PCA Transform in Watermarking Spectral Images

Arto Kaarna, Pekka Toivanen and Kimmo Mikkonen

Lappeenranta University of Technology, Department of Information Technology, Lappeenranta, Finland

In this study we present a technique to embed a digital watermark containing copyright information into a spectral image. The watermark is embedded in a transform domain of the spectral dimension of the image. The transform domain is derived by performing the principal component analysis (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 attacks with various parameter values in embedding and in attacks. The attacks include lossy image compression by the wavelet transform, median filtering and mean filtering. Experimental results indicate that the watermarked image is very similar to the original one and the watermark can be extracted with reasonable visual fidelity from the image after the attacks.

Journal of Imaging Science and Technology 48: 183–193 (2004)

Introduction

Since the volume of image data transfers has increased rapidly in the internet, there has emerged a need for new techniques to insert copyright information to that data. Different kinds of digital watermarks bring solution to this problem. With a digital watermark, the owner of the image can embed some personal information or a logo into the image and prove ownership in case of a copyright violation. Through watermarking the owner of the image can authenticate the authorized use of the image.[1] In steganography, the purpose is to include the actual message as a watermark embedded in the information carrying image.[2]

The watermarking technique must carry the following requirements to be applicable: readability, security, imperceptibility, and robustness. Readability means detectable information content, security means concealing the watermark from unauthorized detection, imperceptibility is important for visually utilized images, and robustness guarantees the existence of the watermark in the image after different attacks. The attacks include image processing operations like compression, smoothing, blurring, sharpening, or even cropping.

Several techniques have been developed to add digital watermarks into gray scale and RGB-color images.[3,4] Most often the watermark is embedded in the transform domain of the image,[3,5] but the original spatial domain has also been used.[6] For RGB-color images the suitability of different color spaces have been considered for watermarking.[7]

This study presents a watermarking technique for spectral images. Spectral images are often used in remote sensing and, nowadays, their utilization has expanded to industrial applications for example in quality control. Spectral images constitute a new area for watermarking technology. The transform domain has also been popular in spectral image watermarking. One solution for spectral images is to embed a watermark in the transform domain of each band. The transform domain is calculated with the discrete cosine transform or the wavelet transform[8] or with the Hadamard transform.[9] The watermarks in the above references are binary or gray scale images.

The 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. Users may alter the image in many different ways. For example, they can compress, crop, smooth, sharpen, or otherwise filter the image. These alterations can be done intentionally in order to remove the watermark or they are operations that are performed based on requirements from the application area. Therefore the watermark must be robust enough to survive these kinds of attacks.[4]

Cropping is a particularly significant attack for spectral images. Against cropping the watermark must remain apparent in all parts of the spectral image. This requires a new type of watermark totally different of the visual watermark previously considered. The embedding procedure must be enhanced from direct summing to a mixing system. In this study the cropping attack is not explicably considered further, however.

The contents of this article are as follows. In the next section we present the embedding and extraction methods for watermarking and the basic guidelines of the principal component analysis (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.

Original manuscript received December 3, 2004

Arto.Kaarna@lut.fi; tel.: +358 5 621 11; fax: +358 5 621 2899

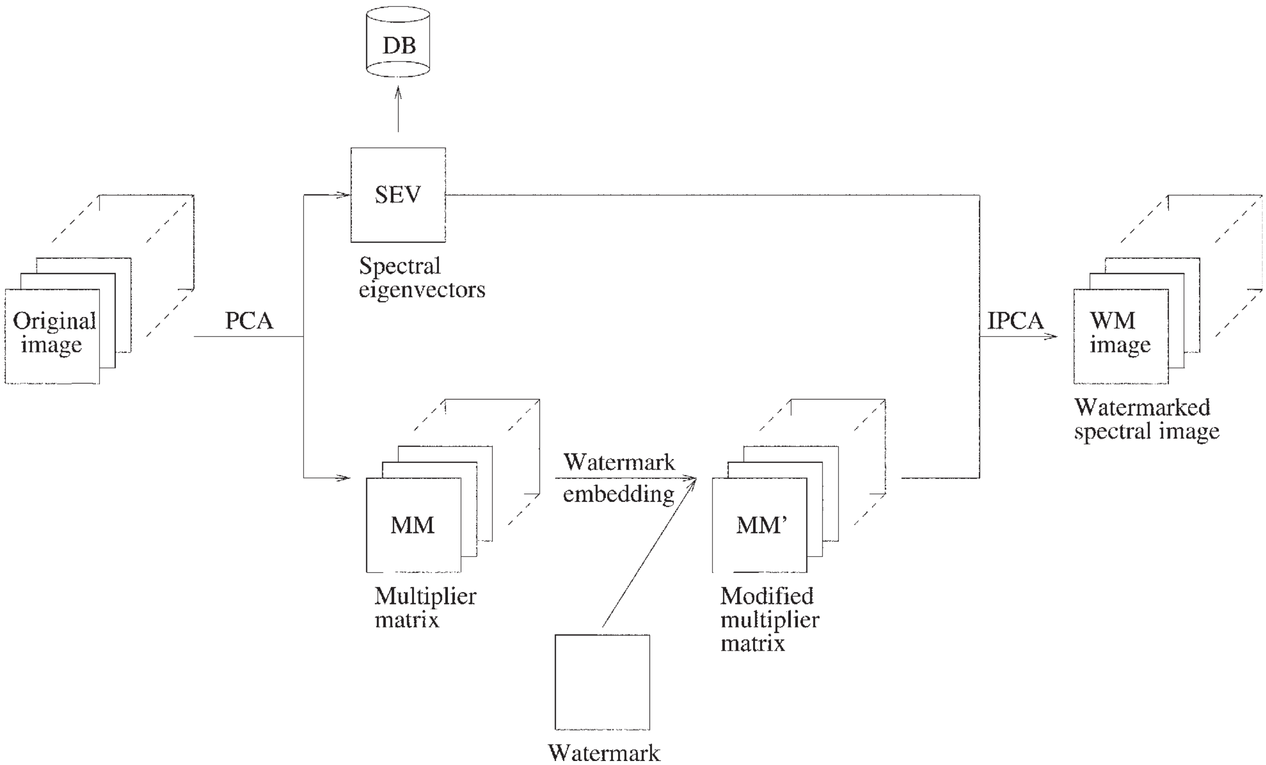


Figure 1. Embedding procedure using PCA transform.

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 may 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.[10]

In our watermarking method we embed the watermark in the transform domain of a spectral image. The spectral domain has been transformed using the principal component analysis (PCA).[11,12] 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 $\hat{C}$,

$$\hat{C} = \frac{1}{n}\sum_{i=1}^{n}\left(x_i - \hat{\mu}\right)\left(x_i - \hat{\mu}\right)^T \tag{1}$$

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.[11] In subspace analysis of the PCA, the eigenvalues are sorted and then the eigenvectors relating to the p largest eigenvalues are selected. These eigenvectors then represent the original spectra with a small error depending on the number p of selected eigenvectors.

The watermark is embedded into the image by adding the watermark to a selected part of the coefficients for eigenvectors. After the embedding, the 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

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

where p is the number of selected eigenvectors.[11,13] The procedure of embedding the watermark is illustrated in Fig. 1.

As a result of the PCA transform the eigenvalues, the eigenvectors, and the multipliers for the eigenvectors are obtained. The two last results are stored into two matrices. The first matrix (SEV) contains the spectral eigenvectors. The owner must save these vectors in a database in order to extract the watermark from the watermarked image. The second matrix is the multiplier matrix (MM), which contains the coefficients for the eigenvectors. These coefficients are in planes and these planes can be also considered as eigenimages, E. The number of eigenimages, E, in the multiplier matrix (MM) is the same as is the number of bands in the original spectral image, i.e., n. The spatial size of the multiplier matrix is the same as that of the original spectral image. The eigenvalues are sorted in ascending order and the multiplier matrix is constructed from the eigenimages corresponding to the order of the sorted eigenvalues.

The owner chooses a set of eigenimages E_K from the multiplier matrix and embeds the watermark W in them. This can expressed as

$$E_K = s_1 E_K + s_2 W \tag{3}$$

where the coefficients s_1 and s_2 control the strength of embedding. The set K may contain only one eigenimage or any number of eigenimages. The summing operation is a symbolic expression for mixing the watermark and the original eigenimages in the set K.

After embedding the image is reconstructed with the inverse PCA transform using the modified multiplier

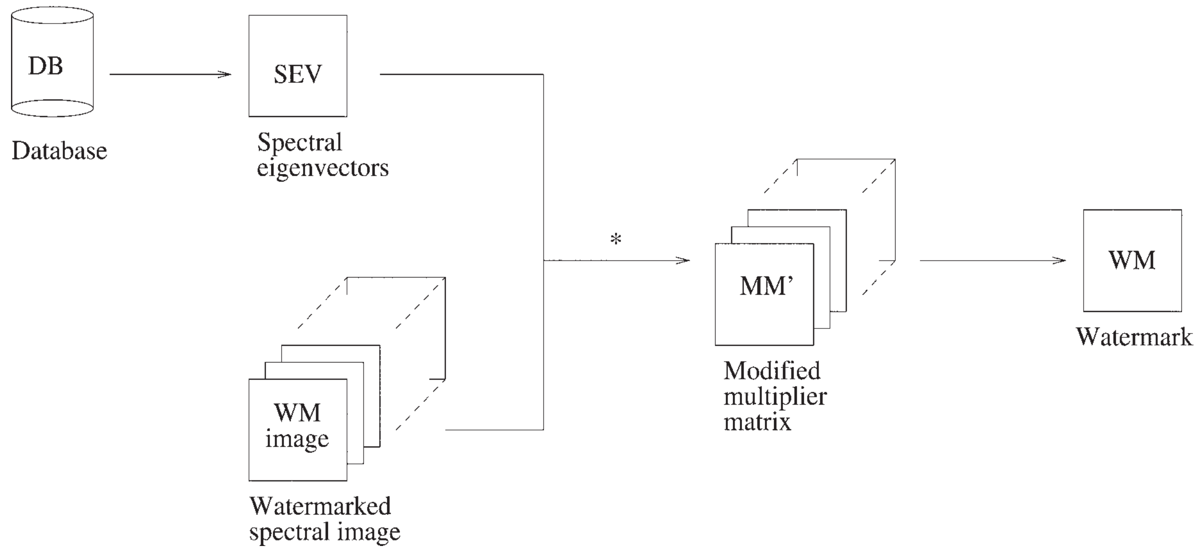


Figure 2. Extraction procedure.

matrix (MM') and the original spectral eigenvectors (SEV). Naturally the reconstructed image differs from the original image due to the embedded watermark.

Extraction of the Embedded Watermark

If the watermark is embedded into a spectral image with the procedure described in Fig. 1 then the owner of the image can extract the watermark with a procedure illustrated in Fig. 2. When the watermarked image is multiplied with the original spectral eigenvectors, the modified multiplier matrix (MM') is restored, see Eq. (2). The watermark can be then found from the same eigenimages of the modified multiplier matrix in which it was originally embedded.

The extraction procedure requires the original spectral eigenvectors. They are stored and kept secret in the database by the owner of the original image. Thus, the watermark can be extracted reliably only by the owner.

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 lossy image compression is usually applied to them. Lossy compression lowers the quality of the image and of the extracted watermark. JPEG 2000 is a new image compression format which is most likely going to become popular in the near future. It uses the discrete wavelet transform (DWT) as a compression scheme instead of the discrete cosine transform (DCT), which is used in the old JPEG format. The wavelet compression method stores the image data as a stream of information instead of square blocks.[14] JPEG 2000 compression can be performed at different bit rates, which determines the quality and file size of the compressed image.[15]

Fast Discrete Wavelet Transform

The fast discrete wavelet transform is computed using perfect reconstruction filter banks. Vetterli showed,[16] that perfect reconstruction was always possible using FIR-filters. The multiresolution approximation lead to two discrete, finite length filters, and, thus, a filter bank was a solution to a fast implementation.

The original data is $f(t)$. Using the definition

$$f(t) = \sum_{n=-\infty}^{\infty} a_0[n]\phi(t-n) \tag{4}$$

and since the set of basis functions $\{\phi(t-n)\}n \in_Z$ is orthonormal, then

$$a_0[n] = \langle f(t), \phi(t-n) \rangle \tag{5}$$

The approximation in the next coarser level is obtained by

$$a_{j+1}[p] = \sum_{n=-\infty}^{\infty} h[n-2p]a_j[n] \tag{6}$$

and the difference between the two levels by

$$d_{j+1}[p] = \sum_{n=-\infty}^{\infty} g[n-2p]a_j[n] \tag{7}$$

where $g[n]$ is defined as

$$g[n] = (-1)^{1-n}h[1-n] \tag{8}$$

Now $h[n]$ and $g[n]$ constitute the filter bank consisting of a lowpass filter $h[n]$ and of a highpass filter $g[n]$.

At the reconstruction the coefficients are obtained as

$$a_j[p] = \sum_{n=-\infty}^{\infty} h[p-2n]a_{j+1}[n] + \sum_{n=-\infty}^{\infty} g[p-2n]d_{j+1}[n] \tag{9}$$

Finally, the discrete values of the original function are recovered from

$$f_d[p] = \sum_{n=-\infty}^{\infty} a_0[n]\phi_d[p-n] \tag{10}$$

Since the scaling and the wavelet filters are finite, the infinite sums in Eqs. (4) through (10) are computed using convolution.

The transform coefficients are the values of a_{j+J} and d_{j+i}, $i = 1,\ldots,J$ where J is the number of levels in the transform. Downsampling by two ($\downarrow 2$) is performed in the transform and upsampling by two ($\uparrow 2$) in the inverse transform. In practice, Eq. (5) is not used and the values for a_0 are obtained directly as discretized values $f[n]$ of $f(t)$. Due to the perfect reconstruction property, the inverse transform returns the discretized values $f[n]$ directly as coefficients a_0.

With higher dimensional data the one-dimensional transform is applied to each dimension separately. For example, for images, the one-dimensional transform is applied to the rows and to the columns of the image. This results in four separate blocks containing approximation coefficients in one block and three different detail coefficients in three other blocks.

The justification for the wavelet transform in signal compression comes from the nonlinear approximation,[17] where the linear combination of N basis functions is used instead of the first M basis functions. In the linear approximation, the space S_n spanned by the first M basis functions Φ_n is

$$S_n = \left\{ \sum_{n=1}^{M} c_n \Phi_n ; c_n \in C \right\} \tag{11}$$

and in the nonlinear approximation the space S_n is

$$S_n = \left\{ \sum_{n} c_n \Phi_n ; c_n \in C, \# \left\{ n, c_n \neq 0 \right\} \leq M \right\} \tag{12}$$

In nonlinear approximation the wavelet coefficients are ordered according to their significance and the most significant coefficients and their addressing are included in the bit rate. The most significant coefficients may originate from any of the blocks.

Filtering the Image

Other possible attacks are different kinds of filtering operations, such as mean filtering, median filtering and vector 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 would be results of actual measurements.

Vector median filtering is suitable for vector valued signals.[18] The vector median filter for vectors x_1, x_2, …, x_L is a vector x_{vm} defined as

$$x_{vm} \in \left\{ x_i \mid i = 1,\ldots,L \right\} \tag{13}$$

such that for all $j = 1, \ldots, L$

$$\sum_{i=1}^{L} dist\left(x_{vm}, x_i\right) \leq \sum_{i=1}^{L} dist\left(x_j, x_i\right) \tag{14}$$

where $dist(x, y)$ is the selected distance between the two vectors x and y.

Experiments

We applied the watermarking method defined above to a multispectral image from the AVIRIS set.[19] The spectral range of the original AVIRIS-image covers a range from 400 nm to 2500 nm and has 224 spectral bands. We selected every seventh band from the Moffet Field image and cropped the image in the spatial dimensions. This resulted in an image of size 256 × 256 × 32 with 16-bit resolution. The test image is displayed in Fig. 3(a). The Moffet Field image contains forests, fields, mountainous terrain, rivers, lakes, and also urban areas.

The watermark was a simple one-band logo containing the letters L, U and T, each with different gray scale value. The size of the watermark was also 256 × 256, but with 8 bit resolution. The watermark is displayed in Fig. 3(b). The purpose of this watermark was only to carry visually a record of the watermark existence in the spectal image. Other types of watermarks may carry authorization information, timestamps or other textual information.

The PCA transform results in 32 spectral vectors and the watermark was embedded in various eigenimages of the multiplier matrix (MM). The purpose of this experiment was to define a suitable eigenimage such that the watermark is not visible and the watermarked image can still survive attacks.

Finally, the watermark was extracted from the image with the detection algorithm for evaluation. We evaluated the quality both from the reconstructed image and from the extracted watermark by using the quantitative difference between the original image and the reconstructed image or between the original watermark and the extracted watermark. The difference was calculated using Signal-to-Noise Ratio (SNR) and Peak Signal-to-Noise Ratio (PSNR), which are defined for spectral images as

$$SNR = 10\log_{10}\frac{E^o}{E^d},\ PSNR = 10\log_{10}\frac{MN^2 s^2}{E^d}, \tag{15}$$

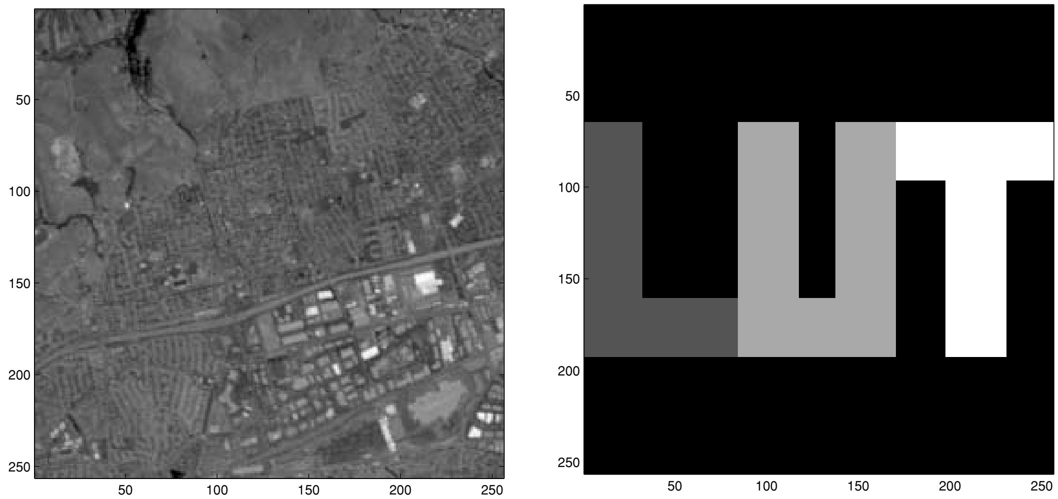
where E^o is the energy of the original image, E^d is the energy of the difference between the original image and the watermarked image, M is the number of bands in the image, N^2 is the number of pixels in the image and s is the peak value of the original image.[20]

In addition to SNR and PSNR we used 12 different similarity measures for vectors[21] 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 SM is $SM = 1.0$ if the images compared are identical. The lower the SM, the lower the similarity between the two vectors or in our case, between the two images. The same measures were used in comparison of the extracted watermark with the original watermark.

The fourth method for quality measurement was the correlation coefficient CC,[22] which is calculated between two images as

$$CC = \frac{\sum_m \sum_n \left(A_{mn} - \hat{A}\right)\left(B_{mn} - \hat{B}\right)}{\sqrt{\sum_m \sum_n \left(A_{mn} - \hat{A}\right)^2 \sum_m \sum_n \left(B_{mn} - \hat{B}\right)^2}} \tag{16}$$

where A_{mn} and B_{mn} are the values from the images of a same size. $\hat{A}$ and $\hat{B}$ are the respective means for the two images A and B. The value of $CC = 1.0$ if the two images are identical.



(a) (b)

Figure 3. (a) Band 5 from the original image, (b) the watermark.

In Fig. 3(a) the band 5 from the original spectral image is shown and in Fig. 3(b) the gray scale watermark applied in the experiments is shown.

Embedding and Extraction of the Watermark

The watermark can be embedded in any set of eigenimages in the multiplier matrix after the PCA transform. In this study the following selections in Eq. (3) were made:

- set of eigenimages K: $K = H$, where H is a single number. Thus, the watermark is embedded in a single eigenimage. The value for H can be selected.
- coefficient s_1: $s_1 = 0$. This means, that the watermark replaces the eigenimage K.
- coefficient s_2: $s_2 = s$. The coefficient s controls the strength in embedding. Now s multiplies the values of the watermark and thus, s can also be considered as extending the resolution of the watermark.

In PCA and in embedding the eigenimages are connected to the sorted eigenvalues. The larger the respective eigenvalue the more visible the watermark will be. Similarly, the selection of a band with a lower eigenvalue means less visual interference but at the same time, lower resistance in attacks.

Figure 4 illustrates the quality of the embedding of the watermark in various eigenimages K of the multiplier matrix. The number of the eigenimage where the watermark was embedded is on the horizontal axis and on the vertical axis, there is the the quality of the watermarked spectral image expressed as PSNR from Eq. (15). The value of strength was $s = 1.0$.

In addition to visual interference the embedding in an eigenimage with too low eigenvalue results in additional discrepancies in spectral domain of the image. This is not acceptable since it may lead to unwanted results in later usage of the watermarked image. Figure 5 shows the average spectra from the original image and from the watermarked image when the strength $s = 1.0$. In Fig. 5(a) the watermark was embedded in the eigenimage $K = 10$ and in Fig. 5(b) the watermark was embedded in the eigenimage $K = 2$. In Fig. 5(b) the largest change is on band 2. In Fig. 5(a) the changes are less significant. The qualities of the average spectra are $PSNR = 44.25$ dB and $PSNR = 42.67$ dB for the embedding in band 10 and in band 2, respectively. More clearly

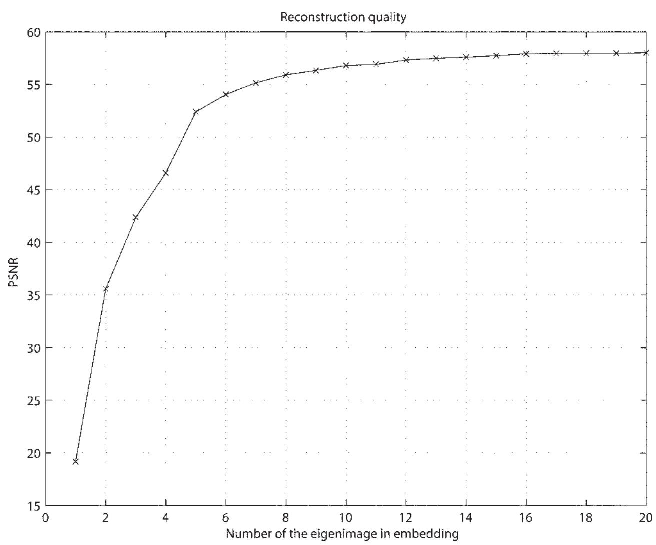
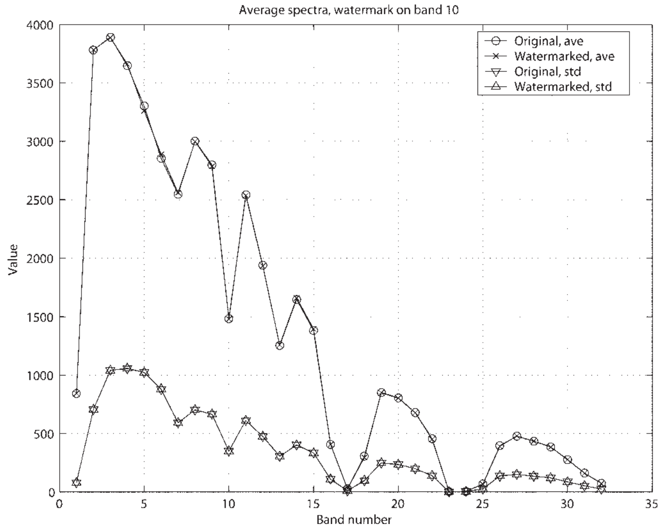


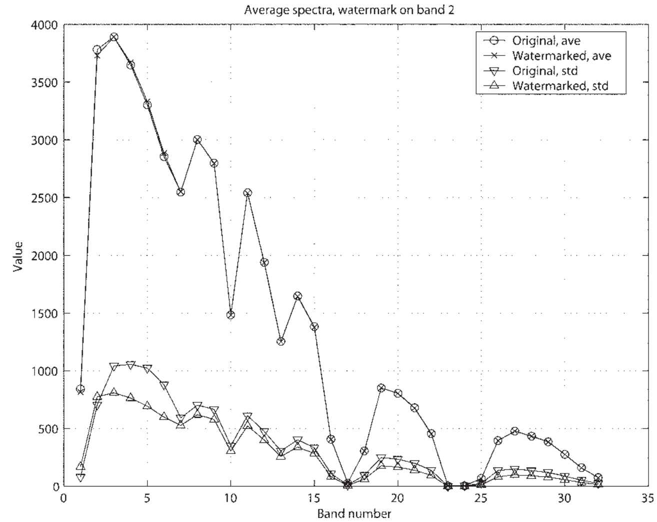
Figure 4. Quality of embedding the watermark in eigenimages $K = 1 \ldots 20$.

the disturbance is seen in the differences in the standard deviations. When the embedding is in eigenimage $K = 10$, the standard deviation curves for the two images are overlapping. When the embedding is in eigenimage $K = 2$, the standard deviation has clearly decreased for the watermarked image. This means that the values in the bands of the original image have moved closer to the average value of each band. These changes may induce incorrect results as, for example, in classification applications.

The strength, s gives an additional freedom to design the embedding procedure. In our case the strength, s, changes the resolution of the watermark. Thus, the higher the strength s, the more visible the watermark will be in the image. With lower values of strength s, the watermark will be more vulnerable in attacks. The value of H for this experiment was set as $H = 10$. In Fig. 6 we illustrate the variable values of strength s, $s = 1.0$, $s = 2.0$, $s = 4.0$. The figure contains average spectra from the three watermarked images.



(a)



(b)

Figure 5. Average spectra from the watermarked image. (a) embedding in eigenimage 10, and (b) embedding in eigenimage 2.

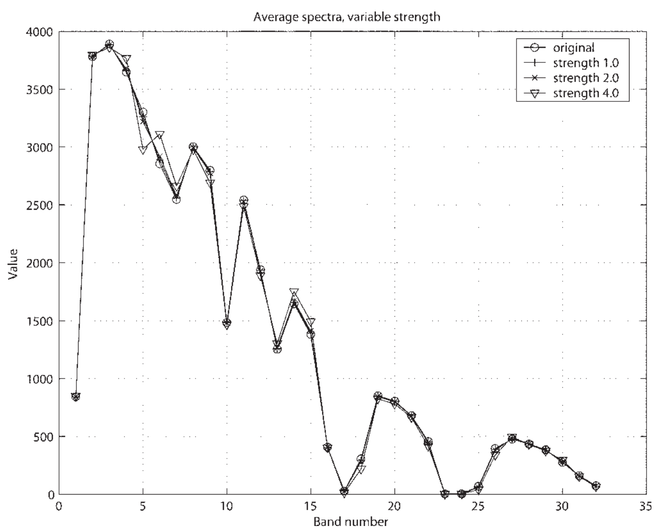


Figure 6. Average spectra from watermarked images. Variable strength s, s = 1.0, s = 2.0, s = 4.0.

With higher values in strength s, s = 4.0 clear spectral discrepancies can be seen. The same phenomenon appears also in the spatial domain of the image as seen in Fig. 7.

The watermark is clearly visible in Fig. 7(c) where the strength is s = 4.0. Thus the values of the strength, s should be limited such that the discrepancies are acceptable and there are no visible distortions, i.e., the strength should be limited to values $s \leq 2.0$.

Attacks Against the Watermarked Image

A series of experiments was run to test the robustness of the watermark. The watermarked image was compressed band-wise with JPEG 2000[15] using various bit rates. After reconstruction the quality of the extracted watermark was evaluated. The total bit rate was apportioned to the 32 bands according to the entropy of each band. The experiment was performed with variable strength in embedding, s = 0.1, 0.2, 0.4, 0.6, 1.0, 2.0.

The results of lossy compression are displayed in Fig. 8. In Figs. 8(a) and 8(b) the qualities of the extracted watermarks are shown and in Figs. 8(c) and 8(d) the qualities of the reconstructed images are shown. In Figs. 8(a) and 8(c) the error measure is the correlation coefficient and in Figs. 8(b) and 8(d), the error measure is the peak signal-to-noise ratio (PSNR).

The experiments show that the vulnerability of the watermark in compression is high compared to the vulnerability of the image (see Fig. 8). For example, the correlation coefficient between the original image and the compressed image is constant even though the strength, s, is changing. With the PSNR measure, at low compression ratios there are clear changes, but they are beyond the perception of human eye. The quality of the watermark undergoes more extensive changes. Therefore the quality of the image is not endangered by watermarking, but the watermark conveys information of the degraded image.

The visual degradation of the watermark in lossy compression is shown in Fig. 9. Each column contains a constant strength s and each row has a constant bit rate expressed in bits/value. The bit rate means the number of bits allocated to store each value of the spectral image. With gray scale images the respective quantity is bits/pixel.

The second set of attacks consisted of filtering operations which were a trimmed mean filter and a median filter, each with two different window sizes, and a vector median filter. The mean filter and the median filters were applied to each band of the spectral image. The trimmed mean filter excluded the smallest and the largest value from mean calculation. The spatial sizes for both the trimmed mean and the median filters were 3 × 3 and 5 × 5.

Visual presentations of the watermark and of band 5 from the spectral image after different attacks are shown in Figs. 10 and 11. After the filtering operations the watermark can be clearly identified visually. The mean filtering softens the bandwise images, with the larger window there is more softening, as shown in Fig. 10. Vector median filtering selected one of the original spectra as a result from filtering and now the largest changes can be seen in the edges of the watermark.

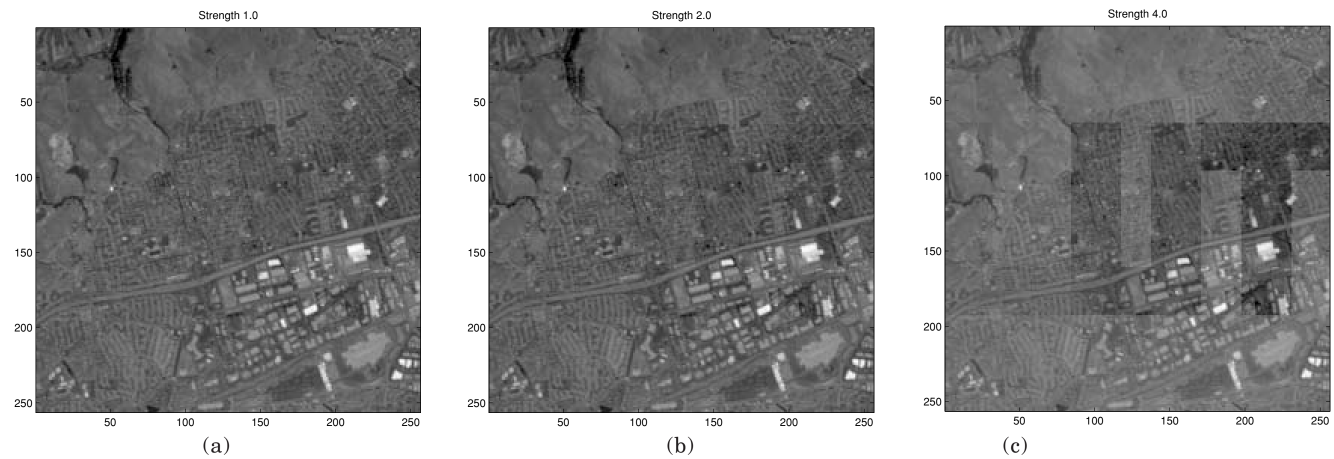


Figure 7. Band 5 from the watermarked image, variable strength s. (a) $s = 1.0$, (b) $s = 2.0$, and (c) $s = 4.0$.

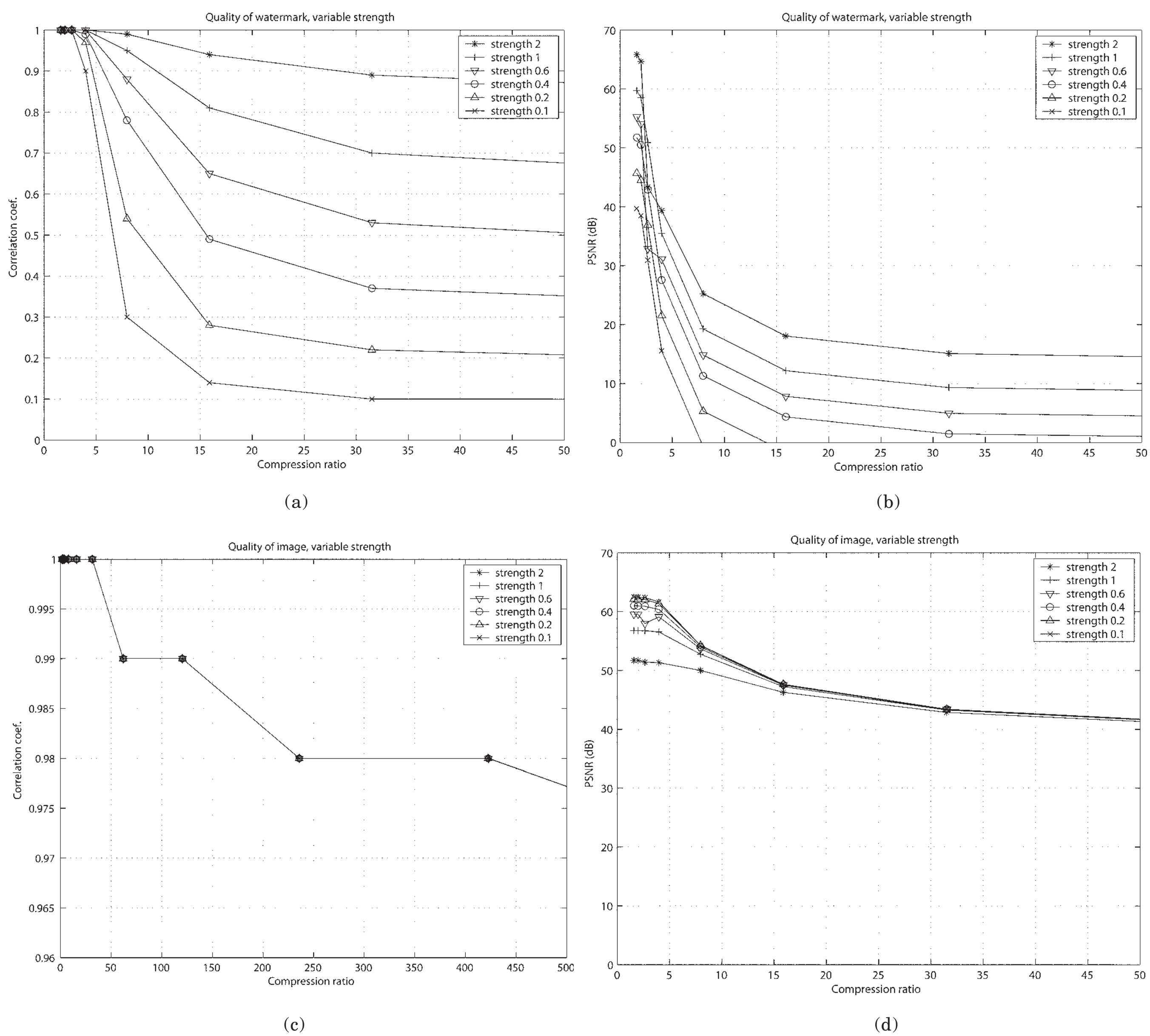


Figure 8. Compression of the watermarked image. The strength s was changing. Top row, watermark: (a) Correlation coefficient, (b) PSNR. Bottom row, spectral image: (c) Correlation coefficient, and (d) PSNR.

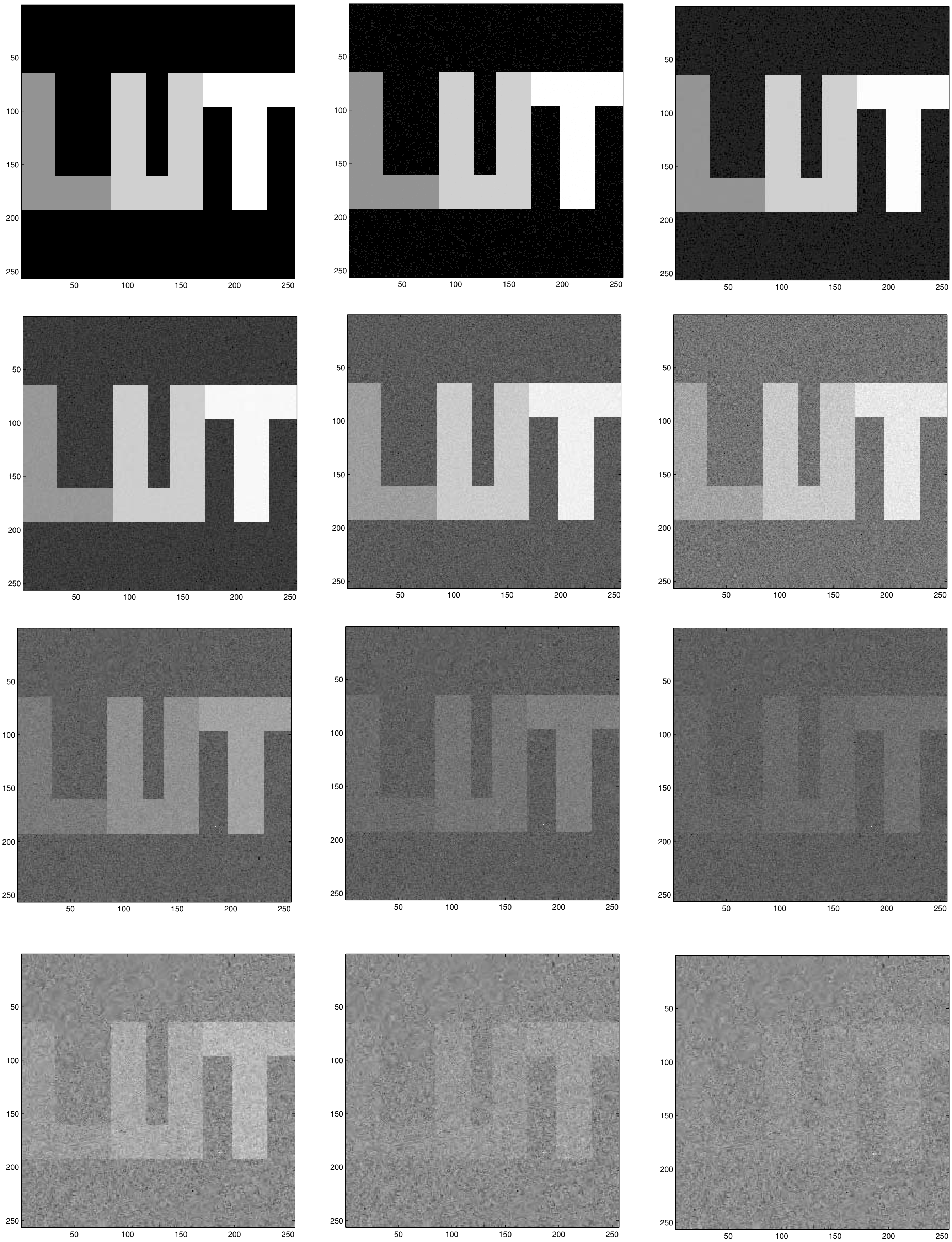


Figure 9. Compression of the watermarked image, quality of the watermark. Bit rates are 8 bits/value for each coefficient, 4 bits/value, 2 bits/value, 1 bit/value from the top row to the bottom row, respectively. Strength is $s = 1.0$, $s = 0.4$, $s = 0.2$ in left, center, and in right column, respectively.

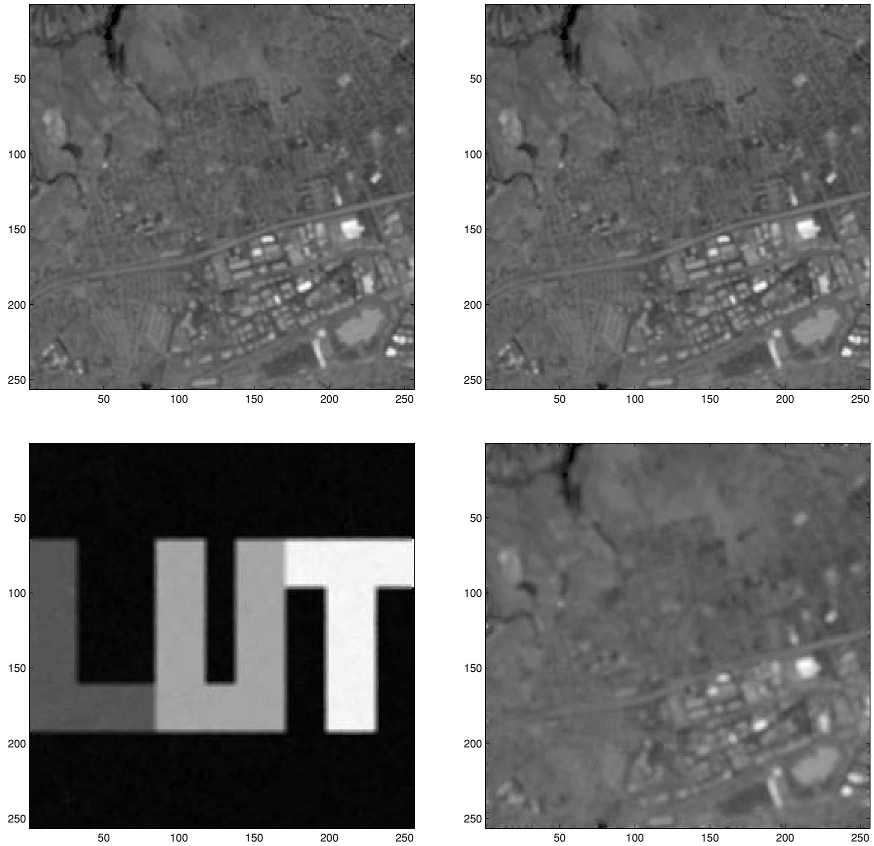


Figure 10. Attacks against the watermarked image. Left column: watermark. Right column: band 5 from the spectral image. First row: trimmed mean filtering with 3 × 3 window. Second row: trimmed mean filtering with 5 × 5 window.

TABLE I. Robustness Against Attacks, Image

Attack	SNR	PSNR	SM	CC
Vector median	21.68	40.80	0.8337	0.9933
Median 3x3	21.85	40.98	0.8337	0.9936
Median 5x5	17.92	37.05	0.7505	0.9842
Trimmed mean 3x3	22.04	41.16	0.8166	0.9938
Trimmed mean 5x5	18.08	37.21	0.7394	0.9845

TABLE II. Robustness Against Attacks, Watermark

Attack	SNR	PSNR	SM	CC
Vector median	15.35	23.26	0.9756	0.9798
Median 3x3	12.70	20.61	0.8154	0.9633
Median 5x5	11.66	19.57	0.7915	0.9529
Trimmed mean 3x3	18.40	26.32	0.9421	0.9900
Trimmed mean 5x5	16.18	24.10	0.9370	0.9833

The numeric results on robustness against different attacks are summarized in Tables I and II. The columns in the tables are: first column contains the attack type; the second and third column contain the signal-to-noise ratio (SNR) and the peak signal-to-noise ratio (PSNR) respectively; the fourth column contains the value of the similarity measure (SM); the fifth column shows the value of the correlation coefficient (CC). All these measures were calculated between the original image and the filtered, watermarked image.

With these filtering operations the watermark contaminates more than the original image, see Tables I, II, column SNR and PSNR. Also the results with different quality measures vary. The similarity measure (SM) suggests a different order for quality than do the others. For example, the vector meadian filtered watermark is considered better than the trimmed mean filtered watermark.

In the experiments we found that the PCA eigenvalues of the watermarked image differ from the PCA eigenvalues of the original image. Especially, the lower

TABLE III. PCA Eigenvalues for the Original Image and the Watermarked Image.

Original image	Watermarked	
0.00001665211	0.00000000554	Smallest eigenvalue
0.00002150161	0.00000000555	
0.00002725959	0.00000000555	
0.00003234345	0.00000000558	
0.00005029566	0.00000000561	
0.00006773485	0.00000000561	
0.00007915329	0.00015242413	10th eigenvalue
0.00015247704	0.00016977910	
0.00017041822	0.00024182648	
0.00024212787	0.00061432684	
0.00063347959	0.00068490515	
0.00100949009	0.00101096671	
0.00991701110	0.00991701114	
0.02382752031	0.02385282182	
0.13277486301	0.13277488686	
7.35281051838	7.35307004786	Largest eigenvalue

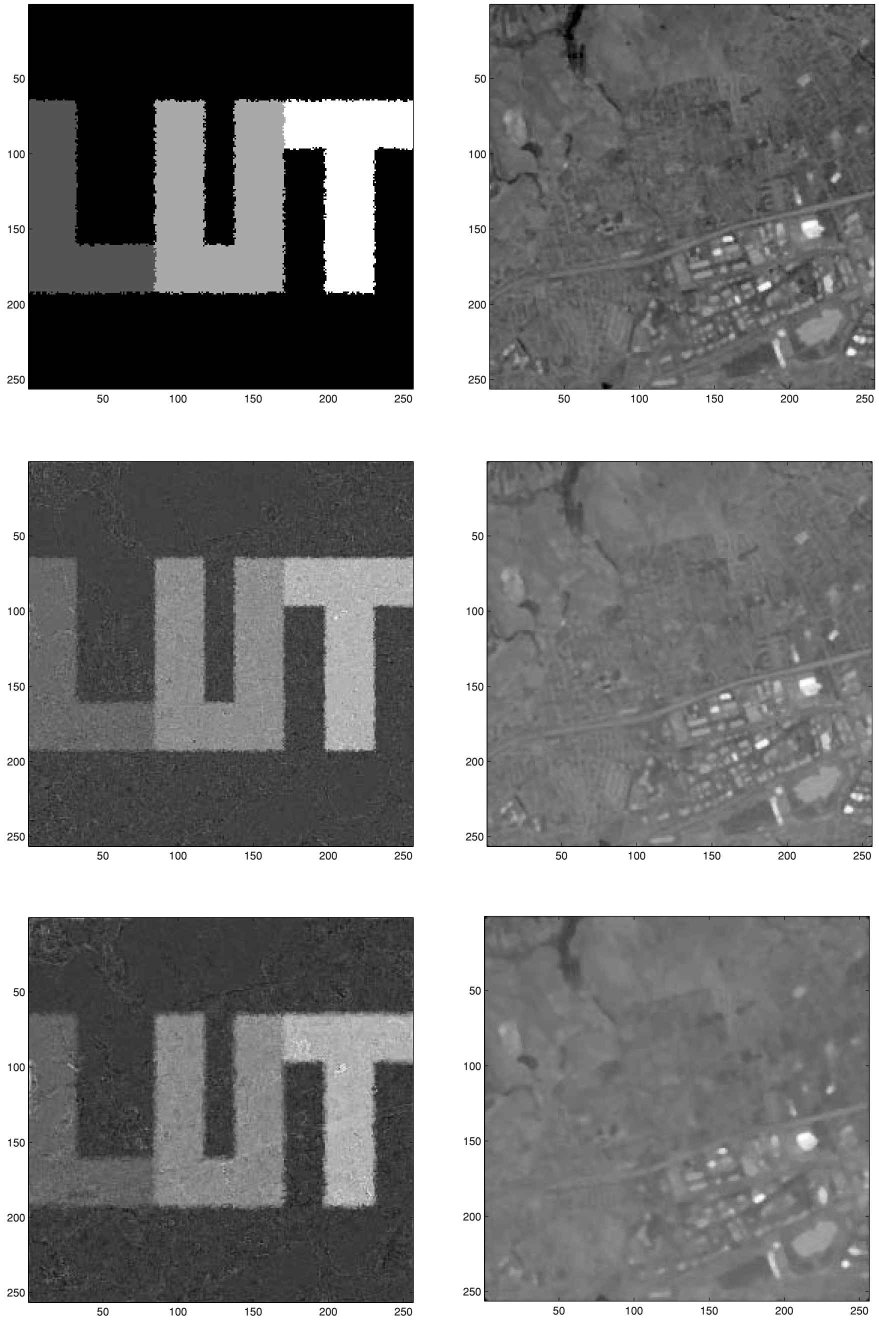


Figure 11. Attacks against the watermarked image. Left column: watermark. Right column: band 5 from the spectral image. First row: vector median filtering, Second row: median filtering with 3 × 3 window. Third row: median filtering with 5 × 5 window.

eigenvalues for the eigenimages after the eigenimage with the watermark embedded, are almost random. Test results for embedding the watermark in eigenimage 10 of the multiplier matrix are show in Table III. The values up to the tenth eigenvalue are similar, but from eleven forward the eigenvalues differ heavily. This characteristic is a clear drawback for the embedding procedure, insofar as it can be used to detect if the spectral image is watermarked.

Conclusions

We propose a watermarking technique which operates on spectral images. We defined a model which various approaches mixing of the watermark with the spectral image. Embedding a watermark into an image using the PCA transform results in only minor influences on the quality of the spectral image. The watermark survives quite well through various attacks and the watermark remains clearly recognizable visually. Even though the values of the parameters selected produced good results, the procedure introduced in this study requires further enhancement.

The robustness of the watermark was explored with a set of attacks which included lossy compression and filtering operations. Lossy compression at low bit rates and with low strength has a larger effect on the watermark quality than other attacks. It can also be noted that the visual quality of the extracted watermark is not always accurately comparable with the SNR results. The similarity measure (SM) proposes a new approach to the quality evaluation between vectorized quantities.

The embedding procedure has an effect on the PCA eigenvalues of the image and this implies that the method requires enhancements both in the embedding procedure and in the definition of the watermark.

Acknowledgment. The authors would like to thank the members of the Department of Information Technology at LUT for helpful discussions.

References

1. C.I. Podilchuk and E.J. Delp, Digital Watermarking: Algorithms and Applications, *IEEE Signal Processing Magazine*, 33–46 (July 2001).
2. D. Artz, Digital Steganography, Hiding Data within Data, *IEEE Internet Computing* **5**(3), 75–80 (May/June 2001).
3. D. Kundur and D. Hatzinakos, A Robust Digital Image Watermarking Method using Wavelet-Based Fusion, *Proc. IEEE Int. Conf. On Image Processing*, vol. 1, 1997, IEEE Press, Los Alamitos, California, pp. 544–547.
4. R. B. Wolfgang, C. I. Podilchuk and E. J. Delp, Perceptual Watermarks for Digital Images and Video, *Proc. IEEE* **87,** 1108–1126 (1999).
5. M.-S. Hsieh, D.-G. Tseng and Y.-H. Huang, Hiding digital watermarks using multiresolution wavelet transform, *IEEE Trans. Industrial Electronics* **48,** 875–882 (2001).
6. W.N. Cheung, Digital image watermarking in spatial and transform domains, *TENCON Proceedings*, vol. 3, 2000, pp. III–374—III–378.
7. A. Parisis, P. Carre and C. Fernandez-Maloigne, Colour watermarking: study of different representation spaces, *Proc. CGIV 2002*, IS&T, Springfield, VA, 2002, pp. 390–393.
8. M. Barni, C.I. Podilchuk, F. Bartolini, and E.J. Delp, Watermark embedding: hiding signal within cover image, *IEEE Comm. Magazine,* 102–108 (Aug. 2001).
9. A.T.S. Ho, J. Shen, S.H. Tan, and A.C. Kot, Digital image-in-image watermarking for copyright protection of satellite images using the fast Hadamard Transform, *Proc. IGARSS'02*, IEEE Press, Los Altamtos, CA, 2002, pp. 3311–3313.
10. M. Hauta-Kasari, K. Miyazawa, S. Toyooka, and J. Parkkinen, Spectral Vision System for Measuring Color Images, *J. Opt. Soc. Amer. A* **16,** 2352–2362 (1999).
11. A. Kaarna and J. Parkkinen, Transform Based Lossy Compression of Spectral Images, *Pattern Anal. Appl.* **4,** 39–50 (2001).
12. J. Parkkinen and T. Jaaskelainen, Color representation using statistical pattern recognition, *Appl. Opt.* **26,** 4240–4245 (1987).
13. A. Kaarna, P. Zemcik, H. Kälviäinen, and J. Parkkinen, Compression of Multispectral Remote Sensing Images Using Clustering and Spectral Reduction, *IEEE Trans. Geosci. Remote Sensing*, **38,** 1073–1082 (2000).
14. http://www.designer.com/focus/articles/web_future/web_future_print.htm, August 16, 2002.
15. D. S. Taubman, M. W. Marcellin, *JPEG2000, Image Compression Fundamentals, Standards and Practice*, Kluwer Academic, Boston, MA, 2002.
16. M. Vetterli, Filter banks allowing perfect reconstruction, *Signal Proc.* **10,** 219–244 (1986).
17. S. Mallat, A theory for multiresolution signal decomposition: the wavelet presentation, *IEEE Trans. Pattern Analysis Machine Intell.* **11,** 674–693 (1989).
18. J. Astola, P. Haavisto and Y. Neuvo, Vector Median Filters, *Proc. IEEE,* **78,** 678–689 (1990).
19. www-site: http://makalu.jpl.nasa.gov/, July 25, 2002.
20. M. Rabbani and P.W. Jones, Digital image compression techniques, *SPIE Optical Engineering Proc.* Bellingham, WA, 1991.
21. M. Hild, On the effectiveness of color similarity measures in background-frame differencing applications, *Proc. CGIV 2002*, IS&T, Springfield, VA, 2002, pp. 304–309.
22. L. Råde and B. Westergren, *BETA, Mathematics Handbook*, Studentlitteratur, Stockholm, 1995.