Steganalysis using hopping cluster algorithm

Ramandeep Kaur¹, Arshdeep Singh²

¹Assistant professor, Adesh Institute of Engineering and Technology, Faridkot, India Rkaur2310@gmail.com

²(Member IEEE) Department of Computer science, Adesh Institute of Engineering and Technology, Faridkot, India Arsh.sra01@gmail.com

Abstract: This work proposes a steganalysis scheme based on Hopping cluster algorithm. The proposed scheme focuses on detection of the steganography algorithm used rather than detection of hidden message only. Even hidden message can also be detected using this algorithm. Experimental results shows that message can also be detected but if once steganography algorithm is detected all the images steganographed can be detected very easily so this algorithm is quite effective than previous algorithms.

Keywords: Data hiding, Hopping neighbor, color cluster, Secret message, Covered Writing.

1. Introduction

Digital steganography is a technique to embed secret message into digital media to secretly communicate, the purpose of steganalysis is to detect the secret hidden data in a digital media. In most steganalysis techniques, some sensitive features extracted from cover and stego media and those sensitive features examined deeply to find the hidden message.

A number of steganalysis tools are already developed which can detect the message from sensitive features and many of these are pretty effective but these techniques works on such a way for example it focuses on disarming one bomb at a time rather than knowing maximum number of possible bomb types and categorizing all the tools to disarm them under these types so that so that as soon as we detect a bomb just check that in which category it lies and applying the specific method rather than trying random blind methods. Similarly in case of steganalysis rather than trying all possible ways to detect message once detect which algorithm is used in steganography and then only specific method for message detection can be applied from present effective algorithms.

This work proposes hopping cluster algorithm which focuses on detection of basic properties of an image and according to change in the properties we can find out which steganography algorithm is used.

2. PROPOSED STEGANALYSIS SCHEME

The proposed steganalysis scheme is comprised of two parts: Algorithm detection and Message detection. In the first part, we check the basic properties of algorithm as least significant bits, color clusters, pixel trace based and then on the basis of change in basic properties we can detect algorithm used in this specific research we have used two algorithm detection one is LSB and other is hopping cluster algorithm. In the second part, we apply specific algorithm for detection of message.

A. Steganography Algorithm Detection:

In this phase we will focus on change in basic properties of image as we will detect color pixels present in the image as we will find red, black and white pixels present in image and then we will find out the maximum color cluster if we find suspicious pixels on any palot Red, Green or Blue of the largest color cluster we can say the algorithm used for steganography is Hopping cluster algorithm. And if we find the least significant bits as suspicious pixels then we can say the algorithm used is LSB for steganography. We can check for any number of algorithms here but in this specific research its limited to these two algorithms only.

Process Image

Check basic Properties

If Suspecious bits

Largest color pixel cluster Bits

LSB Algorithm

Hopping Cluster Algorithm

Ramandeep Kaur IJECS Volume 4 Issue 2 February, 2015 Page No.10356-10358
B. Message Detection(Hopping Cluster Algorithm):

In this phase while we get the algorithm used for steganography if the algorithm is LSB we will use any effective present Steganalysis algorithm for LSB but if algorithm is Hopping cluster algorithm than we will follow following steps for message detection.

- Processing to find the colors to find number of major colors and no. of clusters.
- Counting of colors Red, Black, White etc. (to find out the biggest cluster).
- Search the pixels where Code can be placed possibly (suspicious pixels).
- Trace alterations of the media properties.
- Extract Encoded message and reveal message Using ascii formulation range filtering.

3. RESULTS

In the implementation, we used the proposed steganalysis scheme to detect the secret data embedded by two phases. In results we will display the results related to hopping cluster algorithm.

These images show how GUI interface shows results. In figure :3.2 original message and message revealed are shown.

<table>
<thead>
<tr>
<th>Image Name</th>
<th>Red Pixel</th>
<th>Black Pixel</th>
<th>White Pixel</th>
<th>Original Message Length</th>
<th>Revealed Message Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.jpg</td>
<td>787</td>
<td>43349</td>
<td>4612</td>
<td>10</td>
<td>18</td>
</tr>
<tr>
<td>2.jpg</td>
<td>0</td>
<td>211456</td>
<td>13179</td>
<td>12</td>
<td>12</td>
</tr>
<tr>
<td>3.jpg</td>
<td>0</td>
<td>8050</td>
<td>171551</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>4.jpg</td>
<td>19976</td>
<td>50280</td>
<td>46523</td>
<td>11</td>
<td>25</td>
</tr>
<tr>
<td>5.jpg</td>
<td>12601</td>
<td>0</td>
<td>164793</td>
<td>12</td>
<td>21</td>
</tr>
<tr>
<td>6.jpg</td>
<td>3148</td>
<td>3216</td>
<td>11219</td>
<td>9</td>
<td>14</td>
</tr>
<tr>
<td>7.jpg</td>
<td>219697</td>
<td>8518</td>
<td>790940</td>
<td>10</td>
<td>15</td>
</tr>
<tr>
<td>8.jpg</td>
<td>1839</td>
<td>360550</td>
<td>33149</td>
<td>11</td>
<td>14</td>
</tr>
<tr>
<td>9.jpg</td>
<td>0</td>
<td>641521</td>
<td>4816</td>
<td>12</td>
<td>12</td>
</tr>
<tr>
<td>10.jpg</td>
<td>0</td>
<td>391817</td>
<td>83623</td>
<td>10</td>
<td>10</td>
</tr>
</tbody>
</table>

Percentage Successful:
1. With Black and white images = 100%
2. With colored images = 75%

In table I we have discussed ten different images and calculated red, black and white pixels for each image and when we tried to reveal the message what we have received and the original message all these comparisons are shown in this table.
4. CONCLUSION

According to analysis we can say that Steganalysis using hopping cluster algorithm is almost more than 70% successful with jpeg format and if we consider it for only Black and white JPEG images it increases up to 100%. So basically when we use colored images there may be chances of image quality loss, and the message revealed will not be the exact message it may include some non-relevant characters. But as we have defined in our objectives that our prime focus is not about message it’s about the detection of the algorithm used for steganography.

In the perspective of Algorithm detection, we can say that this algorithm is quite useful as we have been checking only for color clusters in this algorithm and the algorithm is more than 95% successful in detecting hopping cluster algorithm and we can further apply the same thing to detect LSB or any or multiple algorithm detection.

References


