Image Seeded Steganography: Steganography Using Seed Values

Authors
Yogita Puri 1, Gaurav Deep 2

1 Student (M.Tech), Department of Computer Engineering, Punjabi University, Patiala
2 Asst.Professor, Department of Computer Engineering, Punjabi University, Patiala
Email:puriyogita13@gmail.com, deepgaurav48@pbi.ac.in

ABSTRACT

Now a days, because of the electronic eavesdropping information security has become a cause of concern. Information hiding has some important parameters like capability, strength and invisibility. Secured data transmission over computer networks can be achieved through steganography and cryptography. Cryptography scrambles the message so that it is unrecognizable and without proper key the encrypted message is useless. Steganography is a technique used to transmit a secret message from a sender to a receiver in a way such that a potential intruder does not suspect the existence of the message. In steganography different-different carrier files can be used, but the most popular is digital images because they are used a lot now a days on the internet. In image steganography the information is hidden exclusively in images. In this paper, we device and implement a technique that hides text into bits of digital image. This technique hides secret message in form of bits in the efficient bits selected through some procedure. Preprocessing i.e. filtering and segmentation is applied on image before data hiding. Original image and image after data hiding is compared over various parameters.

Keywords-Steganography,PSNR,MSE,LSB,DigitalImage,CoverImage,StegoImage

1. INTRODUCTION

Steganography is the art and science of invisible communication. It is accomplished by hiding information in other information, thus hiding the existence of the information. Steganography is derived from the Greek words “stegos” meaning “cover” and “grafia” meaning “writing” defining it as “covered writing” [1]. It is invisible, and thus the detection is not easy [11]. Secured data transmission over computer networks can be achieved through steganography and cryptography. Cryptography scrambles a message so it cannot be understood. Steganographic techniques have several useful applications including their use for digital watermarking for ownership verification, alteration detection, and annotation [7]. Steganography hides the message so it cannot be seen [2]. The main purpose of steganography is to convey the information secretly by concealing the very existence of information in some other medium [9]. Figure 1.1 shows the process of...
Steganography, in which there is cover image on which secret image has to be embedded then with the help of encoder image is sent. Cover Image, in which Secret image is entrenched and in this way it hides the presence of the secret image. Key which is used is known as stego-key, which is used by encoder on the sender side to hide secret image into cover image and also the key is used on the receiver side to extract the secret image from stego image. Only the receiver will have the key K to decrypt or decipher the code to get back the original message [10]. The cover-image with the image secretly embedded is then called the stego-object.

**Figure 1.1 Basic Steganography Model**

**Features of good steganographic technique:**

a. Data should always remain hidden.

b. Secret data should be visible, but unidentifiable.

c. Data should be directly hidden into carrier.

d. Hiding data should not compromise the quality of carrier.

e. Technique should provide better imperceptibility.

**Techniques of Steganography**

The simplest approach of embedding information in image file is the least significant bits (LSB) insertion method. Least significant bit (LSB) Replacement method is a common approach to embed information in a cover image [1]. In this method, LSB of the pixel is used to replace the data with the secret message. Another approach of data hiding is transform techniques in which bits of the image are transformed into some coefficients and then data is embedded into these coefficients for example the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), or Discrete Wavelet Transform (DWT) [1]. The transform domain Steganography technique is used for hiding a large amount of data and provides high security, a good invisibility and no loss of secret message.

Masking and filtering method is usually restricted to 24 bit images. This method uses specific masking algorithms or mathematical formulae to select pixels from the cover image [4].

**Distortion Method:** In this method some information is stored by distorting signal. By this technique one object is created which is known as stego object.
1.2 Types of Steganography

Text Steganography consists of hiding information inside the text files [3]. In this method, the secret data is hidden behind every nth letter of every words of text message. Image Steganography is the process of hiding the data by taking the cover object as image is referred as image steganography [3]. In image steganography pixel intensities are used to hide the data. In digital steganography, images are widely used cover source because there are number of bits presents in digital representation of an image. Audio Steganography involves hiding data in audio files. This method hides the data in WAV, AU and MP3 files [3]. There are different methods of audio steganography.

Video Steganography is a technique of hiding any kind of files or data into digital video format [3]. In this case video (combination of pictures) is used as carrier for hiding the data. Network or Protocol Steganography involves hiding the information by taking the network protocol [3] such as TCP, UDP, ICMP, IP etc, as cover object.

1.3 Image Steganography

Image Steganography is the process of hiding the data by taking the cover object as image is referred as image steganography. In image steganography pixel intensities are used to hide the data. In digital steganography, images are widely used cover source because there are number of bits presents in digital representation of an image.

In steganography different-different carrier files can be used, but the most popular is digital images because they are used a lot now a days on the internet. In image steganography the information is hidden exclusively in images.

When making a steganography i.e a data hiding system, some properties have to be considered. These properties are:

Imperceptibility [5] property in which no difference can be find by a person in the original file and the stego file.

Embedding Capability means a large amount of data can be embedded into the image and also the embedded image must not be degraded after data embedding.

Toughness is the quantity of complexity required to demolish the information which is embedded without destroying the carrier [5].

The embedded algorithm must be undetectable i.e the image with the embedded message is consistent with a model of the source from which images is drawn.

Size of the message which is secret affects this property and also the cover image or carrier’s format also affects this property [6].

Techniques of image steganography can be divided into two groups. First domain is known as Image-domain and second is Transform-domain. Image-Domain also known as spatial – domain techniques insert secret messages in the pixel’s intensity value directly.
While for transform also known as frequency–domain, in which image which is used as cover is first transformed using DCT, DWT or DFT and then message is embedded into these transformed values of the image.

Various techniques for image steganography have already been developed. All these techniques hide data into the images depending upon the different-different methods used in these techniques. Figure 1.2 shows various Image Steganographic Techniques according to image file formats and the domain in which they are performed.

Figure 1.2 Categories of Image Steganography

All the above mentioned algorithms for image steganography have different strong and weak points. These all methods must have all the properties which is required for a good steganographic system i.e Invisibility, Payload Capacity, Robustness against statistical attacks, Robustness against image manipulation, Independent of file format and unsuspicious files. The following Table 1.1 compares least significant bit insertion in BMP and in GIF files, JPEG compression steganography, and the patchwork approach and spread spectrum techniques according to the above requirements:

Table 1.1 Comparison of various Image Steganography Algorithms

<table>
<thead>
<tr>
<th>Requirement</th>
<th>LSB in BMP</th>
<th>LSB in GIF</th>
<th>JPEG Compression</th>
<th>Patchwork</th>
<th>Spread Spectrum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invisibility</td>
<td>High*</td>
<td>Medium*</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Payload Capacity</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>Robustness against Statistical attacks</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Robustness against Image Manipulation</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
</tr>
<tr>
<td>Independent of File Format</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Unsuspicious Files</td>
<td>Low</td>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
</tbody>
</table>

* - Depends on cover image used

Different levels are defined i.e high, low and medium level. All steganography algorithms which are written in the table have one of these levels and the algorithms are tested on this basis. When the algorithm satisfies all the requirements then algorithm level is defined as high. When the algorithm is weak in these requirements then algorithm is said to have low level. Algorithm which is medium level indicates that the requirement depends on outside influences, for example the cover image used.
1.4 Image Types

To a computer, an image consists of various numbers. All these numbers have different intensities. These numbers are called as pixels [8]. This pixel representation forms a grid. Images are made up of a rectangle type in which there are number of pixels (bits). These bits have colors. These pixels are shown in horizontal direction i.e row by row.

Following Table 1.2 shows comparison of various types of images used in MATLAB Image Processing Toolbox.

Table 1.2 Different Image-Types

<table>
<thead>
<tr>
<th>Image Type</th>
<th>Another Names</th>
<th>Representation</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Binary</td>
<td>Bit Level Image</td>
<td>A binary image is represented by an MxN logical matrix where pixel values are 1 (true) or 0 (false)</td>
<td><img src="image1.png" alt="Binary Image Example" /></td>
</tr>
<tr>
<td>Indexed</td>
<td>Paletted image</td>
<td>Indexed images are represented with an index matrix of size MxN and a color map matrix of size Kx3. The image has in total K different colors.</td>
<td><img src="image2.png" alt="Indexed Image Example" /></td>
</tr>
<tr>
<td>Gray Scale</td>
<td>Intensity, Gray level Image</td>
<td>A grayscale image M pixels tall and N pixels wide is represented as a matrix of double data type of size [M x N]</td>
<td><img src="image3.png" alt="Gray Scale Image Example" /></td>
</tr>
<tr>
<td>Truecolor</td>
<td>RGB (Red, Green, Blue) Image</td>
<td>RGB image is represented as a three-dimensional MxNx3 double matrix. Each pixel has red, green, blue components along the third dimension with values in [0,1]</td>
<td><img src="image4.png" alt="Truecolor Image Example" /></td>
</tr>
</tbody>
</table>

2. PROPOSED METHODOLOGY

Embedding Process:

The Technique proposed in this paper uses seeds i.e. Pixels for data hiding. Pixels are selected by modified seed value criteria. As Explained in the Flow chart i.e Figure 2.1 in Embedding Process, we input an image file. Image is filtered to remove noise from image. After this segmentation technique is applied to filtered image to divide the image into various segments.

Largest segment is picked and custom filter is applied on that segment by changing position of origin every time as filter is moving on the full segment. Custom filter is used to evaluate seed positions which are used for data hiding.

Custom filter works on segment by taking difference of origin of the filter and its neighboring pixels. If difference is between -5 and +5 then use that seed and save it into database and hence seeds are evaluated. Enter data which is to be hidden into image. Perform Encryption on the data so that it can be secured. In this way Plain text is converted into cipher text. Cipher text is converted into bits and then hide secret data into seed positions evaluated.
**Figure 2.1 Proposed Methodology: Embedding Process**

**Extraction Process:**
In Extraction Process as shown in figure 2.2, embedded image is loaded then seed positions which are used for data hiding are loaded. Data is extracted from seeds. The data which is extracted is encrypted data so decryption is performed on data and secret data is converted into plain text.
Figure 2.2 Proposed Methodology: Extraction Process

Graphical user interface of thesis is shown in figure 2.3

Figure 2.3 User Interface

3. EXPERIMENTAL RESULTS

The technique was successfully implemented over various images and results were collected and analyzed for each Image. Results of various test images are shown in the following tables. First PSNR and MSE values of Original i.e main image and filtered image is shown and then in second table PSNR and MSE values of stego image and filtered image(Cover image) is shown.

Table 3.1: PSNR and MSE values of Original i.e main image and filtered image (Cover image)

<table>
<thead>
<tr>
<th>Main Image and Filtered image</th>
<th>PSNR</th>
<th>MSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Testimage1</td>
<td>35.548</td>
<td>0.18268</td>
</tr>
<tr>
<td>Testimage2</td>
<td>40.7063</td>
<td>0.0557</td>
</tr>
<tr>
<td>Testimage3</td>
<td>35.3097</td>
<td>0.19298</td>
</tr>
<tr>
<td>Testimage4</td>
<td>35.2841</td>
<td>0.19412</td>
</tr>
<tr>
<td>Testimage5</td>
<td>36.1661</td>
<td>0.15844</td>
</tr>
</tbody>
</table>
Table 3.2: PSNR and MSE values of stego image and filtered image (Cover image

<table>
<thead>
<tr>
<th>Main Image and Filtered image</th>
<th>PSNR</th>
<th>MSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Testimage1</td>
<td>68.7415</td>
<td>0.0087565</td>
</tr>
<tr>
<td>Testimage2</td>
<td>68.5368</td>
<td>0.0091791</td>
</tr>
<tr>
<td>Testimage3</td>
<td>66.4163</td>
<td>0.014957</td>
</tr>
<tr>
<td>Testimage4</td>
<td>64.8882</td>
<td>0.021265</td>
</tr>
<tr>
<td>Testimage5</td>
<td>65.8723</td>
<td>0.016953</td>
</tr>
</tbody>
</table>

As we can see, Each PSNR value in Table 3.2 is greater than the values in Table 3.1 and each MSE value in Table 3.2 is less than each MSE value in Table 3.1.

Stego image looks like cover image. So image is not degraded after data embedding.

Cover image is shown in figure 3.1(a) and stego image is shown in figure 3.1(b).

**Figure 3.1(a):** Cover Image

**Figure 3.1(b):** Stego image

4. CONCLUSION

We proposed and implemented a new technique that hides data by selecting pixels of an image based upon modified seed value criteria. While doing this we came to know about various types of images and also came to know that images can be used as an efficient carrier file for data hiding. By this technique we came to know that by using filter, embedding capacity can be increased. At seeing the results, and that there is negligible difference among original and Stego-Image, we can conclude that image steganography using seed values is as good as any other technique. A secure image steganography technique is proposed to hide data. Experimental results show that technique produces good quality stego-images, good psnr values with
reasonable execution time. Experimental results show that our method gets stego-image with perceptual invisibility, high security and certain robustness.

5. FUTURE-SCOPE
Steganalysis is used to detect the hidden information from observed data with little or no knowledge about the steganography algorithm. For future work, it provides a research area for seed based steganalysis. It provides a research area to work on various steganography and steganalysis methods which works using seed values.

REFERENCES