Security of Digital Images Using Hybrid Steganography Technique with Statstical and Histogram Analysis

Mr. Kirtan Sanghvi¹ Mr. Viral Sanghvi² Mr. Nitin Kanzaria³

¹Department of Computer Engineering, Shree Pandit Nathulalji Vyas Technical Campus, India ²,³CU Shah College of Engineering and Technology, India

Abstract—To protect private information from unauthorized access robust and secured data hiding technique needed. Steganography is a hiding technique in which third party can not get little bit idea about hiding the data(images, text, audio, video etc.) Good Steganography technique must provide high embedding capacity, security and compressed secret image. In this paper firstly the DCT(Discrete Cosine Transform) of cover image is find. The stego image is constructed by hiding secret image in LSB(Least Significant Bit) of the cover image in random location based on threshold or pseudo random no. Huffman encoding is performed over the secret image before embedding. High security provide since the secret image cannot be extracted without knowledge decoding rules, Huffman table and key matrix. PSNR(Peak Signal To Noise Ratio) value is used to compare the result which existing steganography approaches. We also use Histogram analysis to compare cover image and stego image after embedding secret image. 

Key words: Steganography, LSB, DCT, Huffman Encoding, PSNR, Histogram Analysis

I. INTRODUCTION

The word Steganography is a Greek word, Steganos, which means covered or hidden and graphy means writing or painting. So, meaning of Steganography is hidden writing[2][3][4][6][8]. The image in which we hide is known as cover image and the image after hiding secret image is known as stego image[3]. Main goal of Steganography is to unauthorized party could not detect differentiate between cover image and stego image. Steganography can be used as both legal and illegal interests, e.g., military may use it for protecting secret information, medical for hiding patient information while terrorists may use it for spreading terrorist information[9][10].

II. RELATED WORK

A. LSB (Least Significant Bit) Technique

In spatial domain technique, secret image is directly embedded in to cover image. LSB Technique is a spatial domain technique. In this technique MSBs bits of secret information replace with LSBs pixel of the cover image. It provide high embedding capacity but if embed secret information in sequential bit of cover image then provide low security and easily extracted private information by unauthorized person.2 or upto 4 MSBs pixel can embedded into cover image LSBs pixel[5].

Example of LSB Techniques[3]

A Bit Pattern for 9-pixel of an 8-bit Gray Image

| 00101101 | 00011100 | 11011100 |
| 10100110 | 11000100 | 00001100 |
| 11010010 | 10101101 | 01100011 |

When Decimal no. 200 Which Binary Representation is 11001000, Was Embedded into the LSB of This Part of an Image.

| 00101101 | 00011101 | 11011100 |
| 10100110 | 11000101 | 00001100 |
| 11010010 | 10101100 | 01100011 |

Only 3 bits display underline are modified. Our eye can not perceived these difference

Discrete Cosine Transform

It transform the image from spatial domain to frequency domain and separate image into sub-bands i.e high, middle and low frequency sub bands[2]. First DCT apply on Cover image. Then find potential pixel based on threshold value or pseudo random no. So secret image information hide at random place. this way it provide security, unauthorized
person cannot easily detect secret information\(^6\)\(^8\). LSB technique provide high embedding capacity, DCT technique provide high security. Combine of both technique provide high embedding capacity with security\(^6\)\(^9\).

The DCT is calculated using equation 1:

\[
F(k, l) = \frac{1}{4} C(k) C(l) \sum_{x=0}^{7} \sum_{y=0}^{7} f(x, y) \cos \left( \frac{\pi (2x+1)k}{16} \right) \cos \left( \frac{\pi (2y+1)l}{16} \right)
\]

for \(x=0,...,7\) and \(y=0,...,7\)

\[
C(k) = \begin{cases} \sqrt{2} & \text{for } k = 0 \\ 1 & \text{otherwise} \end{cases}
\]

**B. Huffman Encoding**

Huffman encoding is a lossless compression technique. Secret image is encoded using Huffman encoding and then map one symbol of cover image into one codeword. Then convert Huffman encoded bit into 1-D bit stream\(^6\). Huffman table represent Binary code of each symbol of cover image. It provide advantage like lossless compression, increase the security because Huffman encoded bit does not disclose anything because to extract exact meaning the Huffman table is required and also provide authentication if any single bit change in the Huffman Coded bit stream Huffman table will not be able to decode the data\(^2\)^\(^3\)^\(^6\).

1) **Steganography parameter**\(^6\)

- **Capacity**

Capacity is represented as size of secret information proportional to the size of stego image\(^6\).

\[
\text{Capacity} = \frac{\text{No of bits per pixel in SecretImage}}{\text{No of Bits per pixel in cover image}}
\]

(2)

- **Mean Square error (MSE)**

It is used to measure the distortion in the image between cover image and stego image\(^6\).

\[
\text{MSE} = \frac{1}{N*N} \sum_{i=1}^{N} \sum_{j=1}^{N} [(C(i,j)-S(i,j))^2]
\]

(3)

Where CI(i,j) represent the pixel of the cover image.

SI(i,j) represent the pixel of the stego image.

N*N represent the cover image size.

- **Peak Signal To Noise Ratio (PSNR)**

measurement the quality between cover image and stego image. measured in db.

\[
\text{PSNR} = 10 \times \log(255^2/\text{MSE})
\]

(4)

- **Correlation Coefficient (CC)**

Used to measure the similarity between cover image and stego image\(^8\).

\[
\text{CC} = \frac{\sum(x_i - \overline{x})(y_i - \overline{y})}{\sqrt{\sum(x_i - \overline{x})^2 \sum(y_i - \overline{y})^2}}
\]

(5)

**III. IMPLEMENTATION AND RESULTS**

**A. Embedding Algorithm**

**Input:** Cover image M * N and a secret image.

**Output:** A stego Image.

**Step 1:** Apply DCT on the cover image using equation Eq (1).

**Step 2:** Find Huffman table for secret image.

**Step 3:** Apply Huffman encoding technique using Huffman table found in Step-2 on Secret Image.

**Step 4:** put pixel in Cover Image till end of 1-D bits stream of Huffman codes based on psudeo random no.

**Step 5:** Set value to 1 for that location in the key matrix.

**Step 6:** Stego Image which is look similar to Cover Image is generated.
B. Extracting Algorithm

- Stego Image
- Key Matrix
- Extracting Using LSB
- 1D bits Stream of Huffman Codes
- Huffman Table
- Huffman Decoding
- Secret Image

Fig. 3: The block diagram of extracting Process

C. Recovery Algorithm

**Step 1:** Extract the least significant bits of each of the stego image to get the bit stream Huffman codes using key matrix.

**Step 2:** Decode the bit stream of Huffman codes that are extracted in Step-1 using the Huffman table.

**Step 3:** Construct the Secret Image according to Size

**Step 4:** End.

The stego image 20*20, 80 * 80 and 120 * 120 shown in fig 4 and histogram analysis shown in fig 6.

D. Histogram Analysis

The histogram analysis plays a vital role in image steganography. The histogram analysis is performed on both cover image and stego image. The stego image shows minimum changes in the histogram compared to the cover image histogram. From these minimum changes in the histogram of the stego image, it is difficult to infer that secret data is hidden.

<table>
<thead>
<tr>
<th>Secret image size</th>
<th>4-LSB replace</th>
<th>4-LSB + DCT</th>
<th>4-LSB + Huffman</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSE</td>
<td>PSNR</td>
<td>CC</td>
<td>MSE</td>
</tr>
<tr>
<td>20 X 20</td>
<td>0.1 1</td>
<td>1.0 1</td>
<td>0.1 1</td>
</tr>
<tr>
<td>40 X 40</td>
<td>0.5 2</td>
<td>1.0 1</td>
<td>0.5 2</td>
</tr>
<tr>
<td>60 X 60</td>
<td>1.2 2</td>
<td>0.9 3</td>
<td>1.3 2</td>
</tr>
<tr>
<td>80 X 80</td>
<td>2.2 2</td>
<td>0.9 3</td>
<td>2.4 2</td>
</tr>
<tr>
<td>100 X 100</td>
<td>3.5 2</td>
<td>0.9 3</td>
<td>3.7 2</td>
</tr>
<tr>
<td>120 X 120</td>
<td>5.2 3</td>
<td>0.9 3</td>
<td>5.3 3</td>
</tr>
<tr>
<td>140 X 140</td>
<td>6.9 3</td>
<td>0.9 3</td>
<td>7.1 3</td>
</tr>
<tr>
<td>160 X 160</td>
<td>9.1 3</td>
<td>0.9 3</td>
<td>9.4 3</td>
</tr>
<tr>
<td>180 X 180</td>
<td>11.5 3</td>
<td>0.9 3</td>
<td>11.8 3</td>
</tr>
</tbody>
</table>

Table 1: Comparison of all technique parameter

<table>
<thead>
<tr>
<th>Cover img</th>
<th>Secret img size</th>
<th>Lsb</th>
<th>Lsb+DCT</th>
<th>Lsb+DCT+ Huffman</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSNR</td>
<td>PSNR</td>
<td>PSNR</td>
<td>PSNR</td>
<td></td>
</tr>
</tbody>
</table>
IV. CONCLUSION

We see different technique to perform steganography like DCT, HUFFMAN ENCODING and LSB. The main goal is achieve security, high capacity and robustness. LSB technique which help to increase capacity. We see DCT technique which provide randomization. We see the work of Huffman encoding which use for compress the secret image. Hybrid technique use like LSB, DCT, HUFFMAN ENCODING combination gives better result compare to all other technique. The secret image is also found identical.

REFERENCES


