Watermarking techniques for electronic delivery of remote sensing images

M. Barni[a], F. Bartolini[b], V. Cappellini[b], A. Garzelli[a], E. Magli[c], G. Olmo[c]

[a]University of Siena
Department of Information Engineering
Via Roma 56 - Siena 53100 - ITALY
Ph.: +39 0577 234621
Fax: +39 0577 233602
E-mail: (barni,garzelli)@dii.unisi.it

[b]University of Florence
Dept. of Electronics and
Telecommunications
Via S.Marta 3, 50139 - Firenze - ITALY
Ph.: +39 0577 4796385
Fax: +39 0577 494569
E-mail: (barto,cappellini)@lci.det.unifi.it

[c]Politecnico di Torino
Department of Electronics
Corso Duca degli Abruzzi, 24
10129 Torino - ITALY
Ph.: +39 011 5644195
Fax: +39 011 5644149
E-mail: (magli,olmo)@polito.it

Abstract— **This paper studies the applicability of watermarking techniques to remote sensing imagery. An overview of watermarking is given, and the requirements, imposed by the remote sensing scenario on watermarking techniques, are discussed. As an example, the effect of watermarking on image classification is analyzed.**

I. Introduction

Earth observation missions have recently attracted a growing interest from the scientific and industrial communities, In such systems, a spaceborne platform collects scientific data and transmits them to a ground station; at the ground segment a series of image products are created, that can be made available to scientific or commercial organisations for exploitation. The data delivery process, usually based on CD-ROM hardcopy or on Internet distribution, provides the user with a digital version of the remote sensing data. In the same way as for multimedia contents, the digital format implies an inherent risk of unauthorized copy or use of the product; on the other hand, on the user's side, it is important to be able to verify the integrity of the received data. Therefore, two main issues commonly arise when dealing with image data security, namely authentication and copyright protection. Both problems have been largely addressed in the field of multimedia by resorting to watermarking technology, that consists in permanently embedding a mark in the original image, carrying information such as copyright ownership and user license rights. Later on, the presence or absence of the watermark can be used to prove ownership, to protect the intellectual property rights of the document creator, to discourage unauthorized copying of the protected material, or to prove the integrity of the data.

This paper is concerned with the definition of the requirements imposed by the remote sensing scenario on watermarking techniques, in the case of *copyright protection*. The desired functionalities of watermarking techniques are discussed, and the possible design options of a watermarking algorithm are evaluated in terms of remote sensing specific issues.

II. An overview of watermarking

Image watermarking can be seen as a communication task consisting of two main steps: watermark casting, in which the watermark is transmitted over the channel, which the original image plays the role of, and watermark detection, in which the signal is received and extracted from the possibly corrupted image. Intentional and unintentional attacks and distortions applied to the image, further characterize and complicate the transmission channel. As to the watermark, it usually consists of a pseudo-random sequence, with uniform, binary or Gaussian distribution.

According to the set of features the watermark is injected into, watermarking techniques can be divided into three main categories: (i) *spatial domain techniques* directly add the watermark to pixel values; (ii) *transformed domain techniques* add the watermark to the coefficients of a full-frame transform (DFT, DCT, Mellin, Radon, Fresnell) of the image; and (iii) *hybrid techniques* (mainly using block-wise DCT, and wavelets) working in a transformed domain, but without completely losing spatial localization. Usually, transformed domain techniques exhibit a higher robustness to attacks than spatial domain techniques. Hybrid techniques (in particular wavelet based ones) try to trade off between the advantages of spatial domain techniques in the localization of the watermarking disturb, and the good resistance to attacks of transformed domain techniques.

After watermark insertion, a perceptual hiding step is sometimes performed to make the watermark less perceivable to the eye. In remote sensing applications watermark imperceptibility looses some of its importance, since the unobtrusiveness of the watermark must be judged with respect to other factors such as classification or pattern recognition accuracy.

Among the characteristics of image watermarking algorithms, a crucial role is played by the way the watermark is extracted from data. In *blind* decoding, the decoder does not need the original image or any information derived from it, to recover the watermark. Conversely, *non-blind* decoding refers to a situation where extraction is accomplished with the aid of the original, non-marked data. In spite of the benefits it gives in terms of robustness, non-blind decoding is not desirable in many applications, where the availability of the original data can not be granted. An important distinction can also be made between algorithms embedding a mark that can be *read* (i.e. the bits contained in the watermark can be read without knowing them in advance) and those inserting a code that can only be *detected*.

Watermark detection is a typical binary hypothesis testing problem. Given an observation variable, a decision rule is defined to decide whether the watermark is present (hypothesis H_1) or not (hypothesis H_0). In correlation-based detection, which up to now is by far the most common approach to watermark detection, the observation variable is the correlation ρ between the watermark and the host features. To decide whether the watermark is present or not, ρ is compared to a threshold T_ρ, which is usually set by minimizing the missed detection probability subject to a maximum false detection rate (Neyman-Pearson criterion). It is worth noticing that, despite its popularity, correlation-based detection does not lead to optimum performance, unless the em-

This work was supported by ASI (Italian Space Agency) Grant: "Watermarking techniques for authentication and copyright protection of remote sensing images accessible through public and private thematic networks"

bedding rule is additive and the host features are Normally distributed.

In many applications, especially those dealing with copyright protection, robustness against attacks is of primary importance. The algorithms proposed so far have reached a satisfactory degree of robustness against a number of image processing techniques, including: filtering, compression, histogram manipulations, printing and rescanning, noise addition, and, to a limited extent, geometric manipulations.

Readers interested in a more detailed discussion of watermarking issues, may refer to the excellent tutorials contained in [1].

III. Requirements for watermarking of remote sensing imagery

A typical product formation flow for remote sensing images includes the following steps:

1. Image acquisition and on-board storage.
2. Possible lossless/lossy compression, and transmission to the ground station.
3. Preprocessing (calibration, preliminary geometric corrections, resampling, and others).
4. Formation of products with different degrees of precision (geocorrected, orthorectified, and others).
5. Product delivery to the final users (typically FTP, or CDROM shipping).

Since a number of different products are usually prepared from a single image, it is reasonable to mark each product separately, in order not to reduce the watermark effectiveness.

An interesting aspect, mainly related to optical data, is that multi/hyperspectral instruments provide one image per sensor band; this leads to the requirement that the watermark should be present in each band. While it is possible to mark each channel separately, it is worth noticing that the correlation among different channels could be exploited to improve the robustness to attacks. Watermark detection/decoding can be made e.g. on the basis of a “majority rule”, claiming that a mark is present if it has been found on most of the image channels. This is especially appealing in the case of hyperspectral images, where the number of channels can be larger than 200; exploiting spectral diversity may thus lead to a less invasive marking in each singla band.

As for the choice between blind and non-blind decoding, the following remarks can be made. Although it can be envisaged that the data provider keeps a record of original non-marked images, legal and practical aspects may prevent from using them for watermark inference. On one hand, unless a third-party certifies that the image owned by the provider is the original one, a false original might be built, and used to claim ownership. On the other hand, although access to the customer’s computer facilities is sometimes required by data providers, the non-marked data might be difficult to use; in fact, the original and to-be-verified data would not be stored on the same computer, and the huge file sizes would make the comparison very difficult. Prospectively, future operating systems for PCs are expected to provide selective rights to file access and copy, on the basis of some copyright information embedded in the files. In this case, the watermarking decoding algorithm should be a blind one.

In the design of a suitable watermarking technique, it is important to model the possible attacks that can be performed on remote sensing images. In this field, one can consider 1) attacks that impair the data content, and 2) attacks that preserve it. Examples of the former class are filtering, downsampling, lossy compression, noise addition, quantization, etc.; the latter class comprises e.g. cropping, image translation/rotation, and interpolation/resampling. As for the former class, the idea is that the mark should be robust to such attacks, up to the extent that they render the data useless for remote sensing applications. On the contrary, attacks of the latter type are more dangerous, as the resulting data quality is not impaired. In particular, due to the very large coverage of satellite scenes, small sub-images can still be used for many applications; also, operations based on interpolation, such as translations, rotations, and resampling, can be performed without decreasing the image resolution. Therefore, suitable watermarking techniques should be as much robust as possible to such geometric manipulations. As noted in Sect. II, this is achieved to a limited extent by the techniques proposed in the literature, thus pointing out the need of further study.

While the requirements discussed above are at system level, application level requirements also exist, in the sense that the watermark should affect, in the lowest degree, remote sensing applications to be run on the images. Transparency to the human visual system, which is the accepted objective function for multimedia watermarking, is however expected to provide a poor match to the remote sensing requirements. On the other hand, more suitable metrics should carefully account for the specific characteristics of the applications. While this will be matter of further study by the authors, the case study presented in Sect. IV clearly highlights the need of an accurate control of the watermarking effect on applications.

IV. An example: image classification

In this section we show an example of processing of a watermarked remote sensing image; our aim is to assess the effect of watermarking on the results of an image processing task. We focus on “classification”, which is perhaps the most common application in the field of remote sensing; in particular, in the following we employ the unsupervised clustering algorithm described in [2], with a maximum number of five clusters. As for watermarking, two techniques are considered. The first one has been proposed in [3], and inserts the mark in the DCT domain, while the second one is described in [4], and operates in the wavelet domain. It must be emphasized that neither algorithm has been specifically developed for remote sensing imagery, but rather to match the characteristics of the human visual system.

The results presented in the following have been obtained by applying the two algorithms to a 512x512 image from the SPOT satellite. This multispectral image, acquired by the SPOT XS instrument, has a ground resolution of 30 m; the sensor measurements are in the three bands 0,5-0,59 μm, 0,61-0,68 μm, and 0,79-0,89 μm. The data represent a region in proximity of the “Kakadu National Park” in Northern Australia; a greyscale version of the image is reported in Fig. 1. The results of the unsupervised classification algorithm on the original image are shown in Fig. 2.

The three bands have been marked with the algorithms in [3], [4]. The mark has been inserted in each band separately, with several degrees of energy (case 1 to 6). In the watermark detection phase, it has been assumed that the mark is present if it has been detected in at least two bands. Tab. I summarizes the performance of the two watermarking algorithms for this image. The second, third and fourth columns report the peak signal-to-noise ratio (PSNR), expressed in dB, between each original band and the watermarked band, thus indicating the energy of the inserted mark. The watermark robustness has been measured with respect to the most likely attack on remote sensing images, namely image cropping. The last column of Tab. I reports the minimum crop size (MCS), such that the mark can still be detected. As can be seen, the wavelet-based algorithm turns out to be considerably more robust to cropping than the DCT-based one.

In the remote sensing context, it is important to evaluate the effect

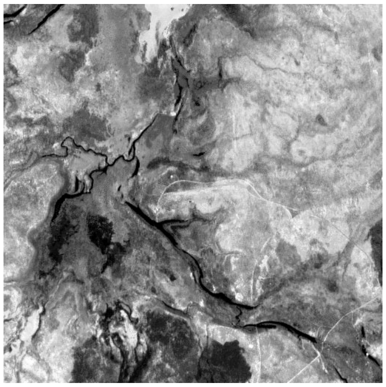

Fig. 1. Greyscale version of the original SPOT image

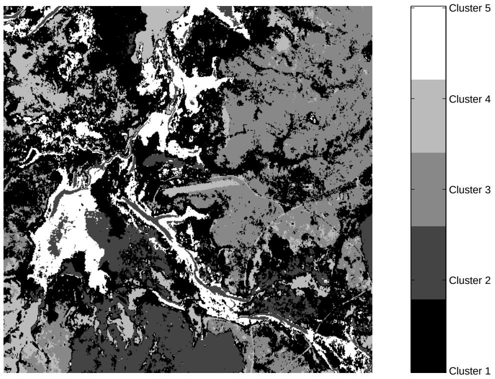

Fig. 2. Unsupervised classification of the original image

TABLE I

WATERMARK DETECTION PERFORMANCE

DCT-based algorithm				
Case	Band 1	Band 2	Band 3	MCS
1	50.8	51.4	51.0	360
2	47.5	48.2	47.2	320
3	44.9	45.7	44.5	240
4	43.0	43.8	42.7	220
5	41.6	42.3	41.4	220
6	40.6	41.2	40.5	200
Wavelet-based algorithm				
Case	Band 1	Band 2	Band 3	MCS
1	51.1	51.3	51.7	90
2	47.9	48.2	48.5	80
3	45.6	45.9	46.2	60
4	43.7	44.0	44.3	50
5	42.2	42.5	42.8	40
6	40.9	41.1	41.5	40

TABLE II

EFFECT OF WATERMARKING ON IMAGE CLASSIFICATION

	DCT		Wavelet	
Case	Nr. MP	% MP	Nr. MP	% MP
1	535	0.204	689	0.263
2	1110	0.423	35497	13.5
3	1871	0.714	35947	13.7
4	36881	14.0	36602	14.0
5	37734	14.4	36949	14.1
6	38582	14.7	38333	14.6

of the mark on the applicative tasks. To this end, the classification algorithm used to obtain the clustering in Fig. 2 has also been run on the watermarked channels. Comparative results are reported in Tab. II for the DCT- and wavelet-based algorithms respectively. For varying values of the watermark energy (case 1 to 6), the tables report the number of misclassified pixels (MP) with respect to the classification of the original, non-marked image; the percentage of MP in the image is reported as well.

As for the DCT-based algorithm, it can be easily seen that, for low watermark energy, very few pixels are misclassified. On the other hand, in case 3 to 6, in which the mark is more robust to cropping, a threshold effect occurs, in that the classification results are abruptly impaired when the mark energy exceeds a certain level.

Similar results have been obtained with the wavelet-based algorithm. In particular, it is worth noticing that, while this latter algorithm exhibits a larger degree of robustness to cropping, it is still characterized by a threshold effect in the classification application; moreover, the threshold is considerably lower than for the DCT-based algorithm.

Notwithstanding its simplicity, this example clearly shows that the watermark energy can heavily impact on the results of applicative tasks. More interestingly, different watermarking algorithms, allowed to insert an equal amount of mark energy, can exhibit very different performance, as for robustness to attacks and performance of the applications; in the specific example reported in this paper, the superior robustness to cropping, achieved by the wavelet-based algorithm, has resulted into poorer classification performance, thus highlighting possible conflicts among the requirements in the remote sensing scenario, and witnessing the need of further research to develop algorithms well-suited to this context.

V. CONCLUSIONS

In this paper we have analyzed the applicability of watermarking techniques to remote sensing images. System-level requirements have been discussed, and an example application (image classification) has been presented. It has been shown that the presence of the watermark heavily affects the results of the applicative tasks. Further work will aim at the development of watermarking techniques specifically designed for remote sensing data, so as to minimize the impact on the applications.

REFERENCES

[1] "Special issue on: Identification and protection of multimedia information," *Proc. IEEE*, vol. 87, no. 7, Jul. 1999.

[2] J.A. Richards, *Remote sensing digital image analysis: an introduction*, Berlin:Springer, 1986

[3] M. Barni, F. Bartolini, A. De Rosa, A. Piva, "A new decoder for the optimum recovery of non-additive watermarks", *IEEE Trans. Image Processing*, vol. 10, no. 5, May 2001

[4] M. Barni, F. Bartolini, A. Piva, "Improved wavelet-based watermarking through pixel-wise masking", *IEEE Trans. Image Processing*, vol. 10, no. 5, May 2001