected and they are reconstructed into the decimal numbers. The decimal numbers are reshaped to the secret image [11].

2.3 Random Encoding Technique

In this technique, A random key is used to choose the pixels randomly and embed the message. This will make the message bits more difficult to find and hopefully reduce the realization of patterns in the image [10]. Data can be hidden in the LSB of a particular color plane (Red plane) of the randomly selected pixel in the RGB color space [7].

2.3.1 Embedding Algorithm

In this process of encoding method, a random key is used to randomize the cover image and then hide the bits of a secret message into the least significant bit of the pixels within a cover image. The transmitting and receiving end share the stego key and random-key. The random-key is usually used to seed a random number generator to select pixel locations in an image for embedding the secret message [6].
Inputs: Cover image, stego-key and the message
Output: stego image

1) Read character from text file that is to be hidden and convert the ASCII value of the character into equivalent binary value into an 8 bit integer array.
2) Read the RGB color image (cover image) into which the message is to be embedded.
3) Read the last bit of red pixel.
4) Initialize the random key and randomly permute the pixels of cover image and reshape into a matrix.
5) Initialize the stego-key and XOR with text file to be hidden and give message.
6) Insert the bits of the secret message to the LSB of the Red plane's pixels.
7) Write the above pixel to Stego Image File.

2.3.2 Extraction of Hidden Message

In this process of extraction, the process first takes the key and then random-key. These keys take out the points of the LSB where the secret message is randomly distributed. Decoding process searches the hidden bits of a secret message into the least significant bit of the pixels within a cover image using the random key. In decoding algorithm the random-key must match i.e. the random-key which was used in encoding should match because the random key sets the hiding points of the message in case of encoding. Then receiver can extract the embedded messages exactly using only the stego-key.

Inputs: Stego-image file, stego-key, random key.
Output: Secret message.

1) Open the Stego image file in read mode and from the Image file, read the RGB color of each pixel.
2) Extract the red component of the host image.
3) Read the last bit of each pixel.
4) Initialize the random-key that gives the position of the message bits in the red pixel that are embedded randomly.
5) For decoding, select the pixels and Extract the LSB value of red pixels.

Licensed Under Creative Commons Attribution CC BY

6) Read each of pixels then content of the array converts into decimal value that is actually ASCII value of hidden character.
7) ASCII values got from above is XOR with stego-key and gives message file, which we hide inside the cover image.

4. Conclusion

The term Steganography is adapted from the Greek word *steganographia,* meaning "covered writing" and is taken in its modern form to mean the hiding of information inside other information. Steganography is a form of science that deals with cryptic information. It is the art of writing in cryptic text that is unrecognizable to a person who doesn't hold the key to decrypt it. Most of the steganographic techniques use sequential encoding and decoding for hiding text or image in a canvas image file. In this paper, we propose a new random encoding technique for image steganography. In this technique a user can hide text or image randomly across pixels in a canvas image file. The final output is an image file that contains the message protected by encryption and encoding. Therefore hidden message is difficult to detect and recover.

References

[1] V. K. Pachghare, Cryptography & Information Security, Prentice-hall of India Pvt Ltd
[2] Eric Cole, Hiding in Plain Text, Wiley Publishing, Inc. :2003
[3] Stefan Katzenbeisser and Fabien A. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, Inc., Norwood, MA, USA, 2000.
[4] Brainos II, A. C. A Study of Steganography and the Art of Hiding Information, East Carolina University, November 13, 2003.
[5] Artz, D. Digital Steganography: Hiding Data within Data. IEEE Internet Computing, May 2001. IEEE.
[6] E Lin, E Delp, "A Review of Data Hiding in Digital Images", Center for Education and Research Information Assurance and Security, 2011.
[7] Shamim Ahmed Laskar and Kattamanchi, "Steganography based on random pixel selection for efficient data hiding". Hemachandran, International journal of computer engineering technology (ijcet), 2013
[8] Mamta Juneja, "Data hiding Algorithm for Bitmap Images using Steganography", Department of computer science and Engineering, RBIEBT,Sahuran, 2013
[9] Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav, "Steganography Using Least Signicant Bit Algorithm", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248 9622 www.ijera.com Vol. 2, Issue 3, May-Jun 2012,
[10] Samir K Bandyopadhyay, Debnath Bhattacharyya, Debashis Ganguly, Swarnendu Mukherjee and Poulami Das, "A Tutorial Review on Steganography", Heritage Institute of Technology, 2013.
[11] Pratap Chandra Mandal, "Modern Steganographic technique: A Survey" International Journal of Computer Science Engineering Technology (IJCSET), 2013.
[12] Ali Al-Ataby and Fawzi Al-Naima "A Modified High Capacity Image Steganography Technique Based on Wavelet Transform" The International Arab Journal of Information Technology, Vol. 7, No. 4, October 2010.
[13] Nitin Jain, Sachin Meshram, Shikha Dubey "Image Steganography Using LSB and Edge – Detection Technique" International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-3, July 2012.

Licensed Under Creative Commons Attribution CC BY