Performance Enhancement of a Transform Domain Based Steganographic Technique Using Segmentation

Harjeet Kaur¹, Er Divya Goyal²

¹M-Tech Research Scholar, Swami Vivekanand Institute of Engineering, Banur, India
²Assistant Professor, Swami Vivekanand Institute of Engineering, Banur, India

Abstract: 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. The software and links mentioned in this article are just a sample of the steganography tools currently available. As privacy concerns continue to develop along with the digital communication domain, steganography will undoubtedly play a growing role in society. For this reason, it is important that we are aware of Steganography enhances rather than replaces encryption. Messages are not secure simply by virtue of being hidden.

Keyword: Stego-object, Cover-object, Steganalysis, Cover Image, Embedding key, Extraction key, Steganography

1. Introduction

The word steganography is derived from the Greek words stegos meaning cover and graphy meaning writing [1] defining it as covered writing. In image steganography the information is hidden exclusively in images. Steganography is the art and science of secret communication. It is the practice of encoding/embedding secret information in a manner such that the existence of the information is invisible. The original files can be referred to as cover text, cover image, or cover audio. After inserting the secret message it is referred to as stego-medium. A stego-key is used for hiding/encoding process to restrict detection or extraction of the embedded data[2].

Image steganography is the art of hiding information into a cover image. This paper presents a novel technique for Image steganography based on Block-DCT, where DCT is used to transform original image (cover image) blocks from spatial domain to frequency domain. Firstly a gray level image of size M x N is divided into no joint 8 x 8 blocks and a two dimensional Discrete Cosine Transform (2-d DCT) is performed on each of the P = MN / 64 blocks. Then Huffman encoding is also performed on the secret messages/images before embedding and each bit of Huffman code of secret message/image is embedded in the frequency domain by altering the least significant bit of each of the DCT coefficients of cover image blocks. The experimental results show that the algorithm has a high capacity and a good invisibility. Moreover PSNR of cover image with stego-image shows the better results in comparison with other existing steganography approaches. Furthermore, satisfactory security is maintained since the secret message/image cannot be extracted without knowing decoding rules and Huffman table.

Steganography is a technique of information security that hides secret information within a normal carrier media, such as digital image, audio, video, etc. An unauthorized attempt to detect and extract the hidden secret information from stego is known as steganalysis. If any steganalytic algorithm can detect whether given media is a carrier then the steganography algorithm is considered to be broken.

In this paper we consider digital image as carrier and develop a steganography algorithm in spatial domain with LSB replacement based on DCT coefficients of the pixels. The basic LSB based technique simply replaces the LSB plane of the carrier image with the bit stream of secret information.

Computational Parameters:

a) PSNR: Peak signal-to-noise ratio, often abbreviated PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the power corrupting noise that affects the fidelity of its representation.

b) MSE: In statistics, the mean squared error of an estimator is one of many ways to quantify the difference between values implied by an estimator and the true values of the quantity being estimated.

C) CAPACITY: It is size of the data in a cover image that can modified without deteriorating the integrity of image.

d) NODE COUNT: It is the number of nodes count when we hide the information or data behind a image.

2. Related Work

[1]Deeply has research described as the method of Steganography based on embedding encrypted message bits using RSA Algorithm in the 1st least significant (LSB Technique) and last 4 significant bits (Modulus 4 bit technique) of the pixel of image. [2]. Attalla M. Al-Shatnawi has discuss the proposed method is compared with the LSB benchmarking method. It is implemented to hide the secret message "I will come to see you on the first of June” on two Bmp images, with size (24 x 502 x 333) and (24 x 646 x...
The DCT for each block of 8x8 pixels was applied in order to improve the capacity and control the compression ratio.

**RSA Algorithm.**
The algorithm was given by three MIT’s Rivest, Shamir & Adleman and published in year 1977. RSA algorithm is a message encryption cryptosystem in which two prime numbers are taken initially and then the product of these values is used to create a public and a private key, which is further used in encryption and decryption. By using the RSA algorithm we are increasing the security to a level above.

**RSA Encryption and Hash-LSB Encoding**
In this process first we converted cipher text into binary form to convert it into bits. Then by using hash function it will select the positions and then 8 bits of message at a time will be embedded in the order of 3, 3, and 2 in red, green and blue channel respectively. The process is continued till entire message of bits will get embedded into the cover image.

**Embedding Algorithm:**

1. **Step 1:** Choose the cover image & secret message.
2. **Step 2:** Encrypt the message using RSA algorithm.
3. **Step 3:** Find 4 least significant bits of each RGB pixels from cover image.
4. **Step 4:** Apply a hash function on LSB of cover image to get the position.
5. **Step 5:** Embed eight bits of the encrypted message into 4 bits of LSB of RGB pixels of cover image in the order of 3, 3 and 2 respectively using the position obtained from hash function given in equation 1.
6. **Step 6:** Send steno image to receiver.

**Hash-LSB Decoding and RSA Decryption**
In the decoding process we have again used the hash function to detect the positions of the LSB’s where the data bits had been embedded. After retrieving the positions of LSB’s that contain secret data, the receiver will decrypt secret data using RSA algorithm. To apply RSA algorithm receiver will use his/her private key because the secret data have been encrypted by recipient public key. Using receiver private key cipher text will be converted into original message which is in readable for Retrieval Algorithm.

**Retrieval Algorithm**

1. **Step 1:** Receive a steno image.
2. **Step 2:** Find 4 LSB bits of each RGB pixels from steno image.
3. **Step 3:** Apply Hash Function to get the position of LSB’s with hidden data.
4. **Step 4:** Retrieve the bits using these positions in order of 3, 3, and 2 respectively.
5. **Step 4:** Retrieve the bits using these positions in order of 3, 3, and 2 respectively.
6. **Step 5:** Apply RSA algorithm to decrypt the retrieved data.
7. **Step 6:** Finally read the secret message.
5. Results

The results are taken in matlab programming. The PSNR and MSE values are calculated using equation (1) and (2). The Peak Signal-to-Noise Ratio (PSNR) is defined as:

\[
\text{PSNR} = 10 \log_{10} \left( \frac{\text{MAX}_i^2}{\text{MSE}} \right)
\]

Equation (1)

The mean-squared error (MSE) between two images \(I_1(m,n)\) and \(I_2(m,n)\) is

\[
\text{MSE} = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]^2
\]

Equation (2)

Where \(M\) and \(N\) are the number of rows and columns in the input images, respectively.

Images

![Figure 1.1: Image1 (leena)](image1)

![Figure 1.2: Image2 (penguins)](image2)

![Figure 1.3: Image3 (koala)](image3)

Table and Graph

<table>
<thead>
<tr>
<th>Image</th>
<th>Capacity</th>
<th>PSNR</th>
<th>MSE</th>
<th>NC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image1</td>
<td>278528</td>
<td>85.11</td>
<td>.0098</td>
<td>.991</td>
</tr>
<tr>
<td>Image2</td>
<td>835584</td>
<td>91.81</td>
<td>.0036</td>
<td>.993</td>
</tr>
<tr>
<td>Image3</td>
<td>835584</td>
<td>91.43</td>
<td>.0018</td>
<td>.997</td>
</tr>
</tbody>
</table>

![Figure 1.4: Capacity Chart](capacity_chart)

![Figure 1.5: PSNR Chart](psnr_chart)

![Figure 1.6: MSE Chart](mse_chart)

![Figure 1.7: NC Chart](nc_chart)
6. Conclusion

This research work has been implemented to enhance the steganography technique so that the quality of the image remains the same. To implement our objectives, we have used Neural Network in a combination with ENCRYPTION MECHANISM along with pixel management.

We overall concluded that managing the pixels to a deeper level increases the capacity of the image to hide certain messages. Neural Network has been found effective enough to find pixels to merge the data bits without much affecting the original pattern of the image. It has been also concluded that if we can encrypt the data up to some level before merging it to the image, it may enhance the chances of security into the image embedding.

7. Future Scope

The current work does not comprises with the noisy image. Future research workers can get to see how the current scheme goes with different levels of noise. The effect of different types of noise may also put some different effect on the approach. Also some other methods of Neural Network can be also tried.

References

[3] Adel Almohammad Robert M. Hierons “High Capacity Steganography Method Based Upon JPEG” The Third International Conference on Availability, Reliability and Security The JPEG standard uses 8x8 quantization tables,
[12] Natee Vongurai and Suphakant Phimoltares, “Frequency-Based Steganography Using 32x32 Interpolated Quantization Table and Discrete Cosine Transform” 2012 Fourth International Conference on Computational Intelligence, Modelling and Simulation.


Author Profile

Harjeet Kaur is Student of M.Tech in the Department of Computer & Sci Engineering at Swami Vivekanand Institute of Engineering, Banur under Punjab Technical University, Jalandhar. She has done B.Tech From Yadawindra College of Engg & Tech Talwandi Sabo(Punjabi Uni Patiala).

Er Divya Goyal is the Asst. Proff in the Department of Computer & Sci Engineering at Swami Vivekanand institute of Engineering, Banur under Punjab Technical University, Jalandhar. She has done her B.tech From PIET college of Engg & Technology under PTU & her M.Tech is from Lovely university Jalandhar.