Techniques of Image Steganography

Mr Kamaldeep Joshi  
( Assistant Professor)  
CSE Department, UIET  
MD University, Rohtak (Haryana)

Ms Kirti Sharma  
M Tech Student  
CSE Department, UIET  
MD University, Rohtak (Haryana)

Abstract: In the present era of digital computing and with the enhanced use of computer network - privacy, trusted computing, intrusion-detection and information protection are important majors to concern. An appropriate approach to short out these problematic concerns is termed as “Steganography”. Steganography is very essential technique basically used for covert transformation of information over a covert communication channel. Steganography maintains the confidentiality of sensitive information by applying prevention to the illegal attention through hiding the secret message in a variety of digitally and electronically representative media. The present paper focuses on Steganography, types and its techniques.

Keywords: Spatial domain- LSB, M-LSB-SM (Magical-LSB-Substitution Method), PVD (Pixel value Differencing), GLM, PIT, Transform Domain-DCT, DWT.

Introduction:  
Introduction to Steganography: Steganography is basically originated from Greek words as combination of “Stegano + Graphia” which means concealed writing[2]. It is an art and science to establish a covert communication between sender and receiver by enclosing a message into an innocuous appearing envelop media such as text, image, audio and video.

Two main reasons for covert communication are:

i. Invulnerability against detection (Information Hiding).
ii. Invulnerability against removal (Watermarking and Fingerprinting).

Information security is a required fact in today’s excessively rapid progressed environment of internet technologies. Information needs to be as much secured from intruder’s attacks during communication over wired or wireless network takes place. Information must be concealed from:

- Privileged accesses (Confidentiality).
- Privileged changes (Integrity).
- And must be available to an authorized body (Availability).

Steganography facilitates to sender and even it hides the survival of the message.

Ancient Steganography:

- The first recorded uses of Steganography can be traced from 440BC when Herodotus sent a message on messenger’s body - also used in ancient Greece. A message tattooed on the shaved head of a slave of messenger, hidden by hair on re-grown over it and exposed by shaving the head[1].
- Hidden message within Wax-Table, people wrote messages on wood and covered it with wax that built an innocent covering message [1].
- In 1945 Morse code used, Messages written in Morse code on Yarn, and knitted into a piece worn by a courier. Messages written on envelopes in area covered by Postage Stamps [1].
- At the time of World War II, espionage agents used photographically produced Microdots (minute in size) to send information back and forth. World War II microdots were inserted in paper and covered with an adhesive that was reflexive and detectable by viewing against glancing light [1].
- As the time processed forward, the various advanced technologies have been emerged to hide any information.
Steganography exploiting the image format: Steganography can be accomplished by simply delivering into a Window OS command:  

```
C: > copy cover.jpg / b + Message.rar stego.jpg
```

This code simply appends the secret message in “Message.txt” into “cover.jpg” and produces the stego-image as “stego.jpg”. When stego.jpg is viewed using any photo editing application, it will just display the picture by ignoring everything which is coming after EOF tag. And when opened with notepad our message reveals itself after displaying some data and embedded message does not damage the image quality [4][9].

![Steganography Types Diagram](image)

**Fig.1: Steganography Types**
Advantages of Steganography: Confidential communication and secret data storing. Invulnerability of data alteration, E-Commerce and Media (copyright), Database Systems and Digital Watermarking.

Limitations of Steganography: Many a terrorist and anti-humanist activities have been carried out veiled under this technique.

Types Of Steganography: Various types of Steganography are as follows:

1. Plaintext Steganography.
2. Digital Image Steganography
3. Audio Steganography.
4. Video Steganography.

1. **Plaintext Steganography**: It consists of covert information within the text files. In this technique, the sensitive information is covert behind the every nth letter of every words of text message.

2. **Image Steganography**: Covering of information through the innocuous cover as image is referred as image Steganography [7]. In it, pixel intensities are used to cover the information. In digital Steganography, images are used as cover source because it has lots of bits inside it.

3. **Audio Steganography**: It consists obscuring of information in audio files [7]. This method covers the information in MP3, AU, MIDI, MPEG, MP4 and WAV sound files.

4. **Video Steganography**: Obscuring any kind of file or data into digital video format is referred as video Steganography [7]. Combination of images (video) is used as medium for obscuring the information.

Image Steganography: In image Steganography, sensitive information transferred to the receiver by embedding to innocuous cover (image) as in form of stego-image. It is used to establish a hidden communication. An image is an aggregation of numbers called Pixels that incorporate different light intensities in different regions of that image. Larger size images acquire larger space over the internet, so to reduce the size of image; method used is called as image compression. Digital images are preserved in 24-bits files and use RGB color model as true color. All 24-bits are derived from three primitive colors Red, Green and Blue; each one represented by 8-bits. Thus, in 1-pixel, there can be 256 different entities of RGB.

**Terminologies used in image Steganography:**

- **Cover-Image**: Actual image which is as media for obscuring information.
- **Message**: Actual information which is used to cover within image.
- **Stego-Image**: Image which formed after enclosing the message inside cover-image.
- **Stego-Key**: A key which is used to insert and extract the message from cover-image and stego-image.
Techniques of Image Steganography:

Two major techniques of images based Steganography are: Spatial Domain Technique and Frequency Domain Technique.

A. Spatial Domain Techniques: Spatial Domain techniques directly deal with the pixel values of images. By altering in pixel values of cover image it hides the sensitive information. It consists of simplest techniques is additive noise that is imperceptible in image which directly affects the Peak Signal-to-Noise Ratio[5]. There are various spatial domain techniques which are broadly classified some of them are as follows:

1. LSB: It stands for Least Significant Bit Replacement Technique. This one is simplest Steganography technique to be performed which is based on LSB of each pixel of the image. In it, insertion of information in the cover image does not lead to the distortion in the image. The LSB value variation does not appear to human eyes (totally invisible)[2][4].

Algorithm: Step1: Convert the message decimal value into binary value: [13] → [1101]
Step2: Let take the cover image having gray value 250.
Step3: Convert it into binary value [250] → [11111010]
Step4: Break the byte to be hidden into bits. MSB : 1111 LSB: 1010
Step5: Replace the LSB bit-by-bit through message bits. After the embedding of information into image, stego image is created and send it to receiver. Now, receiver has to extract the original information from stego-image. Stego a 20*20 matrix hold gray value 253. After extraction of LSB bits (bit-by-bit), message bits will be extracted to the receiver as: Recovered or Original message holding gray value 13.

Advantages: The image does not form any distortion and depreciation. Encryption of large amount of information in a cover image is possible by using LSB replacement technique[2].

Limitations: It is less robust in nature. Hidden information can be disclosed easily i.e. Less Secure. Changes in image may occur lost of information.


Algorithm: Step1: An input image is transposed and converted into a HIS color space.
Step2: Achromatic component is divided into four sub-images of equal-size.
Step3: Rotate the each sub image with a different angle using a secret key.
Step4: Secrete message is divided into four blocks which are encrypted using MLE algorithm.
Step5: Insertion of each of sub blocks of message takes place in rotated sub-images based upon specific sequence using M-LSB-Substitution Method.

Advantages: It provides high quality stego image. Operations applied in this technique make it extremely difficult to extract the actual hidden information. It enhanced the security by using MLEA.

3. PVD: It stands for “Pixel Value Differencing”. It is able to provide a high quality stego image despite of the high capacity of concealed information. In this technique, the number of bits to insert is depends on the pixels area which pixel value lies in edge area or in smooth area. The difference between the adjacent pixels is more in edge area rather than in smooth area. So, the maximum number of information bits is possible to insert in edge area which is less human perceptible as compare to smooth area[5][8].

Advantages: It provides high imperceptibility to stego image by selecting two consecutive pixels. Designing of quantization range table takes place to calculate payload by difference value between consecutive pixels. It conveyed a large number of payloads. Highly embedding capacity. Better image quality[8].

4. GLM: It stands for Gray Level Modification. GLM is explained as a method in which Gray Level value of image pixels are modified by using a mathematical function for representation of binary information. For representation of binary information, distinct odd or even value of the gray level is modified
GLM Steganography is a method to map the data by doing modification in gray level values of image pixels. One-to-One mapping is takes place between data bits and image pixel.

**Algorithm:**

**Step1:** Select a set of pixels which would be used for data hiding. Selected list of pixels of image with even and odd gray values.

**Step2:** If gray level value is even then make comparison between gray level values and bit streams; else if gray level value is odd then increment the gray level value of pixel by one unit to make it even.

**Step3:** On making comparison of gray level value with bit stream; if bit stream is “0” then do not change. If bit stream is “1” then decrement gray level value of pixel by 1. Gray level values are changed according to bit stream. Now every bit stream mapped with corresponding selected image pixel i.e. information hidden.

**Advantages:**

No change in image statistics to notice if GLV of pixels are modified by 1- unit. It requires less computational overheads. It consists variable capacity of mapping and can be decided on the basis of mathematical function and amount of data to be mapped.

5. **PIT:** In Pixel Indicator technique, Steganography has made the utilization of RGB images as cover media. This technique used LSB of one of channels R, G or B as an indicator of secrete data existence in other two channels. LSB bits of indicator are randomly available[6]. If we have ‘R’ as indicator in sequence then ‘G’ acts as channel 1 and ‘B’ as channel 2. First 8 Bytes of image stored the size of the secrete message and checked further on the basis of length of message is even, prime or else in table to the message.

<table>
<thead>
<tr>
<th>Indicator Channel</th>
<th>Channel 1</th>
<th>Channel 2</th>
<th>Type of Message</th>
<th>Select Channel from Indicator</th>
<th>Select Binary N-parity bit</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>No hidden data</td>
<td>No hidden data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01</td>
<td>No hidden data</td>
<td>2 bits of hidden data</td>
<td></td>
<td>R</td>
<td>GB, BG</td>
</tr>
<tr>
<td>10</td>
<td>2 bits of hidden data</td>
<td>No hidden data</td>
<td></td>
<td>B</td>
<td>RG, GR</td>
</tr>
<tr>
<td>11</td>
<td>2 bits of hidden data</td>
<td>2 bits of hidden data</td>
<td></td>
<td>G</td>
<td>RB</td>
</tr>
</tbody>
</table>

**Advantages:** This technique analysis considered two parameters as security and capacity. Security related to minimal probability for breaking a Steganography system and the capacity increases normally as the bits to insert increases. This leaves the decision of best bits to insert, to the application and its needs.

**B. Frequency Domain Techniques:** In Frequency Domain or Transform Domain Steganography, modification does not take place directly in original cover image. In this method, alteration is done in orthogonal image of actual cover image rather than direct covert of data bits in cover image. Coefficients are generated by using any of the 2D transform which is used as carrier of covert data in frequency domain. Various Transform Domain Techniques are as:

1. DCT (Discrete Cosine Transform)
2. DWT (Discrete Wavelet Transform)
3. DFT (Discrete Fourier Transform)

**1. DCT:** Discrete Cosine Transform (DCT) uses the Fourier transform to convert the Spatial Domain into Transform Domain. This technique is useful to separate an image into different sub-bands with the respective visual quality. In DCT techniques, DCT Coefficients attained for the carrier image. If the DCT Coefficient value is less than threshold value then data bits inserted in carrier image. If DCT Coefficient value 0, then it should be avoided to embed data within it to avoid visual distortion[5].
2. **DWT:** In Discrete Wavelet Transform (DWT), wavelets are the functions which have zero average value and also attained over a fixed interval. This technique is basically used to perform local analysis and multi-resolution analysis (MRA). MRA is described as the analysis of a signal at different frequencies at different resolutions\[5\]. In 1D-DWT, the cover image is partitioned in two major components: approximate components and detailed components whereas 2D-DWT segmented image in four components. Approximate Component (LL) and others are as Detailed Components (HL, LH, HH ). DWT Components shown as:

<table>
<thead>
<tr>
<th></th>
<th>LL</th>
<th>HL</th>
<th>LH</th>
<th>HH</th>
</tr>
</thead>
</table>

3. **DFT:** Discrete Fourier Transform (DFT) is used to segment a covered image into two values as cosine and sine value[5]s. Fourier transforms the time and space based data into frequency based information. DFT does not provide all frequencies to build an image as result but it only provides the sufficient constitutes to build an original image. Some of the applications includes are as image filtering and image compression[3].

**Applications of Steganography:** It can be used for shielding information, for example in the field of media where copywriting ensures authenticity. Intelligence Agencies can use Steganography for transforming the secret data.

**Conclusion:** Thus this paper concluded that Steganography is a technique of covering the data in such a way that the message could be transmitted secretly and only the sender and receiver knows the way of decrypting that secret message. Further the paper reviewed on Steganography types, advantages, limitations, techniques and its applications.

**References:**


