Wavelet-Based Watermarking of Remotely Sensed Imagery Tailored to Classification Performance

Sean B. Ziegeler, Hrishikesh Tamhankar, James E. Fowler, Lori Mann Bruce
ERC GeoResources Institute, Mississippi State University, Mississippi State, MS 39762

Abstract – Watermarking is widely being explored as a means of providing protection of ownership rights for multimedia data, and there has been increasing interest in applying watermarking to remotely sensed data for this same purpose. However, watermarking techniques developed for multimedia cannot be applied directly to remotely sensed data due to the fact that the analytic integrity of the data, rather than perceptual quality, is of primary importance. In this paper, a watermarking technique for remotely sensed data based on the discrete wavelet transform (DWT) is proposed, and its impact on unsupervised classification as well as attacks such as cropping is studied.

Index Terms – remotely sensed imagery, discrete wavelet transform, watermarking.

I. INTRODUCTION

The last decade has seen tremendous growth in the utilization of remotely sensed imagery in diverse applications such as precision agriculture and natural-resource management. Additionally, the number of data-acquisition agencies, initially limited to government agencies, has grown to include commercial service providers. Since the acquisition of data, as well the preprocessing that precedes distribution to authorized users, is cost- and manpower-intensive, it is important to protect the ownership rights of the data provider. In the realm of digital multimedia, watermarking has been widely explored as a means for enforcement of ownership rights as well as for other related tasks such as transaction tracking and copy control [1]. It is natural then that watermarking has been recently proposed to protect ownership of remotely sensed data [2-3]. In [3], a model for an Electronic Copyright Management System (ECMS) is proposed wherein the acquisition and distribution process of remotely sensed data is partitioned into three main entities—the image (data) creator, the media distributor, and the user (purchaser) of the data. Under this model, the image creator is the party primarily interested in protection of ownership rights and can choose to use watermarking to that extent.

Watermarking techniques for typical multimedia data are motivated by factors such as the preservation of fidelity for human perception. Remotely sensed images are, however, subjected to a very different range of applications and processing techniques, with the perceptual quality of visualizations produced from the data being strictly auxiliary to the ultimate scientific-analysis purpose. Thus, watermarking schemes designed for ordinary multimedia may not be directly applicable to remote-sensing applications. For example, in [2], existing watermarking schemes are modified to produce a near-lossless watermark wherein the pixel values of a remotely sensed image are clipped in the spatial domain to force the distance between the original and the watermarked pixel below a certain limit, thereby enforcing a known distortion tolerance in order to aid subsequent analysis.

In this paper, we propose a wavelet-based watermarking scheme and evaluate it specifically for its performance with classification, a common analysis performed on remotely sensed data. In Sec. II, a brief overview of the wavelet transform is provided. Sec. III describes the proposed algorithm, the maximum root-mean-squared (Max-RMS) subband method. Finally, Sec. IV discusses the impact of the watermark on classification performance in the face of attacks such as cropping.

II. THE DISCRETE WAVELET TRANSFORM (DWT)

Since the DWT is a separable transform, a two-dimensional DWT can be considered to be a one-dimensional DWT applied first along rows and then along the columns of an image. The well-known filter-bank implementation can be extended and used to compute a two-dimensional DWT, resulting in the pyramid structure of subbands shown in Fig. 1.

![Figure 1. 3 level DWT of an image](image)

The 3-level decomposition depicted in Fig. 1 consists of a total of 10 subbands, labeled Hj, Vj, and Dj, where H, V, and D indicate horizontal, vertical, and diagonal detail subbands, respectively, and j the decomposition scale or level.
The coarsest decomposition coefficients are shown in the top left and denoted \( A \) (approximation coefficients).

### III. The MAX-RMS-Subband Algorithm

In [4], a DWT-based watermarking technique is proposed wherein a 3-level DWT decomposition is performed, and all the subbands, except the approximation subband, are watermarked. We propose a similar scheme in which only one subband at each level of the decomposition is watermarked. The band chosen for watermarking is the band with the highest RMS value for its level. This process effectively results in changing only a third of the coefficients at each level as compared to [4], thereby reducing distortion after watermarking. Also, the spatial features corresponding to the highest-RMS subband at any given level are most likely to be preserved by any processing operation, thus preserving robustness of the watermark to attack. The watermark is added as indicated below.

\[
c_i' = c_i (1 + \alpha w_i)
\]

where \( c_i \) are the original DWT coefficients, \( \alpha \) is the watermark-strength parameter, \( w_i \) is the added watermark, and \( c_i' \) are the modified (watermarked) coefficients. The watermark inserted is of size \((N/8)^2 + (N/4)^2 + (N/2)^2\), where the image is of size \( N \times N \). Watermark extraction is performed by inverting the above equation, assuming the availability of the original unwatermarked image. A normalized correlation operation between the original and the extracted watermark is used to decide the presence or absence of the watermark.

### IV. Impact of Watermarking

In [3], it is noted that the most common application of remotely sensed data is that of classification based on clustering methods. It is also noted that the most dangerous attack for remotely sensed data is “cropping,” as cropped images can be used by unauthorized users without considerable value degradation of the data set. The watermarking scheme proposed above has been evaluated with classification by an unsupervised K-means algorithm and compared to the method outlined in [4], which we note is intended for ordinary still images and not remotely sensed images. The data used in this evaluation was a subset of four bands of data acquired by a CASI sensor with a spatial resolution of 2m. The imagery was acquired by Mississippi State University over Brooksville, Mississippi, on June 16–17, 2001. Fig. 2 shows a band of the acquired imagery.

The four bands were watermarked as per the Max-RMS-subband scheme described above. It is not readily apparent as to what would be an acceptable value for the mean squared error (MSE) after watermarking; however, the minimum and the maximum MSEs were found to be 1.45 and 0.95 respectively. A subjective comparison reveals that very few artifacts were created as a result of the watermarking. Fig. 3 shows the same band as in Fig. 2 after watermark insertion.

Fig. 4 shows the correlation test performed for the detection of the watermark against a true watermark (watermark number 50) and 99 unauthentic watermarks.

### Table 1. Comparison of classification accuracy

<table>
<thead>
<tr>
<th>Band</th>
<th>% Pixels same</th>
<th>% Pixels different</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>90.1</td>
<td>9.9</td>
</tr>
<tr>
<td>2</td>
<td>90.1</td>
<td>9.9</td>
</tr>
<tr>
<td>3</td>
<td>90.8</td>
<td>9.2</td>
</tr>
<tr>
<td>4</td>
<td>94.2</td>
<td>5.8</td>
</tr>
<tr>
<td>Average</td>
<td>91.3</td>
<td>8.7</td>
</tr>
</tbody>
</table>

Table 1 shows the result of a K-means unsupervised classification with 10 clusters performed on the watermarked image with the parameter \( \alpha = 0.1 \). Figure 5 shows the classification results for one of the bands of the image.

The second column in the table shows the percentage of pixels that were assigned the same class in the watermarked image as they were in a classification of the original unwatermarked image, and the third column shows the percentage of pixels that changed classes.
It is worthwhile to note that the percentage of pixels that changed classes after watermarking is not indicative of a classification error per se, since the absence of ground truth does not allow for an absolute measure of the true classification accuracy. Some amount of error is inherent in unsupervised classification, which is the most commonly used classification scenario. With the proposed algorithm, the discrepancy in class assignments due to such a classification procedure can be curtailed below a chosen limit. To compare with the method in [4], the average classification performance for the proposed method was compared to that produced by [4] for various values of the parameter $\alpha$. The results are depicted in Fig 6. As seen in Fig. 6, for a given classification-difference tolerance, the proposed Max-RMS-Subband method can accommodate more watermark strength than can the method of [4]. Equivalently, our method introduces less classification difference for a given watermark strength, due to the fact that the proposed algorithm watermarks only one third of the coefficients as compared to [4].

Next, we compare the performance of the two algorithms in question in the face of a cropping attack. The value of $\alpha$ chosen in this case was 0.1446, which corresponds to a 10% classification difference for our Max-RMS-Subband method as illustrated in Fig. 7. The crop size was varied from 1 to 120, where a crop size of “$x$” corresponds stripping out $x$ rows from the top and bottom and $x$ columns from the left and right of the image. The extracted watermark correlation after cropping is depicted in Fig. 7, which shows that the correlation value is consistently higher for the Max-RMS-Subband method. Fig. 8 shows the detector performance for the Max-RMS-Subband after a cropping attack of a randomly chosen size. Fig. 8 shows that even after a cropping attack, only the true, authentic watermark correlates well with the watermark extracted from the attacked image, demonstrating robustness to the cropping attack.

V. CONCLUSIONS

In this paper, a DWT-based algorithm for the watermarking of remotely sensed images is proposed. In the proposed algorithm, only the subband with the highest RMS value at each decomposition level is watermarked. The impact of watermarking by this algorithm on classification performance is evaluated and seen to be less than that of a similar algorithm that watermarks all subbands. Additionally, the algorithm is also seen to be robust in the face of cropping attacks. The proposed algorithm can be applied to multispectral as well as hyperspectral data since each band of the data is watermarked.

VI. REFERENCES


