The Application of Digital Watermarking in Remote Sensing Image

Peidong Jin， Xuwen Qin

Aero Geophysical Survey & Remote Sensing Center, 31 College Road, Beijing 100083, China

pdjin@public.bta.net.cn

Abstract: To protect the digital image, video and audio from non-authorized use, the digital watermarking technology has received a great attention in the field of multimedia in recent years. An overview of the development of watermark techniques is given in the current paper followed by a discussion of potential application of spatial domain, transform domain watermark techniques in remote sensing images copyright protection and verification in different forms of processed images.

Keyword: digital watermark, attack, transparency, robustness

1. Introduction

The digital technology development makes using the Internet and intranet faster and less expensive in terms of data exchange. To protect the digital image, video and audio from non-authorized use, the digital watermarking technology has been greatly modified in recent years. In the field of multimedia, the digital watermarking techniques is based on the human visual and hearing system. The question is whether these developed techniques can be used in scientific remote sensing, image's copyright protection and verification. To remote sensing images, the watermark algorithms impact the image in a way similar to lossy compression, so the algorithms should have minimum loss of information. The inserted watermarks should have minimum effect on image applications. To the watermark, any step of remote sensing image processing act would be an attack on the watermark. The watermark should be robust towards the attack from remote sensing processing.

The remote sensing image production has a very complex procedure, such as data acquisition, transmission, radiometric and geometric corrections, etc. Usually the product has a series of different level processing in order to satisfy a wide range of application fields. Watermarks inserted in the low level of image processing will influence the result of the following processing. The inserted watermarks looses some important information in one kind of application, however, the same watermark could have no influence to another kind of application. So, when one selects the watermark and algorithms insertion, one must have remote sensing images and future application and processing taken into account. The unobtrusiveness of the watermark should be judged with respect to their application such as classification or pattern recognition accuracy.

2. An overview of watermarking

Digital Watermarking is also known as digital fingerprinting, hidden watermarking, or data hiding. The watermarks are integrated within digital files such as image, or random information that already exists in the file, thereby making the detection and removal of the watermark difficult. Usually, watermarks are dispersed throughout the entire digital file so that the manipulation of one portion of the file does not alter the underlying watermark. Digital Watermarking attempts to copyright the digital data that is freely available on the World Wide Web to protect the originator's rights. Digital Watermarking also serves as a means of advertising within digital images. For instance, a user may download and view a digital image, use a watermark reader to extract the digital signature, then access a web-based directory to find the company's name and up-to-date address, phone number, web and e-mail addresses.

According to the insert technique, watermark can be divided into three main categories: (a) spatial domain techniques directly add the watermark to pixel values; (b) transformed domain techniques add the watermark to the coefficients of a full-frame transform of the image; and (c) hybrid techniques working in a transformed domain, but without completely losing spatial localization. Usually, transformed domain techniques have a higher robustness to attacks than spatial domain techniques. Hybrid techniques try to trade off between the advantages of the spatial domain techniques in the localization of the watermarking disturb, and the tough resistance to attacks of transformed domain techniques. The addition and multiplicative are two most common watermark embedding techniques. The addition technique is mainly used in spatial and hybrid techniques, while the multiplication technique is often found in conjunction with the transformed domain techniques.

The watermarking decoding technique can be classified as blind and non-blind. In blind decoding, the decoder does not need the original image or any information derived from it to recover the watermark. Au contraire, non-blind decoding refers to a situation where extraction is accomplished with the aid of the original, non-marked data.

The watermarking insert 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.

3. Remote sensing image processing

The remote sensing image acquisition processing system is a very complex system. It includes data transmission, compression, re-sampling and geometric correction. A typical processing procedure is as follows.

1) data acquisition from a satellite or airborne sensor.
2) data compression and transmission to a ground station;
3) preprocessing, include radiometric corrections, resampling etc;
4) distribution to final users;
5) final user's processing, including filtering, resampling, cropping, geometric distortion.

This sequence of operations implies that each product, at an increasing degree of precision, is formed from the received raw data undergoing an incremental sequence of processing stages. If the watermark were to be inserted once and for all on the raw data, the subsequent processing steps would act as attacks.

Watermark insertion must be performed in such a way that the user can not significantly perceive its effect. Additionally, in order for the copyright protection system to be effective, the watermark must be robust to those image manipulations that are relevant in the remote sensing context.

3.1 Transparency of the watermark in remote sensing image

In the multimedia field, it is widely acknowledged that the watermark must be transparent to the human eye, meaning that the visual impact on a human observer should be minimal. While this approach is very effective in the multimedia context, it turns out to be too simplistic in the remote sensing image, the main reason is because of the considerably more demanding image exploitation performed by the user. On the other hand, it is very difficult to identify specific requirements, which are valid for a reasonable number of applications;

A watermarking algorithm modifies pixel values, thus impacting on applications in a way similar to lossy compression. There are many of possible applications of remote sensing data. In the case that remote sensing images are used in visual analysis, the watermarking unobtrusiveness requirements can be expressed again in terms of transparency to the human eye. In the case of automatic analysis, the transparency of the watermark should be decided by the scientific algorithms, the watermark should not create a negative impact on the image analysis results, so that it will not create fake structures in the image data.

3.2. Robustness of watermark in remote sensing image

In order to be effective, the inserted mark must be robust towards possible malicious attacks, or intentional manipulations; In general, the attacks to image sensing images watermark are very different from the multimedia's, the main reason is the remote sensing image exploitation by means of image analysis algorithms, rather than the mere visualization.

The most common remote sensing image manipulations include: 1) linear stretching; 2) geometric transformations, such as, translations, rotations and geometric distortions; 3) contrast enhancement; 4) image compression, such as JPEG, MrSid and 5) non-invertible filtering, such as low pass filtering. Suitable watermarking algorithms should thus be robust towards most of these manipulations.

4. Two examples of remote sensing image with watermark

There are two samples showing the effects of different digital watermarking techniques on remote sensing images.

4.1 The application of Digimarc watermarking techniques

Digimarc is an American technology company on relevant applications of digital watermarking techniques. Its software products are wide used in the world, especially in multimedia field. Here, with Digimarc's software, a watermark was inserted into one scene of six-band ETM+ remote sensing image (Figure 1).

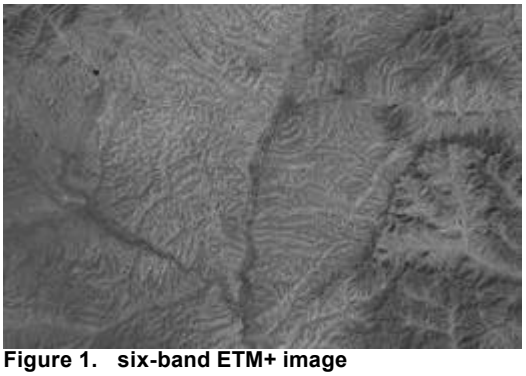

Figure 1. six-band ETM+ image

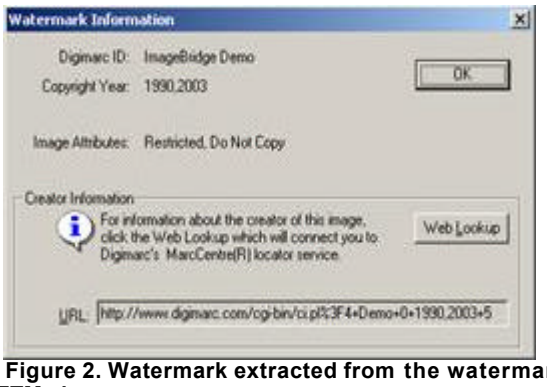

Figure 2. Watermark extracted from the watermark ETM+ image

There was no visual difference between the watermark image and the original image free of watermark. Next was to statistically calculate and classify the two images.

Filename: L:\watermarking\ETM

Band	Min	Max	Mean	Stdev St.D.
1	58	218	85.049374	9.988729
2	38	195	75.128833	13.573550
3	29	211	80.395965	22.476985
4	28	195	104.786917	15.211813
5	17	199	104.343045	23.340459
6	13	186	77.645888	24.543400

Filename: L:\watermarking\ETM_mark.raw

Band	Min	Max	Mean	Stdev St.D.
1	50	218	85.076675	10.864268
2	33	195	75.136354	14.023220
3	25	211	80.381990	22.674076
4	28	195	104.786917	15.211813
5	17	199	104.343045	23.340459
6	13	186	77.645888	24.543400

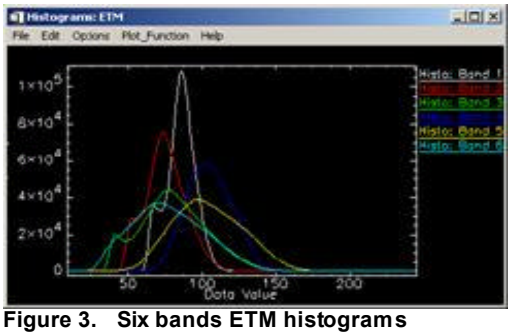

Figure 3. Six bands ETM histograms

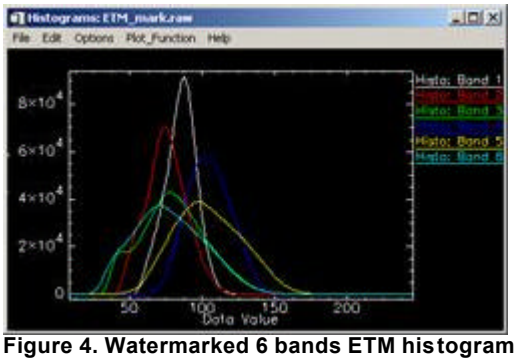

Figure 4. Watermarked 6 bands ETM histograms

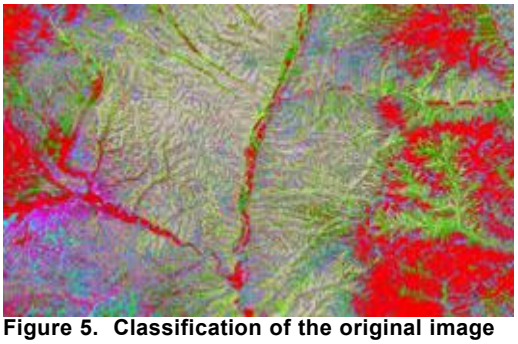

Figure 5. Classification of the original image

As show in the statistical results above, there is obvious change between each band of the first three bands of the original image and the corresponding band in the watermark image. Briefly, it was only the first three bands of a multi-band image that Digimarc watermark was inserted into.

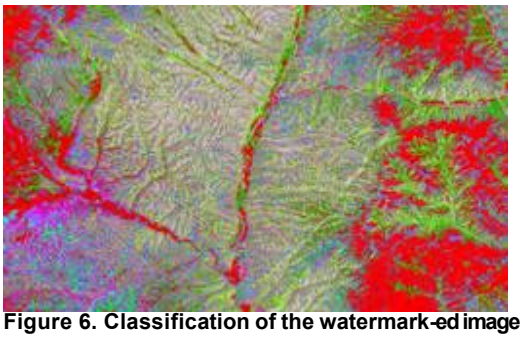

Figure 6. Classification of the watermark-ed image

In software Photoshop® 5.0, the watermark image was modified through color modification, rotation, re-sampling, cropping, high-pass and low-pass filtering respectively. The results of such operations showed the watermark in the multi-band image inserted with Digimarc still existed.

Band by band, the watermark image was processed again according to the operations above. In the resulting six bands, there was watermark in the first three, while no in the later three.

With unsupervised classification method, the full-scene pixels of the original six-band ETM+ image and the watermark image were classified into five classes respectively (Figure 5 & 6). The difference of the two classification results was achieved through subtracting one from another (Figure 7). This difference image detected the obvious change between the original image and the watermark image.

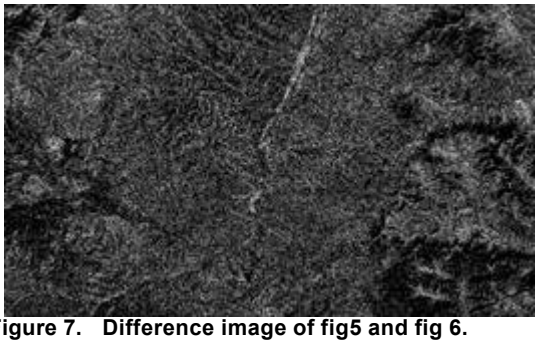

Figure 7. Difference image of fig5 and fig 6.

It clearly shows that Digimarc watermark is robust to the attacks from conventional remote sensing image processing algorithms and the watermarking technique should not be applied onto images to be classified and pattern-recognized.

4.2 The application of Watermarking techniques in spatial domain

With the transparent-layer-stack technique of Photoshop ®5.0, a watermark, the transparency of which was within 1%, was inserted into a color composite of ETM+ bands 7, 4, 3. There is no visual difference between the original image and the watermark image (Figure 8 & 9). Below are the statistical results of the two images:

Filename: L:\watermarking\rgb.tif

Band	Min	Max	Mean	Stdev	St.D.
1	0	255	95.990161	58.717253	
2	8	255	163.943393	38.528658	
3	8	255	101.813052	55.030112	

Filename: L:\watermarking\rgb_marked.tif

Band	Min	Max	Mean	Stdev	St.D.
1	0	255	96.060895	58.712468	
2	8	255	163.988973	38.512696	
3	8	255	101.879750	55.032148	

As shows in the statistical results above, there is trivial statistical difference between the original image and the watermark image.

Such watermark based on spatial domain is robust to attacks from re-sampling, filtering operations, while it may be lost in trimming, cropping and color adjustment operations.

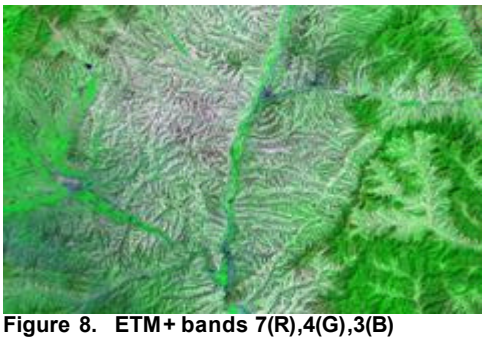

Figure 8. ETM+ bands 7(R),4(G),3(B)

Figure 9. ETM+ bands 7(R),4(G),3(B) with watermark

Figure 10. The watermark detected in the figure 9

5. Conclusion

In this paper, we discussed the potential applications of digital watermarking techniques in remote sensing image processing, gave two samples to say that the present digital watermarking techniques could be wide applied on images to be visually interpreted and analyzed and the watermarking techniques based on spatial domain would less affect the final results of images to be auto-classified and pattern recognized, than those based on frequency domain. In a word, more effort should be made on specific watermarking techniques for remote sensing images.

6. References

1. J. R. Hernandez, M. Amado, and F. Perez-Gonzales, \DCT-domain watermarking techniques for still images: detector performance analysis and a new structure," IEEE Trans. Image Proc. 9, pp. 55-68, Jan. 2000.

2. Niu Xia-mu, Lu Zhe-ming, Sun Sheng-he. Digital watermarking od still images with gray level digital watermarks. IEEE trans. On Consumer Electronics.

3.M.Kutter, F.A.P. Petitcolas. A fair benchmark for image watermarking system (j). in proceedings of SPIE, Jan.1999,3657.

4.W.B.Pennebaker, J.L.Mitchell. JPEG: Still Image Data Compression Standard （M）. New York: Van Nostrand Reinhold,1993.

5. S. Craver, N. Memon, B. L. Yeo, and M. M. Yeung, \Resolving rightful ownership with invisible watermarking techniques: limitations, attacks and implications," IEEE Journ. Sel. Areas Commun. 4, pp. 573-586, May 1998.

6. Web page www.jpeg.org, JPEG2000 Part I Final Committee Draft Version 1.0.

7. J. A. Richards, ed., Remote sensing digital image analysis: an introduction, Springer, Berlin, 1986.

9. M. Barni, F. Bartolini, and A. Piva, \Improved wavelet-based watermarking through pixel-wise masking," IEEE Trans. Image Processing 10, May 2001.