Robust Watermarking using Genetic Algorithm in DCT Domain

Raj Vikram Singh¹, Subodh Waria², Rajiv Kumar Singh³, Harsh Vikram Singh⁴

¹, ²Department of Electronics & Communication, IET Lucknow
³Department of Electronics, KNIT Sultanpur

Abstract

In this paper, a novel and efficient data hiding using Genetic Algorithm in DCT Domain implemented. Watermarking is an essential zone of research as of late including various applications. It is the investigation of inserting data into the cover picture viz., content, video, and picture (payload) without making measurably huge change the cover picture.

Keywords: Least Significant Bit (LSB), 5th Significant Bit, Discrete Cosine Transform (DCT), Digital Watermarking

1. Introduction

The word steganography (Data Hiding) is gotten commencing the ancient Greek vocabulary stegos means cover and graafia means hiding [1]. In image hiding the data is concealed only in images. The uniqueness can be alluded to as cover content, cover picture, or cover sound. After embedding the mystery data it is alluded to as stegomedium. A stegokey is utilized for concealing/encoding procedure to limit location or extraction of the implanted message [2]. Imperceptible hiding for a dependable device. So pictures are caught with a computerized camera for later incorporation in news articles. Here, it is the craving of a news organization to confirm that a picture is consistent with the first catch and has not been altered to adulterate a scene [3-8]. For this situation, an undetectable watermark is installed at catch time; its quality at the season of distribution is planned to show that the picture has not been gone to since it was caught [9-12].

Numerous specialists have utilized DCT, DWT and different strategies for watermarking yet at the same time there is an expansive extent of change for concealing the information in Images. At first, existing calculations will be utilized for watermarking and further vigorous calculations will be proposed through this work for information stowing away in Images. The result of research will be valuable for different applications, for example, Military, Network security, information verification and so on [13-18].

In this paper Section 2 provides the definitions and algorithms of all three methods i.e. LSB Insertion Method, 5th Significant Bit Insertion Method and DCT Method. Section 3 provides simulation Results using MATLAB and comparative chart for analysis. Finally section 4 concludes the paper.

2. Proposed Methods and their Algorithms for Digital Watermarking

2.1 Least Significant Bit (LSB)

Digital Watermarking based on LSB is simplest method, used to embed the secret data into the least significant bits of the pixel.

Part 1: Embedding Algorithm

(i) Read the secret key
(ii) Convert secret key into binary form
(iii) Compare both the secret keys
(iv) If both secret keys are same, Extract stream of bits of secret text message from Watermarked image by extracting the LSBs sequencely.
(v) Rearrange the extracted bits and regenerate the ASCII secret text.

2.2 5th Significant Bit Insertion Method

In this method, the 5th significant bit of each 8-bit pixel of a cover image is used to hide the binary data. To hide 240 (11110000) can be hidden in the first eight bytes of 8-bit grayscale image.

Result:

<table>
<thead>
<tr>
<th>Binary</th>
<th>ASCII</th>
</tr>
</thead>
<tbody>
<tr>
<td>00101111</td>
<td>00101111</td>
</tr>
<tr>
<td>11101001</td>
<td>11001000</td>
</tr>
</tbody>
</table>

Part 1: Embedding Algorithm

(i) Read cover
(ii) Read the hidden message
(iii) Read the Secret key
(iv) Convert the secret text into binary form
(v) Encoding: Hide stream of bits of secret text message into the image at 5th significant bit positions sequencely.
(vi) Save the Watermarked image

Original as well as hidden Watermarked images are shown in Figure 3 and Figure 5 respectively.

Part 2: Algorithm to Extract Secret Text Message

Extracting is done as:
(i) Read the Watermarked image.
(ii) Read the Secret Key
(iii) Convert the secret key into binary form
(iv) Extract stream of bits of Secret key
(v) Compare both the secret keys
(vi) If both secret keys are same, Extract stream of bits of secret text message from Watermarked image by extracting the 5th significant bit sequencely.
(vii) Rearrange the extracted bits and regenerate the ASCII secret text.

2.3 Proposed DCT Algorithm

Part 1: Embedding Algorithm

Embedding is done as:
(i) Reading original cover image I of size (M,N) in BMP.
(ii) Read the Secret text message
(iii) Read the Secret Key.
(iv) find the length of the secret text (T)
(v) Find the maximum text length which can be embedded in the Image(Tmax)
(vi) If Tmax > T
(vii) Convert cover image into Blocks. Each Block consists of 64 pixels (8x8).
(viii) Perform DCT to convert spatial Domain into Transform Domain and get 64 DCT coefficients of each (8x8) pixels block.
(ix) Convert the secret text into n-bit binary form (Dk).
(x) For Dk=1 to n,
Hide the Dkth bit of the secret message into Dkth DCT block of the cover image as follows:
   a) If bit of binary message = "0",
      B(i,j) should be greater than B(u,v). If B(i,j) is less than B(u,v) than interchange the value of these two coefficients.
   b) If bit of binary message = "1",
      B(u,v) should be greater than B(i,j). If B(u,v) is less than B(i,j) than interchange the value of these two coefficients.
Where B(i,j) and B(u,v) are the two mid-band DCT coefficients of Dkth block of the cover image.
(xi) Apply Inverse DCT to reconstruct the image by recombining all the blocks.
(xii) Save the Watermarked image I(M,N) in BMP format of size MxN

Part 2: Extracting Algorithm

The extracting is done as:
(i) Reading the Watermarked image I of size MxN.
(ii) Read the secret key.
(iii) Convert the secret key into binary form
(iv) Extract stream of bits of secret key
(v) If both secret keys are same, Convert Watermarked image into Blocks. Each Block consists of 64 pixels (8x8).
(vi) Perform DCT to convert spatial Domain into Transform Domain and get 64 DCT coefficients of each (8x8) pixels block.
(vii) For Dk=1 to n,
Extract the Dkth hidden bit ‘bk’, using relationship given below:
\[ b_k = \begin{cases} 
0, & \text{if } B(i,j) > B(u,v) \\
1, & \text{if } B(i,j) < B(u,v) 
\end{cases} \]
Where, ‘bk’ is the bit of the secret text.
(viii) Rearrange the extracted bits and regenerate the ASCII secret text.

3. Results and Analysis

Peak Signal to Noise Ratio (PSNR) as well as Mean Square Error (MSE) are mostly applicable parameters for feature measure and their corresponding equations are also given below. [9] Consider two images, x (a, b) and y (a, b) of MxN dimensions. The formula for mean square error is [12]
\[ \text{MSE} = \frac{1}{MN} \sum_{a=1}^{M} \sum_{b=1}^{N} (x(a,b) - y(a,b))^2 \]
\[ \text{PSNR} = 10 \log_{10} \left( \frac{255}{\sqrt{\text{MSE}}} \right) \]

From figure 5, it can be obeserved that, for the same length of the secret text, the PSNR values are not same. In LSB Method, the PSNR values are comparatively high. It shows that the imperceptibility of hidden picture is comparatively high. In 5th significant bit insertion method, the PSNR values are less than the LSB Method but more than the DCT Method. It shows that the imperceptibility of the watermarked image is better than the DCT Method.
Method but less than LSB Method. In case of the DCT Method, the PSNR values are comparatively low.

From figure 7, it can be observed that, using the LSB Method or using the 5th significant bit insertion method, the bit error rates are almost same. In case of the DCT Method, the BERs are comparatively high. It shows that, for the same length of the secret text, DCT Method changes more number of bits of the image.

The conclusion of the analysis, that have been conducted in this section, is tabulated in following table.

<table>
<thead>
<tr>
<th>Table 1: The Conclusion of all analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Items</strong></td>
</tr>
<tr>
<td>Domain</td>
</tr>
<tr>
<td>Security</td>
</tr>
<tr>
<td>Detection</td>
</tr>
</tbody>
</table>

4. Conclusion

This paper has presented three algorithms i.e. LSB insertion Method, 5th Significant Bit Insertion Method and DCT Method for data hiding. It can be concluded from table that present method is very useful for watermarking.

References


