DCT-based Robust Steganographic Scheme to Hide a Secret Image

OSWALDO JUAREZ-SANDOVAL, ANGELINA TRUJILLO-ESPEJEL, MARIKO NAKANO-MIYATAKE, HECTOR PEREZ-MEANA
Postgraduate Section of Mechanical Electrical Engineering School
National Polytechnic Institute
Av. Santa Ana no. 1000, Col. San Francisco Culhuacan, Mexico D.F.
MEXICO
mnakano@ipn.mx  http://www.posgrados.esimecu.ipn.mx

Abstract: - The steganography research has grown rapidly since last decade. This technique has been used to hide different types of information, such as medical, personal and business information and also in some cases it was used in criminal act. This paper presents a robust steganographic scheme focused on the embedding of a secret image into a cover image in the DCT domain using quantization-based embedding algorithm. The experimental results show the robustness of the proposed scheme against the JPEG compression and noise contamination, while keeping an imperceptibility of hidden data. The proposed scheme also is robust to commercial stego-analyzers, which cannot detect the presence of the hidden data in the stego-image generated by the proposed scheme. The better performance of the proposed scheme is shown comparing with a previously reported steganography algorithm with same objective of the proposed one.

Key-Words: - Steganography, DCT, JPEG, Quantization based embedding, payload, robustness

1 Introduction

The growth of sharing of digital files, such as images, audio and video, on social networks or Internet, animates the study of steganography as an important technique to transport and share hidden information among world sectors. Recently this technique has been used to hide different types of information, such as medical, personal and business information and also in some cases it was used in criminal act.

Steganography is the art and science of hiding confidential information in a carrier file, the word steganography is derived from the Greek "Stego", meaning cover, and "Graphs" meaning writing [1]. The digital steganography must satisfy three important requirements, which are imperceptibility of hidden information, the capacity of large amount of hidden data and robustness against some common signal processing procedures [2].

Until now several digital steganographic schemes to hide secret information into digital files, such as Stool [3], JSteg [4], F5 [5], Bit-Plane Complexity Steganography (BPCS) [6], JpHide [7], Outguess [8] and so on, have been developed. Among them, Least Significant Bit (LSB) steganographic algorithms, such as Stool and BPCS, are able to hide great amount of information, however generally they are vulnerable to statistical analysis and the hidden information is destroyed easily after lossy compression, such as JPEG compression.

The frequency domain steganographic algorithms, such as J-Steg, F5 and Outguess, embed secret data in frequency domain, which is relatively robust to lossy compression; however generally the hidden data amount is limited. The authors of [9] proposed a robust steganography method called RIASIWT, in which data hiding is carried out in Integer Wavelet Transform (IWT) domain. The approximation sub-band of the IWT of the cover image is divided into non-overlapping blocks of 4x4 coefficients and then the secret information bits are hidden adaptively depending on the condition number of each block. In this algorithm, a gray-scale image is considered as a secret data.

The proposed steganography scheme provides robustness to common non-intentional image processing, such as JPEG compression and noise contamination, and also it provides the high data hiding capacity, while keeping sufficient imperceptibility. In the proposed scheme, an image data is considered as secret data, because in many applications an image provides a lot of visual information. The proposed scheme is also robust to commercial analyser for steganography [10], which cannot detect the presence of hidden data in the stego-image generated by the proposed scheme.

The rest of this paper is organized as follows. Section 2 provides a detail description of the proposed scheme, and experimental results and
performance comparison with previous work are shown in Section 3. Finally, in Section 4 we conclude this work.

2 Proposed Algorithm

2.1 Embedding process

The block-diagram of the proposed steganography algorithm is shown in Fig. 1. The embedding process is given by following steps.

1. Adjustment: Firstly the pixel values of the cover image are adjusted to avoid overflow or underflow of the range of pixel values \([0,255]\).

2. 2D-DCT: The adjusted cover image is divided into non-overlapped blocks with 8x8 pixels, consecutively bi-dimensional Discrete Cosine Transform (2D-DCT) is applied to each block to obtain DCT coefficients.

3. Permutation: The secret gray-scale image is permuted using chaotic mixing algorithm using two secret keys [11], whose objective is aggregate a security issue in the proposed scheme. The chaotic mixing algorithm is given by

\[
U^{(i)} = A_N(k)U^{(0)}, \ i = 1,2,...,P-1
\]

where \(U^{(i)}\) is state of the input image \(U^{(0)}\) after applying \(A_N(k)\) \(i\) times to \(U^{(0)}\), \(A_N(k)\) is given by (2).

\[
A_N(k) : L_N \rightarrow L_N, \ (x_{n+1}, y_{n+1}) = \left[ \begin{array}{cc} 1 & 1 \\ k & k + 1 \end{array} \right](x_n, y_n) \mod N
\]

where \((x_n, y_n)\) is index of each pixel, \(k\) is a integer secret key which forms a transform matrix and \(N \times N\) is the size of the secret image. Here \(k\) and \(i\) are two user’s keys. Figure 2 shows a result of this process.

4. MSB-LSB Change: In the proposed scheme, two pixels of the secret image are embedded into each DCT block. Considering that the MSB-bits of each pixel of any image are more important than their LSB-bits, then we arrange the bits sequence of two pixels as shown by Fig. 3.

Fig. 1. Block diagram of the proposed steganography scheme.

Fig. 2 A example of permutation. (a) original image, (b) permuted image after applying chaotic mixing algorithm.

Fig. 3 Bit arrangement used in the proposed scheme. (a) two pixel \(P_1\) and \(P_2\) with 8 bits and (b) arranged 16 bits-sequence \(S\).
Here B1 and B2 are two pixels with 8 bits data. Four MSB bits (MSB1 and MSB2) of both pixels are collocated in the first 8 bits of the 16 bits-sequence and four LSB bits (LSB1 and LSB2) of both pixels are collocated in the least 8 bits of the sequence.

5. Embedding: The arranged 16 bits-sequence \( S_k \) is embedded into \( k \)-th DCT block using quantization-based embedding algorithm. Firstly the DCT block of the cover image is ordered in zig-zag manner as shown by Fig. 4 to obtain a vector with 16 coefficients, \( C_k = [B(1,3), B(2,2), \ldots, B(4,3), B(3,4)] \), \( k=1..K \), where \( K \) is total number of blocks. Here only lower 16 coefficients, except DC and two lowest ACs, are used for data hiding to reduce the distortion caused by data hiding. The quantization-based embedding algorithm is given by (3).

\[
\text{if } S_k(b) = 0 \quad \tilde{C}_k(b) = 2q \\
\text{where } q = \arg \min \left\| C_k(b) - 2j\Delta \right\| \\
\text{if } S_k(b) = 1 \quad \tilde{C}_k(b) = 2q + 1 \\
\text{where } q = \arg \min \left\| C_k(b) - (2j + 1)\Delta \right\|
\]

where \( S_k(b) \) is \( b \)-th bit of 16 bits sequence of \( k \)-th block, \( C_k(b) \) and \( \tilde{C}_k(b) \) are \( b \)-th DCT coefficients of \( k \)-th block, respectively, and \( \Delta \) is step-size.

Fig. 4 Zig-Zag order to obtain 16 DCT coefficients

6. Finally stego-image is obtained applying inverse DCT to each DCT block with hidden 16 bits sequence.

In the proposed scheme, two pixels of the secret image are embedded into each block of the cover image; therefore there is a relationship between size of the cover image and that of the secret image, which is given by (4).

\[
L \geq \frac{8N}{\sqrt{2}}
\]

where \( (N \times N) \) is the size of secret image and \( (L \times L) \) is the size of the cover image

2.2 Hidden data extraction process

The hidden data extraction process is similar to the embedding process, which is described as follows:

1. Extraction of 16 stego-coefficients: Firstly 2D-DCT is applied to each block of the stego-image, and then 16-bits sequence is extracted in zigzag manner as shown by Fig. 3.

2. Extraction of the 16 bits-sequence: From the 16 coefficients obtained in previous process, extract 16 bits-sequence using the quantization-based extraction algorithm, which is given by (5).

\[
\tilde{S}_k(b) = \text{mod} \left( \tilde{C}_k(b), 2\Delta \right)
\]

where \( \tilde{C}_k(b) \) is the \( b \)-th bit of the \( k \)-th DCT block of the stego-image, which is probably distorted by non-intentional attacks, such as JPEG compression and noise contamination. \( \tilde{S}_k(b) \) is extracted \( b \)-th hidden bit and \( \Delta \) is step size used in the embedding process.

3. Rearrangement: The extracted 16 bits in the previous process is rearranged to generated two pixels values in each block.

4. Inverse permutation: Applying inverse process of the chaotic mixing algorithm to all extracted pixels to obtain the secret image. The inverse chaotic mixing algorithm is given by

\[
\tilde{U}^{(0)} = A_N^i(k)\tilde{U}^{(i)}, \quad i=1,2,\ldots,P-1
\]

where \( \tilde{U}^{(i)} \) is extracted secret image in process 3, whose pixels are disordered and \( \tilde{U}^{(0)} \) is resultant image after applying inverse permutation process, i.e. the extracted secret image.
3 Experimental Results

The performance of the proposed scheme is evaluated from several points of view: payload that is the hiding capacity, imperceptibility of hidden information, extracted secret image quality and robustness to JPEG compression and noise contamination. The secret image used in the experiment is shown in Fig. 2 (a), and several images with size $512 \times 512$, such as “Lena”, “Chiles”, “Mandrill”, etc. are used as cover images.

3.1 Hiding capacity

As mentioned above, the hiding capacity of the proposed scheme is given by (4), which is independent on characteristics of either cover image or secret image. When the size of the gray-scale cover image is $512 \times 512$, the maximum size of secret image is $90 \times 90 = 8,100$ pixels. If the cover image is color image with $512 \times 512$ pixels, the payload can be greater than three times, that is 24,300 pixels. The payload of the RIASIWT [9] depends strongly on the cover image characteristics. The maximum hiding capacity of the RIASIWT reported for a color cover image is 17,193 pixels. Considering this, the proposed steganographic scheme offers a higher capacity to hide secret image.

3.2 Imperceptibility of hidden data

The table I shows the quality of stego-images with different quantities of hidden data, with respect to their original image. The Peak Signal to Noise Ratio (PSNR) shown in the table is an average value using 30 color images with different characteristics.

Table I. Quality of stego-image with different
Hidden data quantities (pixels) Quality of stego-image
6,075 44.40
12,288 41.28
18,252 39.61
24,300 38.44

3.3 Quality of the extracted secret image

The qualities of the extracted secret image using the proposed algorithm under JPEG compression and contamination by Gaussian noise are evaluated. These evaluations reflect the robustness of the proposed scheme to non-intentional image processing, such as JPEG compression and noise contamination. Table II shows the quality of the extracted secret image (Ext_I) under JPEG compression with different quality factors together with the quality of the stego-image (SI). Here gray-scale images are used as cover images. The quality degradation of stego-image is caused by data hiding and also JPEG compression. Table III shows the quality of the extracted secret image under contamination by Gaussian noise with different variance $\sigma^2$. From table II, we can conclude that in the proposed scheme, the extracted secret image from the compressed stego-image by JPEG compression with quality factor 70 provides sufficient visual information. Also from table III, we can conclude that the visually significant information can be extracted from stego-image contaminated by Gaussian noise.

The principal reason of the good quality of the extracted secret image after JPEG compression is due to the rearrangement of MSBs and LSBs of two embedding pixels. The RIASIWT algorithm [9] is not robust to these attacks, obtaining the quality of the extracted secret image respect to the embedded one is approximately PSNR=14.70 dB.

3.4 Robustness to commercial Analyzer

Recently there are many commercial analyzers of steganography which detect the presence of data hiding in any image file [10]. The principal objective of steganographic algorithms is generating a stego-image that any commercial steganographic analyzer cannot detect as stego-image. All stego-images generated by the proposed scheme are classified as natural images, meaning that analyzers cannot detect the presence of hidden data into the stego-images.

4 Conclusions

This paper proposed a steganographic algorithm, which embeds and extracts a secret image in DCT domain using the quantization-based embedding algorithm. The experimental results show that the hiding capacity of the proposed scheme is sufficiently high, while keeping a high quality of the stego-image. The quality of the extracted secret image from the compressed stego-image by JPEG compression is reasonably high, which provides a sufficient visual information in receptor side. Also the stego-images generated by the proposed scheme are not detected as stego-image by the commercial analyzers of stego-images. The desirable performance of the proposed scheme is shown comparing with RIASIWT [9], whose payload is limited due to the embedding condition based on condition number and it is not robust to JPEG compression.
Table II. Robustness of the proposed scheme to JPEG compression with different quality factors QF, SI means stego-image, Ext_I means extracted secret image.

<table>
<thead>
<tr>
<th>Secret image size (pixels)</th>
<th>PSNR</th>
<th>QF=60</th>
<th>QF=70</th>
<th>QF=80</th>
<th>QF=90</th>
<th>QF=100</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SI (dB)</td>
<td>Ext_I (dB)</td>
<td>SI (dB)</td>
<td>Ext_I (dB)</td>
<td>SI (dB)</td>
<td>Ext_I (dB)</td>
</tr>
<tr>
<td>2025</td>
<td>34.54</td>
<td>15.90</td>
<td>35.07</td>
<td>25.57</td>
<td>36.06</td>
<td>37.43</td>
</tr>
<tr>
<td>4096</td>
<td>34.11</td>
<td>15.86</td>
<td>34.45</td>
<td>25.12</td>
<td>35.46</td>
<td>37.12</td>
</tr>
<tr>
<td>6084</td>
<td>33.73</td>
<td>16.03</td>
<td>33.95</td>
<td>25.47</td>
<td>34.99</td>
<td>36.50</td>
</tr>
<tr>
<td>8100</td>
<td>33.38</td>
<td>15.34</td>
<td>33.50</td>
<td>25.25</td>
<td>34.56</td>
<td>36.21</td>
</tr>
</tbody>
</table>

Table III. Robustness of the proposed scheme to contamination by Gaussian noise with different variance.

<table>
<thead>
<tr>
<th>PSNR (dB)</th>
<th>$\sigma^2 = 10^{-6}$</th>
<th>$\sigma^2 = 5.0 \times 10^{-6}$</th>
<th>$\sigma^2 = 10^{-5}$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SI</td>
<td>Ext I</td>
<td>SI</td>
</tr>
<tr>
<td>2025</td>
<td>44.31</td>
<td>29.96</td>
<td>43.72</td>
</tr>
<tr>
<td>4096</td>
<td>44.24</td>
<td>28.23</td>
<td>40.93</td>
</tr>
<tr>
<td>8100</td>
<td>38.41</td>
<td>27.17</td>
<td>38.26</td>
</tr>
</tbody>
</table>

References: