Adaptive Spatial Steganography Based on the Correlation of Wavelet Coefficients for Digital Images in Spatial Domain

Ningbo Li, Pan Feng, Liu Jia

Key Laboratory of CAPF for Cryptology and Information Security, Engineering University of Armed Police Force, Xi'an 710086, China

Keywords. Adaptive steganography; minimizing the embedding distortion; wavelet coefficient; distortion cost function; Syndrome Trellis Code (STC)

Abstract. How to define the pixel’s embedding distortion is a key problem of image adaptive steganography. This paper proposes an adaptive spatial steganography in spatial domain based on the correlation of wavelet coefficients for digital images according to the principle of minimizing a suitable defined distortion. Firstly, one-dimensional high-pass and low-pass filters are used to construct directional filters. Secondly, do direction filtering to images through the direction of horizontal, vertical and diagonal, and design the distortion cost function according to the correlation of wavelet coefficients. Finally, the secret message is embedded by STC (Syndrome Trellis Code) according to the pixel’s embedding distortion. The experiment results illustrate that the proposed method not only make the embedding region focus on the texture regions whose content is complex, but also can resist the common steganalysis detection effectively.

Introduction

Adaptive steganography make the embedding areas focus on textured or noisy areas according to the image content, and adaptive steganography based on distortion cost functions goes mainstream. Firstly define the pixel’s embedding distortion through the distortion cost function, secondly make the secret information embedded into the cover by special coding scheme (such as STC[1], Syndrome Trellis Code) in order to make the overall distortion least.

In this paper, we borrowed the idea of direction filtering from WOW [2] and UNIWARD [3], and propose an adaptive spatial steganography in spatial domain based on the correlation of wavelet coefficients for digital images: Firstly, we use one-dimensional high-pass and low-pass filters to construct directional filters (three directions: horizontal, vertical, diagonal), and do direction filtering to images through the direction filters. Secondly, design the distortion cost function according to the correlation of wavelet coefficients. Finally, the secret message is embedded by STC according to the pixel’s embedding distortion. Experiment shows that the new embedding scheme can resist the steganalysis using rich models more effectively, and get better performance than HUGO [4], WOW, and S-UNIWARD [3].

A new steganography algorithm

Analysis of the correlation of wavelet coefficients

There is a common hypothesis in both WOW and UNIWARD that wavelet coefficients in different directions are independent of each other, and wavelet coefficients themselves are also independent of each other. But this hypothesis ignores a fact that there is a certain correlation between the wavelet coefficients [5], and the correlation will be changed after the secret has been embedded.
The proposed steganography will be introduced in three parts: designing of the distortion cost function, embedding process, extracting process.

**Designing of the distortion cost function**

Denote a directional filter bank along the horizontal, vertical, and diagonal direction as \( F^{(1)} \), \( F^{(2)} \), \( F^{(3)} \), \( L^H \) represents for one-dimensional low-pass (and high-pass) wavelet decomposition filters, the cover and stego image are denoted by \( X \) and \( Y \). The image’s embedding distortion is defined in three steps:

1) Design direction filters

\[
F^{(i)} = L \cdot H^i, F^{(i)} = H \cdot L^i, F^{(i)} = H \cdot H^i. \tag{1}
\]

2) Do direction filtering to image

\[
W^{(i)}(X) = F^{(i)} \ast X, k \in \{1, 2, 3\}. \tag{2}
\]

Where "\( \ast \)" is a mirror-padded convolution so that \( W^{(i)}(X) \) has again \( n_1 \times n_2 \) elements.

3) Define the pixel cost \( \rho_{i,j} \)

\[
\rho_{i,j} = \sum_{u=1}^{n_1} \sum_{v=1}^{n_2} \left| \frac{W^{(i)}_{uv}(X) - W^{(i)}_{uv}(Y)}{\phi + \|W^{(i)}_{uv}(X)\|} \right| (i = u, j = v). \tag{3}
\]

Where \( \phi \) is a constant stabilizing the numerical calculations.

3) define the total distortion \( D(X,Y) \)

\[
D(X,Y) = \sum_{i=1}^{3} \sum_{u=1}^{n_1} \sum_{v=1}^{n_2} \left| \frac{W^{(i)}_{uv}(X) - W^{(i)}_{uv}(Y)}{\phi + \|W^{(i)}_{uv}(X)\|} \right|. \tag{4}
\]

\( W^{(k)}_{uv}(X) \) contains the correlation between the wavelet coefficient \( x_{uv} \) and its neighborhood.

The calculation process is as follows:

Horizontal direction:

\[
W^{(i)}_{uv}(X) = \left| W^{(i)}_{uv}(X) - W^{(i)}_{uv}(X) \right| + \left| W^{(i)}_{uv}(X) - W^{(i)}_{uv}(X) \right|. \tag{5}
\]

Vertical direction:

\[
W^{(i)}_{uv}(X) = \left| W^{(i)}_{uv}(X) - W^{(i)}_{uv}(X) \right| + \left| W^{(i)}_{uv}(X) - W^{(i)}_{uv}(X) \right|. \tag{6}
\]
Diagonally direction:

\[
W_{uv}^{(k)}(X) = W_{uv}^{(0)}(X) + W_{uv}^{(1)}(X) - W_{uv}^{(2)}(X) + W_{uv}^{(3)}(X) - W_{uv}^{(4)}(X) + W_{uv}^{(5)}(X) - W_{uv}^{(6)}(X). \tag{7}
\]

For \(W_{uv}^{(k)}(Y)\), the calculation process is same as \(W_{uv}^{(k)}(X)\), and we can use LSB steganography to obtain the stego image \(Y\).

**Embedding process**

After defining the pixel cost \(\rho_{i,j}\), embedding a random sequence of bits with minimal expected distortion can achieved by a practical algorithm, based on STC, that embeds near the payload–distortion bound. Here we introduce the fundamental of STC.

\[
Hy^T = m^T. \tag{8}
\]

\[
Y = \text{Emb}(X, m) = \arg \min d(X, y). \tag{9}
\]

Here, \(H\) is called the check matrix, it is obtained by splicing a number of sub-matrix \(H (h \times w)\) in the form of cascade and is shared by sender and receiver. Parameter \(h\) affect the time complexity of STC coding, \(h \in [6, 15]\). Larger the value of \(h\) is, longer the time of STC coding will be. In experiment, \(h\) is set to 6 and \(w\) is determined by the payload \(\alpha\).

The embedding process of STC coding conduct in the form of grid graph, and its brief process is as follows:

Firstly, we can get coset of secret \(m\) about the check matrix \(H\) according to the formula (8), and every coset can be showed as a path in a grid graph. Secondly, choose the path (codeword) that has the minimum hamming distance \(d(X, y)\) to cover \(X\), and this is the final stego \(Y\) we need to find. The process of finding \(Y\) can received through Viterbi algorithm.

**Extracting process**

After the receiver has received the stego image \(Y\), we can get the secret \(m\) through the formula (8) according to the check matrix \(H\).

**The simulation and analysis**

The secret \(m\) is simulated by a binary sequence through a pseudo-random number generator, and all experiments are conducted on the BOSSbase database ver. 1.01[6] containing 10,000 512 \(\times\) 512 8-bit grayscale images, A number of 5,000 images are randomly selected for training, and the rest 5,000 images are used for testing. Ensemble classifier [7] is used to do training and testing between cover and stego images. And the algorithm’s is evaluated by steganalyzers using 34,671-dimensional feature set SRM[8], and the security is quantified using the
ensemble’s “out-of-bag” (OOB) error \( E_{OOB} \), which is an unbiased estimate of the minimal total testing error under equal priors.

\[
P_k = \min_{p_k} \frac{1}{2} \left( P_{FA} + P_{MD} \right).
\]

(10)

Where \( P_{FA} \) and \( P_{MD} \) are the false-alarm and missed-detection probabilities. When the value of \( E_{OOB} \) is larger, it means that the probability of detecting the secret message incorrectly is greater, thus the steganography algorithm can resist steganalysis more effectively.

**choosing the proper filter**

To determine the proper filter, in this paper, six kinds of wavelet was experimented. The payload \( \alpha \) is set to 0.4bpp (bit /per pixel), \( \phi \) is set to 1 or 3 or 5, and investigate each filter’s performance resisting the steganalysis. Table 1 shows the results.

<table>
<thead>
<tr>
<th>( \phi ) = 1</th>
<th>( \phi ) = 3</th>
<th>( \phi ) = 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Haar</td>
<td>0.087</td>
<td>0.032</td>
</tr>
<tr>
<td>Daubechies 2</td>
<td>0.201</td>
<td>0.134</td>
</tr>
<tr>
<td>Daubechies 8</td>
<td>0.232</td>
<td>0.167</td>
</tr>
<tr>
<td>Symlet 8</td>
<td>0.210</td>
<td>0.163</td>
</tr>
<tr>
<td>Coiflet 1</td>
<td>0.166</td>
<td>0.081</td>
</tr>
<tr>
<td>Biorthogonal 44</td>
<td>0.174</td>
<td>0.113</td>
</tr>
</tbody>
</table>

From table 1 we can see that the Daubechies 8 wavelet shows a best performance in resisting steganalysis, so in this paper we choose Daubechies 8 to construct direction filters.

**Parameter \( \phi \) setting**

To determine the proper value of \( \phi \), we fixed the value of payload \( \alpha \) from 0.05bpp to 0.50bpp (the interval is 0.05), and the value of \( E_{OOB} \) is taken to three decimal places, the results of experiment is shown in table 2, and we can see from table 2 that under the certain condition of \( \alpha \), the value of \( E_{OOB} \) is the largest when the \( \phi \) is set to 1, and when the \( \phi \) is set to negative number, the value of \( E_{OOB} \) is decrease quickly, even reduced to 0. So in this paper, we set the value of \( \phi \) to 1.

<table>
<thead>
<tr>
<th>( \alpha ) = 0.0</th>
<th>( \alpha ) = 0.1</th>
<th>( \alpha ) = 0.2</th>
<th>( \alpha ) = 0.3</th>
<th>( \alpha ) = 0.4</th>
<th>( \alpha ) = 0.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \phi ) = 5</td>
<td>0.438</td>
<td>0.401</td>
<td>0.333</td>
<td>0.287</td>
<td>0.237</td>
</tr>
<tr>
<td>( \phi ) = 4</td>
<td>0.442</td>
<td>0.408</td>
<td>0.357</td>
<td>0.308</td>
<td>0.242</td>
</tr>
<tr>
<td>( \phi ) = 3</td>
<td>0.459</td>
<td>0.414</td>
<td>0.368</td>
<td>0.313</td>
<td>0.272</td>
</tr>
<tr>
<td>( \phi ) = 2</td>
<td>0.469</td>
<td>0.423</td>
<td>0.378</td>
<td>0.333</td>
<td>0.287</td>
</tr>
<tr>
<td>( \phi ) = 1</td>
<td><strong>0.477</strong></td>
<td><strong>0.444</strong></td>
<td><strong>0.394</strong></td>
<td><strong>0.343</strong></td>
<td><strong>0.323</strong></td>
</tr>
<tr>
<td>( \phi ) = 0</td>
<td>0.445</td>
<td>0.424</td>
<td>0.368</td>
<td>0.325</td>
<td>0.303</td>
</tr>
<tr>
<td>( \phi ) = -1</td>
<td>0.027</td>
<td>0.021</td>
<td>0.017</td>
<td>0.015</td>
<td>0.013</td>
</tr>
<tr>
<td>( \phi ) = -2</td>
<td>0.002</td>
<td>0.001</td>
<td>0.001</td>
<td>0.001</td>
<td>0.001</td>
</tr>
</tbody>
</table>
Algorithm’s Security Analysis

The secret m is simulated by a binary sequence through a pseudo-random number generator, all experiments are conducted on the BOSSbase database ver. 1.01, and make comparison of four kinds of steganography algorithm in the security of resisting the steganalysis of SRM feature. For HUGO, parameter T is set to 255. For WOW, \( \gamma = 1, \sigma = 1, T = 255 \). For S-UNIWARD, parameter \( \sigma \) is set to \( 2^{-6} \) [9]. For the algorithm proposed in this paper, we set the \( \phi \) to 1. The results is shown in Fig.1.

![Figure 1](image1.png)

**Figure 1.** The security comparison of four kinds of steganography algorithm.

![Figure 2](image2.png)

**Figure 2.** The comparison between the cover and the pixels modified after embedding.

Figure 1 shows that the algorithm in this paper performs better than HUGO, WOW and S-UNIWARD in the condition of the same payload. Figure 2 shows that the algorithm in this paper can make the embedding area focus on the texture areas where the content is unpredictable in every direction. In general, the proposed algorithm can effectively resist the attack of SRM steganalysis, and improve the safety of steganography algorithm.

Conclusions

To further enhance the safety of adaptive image steganography, we design a new distortion cost function according to the correlation of wavelet coefficients, and propose an adaptive spatial steganography in spatial domain for digital images according to the principle of minimizing a suitable defined distortion. Experiments show that the proposed algorithm can make the embedding area focus on the texture areas and can effectively resist the attack of SRM steganalysis.

Since the knowledge of game theory can be well utilized in the image steganography, we will try to generalize the cost function by game theory in our future work.

References


