Hybrid Information Hiding Technique Using Parametric Spline and DFT

Dr. Abdul Monem S. Rahma*, Dr. Hala Bahjat Abdul Wahab * & Dr. Hana’a M. *  
Received on: 9/3/2008  
Accepted on: 7/8/2008

Abstract

Information hiding is a means to conical and transmitting information using apparently innocent carrier without depiction any suspicions. This paper presents a new means for information hiding based images by using Hybrid of Parametric Spline and DFT. A set of control points, which represents secret key, are selects randomly from the carrier, and a curve pass by the selected control points is implement using B-Spline. A hiding process for the secret message bits takes place on the spectral real part of the intensity pixels where the B-Spline curve passes by using LSB technique, followed by the IDFT. The paper also presents the information hiding features, and techniques for images, and Interpolation techniques. The Objective fidelity criteria are depicts the improvements in algorithm with an application example.

Keywords: Information Hiding, DFT, Parametric Spline Curve, Hybrid

DFT و Parametric Spline

تهوية إخفاء المعلومات الهجينة باستخدام

الخليصة

تية إخفاء البيانات هي وسيلة لتغطية ونقل المعلومات باستخدام وسط حامل غير مثير للشكوك. في هذا البحث نقدم وسيلة جديدة لإخفاء البيانات في الصور باستخدام مزيج من نقاط السيطرة و التحليل الفوري المستقل. مجموعة من نقاط السيطرة يتم اختيارها بصورة عشوائية (B-Spline) من الوسط الحامل والتي تمثل المفتاح السري. وال الذي يمر بنطاق السيطرة هذه، عملية إخفاء البيانات الخاصة بالرسالة السرية يتم من خلال أخذ مستخدمين (B-Spline) الجزء الحقيقي للوحدة الفردية الطيفية للمناطق التي يمر بها المفتاح بتقنية البث الألكتروني، البحث يقدم أيضًا السمات الخاصة بإخفاء البيانات، والتقنيات المستخدمة في الصورة، وتقييم الاستكشاف الخليطي، وقد تم تطبيق المقاييس المعتددة في فحص الصورة، والتي أظهرت نتائج مشجعة جداً في استخدام الخوارزمية مع مثال تطبيقي للخوارزمية.

1. Introduction

Images provide excellent carriers for hidden information and many different methods and tools have been introduced, from these are [1]:

1. Least Significant Bits insertion (LSBs): LSBs insertion modifies the LSBs of each color in 24-bit images, or the LSBs of the 8-bit value for 8-bit images.

2. Spread Spectrum (SS): The core of Spread Spectrum Information System (SSIS) is a spread spectrum encoder. These devices work by modulating a narrow band signal over a carrier. The carrier's frequency is continually shifted

*Computer Science Department, University of Technology/ Baghdad

827
using a pseudorandom noise generator feed with a secret key. In a way, the spectral energy of the signal is spread over a wide band, thus decreasing its density, usually under the noise level. To extract the embedded message, the receiver must use the same key and noise generator to tune on the right frequencies and demodulate the original signal. A casual observer will not be able even to detect the hidden communication, since it is under the noise level.

3. Dithering Manipulation: Dithering manipulation chooses the different patterns used to dither images to encode a message. It can achieve a high data rate, 1 hidden_byte/4 cover_bytes. Its major drawback is to rely only on dithered images and to be extremely sensitive to errors in the stego-image.

4. Perceptual Masking: This approach tries to embed information into regions that are masked by others with respect to the Human Visual System. The embedding can be done in the spatial or in the frequency space. The amount of information that can be hidden depends on the cover image and usually the choice of the areas to be modified has to be done under human control.

5. Discrete Cosine Transform coefficients manipulation: These techniques are used every time a lossy compression algorithm is on the signal path. Since those algorithms usually process the image using a 'Discrete Cosine Transform' DCT, which produces a matrix of floating point coefficients, while the same coefficients will be stored as its, a rounding process is involved. The embedding of information is acquired piloting the rounding function. Information hiding should be capable of embedding data in a host signal with the following restrictions and features[2]:

1. The cover data should not be significantly degraded by the embedded data, and the embedded data should be as imperceptible as possible. "This does not mean the embedded data needs to be invisible; it is possible for the data to be hidden while it remains in plain sight”.

2. The embedded data should be directly encoded into the media, rather than into a header or wrapper, to maintain data consistency across formats.

3. The embedded data should be as immune as possible to modifications from intelligent attacks or anticipated manipulations such as filtering and re-sampling.

4. Some distortion or degradation of the embedded data can be expected when the cover data is modified. To minimize this, error correcting codes should be used.

5. The embedded data should be self-clocking or arbitrarily re-entrant. This ensures that the embedded data can still be extracted when only portions of the cover data are
available. For example, if only a part of image is available, the embedded data should still be recoverable.

Although breaking a Steganography system normally consists of three parts: detecting, extracting, and disabling embedded. A system is already insecure if an attacker is able to prove the existence of a secret message. In developing a formal security model for Steganography we must assume that an attacker has unlimited computation power and is able and perform a variety of attacks. If he cannot confirm his hypothesis that a secret message is embedded in cover, then a system is theoretically secure [1]. The goal of secure steganographic methods is to prevent an observant intermediary from even obtaining knowledge of the mere presence of the secret data [3]. There are two necessary conditions of secure steganography [4]:

1. Key remains unknown to attacker.
2. The attacker does not know the actual cover.

A Hybrid method of Parametric Spline and DFT for information hiding is applied instead of hiding information in all over the image. A curve selection method is applied as positions where the secret bits to be hidden. The shape of the curve is based upon a set of control points that fundamentally describe its properties and its curvature, these control points represents the secret key to the purposed method. The B-Spline is one of the interpolation methods that is uses to generate a curve. The algorithm is primarily base on a set of control points. Thus if the intruder knows the set of control points it may lead to discover the shape of the curves with a trial and error on the method or algorithms that are originally used to produced the curve. An improvement is made by:

1. Extraction the intensity values of pixels along a curve in an image.
2. Applying the Discrete Fourier Transform (DFT) for the result intensity vector values.
3. Hiding information into the LSB's of the real part of DFT.
4. An inverse Discrete Fourier Transform IDFT is implemented.

The paper is organized as follows: Interpolation techniques is in Section 2, Objective fidelity criteria is in Section 3, The new algorithm with an application example is in Section 4 and 5 consequently, followed by the conclusions in section 6.

2. Interpolation Techniques

Interpolation techniques are of great importance in numerical analysis since they are widely used in a variety of science and engineering domains where numerical solution is the only way to predict the value of tabulated function for new input data [5]. There are three reasons for using interpolation first: interpolation methods are the basis, for many other procedures like numerical differentiation, integration and solution methods for ordinary and
partial-differential equations. Second, these methods demonstrate some important theory about polynomials and the accuracy of numerical methods. Third, interpolating with polynomials serves as an excellent introduction to some techniques for drawing smooth curves [5]. Although Bezier curves and surfaces are well suited to many shape-modeling problems, complex geometric constructions are required to guarantee continuity when piecing curves together [6]. The use of Spline functions avoids this by using mathematical constrains to allow only those curves that possess the required continuity at joints [7]. The B-Spline function generates curve section, which has continuous slopes so that they fit together smoothly. A B-spline of order k=3 consisting of n-k+2 segments is defined by a linear combination of basis functions \( C_i \) using n+1 control points \( v_i \).

Where the base functions are defined by [7]:

\[
\begin{align*}
b_{-1}(u) &= 1/6(-u^3 + 3u^2 - 3u + 2) \\
b_0(u) &= 1/6(3u^3 - 6u^2 + 4) \\
b_1(u) &= 1/6(-3u^3 + 3u^2 + 3u + 1) \\
b_2(u) &= 1/6u^3 
\end{align*}
\]

The algorithm for drawing a B-Spline curve is depicted in subsequent, followed by the output of the implemented algorithm in Figure (1), where a set of 10 control points \((x_i, y_i)\) with a parameter \( t \) that increment (10) each time is used.

### Algorithm (1): for drawing a B-spline curve

**Input:** Given n+1 points
\[ v_i = (x_i, y_i), i = 0, L, n \]

**Output:** Interpolate the get new values for each of \( x \) and \( y \) to draw.

**Process:**

1. Set \( v_0 = v_n = v_0 \) and set \( v_{n+1} = v_{n+2} = v_n \)
2. For \( i = 0 \) to \( n-1 \)
3. For \( u = 0 \) to \( 1 \) step 0.01
4. \( \ldots \)
5. \( \ldots \)
6. Plot \((X, Y)\).
7. Next \( u \)
8. Next \( i \)
9. End

3. **Objective Fidelity Criteria**

   The objective fidelity criteria provide equations that measure the amount of error in the reconstructed signals or to measure the amount of error between the original signal and the reconstructed one. Commonly used objective measures are the Root-Mean-Square-error (RMSE), Signal-to-Noise Ratio (SNR) and the Peak Signal-to-Noise Ratio (PSNR) [8]. The following are the definitions of RMSE, SNR, and PSNR.

   1. **Root-Mean-Square Error (RMSE)**

      The MSE is the average of the square of errors (value differences) of the two signals. RMSE defined by taking the square root of the error squared divided by the total number of elements in the signal [9]:

\[
MSE = \frac{1}{H \times W} \sum_{i=0}^{H} \sum_{j=0}^{W} [f(x,y) - f'(x,y)]^2
\]
The Root Mean Square error (RMSE) defined as the square root of the MSE:

$$\text{RMSE} = \sqrt{\frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} (f(x,y) - f'(x,y))^2}$$

Hence, the smaller the value of RMSE, the better-reconstructed signal represents the original signal. The larger the value of RMSE, the inferior reconstructed signal represents the original signal.

2. Signal to Noise Ratio (SNR) [9]:

It is a fidelity parameter used to measure the distortion level caused by the reconstructed signal, and define as:

$$\text{SNR} = \frac{\sum_{i=1}^{N} \sum_{j=1}^{N} (f(x,y))^2}{\sum_{i=1}^{N} \sum_{j=1}^{N} (f(x,y) - f'(x,y))^2}$$

3. The Peak Signal to Noise Ratio (PSNR) defined as [10]:

$$\text{PSNR} = 10 \log_{10} \left( \frac{(B-1)^2}{\text{MSE}} \right)$$

Where, MSE is the mean square error. $B = 2^n$, $n$ is the number of bits used.

In reconstructed signal, the large value of PSNR implies a better-deciphered image, and smaller number implies better image concealment of original image is obtained.

4. Similarity Measure [8]:

The most common form of the similarity measure can be interpreted in two given matrices $A_{ij}$, $B_{ij}$.

Where:

$$A = \begin{bmatrix} a_{11} & a_{1j} & \ldots & a_{1N} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{nj} & \ldots & a_{nN} \end{bmatrix}$$

and,

$$B = \begin{bmatrix} b_{11} & b_{1j} & \ldots & b_{1N} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{nj} & \ldots & b_{nN} \end{bmatrix}$$

The inner product matrix defined as:

$$\sum_{i=1}^{N} \sum_{j=1}^{N} a_{ij} b_{ij}$$

Then, the similarity test finally is given by considering $A_{ij}$ and $B_{ij}$ as two images matrices size $(N \times N)$.

$$\text{Similarity} (A_{ij}, B_{ij}) = \frac{\sum_{i=1}^{N} \sum_{j=1}^{N} a_{ij} b_{ij}}{\sqrt{\sum_{i=1}^{N} \sum_{j=1}^{N} a_{ij}^2 \sum_{i=1}^{N} \sum_{j=1}^{N} b_{ij}^2}}$$

The similarity measure shows the amount of correlation between $A_{ij}$ and $B_{ij}$. Therefore, when the similarity between the ciphered image and the original image, is small, then good concealment to the original image is obtains. The similarity between two image matrices gives its maximum value of (1) if the two images are perfectly similar.

4. The Proposed Algorithm

A Hybrid algorithm of Parametric Spline and DFT for information hiding is presented in this section,
where algorithm 2 illustrates the hiding Process, and algorithm 3 illustrates the extraction process as depicted bellow:

Algorithm (2): Hiding Process:

<table>
<thead>
<tr>
<th>Input: Cover image, and Secret message bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output: Stego-image</td>
</tr>
</tbody>
</table>

Process:
Step 1: Select by using the mouse from cover image any number of pixels that represent the control points.
Step 2: Apply B-Spline algorithm to the selected pixels to draw the interplant curve.
Step 3: Extract from the cover image pixels in which the interplant curve pass by
Step 4: While the extracted image pixels is not empty get the extracted image byte
Step 5: While the hidden message bits, is not empty get a bit and assigned it to the first bit of the real part of the DFT of the step 4
Step 6: Apply the IDFT to the result of step 5
Step 7: End of while
Step 8: End of while
Step 9: End

Algorithm (3): Extraction Process:

<table>
<thead>
<tr>
<th>Input: Stego-image and the selected cover image pixels (control points)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output: Secret message bits</td>
</tr>
</tbody>
</table>

Process:
Step 1: Select by mouse from image any number of pixels

Step 2: Apply B-Spline algorithm to the selected pixels to find the interplant curve
Step 3: Extract the cover image pixels in which the interplant curve pass by

4. Test Example
This section presents the results of applying the purposed algorithm according to its steps. The algorithm for hiding is implementers in section 4.1, and the algorithm for extraction is implemented in section 4.2

4.1 The Hiding Process
Input: Cover image, and Secret message bits

Process:
Step 1: Select by mouse from image any number of pixels

| 1 0 |
| 0 0 |
| 0 0 |
| 0 0 |
| 0 1 |
| 0 0 |
| 0 0 |
| 0 0 |
Step3: Extract the image pixels in which the interplant curve pass by

Step4: while the hidden message bits are not empty, get a bit, assigned it to the first bit of the real part of the DFT of the step3, and then apply the IDFT to the result.

Step5: End of while
Step6: End
Output: Stego-image

4.2 The Extraction Process
Input: Stego-image, and the selected image pixels

Process:
Step1: Apply B-Spline algorithm to the selected pixels to find the interplant curve

Step2: Extract the image pixels in which the interplant curve pass by
**Step3:** While the extracted image pixels are not empty, get the first bit of the each byte.

```
1 0
0 0
0 0
0 1
1 0
0 0
0 0
```

**Step4:** End

4. **Experiment Results**
   1. A set of control points are select in different directions of the carrier intensity pixels by mouse result in different interplant B-Spline shapes, the result secret key is differing by. Table (1) depict the carrier, and the selected control points \((x, y)\), which are represented as a star in the carrier image, and the sold line is the result curve, where the secret message is insert in.
   2. Similarity testes result, such as RMSE, SNR, PSNR, and SIM are depict in table (2) is compute for a five images in different image file size.

5. **Conclusions**
   A Hybrid method of Parametric Spline and DFT for information hiding based image is presented in this paper, where a set of control points, which represents secret key, are selects randomly from the carrier, and a curve pass by the selected control points is implement using B-Spline interpolation method. A hiding process for the secret message bits is implemented on the result curve using spectral real part of the intensity value of pixels, followed by inverse Discrete Fourier Transform IDFT. The example in section 4 highlight the algorithm steps implementation from the sender side "hiding process", and receiver side "extraction process".
   The table presents also, mean, median, standard deviation Different selection to different number and positions of image pixels by mouse gives the interplant B-Spline different shapes. Hence, the result secret key is differing by.
   The use of B-Spline interpolation as a method for secret key generation, gives the result secret key it's strong.
   The different selection to different number of positions and direction of image pixels by mouse gives the interplant B-Spline different shapes. Hence, the result secret key is differing by.
   The randomly selected part of the cover image depends mainly on the selected control points and its direction, hence the result algorithm is more secure even though, if the intruder knows the real control points.
   The embedding process is implemented in the frequency

<table>
<thead>
<tr>
<th>253</th>
<th>253</th>
<th>253</th>
<th>251</th>
<th>251</th>
</tr>
</thead>
<tbody>
<tr>
<td>249</td>
<td>249</td>
<td>250</td>
<td>247</td>
<td>244</td>
</tr>
<tr>
<td>244</td>
<td>233</td>
<td>233</td>
<td>239</td>
<td>239</td>
</tr>
<tr>
<td>229</td>
<td>229</td>
<td>233</td>
<td>233</td>
<td>233</td>
</tr>
<tr>
<td>233</td>
<td>233</td>
<td>233</td>
<td>233</td>
<td>233</td>
</tr>
<tr>
<td>233</td>
<td>233</td>
<td>233</td>
<td>233</td>
<td>233</td>
</tr>
</tbody>
</table>
domain, which is consider more secure then the time domain implantation for the LSB methods.

A similarity test the result stego-image is computed using the correlation as presented in table (1). This technique could be implemented to any image file type, and size

7. References
### Table (1) different selected control points and directions

<table>
<thead>
<tr>
<th>Carrier</th>
<th>X</th>
<th>Y</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>47.5000</td>
<td>84.5000</td>
</tr>
<tr>
<td></td>
<td>120.5000</td>
<td>48.5000</td>
</tr>
<tr>
<td></td>
<td>193.5000</td>
<td>109.5000</td>
</tr>
<tr>
<td></td>
<td>194.5000</td>
<td>196.5000</td>
</tr>
<tr>
<td></td>
<td>51.5000</td>
<td>97.5000</td>
</tr>
<tr>
<td></td>
<td>34.5000</td>
<td>158.5000</td>
</tr>
<tr>
<td></td>
<td>63.5000</td>
<td>67.5000</td>
</tr>
<tr>
<td></td>
<td>38.5000</td>
<td>161.5000</td>
</tr>
<tr>
<td></td>
<td>49.5000</td>
<td>204.5000</td>
</tr>
<tr>
<td></td>
<td>223.5000</td>
<td>200.5000</td>
</tr>
<tr>
<td></td>
<td>202.5000</td>
<td>97.5000</td>
</tr>
<tr>
<td></td>
<td>134.5000</td>
<td>62.5000</td>
</tr>
<tr>
<td></td>
<td>57.5000</td>
<td>66.5000</td>
</tr>
<tr>
<td></td>
<td>224.5000</td>
<td>200.5000</td>
</tr>
<tr>
<td></td>
<td>36.5000</td>
<td>164.5000</td>
</tr>
<tr>
<td></td>
<td>55.5000</td>
<td>212.5000</td>
</tr>
<tr>
<td></td>
<td>209.5000</td>
<td>100.5000</td>
</tr>
<tr>
<td></td>
<td>132.5000</td>
<td>55.5000</td>
</tr>
<tr>
<td></td>
<td>60.5000</td>
<td>57.5000</td>
</tr>
<tr>
<td></td>
<td>37.5000</td>
<td>166.5000</td>
</tr>
<tr>
<td></td>
<td>226.5000</td>
<td>196.5000</td>
</tr>
<tr>
<td></td>
<td>211.5000</td>
<td>100.5000</td>
</tr>
<tr>
<td></td>
<td>54.5000</td>
<td>215.5000</td>
</tr>
<tr>
<td></td>
<td>136.5000</td>
<td>57.5000</td>
</tr>
<tr>
<td></td>
<td>50.5000</td>
<td>77.5000</td>
</tr>
<tr>
<td></td>
<td>49.5000</td>
<td>213.5000</td>
</tr>
<tr>
<td></td>
<td>224.5000</td>
<td>204.5000</td>
</tr>
<tr>
<td></td>
<td>35.5000</td>
<td>166.5000</td>
</tr>
<tr>
<td></td>
<td>202.5000</td>
<td>103.5000</td>
</tr>
<tr>
<td></td>
<td>130.5000</td>
<td>57.5000</td>
</tr>
</tbody>
</table>
Table (2) Similarity test results

<table>
<thead>
<tr>
<th>File name</th>
<th>File size</th>
<th>RMSE</th>
<th>SNR</th>
<th>PSNR</th>
<th>SIM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image0 &amp; Stego_image 0</td>
<td>23KB</td>
<td>0.0199</td>
<td>5.5176</td>
<td>82.1740</td>
<td>0.9464</td>
</tr>
<tr>
<td>Image1 &amp; Stego_image1</td>
<td>7KB</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Image2 &amp; Stego_image2</td>
<td>10KB</td>
<td>0.0135</td>
<td>20.4964</td>
<td>85.5506</td>
<td>0.9974</td>
</tr>
<tr>
<td>Image3 &amp; Stego_image3</td>
<td>13KB</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Image4 &amp; Stego_image4</td>
<td>19KB</td>
<td>0.0192</td>
<td>10.1796</td>
<td>82.4677</td>
<td>0.9988</td>
</tr>
</tbody>
</table>

Figure (1) Applying a B-spline curve algorithm to the 10 control points