Watermarking Spectral Images through PCA Transform

Arto Kaarna, Pekka Toivanen and Kimmo Mikkonen
Lappeenranta University of Technology
Department of Information Technology, Lappeenranta, Finland

Abstract

In this paper we present a technique to embed a digital watermark containing copyright information into a spectral image. The watermark is embedded in the transform domain of the image. The transform domain is derived by performing the PCA transform on the original image. The watermark is embedded by modifying the coefficients of the eigenvectors from the PCA transform. After modification the image is reconstructed by the inverse PCA transform, thus containing the watermark. We provide analysis of watermark's imperceptibility and robustness against some attacks. Experimental results indicate that the watermarked image is very similar to the original one and the watermark can be extracted from the image after those attacks.

Introduction

Since the amount of image data transfers have increased rapidly in the Internet, there has emerged the need of new techniques to insert copyright information to the data. Different kinds of digital watermarks bring solution to this problem. With digital watermark, the owner of the image can embed some personal information or a logo into the image and prove the ownership in case of a copyright violation. Several techniques have been developed to add digital watermarks into gray-scaled and color images.[1,2] This paper presents a watermarking technique for spectral images.

Digital watermark information must be hidden so that the image stays perceptually unchanged. However, the watermark must be detectable using a particular extraction algorithm. Another important demand for watermarking method is robustness. Different users may alter the image in many different ways. For example, they can compress, crop and filter it. These alterations can be done intentionally in order to remove the watermark or for some other reasons. Therefore the watermark must be robust enough to survive these kinds of attacks.[2]

The contents of this article is as follows. In the next section we present the embedding and detection methods for watermarking and the basic guidelines of the PCA transform. In the third section we describe the attacks. The fourth section contains the experiments. In the last section we evaluate the results, make conclusions and discuss the pros and cons of this watermarking method.

Watermarking Method

Embedding the Watermark

Whereas normal RGB images have three color bands and the information for those bands is integrated from the wavelengths of visible light, the spectral images have a large number of bands and they contain information from a wider spectrum, also outside the visible range. Spectral images are widely used in remote sensing and their usage in computer vision and industrial applications is growing.[3]

In our watermarking method we embed the watermark in the transform domain of a spectral image. The spectral domain has been reduced using the principal component analysis (PCA).[3] The PCA algorithm creates the covariance matrix C from the spectral data and then computes eigenvalues and eigenvectors u of that matrix. In practical calculations C is replaced by an estimated $\hat{C}$,

$$\hat{\mathrm{C}} = \frac{1}{\mathrm{n}} \sum_{i=1}^{n} (x_i - \hat{\mu})(x_i - \hat{\mu})^T \qquad (1)$$

where x_i is a sample vector, $\hat{\mu}$ is the estimated mean vector of the sample set and the sum is over all samples.[3] The PCA selects the eigenvectors relating to the largest eigenvalues and the presents the original spectra using the selected eigenvectors.

The watermark is inserted into the image by replacing part of coefficients for eigenvectors with the watermark. After the insertion, inverse principal component analysis (IPCA) is performed. It reconstructs the image into its original format, now containing the watermark. The estimation of original data is received from

$$x^* = \sum_{j=1}^{p} (x^T u_j) u_j \qquad (2)$$

where p is the number of selected eigenvectors.[3] The embedding of the watermark is illustrated in Figure 1.

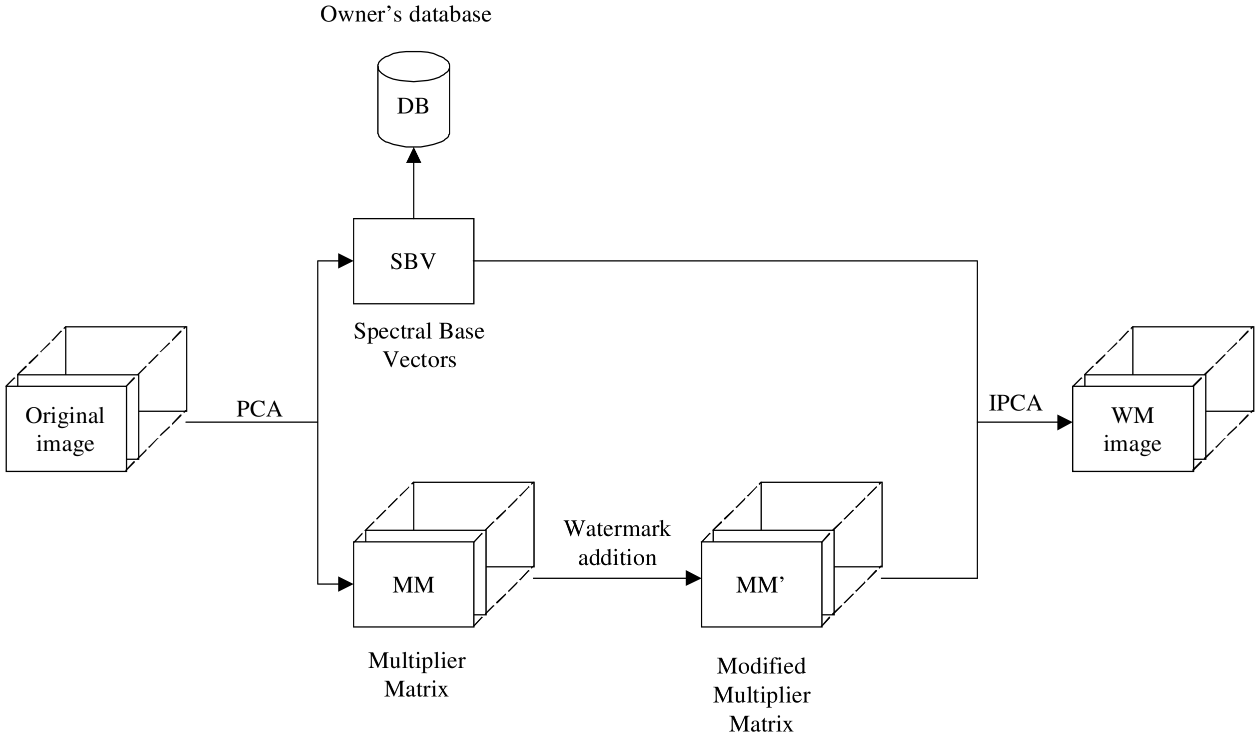

Figure 1. Watermarking method using the PCA transform

As a result from the PCA transform, two matrices are produced. The first matrix (SBV) contains the spectral eigenvectors. The owner must save these vectors into a database in order to later detect the watermark from the image. The second matrix is the multiplier matrix (MM), which contains the coefficients for the eigenvectors. The owner chooses one band from this matrix and replaces it with watermark. Then the image is reconstructed with the inverse PCA transform using the modified multiplier matrix.

Naturally the reconstructed image differs from the original image due to the embedded watermark.

Detection of the Embedded Watermark

Later the owner can detect the watermark with a simple procedure. When the watermarked image is multiplied with the original eigenvectors, the modified MM matrix is restored. The watermark can be then found at the same band of the matrix as it was originally inserted. The watermark detection process is illustrated in Figure 2.

Attacks

The watermark must be not only imperceptible but also robust so that it can survive some basic attacks and signal distortions. Since spectral images are often very large in both spectral and spatial dimensions, then image compression is usually needed. Lossy compression lowers the quality of the image and the watermark. JPEG 2000 is a new image compression format, which is most likely going to become popular in the near future. It uses the wavelet transform (DWT) as a compression scheme instead of the Discrete Cosine Transformation (DCT), which is used in the old JPEG format. Wavelet compression method stores the image data as a stream of information instead of square blocks.[6] JPEG 2000 compression can be performed at different bit-rates, which determines the quality and file size of the compressed image.[7]

Other possible attacks are different kind of filtering operations, such as mean and median filtering. Mean filtering softens the image by calculating the mean of the pixel neighborhood in the image. Median filtering removes occasional bit errors or other outliers of a pixel value. It also removes exceptional spectral values even though they were actual measurements. Finally, filtering modifies the pixel value according to the selected filtering operation.

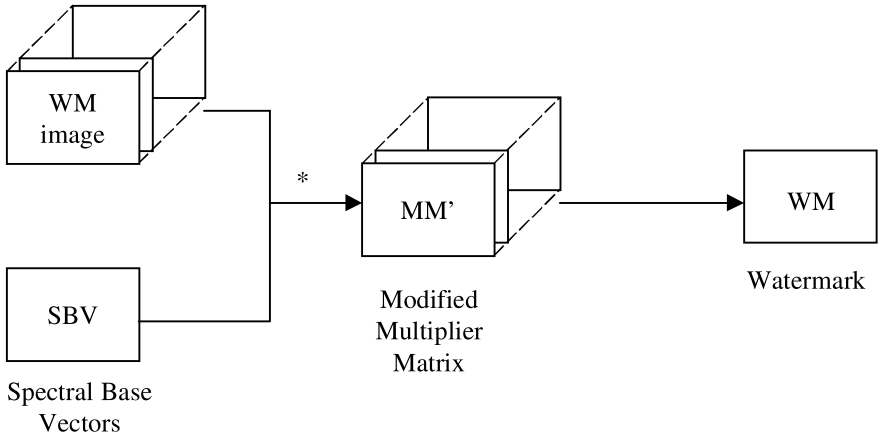

Figure 2. Watermark detection algorithm

Experiments

We applied this watermarking method to a multispectral image from the AVIRIS set.[8] The spectral range of the original AVIRIS-image is from 400 nm to 2500 nm and it has 224 spectral bands. We selected every 7th band from the Moffett Field image and cropped the image in spatial dimension. This resulted into image of size 256*256*32 with 16-bit resolution. The watermark was a simple one-band logo containing the letters L, U and T, each with different gray-scale value. The watermark resolution was also 256*256. The PCA transform results to 32 spectral vectors and the watermark was embedded into 10th band of the multiplier matrix (MM). Then the watermark was extracted from the image with the detection algorithm for evaluation.

We measured the difference between the watermarked image and the original image. The difference was calculated using Signal-to-Noise Ratio (SNR) and Peak Signal-to-Noise Ratio (PSNR), which are defined for spectral images as

$$SNR = 10\log_{10}\frac{E^{o}}{E^{wm}},\ PSNR = 10\log_{10}\frac{MN^{2}s^{2}}{E^{wm}} \quad (3)$$

where E^{o} is the energy of the original image, E^{wm} is the difference between the energy of the original image and the energy of the watermarked image, M is the number of bands in the image, N^{2} is the number of pixels in the image and s is the peak value of the original image.[9]

In addition to SNR and PSNR we used 12 different similarity measures for vectors[7] and calculated a weighted mean of those 12 measures. The weight for each measure was defined experimentally based on each measure's adaptability on spectral images. The value of the weighted mean S_M is *1.0* if the compared images are identical. The lower the S_M, the lower the similarity between the two vectors or in our case, between two images. The same measures were used comparing the extracted watermark with the original watermark.

The fourth method we used for quality measurement was calculating the correlation coefficient *CC* (-1 ≤ *CC* ≤ 1), which is calculated between two images using

$$CC = \frac{\sum_m\sum_n\left(A_{mn}-\overline{A}\right)\left(B_{mn}-\overline{B}\right)}{\sqrt{\left(\sum_m\sum_n\left(A_{mn}-\overline{A}\right)^2\right)\left(\sum_m\sum_m\left(B_{mn}-\overline{B}\right)^2\right)}} \quad (4)$$

where *A* and *B* sized images.[10] The value of *CC* is *1.0* if the two images are identical.

In Figure 3 we show the first band from the original image and from the watermarked image. In Figure 4 there is the band 10 similarly. Figure 5 illustrates the original logo and the logo extracted from the watermarked image.

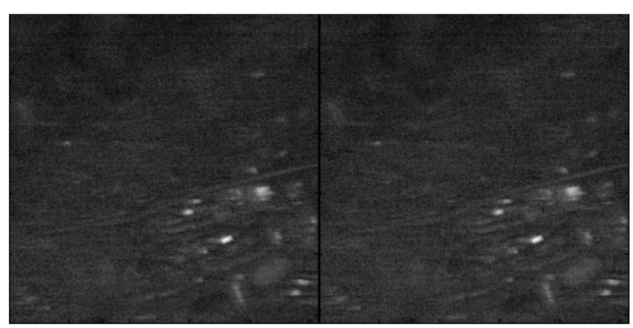

Figure 3. Band 1 of the original image (left), band 1 of the watermarked image (right).SNR = 46.0, PSNR = 55.7, S_M = 0.9764 and CC = 0.9987

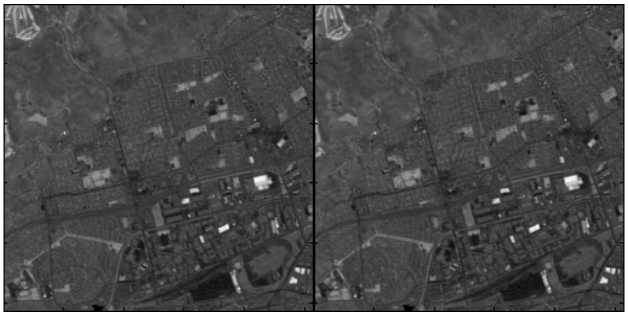

Figure 4. Band 10 of the original image (left), band 10 of the watermarked image (right). SNR = 36.3, PSNR = 46.5, S_M = 0.8605 and CC = 0.9978

Figure 5. Original watermark (left), extracted watermark (right). SNR = 52.4, PSNR = 60.3, S_M = 0.9980 and CC = 1.000.

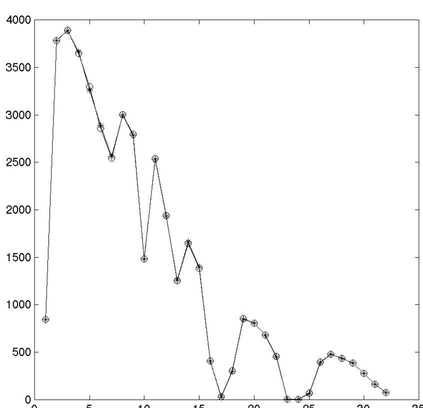

Figure 6. Mean spectrum from the original image (o) and from the watermarked image (*).

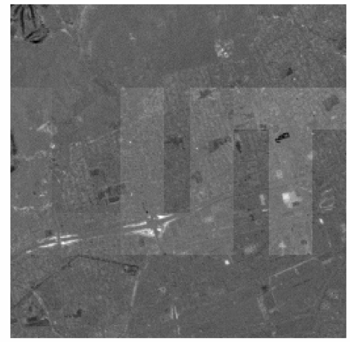

Figure 7. Band 12 from the difference image between the original image and the watermarked image. Maximum absolute error is 384 in the 16 bit resolution image.

Table 1. Eigenvalues of Original Image and of the Watermarked Image.

Eigenvalues (1.0e+012 *)	
Watermarked Image	Original image
0.00000000554	0.00001665211
0.00000000555	0.00002150161
0.00000000557	0.00002725959
0.00000000558	0.00003234345
0.00000000561	0.00005029566
0.00000000561	0.00006773485
0.00015242413	0.00007915329
0.00016977910	0.00015247704
0.00024182648	0.00017041822
0.00061432684	0.00024212787
0.00068490515	0.00063347959
0.00101096671	0.00100949009
0.00991701114	0.00991701110
0.02385282182	0.02382752031
0.13277488686	0.13277486301
7.35307004786	7.35281051838

A series of experiments was run to test the robustness of the watermark. The watermarked image was compressed with JPEG 2000[9] using bit-rate 3 bps/band and after decompression the quality of the extracted watermark was evaluated. Other tested attacks on the watermark were trimmed mean filter, median filter with two different window sizes and vector median filter. Visual presentations of the image and of the watermark logo after different attacks are shown in Figures 8 and 9. The results on robustness against different attacks are summarized in Table 2 and in Table 3.

Conclusions

We proposed a watermarking technique, which works well with spectral images. Embedding a watermark into an image using the PCA transform has only minor influences on image quality and the watermark survives quite well through tested attacks and it remains clearly recognizable. JPEG 2000 compression seems to have a larger effect on the watermark quality than other attacks, but it degrades visual image quality less than others. It can also be noted that the visual quality of the extracted watermark isn't always accurately comparable with the SNR results.

The application of a watermarking method can be detected from the eigenvalues of the watermarked image, see Table 1. The values up to the tenth eigenvalue are similar, but from ten forward the eigenvalues differ heavily. This implies that the method requires enhancements concerning both the embedding process and the definition of the watermark.

Table 2. Robustness Against Attacks, Image

Attack	SNR	PSNR	S_M	CC
Vector median	21.7	40.8	0.8337	0.9933
Median 3x3	21.9	41.0	0.8337	0.9936
Median 5x5	17.9	37.0	0.7505	0.9842
Trimmed mean	22.0	41.2	0.8166	0.9938
JPEG 2000	36.7	55.8	0.9608	0.9998

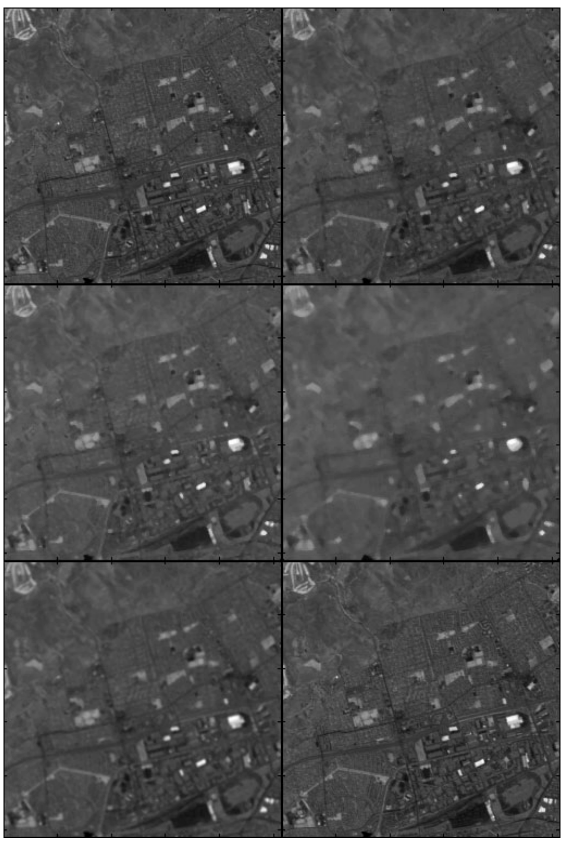

Figure 8. Band 10 of the watermarked image: original (top left), after vector median filtering (top right), after median filtering with 3x3 window (middle left), after median filtering with 5x5 window (middle right), after trimmed mean filtering (bottom left) and after JPEG 2000 compression (bottom right)

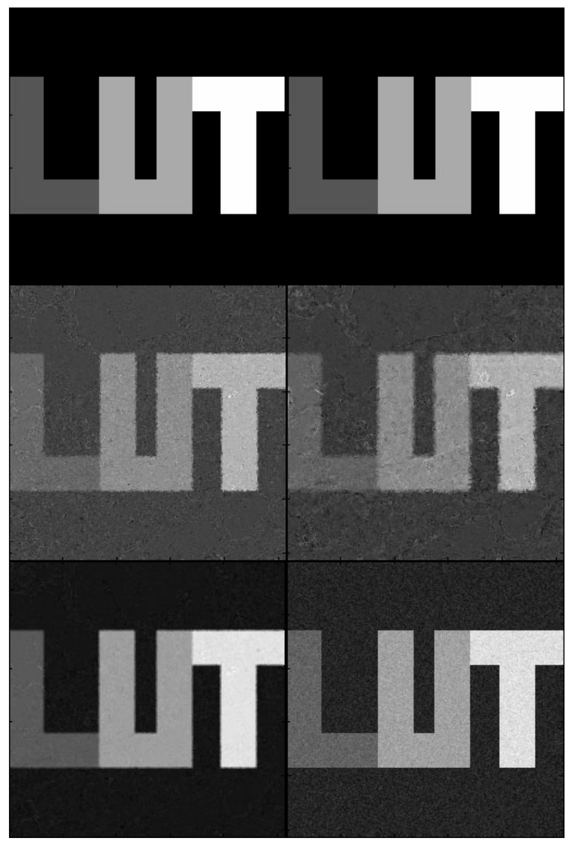

Figure 9. Watermarks: original (top left), after vector median filtering (top right), after median filtering with 3x3 window (middle left), after median filtering with 5x5 window (middle right), after trimmed mean filtering (bottom left) and after JPEG 2000 compression (bottom right)

Table 3. Robustness Against Attacks, Watermark

Attack	SNR	PSNR	S_M	CC
Vector median	15.3	23.3	0.9756	0.9798
Median 3x3	12.7	20.6	0.8154	0.9633
Median 5x5	11.7	19.6	0.7915	0.9529
Trimmed mean	18.4	26.3	0.9421	0.9900
JPEG 2000	18.3	26.3	0.8803	0.9900

References

1. D. Kundur, D. Hatzinakos, A Robust Digital Image Watermarking Method using Wavelet-Bsed Fusion, Proc. IEEE Int. Conf. On Image Processing, Santa Barbara, California, vol. 1, pp. 544-547, 1997.
2. R.B. Wolfgang, C.I. Podilchuk, E.J. Delp, Perceptual Watermarks for Digital Images and Video, Proceedings of The IEEE, vol. 87, Iss. 7, July 1999, pp. 1108-1126.
3. Kaarna, Multispectral Image Compression Using the Wavelet Transform, Lappeenranta University of Technology, 2000.
4. J. Parkkinen, T. Jaaskelainen, Color representation using statistical pattern recognition, Applied Optics, Vol. 26, No. 19, 1987, pp 4240-4245.
5. Kaarna, P. Zemcik, H. Kälviäinen, J. Parkkinen, Compression of Multispectral Remote Sensing Images Using Clustering and Spectral Reduction, IEEE Transactions on Geoscience and Remote Sensing, Vol. 38, No. 2, March 2000, pp 1073-1082.
6. www-site: http://www.designer.com/focus/articles/web_future/web_future_print.htm, August 16, 2002.
7. D. S. Taubman, M. W. Marcellin, JPEG2000, Image Compression Fundamentals, Standards and Practise, Kluwer Academic, 2002.
8. www-site: http://makalu.jpl.nasa.gov/ , July 25, 2002.
9. M. Rabbani, P.W. Jones, Digital image compression techniques, SPIE, Volume TT 7, USA, 1991.
10. M. Hild, On the effectiveness of color similarity measures in background-frame differencing applications, Proc. CGIV 2002: The First European Conference on Colour in Graphics, Image and Vision, 2002, pp 304-309.
11. Matlab 6 help files, function `corr2`. www-site: http://www.jpeg.org/JPEG2000.htm , July 19, 2002.

Biography

Arto Kaarna received his M.Sc. degree in 1980 in Mechanical Engineering and Lic.Tech. degree in 1990 and Dr. Tech. degree in 2000 in computer science at Lappeenranta University of Technology, Finland (LUT). Currently he is working as a professor in media in networks with LUT. His main research interests are in color and spectral image processing. He is a member of IEEE and Pattern Recognition Society of Finland.