

Removal of Watermarks from Spectral Images Through Principal Component Analysis

Jarno Mielikainen and Pekka Toivanen

Lappeenranta University of Technology, Department of Information Technology, Lappeenranta, FINLAND

This article presents a method to remove watermarks from watermarked spectral images. The watermarks were added through the Principal Component Analysis (PCA). The removal is also performed using the PCA transform. Experimental results indicate that the removal of the watermark can be performed successfully.

Journal of Imaging Science and Technology 49: 474–480 (2005)

Introduction

Digital watermarking protects intellectual property in the digital world. Watermarks are designed so that their detection and removal is difficult. Usually, the information of the watermark is spread through the whole image. Therefore, a change in one part of the image does not alter the underlying watermark.¹

In this article, a method is described that enables the removal of the watermark from watermarked spectral images. The watermarks were added through the PCA transform. The watermark information is contained in the coefficients for the N^{th} principal component. The removal is also performed using the PCA transform. For removal, an estimate for the same N^{th} principal component is computed. The removal of the watermark does not degrade the image. Actually, the peak-signal-to-noise ratio (PSNR) of the image is increased by the removal operation compared to the watermarked image.

Watermarking and Watermark Attacks

Review of Watermarking Techniques

The watermarking techniques can be divided into two different groups; one is applied in the spatial domain and the other is applied in the frequency domain. Spatial techniques are simple but the spatial watermarks can easily be distorted or removed. On the other hand, frequency techniques are more complex and robust. Also, transform domain-based techniques are capable of containing a larger number of watermark information without incurring visible artifacts. Next, we will review previous work on spatial and frequency watermark techniques.

Yeung and Mintzer² used a Look-Up Table (LUT) to map input image to watermarked image. Wu³ proposed adding a distortion compensation to LUT embedding. Schyndel et al.⁴ used bit plane manipulation of least significant bits (LSB) to embed a watermark. Chou and Wu⁵ embedded watermarks in color images by modifying the quantization index of each color pixel. The watermarking scheme of Hwang et al.⁶ is based on one-way hash functions; the embedding positions of the watermark are selected using a pseudo-random number. Voyatzis and Pitas⁷ used chaotic mixing to map the watermark in the image. Wong et al.⁸ proposed a modulating watermark with a pseudorandom sequence to get a modulated watermark sequence. One bit of the modulated watermark sequence is embedded into the image block by adding a small deviation in the direction determined by the secret key. Lin presented a modular arithmetic watermarking scheme on the spatial domain in Ref. 9. Chen and Leung¹⁰ watermarked remote sensing images using chaotic spreading sequences. Each bit of the watermark is spread out by multiplying it with a pseudo-noise sequence. Chen and Wornell¹¹ proposed embedding information by first modulating an index or a sequence of indices with a watermark and then quantizing the signal in a procedure named spread-transform dither modulation (STDM). The procedure is a practical implementation of quantization index modulation (QIM). The watermark data is rounded to the closest even multiples to embed a “0” and to odd multiples to embed a “1”. Eggers et al.¹² proposed a distortion compensated version of QIM to reach a higher payload than odd-even embedding alone. Malvar and Florencio¹³ claimed that their improved spread spectrum watermarking technique achieves the same noise robustness as QIM without its amplitude scale sensitivity. Fei et al.¹⁴ combined the advantages of a spread spectrum and quantization-based watermarking. Yu et al.¹⁵ proposed a watermarking technique for color images based on neural network. A neural network was trained to recognize the watermark from a watermarked image. Due to a neural network’s learning and adaptive

Original manuscript received July 12, 2004

Corresponding Author: J. Mielikainen, mielikai@lut.fi

©2005, IS&T—The Society for Imaging Science and Technology

capabilities, the technique was shown to be robust against several known attacks.

Hsu and Wu¹⁶ used multiresolution based techniques to embed watermarks into images. DWT was used to obtain a multiresolution representation of the image. Hsu and Wu¹⁷ embedded a watermark in the image by selectively modifying the middle-frequency parts of the DCT coefficients. Lie et al.¹⁸ embedded watermark data into the middleband of the DCT. Chen et al.¹⁹ used image features to synchronize the binary image watermark positions in the DCT domain of the image. Wu and Hsieh²⁰ rearranged the DCT coefficients and embedded a watermark into the rearranged coefficients. Loo and Kingsbury²¹ proposed watermarking in a complex wavelet domain as it allows to adapt the watermark strength to the local activity of the image better than the discrete wavelet transform (DWT). Hwang et al.¹⁵ used a DCT/back-propagation neural network hybrid to embed watermarks. At first a location in the image is selected where DCT is computed and watermark is embedded in AC coefficient. The original 12th AC coefficient is replaced by a value computed using back-propagation neural network. Tsai et al.²² combined the chaotic spatial transform and the wavelet multi-resolution structure for watermark embedding by using the spatial transform to perform the embedding scheme for the wavelet coefficients. Xiao et al.²³ generated a chaotic sequence from the initial condition and parameters. The watermark is added randomly to the middle frequency coefficients of the wavelet domain using a 2-D chaotic system. Fang et al.²⁴ integrated DWT with the Code Division Multiple Access (CDMA) based spread spectrum watermarking technique.

Shih and Wu²⁵ embedded a watermark both in the spatial and the transform domain in hope of increasing the payload without increasing the distortion of the watermark. Another claimed advantage is the double protection. In the spatial domain the LSB bits were substituted with a watermark image. In the frequency domain, a watermark is inserted into the low frequency coefficients. Chan and Chang²⁶ proposed embedding two different watermarks. A robust watermark is embedded first into the low frequency wavelet coefficients of the image. An advanced encryption standard is used to hide the watermark positions of the image. Secondly, a fragile watermark is embedded into the LSB in the spatial domain.

Review of Attacks Against Watermarks

Several types of attacks against watermarks have been developed. The attack can remove the embedded watermark completely, just like our proposed attack does. Barnett and Pearson²⁷ applied the Laplacian operator multiple times to the watermarked image. The operation was effective at removing the watermark from DCT-watermarked images. The Voloshynovskiy et al.²⁸ attack scheme consisted of the following stages. The first stage is watermark estimation and partial removal by filtering based on the Maximum *a posteriori* (MAP) approach. In the second stage the watermark is altered and hidden by the addition of noise to the filtered image. In the tests the approach worked against both spatial and transform domain watermarks.

Collusion attacks are mounted by a coalition of users with the same content that contains different watermarks. Stone presented one of the simplest collusion attacks in Ref. 29 by averaging multiple copies of the content together. Cox and Linnartz³⁰ used statistical averaging to the attack against watermarks.

Wu and Liu³¹ presented an attack on a block-DCT based spread spectrum watermark that replaced image blocks by interpolating a block from its neighboring blocks. Petitcolas et al.³²⁻³³ analyzed the weaknesses of several watermarking schemes and proposed attacks on watermarks. The proposed attacks use a combination of non-linear geometric distortions and compression. Also, an attack called the mosaic attack for web images is proposed. It splits images into several smaller sub-images that are displayed seamlessly in a web-browser. The individual image's sub images are too small to convey the watermarking information.

Different kinds of protocol attacks have also been proposed. For example, Craver et al.³⁴ have showed that one can claim ownership to any images one has access to using a so-called inversion attack. The idea of an inversion attack is that the attacker can claim that the image contains the attacker's watermark in parts of the image. A fake original image is generated by subtracting the forged watermark from the original image. In Ref. 35, Holliman and Memon showed that in block-wise independent watermarking schemes it is possible to counterfeit an existing watermark into an unwatermarked image. Similarly Kutter³⁶ estimated the embedded watermark through a filtering process and then adapted and inserted the watermark into an unwatermarked image. Kirovski and Petitcolas³⁷ used a procedure called Blind Pattern Matching (BPM) to replace blocks of samples of a watermarked signal with similar blocks that are either not watermarked or are watermarked with a different watermark.

Watermarking Spectral Images Through the PCA Transform

PCA is both an optimal decorrelating transform and a transform that gives the minimum Mean Squared Error (MSE) when the source is approximated with a certain number of transform coefficients. For Gaussian random processes, PCA maximizes the compression ratios if the transform coefficients are quantized and coded independently.³⁸

PCA has previously been used for color transformation for JPEG 2000 image compression³⁹ Kaarna et al.⁴⁰ used PCA for multispectral image compression. PCA coefficients are also often used as an extracted features for classification, e.g., Ahmadi⁴¹ used it to classify banknotes. Face recognition has also utilized PCA.⁴²⁻⁴⁵ Among other things, PCA has also been used in compressing histogram representations for automatic color photo categorization.⁴⁶

In Ref. 47 Kaarna et al. applied PCA to the spectra in the image and then embedded the watermark into the image by replacing the coefficients of the 10th eigenvectors with the watermark image. By multiplying the watermarked image with the original eigenvector, the watermark is recovered. The basis functions are kept secret in order to prevent others from detecting/modifying the watermark.

In PCA, one finds in the mean square error sense the optimal representation of the spectra set by a low dimensional subspace. The covariance matrix C of the original data is composed and then the eigenvalues and the eigenvectors of C are found.

The covariance matrix of the original data C is defined as

$$C = E\left\{(x - \mu)(x - \mu)^T\right\} \quad (1)$$

where μ is the mean vector.



Figure 1. Moffatt Field Image.

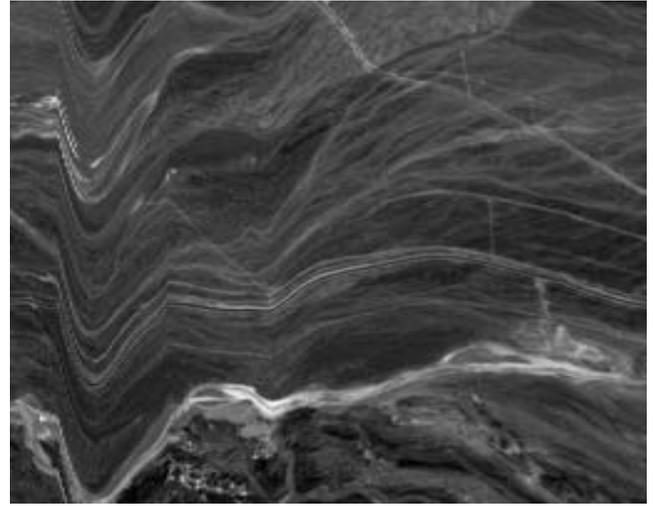


Figure 2. Cuprite Image.

In practice, the covariance matrix C is estimated by

$$\hat{C} = 1/n \sum_{j=1}^n (x_j - \hat{\mu})(x_j - \hat{\mu})^T, \quad (2)$$

where x_i is an M -dimensional sample vector, $\hat{\mu}$ is the estimated mean vector of the sample set and the sum is over all the samples. The eigenvalues and respective eigenvectors u_1, u_2, \dots, u_M are calculated from the matrix $[\hat{C}]$. In reconstruction, the estimation of the original data is received from

$$\hat{x}_i = \sum_{j=1}^K (x_i^T u_j) u_j, \quad (3)$$

where K is the number of selected basis vectors. The eigenvector with the largest eigenvalue explains more of the variance of the data than any of the other eigenvectors, and so on.^{48,49}

The inserted watermark is blind, i.e., the verification of the watermark can be performed without use of the original image. The use of the same keys for embedding and detecting watermarks makes the watermarking procedure symmetric. Since the users are unaware of the presence of the watermark, the watermark is steganographic.

In Ref. 50 Kaarna et al. also conducted experiments in which the watermark was added to other bands than the least significant one (10th).

Removal of the Watermark

The detection/removal of the watermark is done by performing the principal component analysis locally on the watermarked image. The coefficients for the least significant principal component are used as an estimate for the watermark. By multiplying the watermarked image with the estimated eigenvector and setting its coefficients to zero, the watermark can be removed.

Experiments

We applied the watermarking/removal procedure to two images. One is the same image and watermark pair as in Refs. 47 and 50. The image used is the Moffatt Field



Figure 3. Original 'LUT' watermark.

image, see Fig. 1, from the AVIRIS '97 set.⁵¹ The original image of size 614*512*224 with a 16-bit resolution was transformed into an image of size 256*256*32 by taking every 7th band and cropping the image spatially. The second image is from the Cuprite area from the same AVIRIS '97 set and the image can be seen in Fig. 2. The first watermark we used is a simple 'LUT' watermark that can be seen in Fig. 3. The same logo was also used in Refs. 47 and 50. The second watermark is an LUT-logo; see Fig. 4.

The information loss is measured by the PSNR, which we define for multispectral images as

$$PSNR = 10/gMn^2s/E^{Cr}, \quad (4)$$

where s is the peak value of the original image. E^{Cr} is the difference between the energy of the original image and the energy of the watermarked image, N is the number of pixels in the image, and M is the number of bands in the image.⁵²



Figure 4. LUT-logo watermark.

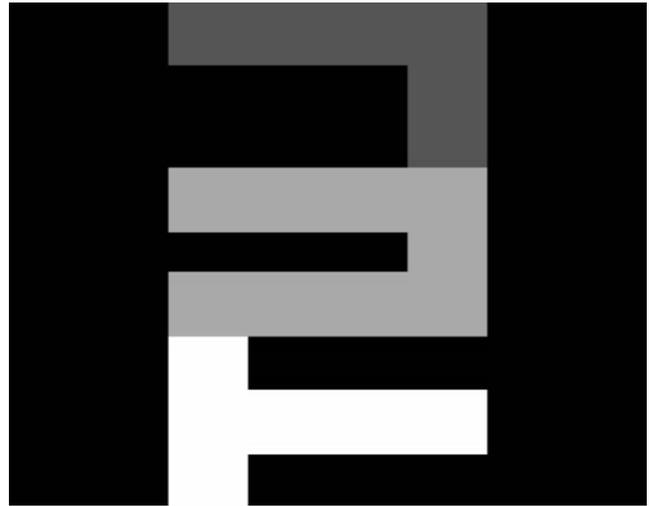


Figure 5. Removed 'LUT' watermark.

For the calculation of the PCA for watermark removal, 100 consecutive values from the watermarked image were determined to give good results for the watermark removal. It did not matter which 100 consecutive values were used as samples for the basis estimation, all choices gave similar results.

From the PSNR values for the Moffatt image using an 'LUT' watermark in Table I it can be seen that when the watermark is added to the more significant band, the PSNR drops dramatically. Nevertheless, our proposal for watermark removal is able to achieve almost the same PSNR as the recovery operation using the secret base functions. In addition, our estimated base functions capture most of the base's energy and nothing else so that the recovery operation after the removal of the watermark increases the PSNR slightly.

Similar effects can be observed using an LUT-logo for the same Moffatt image from Table II.

Table III shows that the removed 'LUT' watermark from the Moffatt image is not equal to the recovered watermark in terms of PSNR.

When the removed watermark and the recovered watermarks for the least significant principal component are visually compared in Figs. 5 and 6 to the original watermark in Fig. 3 they look the same. On the other hand, after our removal operation the recovery operation produces an image in Fig. 7 which does not resemble the original watermark image. When the most significant principal component is used for the watermark, the removed watermark is not so good. This can be observed in Fig. 8. As can be observed in Fig. 9, the recovery operation is still not able to generate the watermark image after the removal operation.

Removal of the LUT-logo from the Moffatt image that was watermarked in the first and the tenth band produced the images seen in Figs. 10 and 11, respectively. As can be observed from the images the removal is quite successful in recovering the embedded watermark. On the other hand, the recovery operation after the removal operation produced the watermarks seen in Figs. 12 and 13, respectively. Clearly, they do not look anything like the original watermark. Therefore, our removal operation can be considered successful.



Figure 6. Recovered 'LUT' watermark.



Figure 7. Recovered 'LUT' watermark after removal operation.



Figure 8. Removed 'LUT' watermark.

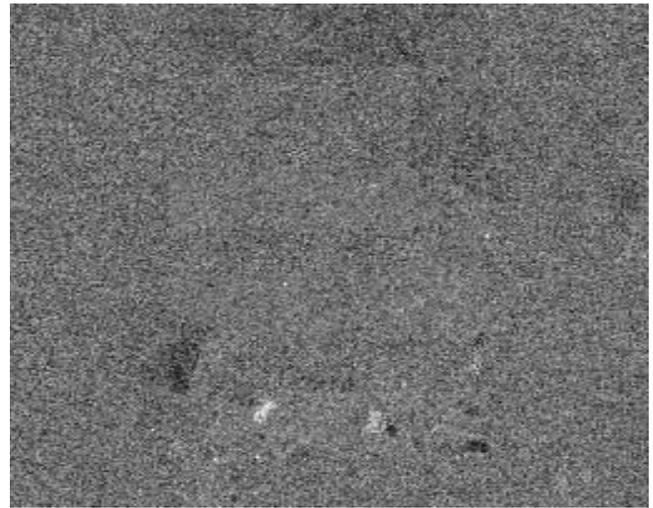


Figure 9. Recovered 'LUT' watermark after removal operation.



Figure 10. Removed LUT-logo watermark from the first band of the Moffatt Field image.



Figure 11. Removed LUT-logo watermark from the 10th band of the Moffatt Field image.



Figure 12. Recovered LUT-logo watermark after removal operation from the first band of the Moffatt Field image.



Figure 13. Recovered LUT-logo watermark after removal operation from the 10th band of the Moffatt Field image.

TABLE I. PSNR for Moffatt Hyperspectral Image Using ‘LUT’ Watermark

band #	image after watermarking	image after watermark removal	image after watermark recovery	image after watermark removal and recovery
1	19.2677	19.2161	19.2161	19.2161
2	36.5988	36.6412	36.6413	36.6386
3	44.1699	44.0637	44.0638	44.0495
4	47.4033	47.8061	47.8060	47.7724
5	54.3300	56.8562	56.8566	56.5930
6	55.3744	58.3868	58.3871	58.0171
7	56.1911	60.9012	60.9029	60.2624
8	56.5926	61.5758	61.5768	60.8384
9	56.5701	61.7620	61.7640	60.9950
10	56.7858	62.6190	62.6219	62.6220

TABLE II: PSNR for Moffatt Hyperspectral Image Using LUT-Logo Watermark

band #	image after watermarking	image after watermark removal	image after watermark recovery	image after watermark removal and recovery
1	19.2268	19.2161	19.2161	19.2161
2	36.6610	36.6412	36.6412	36.6386
3	44.0063	44.0633	44.0634	44.0490
4	47.7087	47.8069	47.8061	47.7731
5	56.4606	56.8558	56.8565	56.5928
6	57.8497	58.3858	58.3871	58.0161
7	60.1077	60.9004	60.9032	60.2619
8	60.5878	61.5750	61.5776	60.8378
9	60.6694	61.7612	61.7643	60.9941
10	61.4102	62.6178	62.6224	62.6220

TABLE III. PSNR for ‘LUT’ Watermark on Moffatt Hyperspectral Image

band #	removed watermark	recovered watermark after removal operation	recovered watermark
1	5.0812	60.3343	7.5836
2	11.8918	60.3310	7.5781
3	10.2322	60.3242	7.5753
4	5.6472	60.3203	7.5819
5	6.5099	60.3260	7.5809
6	4.9994	60.3455	7.5723
7	5.5924	60.3473	7.5728
8	7.5030	60.3284	7.5838
9	8.5388	60.2831	7.5696
10	10.0688	60.3082	7.9280

TABLE IV. PSNR for LUT-Logo Watermark on Moffatt Hyperspectral Image

band #	removed watermark	recovered watermark after removal operation	recovered watermark
1	47.1878	54.7707	9.4069
2	5.8785	54.7732	9.3951
3	45.5840	54.7437	9.4021
4	45.7095	54.7569	9.4056
5	5.8688	54.7596	9.4031
6	5.8845	54.7582	9.4002
7	5.8788	54.7757	9.3904
8	5.8773	54.7639	9.4110
9	5.8842	54.7169	9.3973
10	40.4993	54.7280	11.9113

TABLE V. Summary of the Results for the Cuprite Hyperspectral Image

band #	image after ‘LUT’ watermark removal	image after ‘LUT’ watermark recovery	image after LUT-logo watermark removal	image after LUT-logo watermark recovery
1	22.2478	22.2478	22.2479	22.2478
2	26.1801	26.1801	26.1801	26.1801
3	49.3998	49.3999	49.3999	49.3921
4	57.3930	57.3929	57.3930	57.3448
5	61.0362	61.0360	61.0369	60.9257
6	68.6755	68.6778	68.6769	68.0687
7	69.0686	69.0691	69.0700	68.4073
8	69.7093	69.7104	69.7088	68.9495
9	70.7226	70.7252	70.7256	69.7861
10	71.9404	71.9418	71.9423	71.9412

In Table IV similar results are provided for the LUT-
logo for the same Moffatt image. The same observations
apply also to those results. A summary of the results for
the Cuprite image can be seen in Table V. Based on the
summary it is obvious that the method works equally
well for the Cuprite image: the PSNR for the image after
removal and recovery operations is almost identical.

Conclusions

The estimation of the N^{th} principal component, which
forms the basis for the watermark removal, is based on
the assumption that the inserted watermark is simple.
Therefore, also the inserted signal can be estimated
using the least significant principal component. The
tests prove that the removal operation does work for
the same image/watermark combination that was used
in the article that originally proposed the watermarking
procedure. In addition, the method was successfully
tested using a different image and watermark. ▲

References

1. A. Kejariwal, "Watermarking", *IEEE Potentials* **4**, 37 (2003).
2. M. Yeung and F. Mintzer, "Invisible watermarking technique for image verification", *J. Electronic Imaging* **7**, 578 (1998).
3. M. Wu, Joint security and robustness enhancement for quantization based data embedding, *IEEE Trans. Circuits and Systems for Video Technology* **13**, 831 (2003).
4. R. van Schyndel, A. Tirkel and C. Osborne, "A digital watermark", *Proc. IEEE International Conference on Image Processing*, (IEEE, Piscataway, NJ, USA 1994), pp. 86-90.
5. C. H. Chou and T. L. Wu, "Embedding color watermarks in color images", *IEEE Fourth Workshop on Multimedia Signal Processing*, (IEEE, Piscataway, NJ, USA 2001), pp. 327-332.
6. M. S. Hwang, C. C. Chang, and K.-F. Hwang, "A watermarking technique based on one-way hash functions", *IEEE Trans. Consumer Electronics* **45**, 286 (1999).
7. G. Voyatzis and I. Pitas, Digital image watermarking using mixing systems", *Computers & Graphics*, SPIE **22**, 405 (1998).
8. P. Wong, O. Au, and Y. Yeung, "A novel blind multiple watermarking technique for images", *IEEE Trans. Circuits and Systems for Video Technology* **13**, 813 (2003).
9. P. Lin, "Oblivious digital watermarking scheme with blob-oriented and modular-arithmetic-based spatial-domain mechanism", *J. Visual Comm. Image Represent.*, **12**, 136 (2001).
10. S. Chen and H. Leung, "Chaotic spread spectrum watermarking for remote sensing images", *J. Electronic Imaging* **13**, 220 (2004).
11. B. Chen and G. Wornell, "Quantization index modulation: a class of provably good methods for digital watermarking and information embedding", *IEEE Trans. Information Theory* **47**, 1423 (2001).
12. J. Eggers, R. Bauml, R. Tzschoppe, and B. Girod, "Scalar Costa scheme for information embedding", *IEEE Trans. Signal Proc.* **51**, 1003 (2003).
13. H. Malvar and D. Florencio, "Improved spread spectrum: a new modulation technique for robust watermarking", *IEEE Trans. Signal Proc.* **51**, 898 (2003).
14. C. Fei, D. Kundur and R. Kwong, "Analysis and design of watermarking algorithms for improved resistance to compression", *IEEE Trans. Image Processing* **13**, 126 (2004).
15. P. Yu, H. Tsai and J. Lin, "Digital watermarking based on neural networks for color images", *Signal Proc.* **81**, 663 (2001).
16. C. T. Hsu and J. L. Wu, "Multiresolution watermarking for digital images", *IEEE Trans. Circuits and Systems II: Analog and Digital Signal Proc.* **45**, 1097 (1998).
17. C. T. Hsu and J. L. Wu, "Hidden digital watermarks in images", *IEEE Trans. Image Processing* **8**, 58 (1999).
18. W. N. Lie, G. S. Lin, C. L. Wu, and T. C. Wang, "Robust image watermarking on the DCT domain", *Proc. IEEE International Symposium on Circuits and Systems*, (IEEE, Piscataway, NJ, USA 2000), pp. 228-231.
19. D. Y. Chen, M. Ouhyoung and J. L. Wu, "A shift-resisting public watermark system for protecting image processing software", *IEEE Trans. Consumer Electronics* **46**, 404 (2000).
20. C.-F. Wu and W.-S. Hsieh, "Digital watermarking using zerotree of DCT", *IEEE Trans. Consumer Electronics* **46**, 87 (2000).
21. P. Loo and N. Kingsbury, "Digital watermarking using complex wavelets", *Proc. IEEE's International Conference on Image Processing*, (IEEE, Piscataway, NJ, USA 2000), vol. 3, pp. 29-32.
22. M. J. Tsai, K. Y. Yu and Y. Z. Chen, "Joint wavelet and spatial transformation for digital watermarking", *IEEE Trans. Consumer Electronics* **46**, 241 (2000).
23. W. Xion, Z. Ji, J. Zhang, and W. Wu, "A watermarking algorithm based on chaotic encryption", *Proc. IEEE Region 10 Conference on Computers, Communications, Control and Power Engineering*, vol. 1, (IEEE, Piscataway, NJ, USA 2002), pp. 545-548.
24. Y. Fang, J. Huang and S. Wu, "CDMA-based watermarking resisting to cropping", *Proc. 2004 International Symposium on Circuits and Systems*, vol. 2, (IEEE, Piscataway, NJ, USA 2004), pp. 25-28.
25. F. Shih and S. Wu, "Combinational image watermarking in the spatial and frequency domain", *Pattern Recognition* **36**, 969 (2003).
26. K. M. Chan and L. W. Chang, "A novel public watermarking system based on advanced encryption system", *IEEE's 18th International Conference on Advanced Information Networking and Applications*, vol. 1, (IEEE, Piscataway, NJ, USA 2004), pp. 48-52. ISBN 0-7695-2051-0.
27. R. Barnett and D. Pearson, "Attack operators for digitally watermarked images", *IEEE Proc. Vision, Image and Signal Proc.* **145**, 271 (1998).
28. S. Voloshynovskiy, S. Pereira and A. Herrigel, "Generalized watermarking attack based on watermark estimation and perceptual remodulation", *Proc. SPIE* **3971**: 358 (2000).
29. H. Stone, "Analysis of attacks on image watermarks with randomized coefficients", *NEC Research Institute, Technical Report* **96-045** (1996).
30. I. Cox and J. Linnartz, "Some general methods for tampering with watermarks", *IEEE J. Selected Areas in Communications* **16**, 587 (1998).
31. M. Wu and B. Liu, "Attacks on digital watermarks", *Proc. IEEE's Conference Record of the 33rd Asilomar Conference on Signals, Systems, and Computers*, vol. 2, (IEEE, Piscataway, NJ, USA 1999), pp. 1508-1512.
32. F. Petitcolas, R. Anderson and M. Kuhn, "Attacks on copyright marking systems", *Second International Workshop on Information Hiding*, (Springer-Verlag, Berlin, 1998) pp. 219-239. ISBN 3-540-65386-4.
33. F. Petitcolas, "Watermarking schemes evaluation", *IEEE Signal Proc.* **17**, 58 (2000).
34. S. Craver, N. Memon, B. L. Yeo, and M. M. Yeung, "Resolving rightful ownerships with invisible watermarking techniques: limitations, attacks, and implications", *IEEE J. Selected Areas in Communications* **16**, 573 (1998).
35. M. Holliman and N. Memon, "Counterfeiting attacks on oblivious block-wise independent invisible watermarking schemes", *IEEE Trans. Image Processing* **9**, 432 (2000).
36. M. Kutter, S. Voloshynovskiy and A. Herrigel, "The watermark copy attack", *Proc. SPIE* **3971**, 371 (2000).
37. D. Kirovski and F. Petitcolas, "Blind pattern matching attack on watermarking systems", *IEEE Trans. Signal Proc.* **51**, 1045 (2003).
38. D. Taubman and M. Marcelin, *JPEG2000 Image Compression Fundamentals, Standards and Practice*, (Kluwer Academic Publishers, Boston, MA, 2002).
39. S. Han, B. Tao, T. Cooper, and I. Tastle, "Comparison between Different Color Transformations for the JPEG 2000", *Proc. IS&T's PICS Conference*, (IS&T, Springfield, VA, 2000), p. 259-263.
40. A. Kaarna, P. Zemcik, H. Kalviainen, and J. Parkkinen, "Compression of multispectral remote sensing images using clustering and spectral reduction", *IEEE Trans. Geoscience and Remote Sensing* **38**, 1073 (2000).
41. A. Ahmadi, S. Omatua, T. Fujinaka and T. Kosakab. "Improvement of reliability in banknote classification using reject option and local PCA", *Information Sci.* **168**, 277 (2004).
42. V. Perlibakas, "Distance measures for PCA-based face recognition", *Pattern Recognition Lett.* **25**, 711 (2004).
43. B. Draper, K. Baek, M. Bartlett, and J. Beveridge, "Recognizing faces with PCA and ICA", *Computer Vision and Image Understanding* **91**, 115 (2003).
44. J. S. Janga, K. H. Hanb and J. H. Kima, "Evolutionary algorithm-based face verification", *Pattern Recognition Lett.* **25**, 1857 (2004).
45. S. Chen, D. Zhang and Z. H. Zhou, "Enhanced (PC)²A for face recognition with one training image per person", *Pattern Recognition Lett.* **25**, 1173 (2004).
46. G. Qiu, X. Feng and J. Fang, "Compressing histogram representations for automatic colour photo categorization", *Pattern Recognition* **37**, 2177 (2004).
47. A. Kaarna, P. Toivanen and K. Mikkonen, "Watermarking spectral images through the PCA transform", *Proc. IS&T's PICS Conference*, (IS&T, Springfield, VA 2003) pp. 220-225.
48. R. Gonzalez and R. Woods, *Digital Image Processing*, 2nd ed., (Prentice-Hall, Upper Saddle River, NJ, 2002).
49. D. Lay, *Linear Algebra and Its Applications*, 3rd ed., (Addison-Wesley, Reading, MA, 2003).
50. A. Kaarna, P. Toivanen and K. Mikkonen, "PCA transform in watermarking spectral images", *J. Imaging Sci. Technol.* **48**, 183 (2004).
51. www-site: <http://aviris.jpl.nasa.gov/html/aviris.freedata.html>, cited 23.6.2005.
52. M. Rabbani and P. W. Jones, *Digital Image Compression Techniques*, (SPIE Press, Bellingham, WA, 1991).