HASH BASED APPROACH FOR SECURE IMAGE STEGANOGRAPHY USING CANNY EDGE DETECTION METHOD

Kritika Singla¹, and Sumeet Kaur²

¹Post Graduate Student, Yadavindra College of Engineering, Punjabi University, Patiala
E-mail: kritikasingla23@gmail.com
²Assistant Professor, Yadavindra College of Engineering, Punjabi University, Patiala
E-mail: purhasumeet@yahoo.co.in

ABSTRACT

In this paper, hash based approach for secure steganography using edge detection is presented. Besides employing the hash based approach as a fundamental stage, we take advantage of edge detection technique. The proposed scheme achieves high embedding capacity and enhances the quality of the encoded image. The proposed scheme first detects the edges in the image by well known canny method and then the hash sort is used to embed the text data in to the edges of the color image. The hash function provides a secure and fast approach for image steganography.

Keywords: Decoding, Encoding, Hash function, Steganography.

1. INTRODUCTION

Steganography is the art of hiding and transmitting data through apparently innocuous carriers in an effort to conceal the existence of the data, the word Steganography literally means covered or hiding writing as derived from Greek. Steganography has its place in security. It is not intended to replace cryptography but supplement it. Hiding a message with Steganography methods reduces the chance of a message being detected. If the message is also encrypted then it provides another layer of protection [1]. Steganography and cryptography are cousins in the spy craft family. Cryptography scrambles a message so it cannot be understood. Steganography hides the message so it cannot be seen. A message in cipher text, for instance, might arouse suspicion on the part of the recipient while an “invisible” message created with steganographic methods will not [2].

There are lots of algorithms used in image steganography area. However, they have their own weaknesses and strengths. Since Least Significant Bit (LSB) insertion method is one of the simplest data hiding techniques, it has long been a focus for researchers to propose attacking methods and they are called either steganalytic or steganalysis attacks. It is proved that sometimes simple LSB method is not secured at all [3].

In this study most of the effort is done to get a better imperceptibility and increasing capacity without losing stego-image quality. Hash function is used to generate a pattern, which is random selection of edge pixels, for more security and better stego-image quality.

2. PROPOSED SCHEME

In this section proposed method for text encoding and decoding is given.

A. Proposed System Model

The System model of proposed work is described in Figure. 1 and Figure. 2. Figure. 1 shows the encoding model and Figure.2 shows the decoding model.

Figure 1: Proposed Encoding Model

Above shown Figure. 1 is about our encoding process in which we detect edges to embed text data in edges using hash function, the proposed algorithm for encoding data in image is as follows in section B.

B. Proposed Algorithm for Encoding Data in Image

Step 1: Read the RGB image I of size rxc.
Step 2: Detect the edges of the input image by canny method and use these edge pixels as the hash key (K).
Step 3: Read the text file (.txt) and store the data in an array list (Lc).
Step 4: The hash function uses the hash key (K) and the text data to generate a pattern i.e. sequence of hash values those are the position of the pixels where data will be stored.
Step 5: The generated pattern is stored in the array list \((L_p)\).
Step 6: The ASCII value of \(L_c[i]\) is replaced with blue-byte of \(L_p[i]\).
Step 7: The output is the image containing coded data.

After encoding the decoding process is here, Figure 2 below shows the decoding model in which hash key is used to decode the data from the text encoded image, the proposed algorithm for decoding data from image is as follows in section C.

C. Proposed Algorithm for Decoding Data from Image

Step 1: Read the RGB image that contains encoded information.
Step 2: Input hash key is used with hash function to generate the pattern where data has been stored.
Step 3: Values of blue-byte at \(L_p[i]\) are read. As each byte contains the ASCII value of the character, the read ASCII value is converted to the character and each character is written to text file.
Step 4: The output is the text file that contains the decoded data from the image.

3. EXPERIMENTAL RESULTS

To demonstrate the effectiveness of proposed algorithm, MATLAB simulations are performed. We have taken different RGB images and text files for simulation results. Figure 3 shows original images of size 512 × 512 pixels, Figure 4 shows the edge detected of the original images, Figure 5 shows the text encoded images, Figure 6 shows histograms of original images and Figure 7 shows histograms of text encoded images.

Table 1: PSNR Output for Text Encoding

<table>
<thead>
<tr>
<th>Text Data</th>
<th>Lena</th>
<th>Peppers</th>
<th>Baboon</th>
</tr>
</thead>
<tbody>
<tr>
<td>849 Bytes</td>
<td>46.7704</td>
<td>42.4704</td>
<td>44.5141</td>
</tr>
<tr>
<td>1698 Bytes</td>
<td>43.1161</td>
<td>39.8468</td>
<td>41.4249</td>
</tr>
<tr>
<td>2547 Bytes</td>
<td>40.4854</td>
<td>37.9358</td>
<td>37.7590</td>
</tr>
<tr>
<td>3396 Bytes</td>
<td>39.5810</td>
<td>36.7382</td>
<td>36.3541</td>
</tr>
<tr>
<td>4287 Bytes</td>
<td>38.5342</td>
<td>35.7352</td>
<td>35.1693</td>
</tr>
</tbody>
</table>

In the above table, PSNR (peak signal to noise ratio) is calculated for all the standard images.

In Figure 8, The graph shows that as the data to be hide increases, PSNR decreases and Lena image results are better than peppers and baboon image results.
4. CONCLUSION

In this paper, we have proposed a hash based approach for secure steganography scheme using edge detection. The proposed method produces high capacity and higher quality stego images under HVS due to use of edge detection method. Experimental results show that the proposed scheme is successful in not only achieving a high embedding payload but also in obtaining a stego image of satisfactory quality.

REFERENCES


