Efficient Steganography Algorithm Based on DCT and Entropy Thresholding Technique

Dr. Paramjeet Singh  
Professor, Dept. of CSE, GZSCCET, Bathinda, Punjab, India

Satvir Singh  
GZSCCET  
Bathinda, Punjab, India

Dr. Shaveta Rani  
Professor, Dept of CSE, GZSCCET  
Bathinda, Punjab, India

Abstract— Steganography is the special art of hiding important and confidential information in appropriate multimedia carrier. It also restrict the detection of hidden messages. In this paper we propose steganographic method based on dct and entropy thresholding technique. The steganographic algorithm uses random function in order to select block of the image where the elements of the binary sequence of a secret message will be inserted. Insertion takes place at the lower frequency AC coefficients of the block. Before we insert the secret message. Image under goes dc transformations after insertion of the secret message we apply inverse dc transformations. Secret message will only be inserted into a particular block if entropy value of that particular block is greater then threshold value of the entropy and if block is selected by the random function. In Experimental work we calculated the peak signal to noise ratio(PSNR), Absolute difference, Relative entropy. Proposed algorithm give high value of PSNR and low value of Absolute difference which clearly indicate level of distortion in image due to insertion of secret message is reduced. Also value of relative entropy is close to zero which clearly indicate proposed algorithm is sufficiently secure.

Keywords— Discrete cosine transform, Absolute difference, Relative entropy, Joint photographic expert group, Peak Signal to noise ratio.

I. INTRODUCTION

Steganography is the art of hiding important information so that no unauthorized person should able to access that important information. This task is completed through hiding the information in other multimedia. The ultimate performance of the steganographic algorithms can be measured by two parameters embedding capacity and detectability. Embedding capacity means maximum amount of data that can be inserted in the respective cover image. So that distortion level should be minimum and a normal person should not be able to detect that some information is hidden in image. It should be exactly looks equivalent to the cover image. Capacity of the image can be increased by selecting appropriate location where to insert the secret information. but one thing should be taken care that their should negligible probability of detecting the message with in the image. Data are embedded into the images commonly by two methods, one is spatial domain method in which bits of the secret message is directly inserted into least significant bits of image pixels. Where as in the frequency domain method cover image is firstly transformed into frequency domain using discrete fourier transform(DFT), discrete wavelet transform (DWT), Discrete cosine transform (DCT). so finally our secret message is inserted in the transformed coefficients. Now we should not mix up the concept of cryptography and steganography. Cryptography just convert the original data into some other form, so that it become unreadable and non understandable for any unauthorized person. Where as steganography hides the secret data within other multimedia like image files, audio files, video files. up to the capacity so that our secret message remain undetectable. Some times combination of both cryptography and steganography give us high level of security to our important information. Some new steganography methods which are based on the joint photographic expert group and modification of the quantization table. In those methods secret message is firstly encrypted and then finally it is embedded in the coefficients located in the middle frequency area of the cover image. in some methods lossless and reversible embedding of secret data in each block of DCT coefficients based on the compressed image technique JPEG is used. in this method two successive zero coefficients of the medium frequency components in each block are used to hide our most important secret data. There is a reversible data hiding method which is based on the DCT of the cover image. The image which we have taken as cover image is divided into different frequencies, then finally the secret message is embedded into the high frequency parts. Basically in our proposed method we insert the secret message in the lower ac coefficients as zero ac coefficients occur at middle and high frequency, so if we modify them they will break the structure of the continuous zeros. As abrupt non zero values can give a hint of the secret message.
II. LITERATURE REVIEW

A. Soria[1] in frequency domain Soria introduced a new steganographic algorithm. In this method 64 bit private key is used in order to determine the locations where the secret message is inserted after applying entropy thresholding technique.

C.L. Velasco-Bautista[2] this method does not use 64 bit private key, but present entropy thresholding method, where the secret message is inserted in the DCT domain.

S. Berres and A. Soria-Lorente [3] this method uses one public key and one private key to generate a binary sequence of pseudorandom numbers that indicate where the elements of the binary sequence of a secret message will be inserted. It improve the level of imperceptibility analyzed through the PSNR values.

A. Westfeld [4] introduced the F5 steganographic algorithm, where, instead of replacing the LSB of the quantized DCT coefficients by the secrets bits, the absolute value of the coefficients is reduced by 1. Since the F5 algorithm randomly chooses DCT coefficients to embed the secret bits it is strong against the Chi square attack.

C. Chang, T. Chen and L. Chung. [5] presented a new steganography method based upon joint photographic expert group (jpeg) and a quantization table modification. In this case the secret message is first encrypted and then embedded in the 26 coefficients located in middle frequency area of the cover image. As the high frequency ac coefficients have continues zeros so it become difficult to safely insert the secret message into those coefficients. As abrupting the sequence of continues zeros can give the clear hint of existence of the secret message into the high frequency coefficients.

C. Lin, S. Tseng, C. Chang. [6] proposed a lossless and reversible embedding of secret data in each block of DCT coefficients based on the compressed image technique JPEG. In this scheme, two successive zero coefficients of the medium-frequency components in each block are used to hide the secret data.

III. PROBLEM FORMULATION

Nowadays, there is a huge risk that our important information may be detected which we think that is protected by using steganographic algorithms. Some methods have limitation of having low PSNR (peak signal to noise ratio) which means distortion in the stego image can be easily detectable when the secret message is inserted in the cover image. The value of absolute difference is also high in those methods. Which also give us the clear indication that overall distortion level in the image is high. So the over all difference between the cover image and Stego image is high. Also the values of the relative entropy are not close to zero, which affirms that those steganographic system are not sufficiently secure.

So to overcome this problem we proposed better and efficient algorithm for stegnography which improves PSNR, lowers the value of absolute difference and make stegnography algorithm more secure by having value of relative entropy close to zero.

IV. RESEARCH METHODOLOGY

STEP 1: It splits the cover image up into non overlapping blocks of 8*8 bytes. These blocks are made so that we can individually calculate and analyzed the entropy of blocks. We can compare the entropy of the block with overall mean entropy.

STEP 2: Calculate the Discrete Cosine Transform (DCT) coefficients for each block.

So dct coefficients $B_{K_{U,V}}$ For each 8*8 byte matrix ($B_{I,J}$)

STEP 3: Compute the entropy of each block.

$$E_K = \sum_{0 \leq U, V \leq 7} |B_{K_{U,V}}|^2$$

STEP 4: calculate the mean entropy ($E'$) of all transformed blocks. So that in further step we can take it as a threshold value in order to decide weather we have to select that particular block for embedding the secret message into it or not.

STEP 5: Now take this mean entropy as threshold entropy and compare with the entropy of all blocks. Now select those blocks only whose entropy value is above threshold value. If $E_K > E'$ then

("select the block for embedding bits of secret message")

Else

("block is not selected for embedding bits of secret message")

STEP 6: Now apply the random function in Mat Lab to randomly select the block in which further AC coefficients of low frequency range is selected as compared to middle and high frequency AC coefficient in order to embed the bits of the secret message.
STEP 7: Now store the sequence of selected blocks in the first block after applying the encryption on the sequence stored.

STEP 8: Apply the inverse discrete cosine transformations on the image.

V. RESULTS

In this Section the experimental results of the proposed algorithm are presented. The proposed algorithm is implemented in Mat lab. Five different images consisting of 784×512 pixel used to perform the test cases. Two types of test cases has been performed as follows:

1. Imperceptibility Test. The information security through steganography depends in great part on the level of imperceptibility, since a stegano graphic system has to generate a sufficiently innocent stego image. Therefore, the degree of distortion or imperceptibility of a stego image in relation to the original image plays a fundamental role. Usually, the image distortion is measured by the peak signal-to-noise ratio (PSNR), which is given by

\[ \text{PSNR} = 10 \log_{10} \left( \frac{255^2}{\text{MSE}} \right) \]

where \( \text{MSE} = \frac{1}{mn} \sum (C(\gamma) - S(\gamma))^2 \)

and \( C \) and \( S \) are the cover and stego image, respectively. The index set \( \gamma = (\gamma_1, \gamma_2, \gamma_3) \) sums over the set of bytes as \( \Gamma = \{1, \ldots, m\} \times \{1, \ldots, n\} \times \{1, 2, 3\} \), (14)

where \( m, n \) account for the image size, and \( C, S \in \{0, 1, \ldots, 255\} \).

The comparison for PSNR of proposed system with the existing systems is shown in the following table:

<table>
<thead>
<tr>
<th>Image</th>
<th>Proposed Method</th>
<th>Existing System</th>
<th>Soria Method</th>
<th>Velasco Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lenna</td>
<td>87.001</td>
<td>63.195</td>
<td>63.100</td>
<td>62.740</td>
</tr>
<tr>
<td>Airplane</td>
<td>87.557</td>
<td>63.815</td>
<td>64.720</td>
<td>63.730</td>
</tr>
<tr>
<td>City</td>
<td>90.592</td>
<td>63.740</td>
<td>63.740</td>
<td>63.700</td>
</tr>
<tr>
<td>Leaves</td>
<td>83.498</td>
<td>63.290</td>
<td>63.127</td>
<td>62.900</td>
</tr>
</tbody>
</table>

As shown in the table 1, proposed system generate the output with high PSNR values as compared to existing systems. It can also be shown as in the following graph.

Image Quality Measures: The relationship between the display and the human visual system can be quantitatively expressed by mathematical relationships of Image Quality Measures (IQMs). Steganographic schemes eventually leave statistical evidence that can be used to quantify the hidden content in the stego image relative to the cover image.
The IQMs based on correlation of the content of the images include Correlation Quality (CQ) and Structure Content (SC). In addition, the IQMs based on difference distortion and pixel distance include Image Fidelity (IF) and Average Absolute Difference (AD).

The following Table 2 shows the comparison of Absolute Difference of proposed and existing systems.

<table>
<thead>
<tr>
<th>Image</th>
<th>Proposed Method</th>
<th>Existing System</th>
<th>Soria Method</th>
<th>Velasco Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lenna</td>
<td>0.004500</td>
<td>0.006847</td>
<td>0.006607</td>
<td>0.005021</td>
</tr>
<tr>
<td>Airplane</td>
<td>0.004700</td>
<td>0.006806</td>
<td>0.007415</td>
<td>0.005021</td>
</tr>
<tr>
<td>City</td>
<td>0.005200</td>
<td>0.006800</td>
<td>0.006327</td>
<td>0.005021</td>
</tr>
<tr>
<td>Leaves</td>
<td>0.005200</td>
<td>0.006673</td>
<td>0.006941</td>
<td>0.005021</td>
</tr>
</tbody>
</table>

As shown in the above table absolute difference is lowest than that of existing system. It can be shown in the following graph:

Relative Entropy:

$$RE(P_C \| P_S) = \sum P_C \log \frac{P_C}{P_S} \leq \varepsilon$$

where $P_C$ and $P_S$ represent the distribution of cover image and stego image, and $RE(P_C \| P_S)$ is the relative entropy between the two probability distributions. Moreover, a steganographic system is called perfectly secure if $RE(P_C \| P_S) = 0$.

The following Table 2 shows the comparison of values Relative Entropy pairs of proposed and existing systems.

<table>
<thead>
<tr>
<th>Image</th>
<th>Proposed Method</th>
<th>Existing System</th>
<th>Soria Method</th>
<th>Velasco Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lenna</td>
<td>0.000997</td>
<td>0.002055</td>
<td>0.002051</td>
<td>0.001409</td>
</tr>
<tr>
<td>Airplane</td>
<td>0.005514</td>
<td>0.002525</td>
<td>0.002487</td>
<td>0.002025</td>
</tr>
<tr>
<td>City</td>
<td>0.000365</td>
<td>0.001755</td>
<td>0.001650</td>
<td>0.001225</td>
</tr>
<tr>
<td>Leaves</td>
<td>0.000232</td>
<td>0.001501</td>
<td>0.001622</td>
<td>0.001225</td>
</tr>
</tbody>
</table>
As shown in the above table value of entropy pair is close to zero in the proposed system that shows the high robustness of the proposed system. It can be shown in the following graph:

VI. CONCLUSION

In this contribution, we propose a new steganographic algorithm which uses random function method to choose the dct coefficient in order to store the secret message bits which will reduce the detectability. According to the analysis of PSNR and AD values, it is demonstrated that in the stego image there are no detectable anomalies with respect to the cover image. Moreover, the obtained values for the relative entropy show that the stegnographic system obtained by the proposed algorithm is sufficiently secure.

REFERENCES


[3] S. Berres and A. Soria-Lorente, a secure steganographic algorithm based on frequency domain for the transmission of hidden information, Hindawi security and communication Networks volume 2017, Article ID 5397082


