PCA/WAVELET BASED WATERMARKING OF MULTISPECTRAL IMAGE

Y. RANGSANSERI, J. PANYAVARAPORN, P. THITIMAJSHIMA

Department of Telecommunications Engineering, Faculty of Engineering
King Mongkut's Institute of Technology Ladkrabang, Bangkok 10520, Thailand
rangsanseri@yahoo.com, jippy26@hotmail.com, ktpunya@kmitl.ac.th

ABSTRACT

In this paper, we propose a watermarking technique of multispectral images. In our method, the Principal Component Analysis (PCA) is preliminarily applied on the multispectral image. The most principal component image is used for embedding with a watermark, which is a pseudo-random number sequence generated with a secret key. The embedding process is performed in the wavelet domain. The resulting image is then reinserted into the principal component images, and the final multispectral image containing the watermark can be produced by the inverse PCA. Experimental results are provided to illustrate the performance of the algorithm against various kinds of attacks.

1. INTRODUCTION

The growth of new imaging technologies has created a need for techniques that can be used for copyright protection of digital images. Copyright protection involves the authentication of image content and/or ownership and can be used to identify illegal copies of a (possibly forged) image. One approach for copyright protection is to introduce an invisible signal known as a digital watermark in the image.

In order to be effective, an imperceptible watermark should meet the following requirements (Hsieh 2001):

Invisibility: Perceptual transparency. This concept is based on the properties of the human visual system or the human audio system.

Security: The embedded information cannot be removed beyond reliable detection by targeted attacks based on a full knowledge of the embedding algorithm and the detector (except a secret key), and the knowledge of at least one carrier with hidden message.

Robustness: The ability to extract hidden information after common image processing operations: linear and nonlinear filters, lossy compression, contrast adjustment, recoloring, resampling, scaling, etc.

Undetectability: Impossibility to prove the presence of a hidden message. This concept is inherently tied to the statistical model of the carrier image. The ability to detect the presence does not automatically imply the ability to read the hidden message. Undetectability should not be mistaken for invisibility, a concept related to human perception.

The digital image watermarking techniques can be classified into two categories, first techniques is in spatial domain watermark embedded by directly modifying the pixels values, the other techniques is in the frequency domain watermark embedded in the transform space (e.g. DCT, FFT or wavelet transform) by modifying coefficients. These two techniques have different advantages because most the signal processing operations can be well characterized in the frequency domain and several good perceptual models are developed in the frequency domain. The technique proposed in this paper is also based on frequency domain.

In this paper, we propose a new technique in frequency domain for embedded watermark base on wavelet domain (Tay 2002, Wang 2000, Wei 1998, Xie 2004) that does not require the original image for the watermark detection. Watermark is inserted into all high frequency subbands. Furthermore, we discuss the threshold value used to determine whether the watermark is present or not. Finally, we will investigate the limitations of the watermarking techniques and discuss further research issues.

2. THE PROPOSED ALGOLITHM

In our experiment, the watermark was embedded in the most principal component image resulted from PCA. Inverse PCA will reconstruct the multispectral image which already had the watermark. The watermark is supposed to be a pseudo-random number (PN). The watermarking process consists of three main steps: PCA process, watermark embedding and watermark detecting, to be described as follows.

2.1 Watermarking in PCA image

Fig. 1 shows a block diagram of the watermark insertion process. First, the multispectral image is brought to the PCA process as N dimensional vectors being N the number of spectral bands. Let X be the vector containing the N components for a given pixel and U the mean vector $U=E[X]$. The covariance matrix C_x is defined as

$$C_x = \mathrm{E}\left[(X-U)(X-U)^t\right] \quad (1)$$

The PCA (or T) is defined as the one that diagonalizes C_x in the following way:

$$C_y = TC_xT^t = \Lambda \quad (2)$$

Being C_y the covariance of the transformed vector (Y) and Λ the diagonal matrix representing eigenvalues. Y can then be obtained by:

$$Y = T(X-U) \quad (3)$$

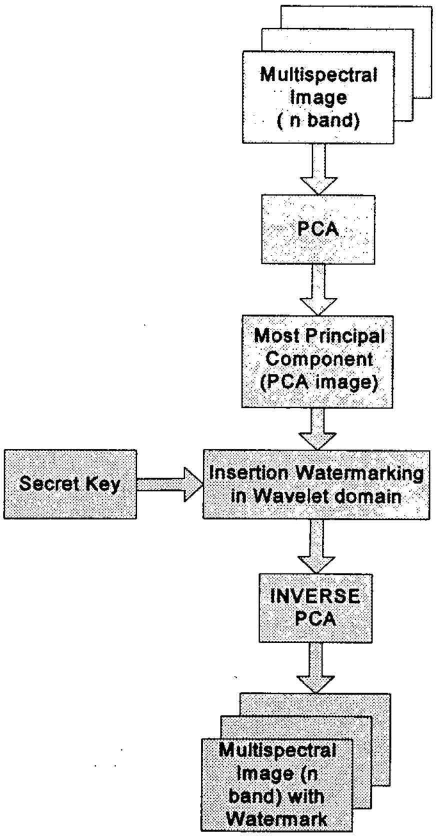


Fig. 1 Watermark insertion process

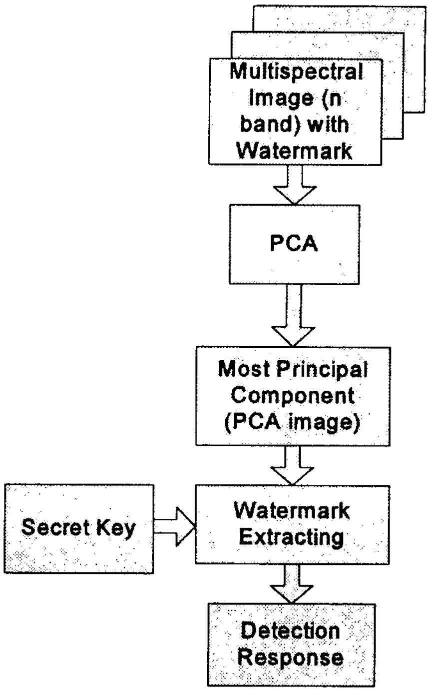


Fig. 2 Watermark detection process

Since the transformation optimally diagonalizes the co-variance matrix between spectral bands, the spectral correlation of the transformed components is removed. The images in the transformed domain are sorted in order of importance or with decreasing variance (Value of the eigenvalues). This energy compaction in the spectral axis is quite suitable for selection to insert the watermark.

Fig. 2 shows the block diagram of the watermark detection process. Before extracting the watermark the image will transform by PCA process to get most principal component as described.

2.2 Watermark Insertion

Fig. 3 shows a block diagram of the watermark insertion. We decompose an original image I until the scale N and obtain multiresolution representation (MRR) LH_n, HL_n, HH_n ($n = 1,2,\ldots, N$) and the multiresolution approximation (MRA) LL_N.

To find the perceptually significant wavelet coefficients for each subband, the threshold value is calculated according to the decomposition level. For example in the three-level decomposition, the largest coefficient C_1 for the first-level subbands (LH_1, HL_1, HH_1) is selected and the threshold $T1$ is calculated by (4) and $T2$ for the subsequent levels are respectively calculated using the same procedure.

$$T_i = 2^{\lfloor \log_2 C_i \rfloor - 1} \tag{4}$$

where i is the decomposition level and X represents the largest integer which is no greater than X. The watermark is embedded only to the selected coefficients.

The watermark (X) is generated by the pseudo random sequence whose probability law has a normal distribution of zero mean and unit variance. The watermark is then inserted into the image by:

$$V_i' = V_i + \alpha |V_i| x_i \tag{5}$$

where we runs over all DWT coefficients $> T_i$. V_i and V_i' denote respectively the DWT coefficient of the original image, the watermarked image and α is a scaling parameter. Finally, we reconstruct the watermarked image I' using the inverse DWT.

2.3 Watermark Detection

The watermark detection process is showed in Fig. 4. It is composed of DWT of watermarked image. We choose all the high-pass coefficients with amplitude greater than T2, and correlate them with the original copy of the watermark.

The similarity between the DWT coefficients of the corrupted watermarked image and a possibly different watermark (Y) can be measured by the correlation (z) :

$$z = \frac{1}{M}\sum_{i} |\hat{V}_i| y_i \tag{6}$$

If the similarity value is greater than a threshold value S_z in (7), it is possible to determine whether a given watermark is present.

$$S_z = \frac{\alpha}{2M}\sum_{i} |\hat{V}_i| \tag{7}$$

where M is the number of coefficients where the watermark is inserted.

3. EXPERIMENTAL RESULTS

A 3-band LANDSAT image, size of 256x256 pixels, was used for the experiments. Fig. 5(a) shows the color-composite of the original multispectral image and Fig. 5(b) shows the watermarked image with parameter α=0.5 and key =100. The wavelet filter used is 3-tap Daubechies. Fig. 5(c) shows the response of the watermark detector using the key scanned from 1 to 1000. The dotted line shows the threshold S_z. We find that the positive response to the correct watermark is much stronger than the response to incorrect watermarks.

The robustness capability is very critical for watermarking. We tested the robustness with some attacks such as median filter, Gaussian noise and JPEG compression. Figs. 6 and 7 shows the results of watermark detection after smoothing with a 3x3 median filter and JPEG compression with quality factors of 50%. The robustness against Gaussian noise is illustrated in Fig. 8. We can see that in all cases the detector responses are still well above the threshold.

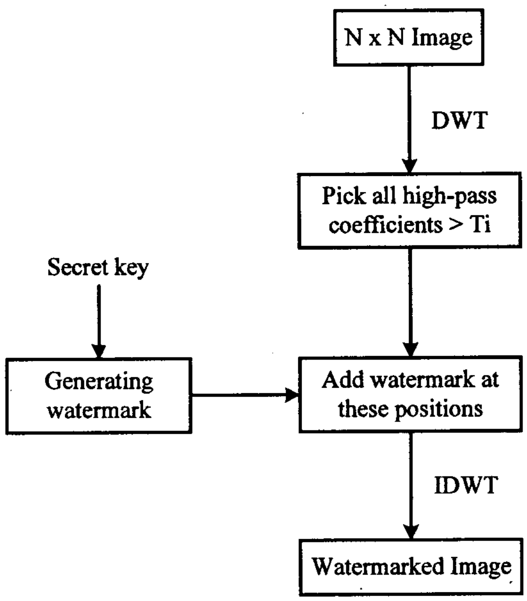


Fig. 3 Watermark insertion process in wavelet domain

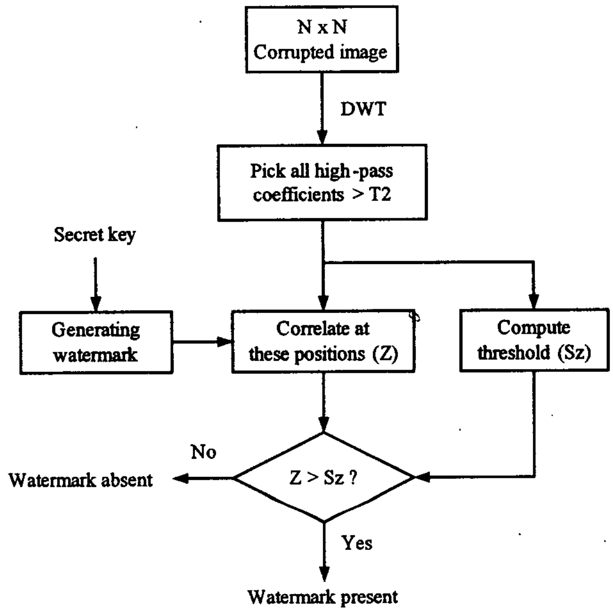
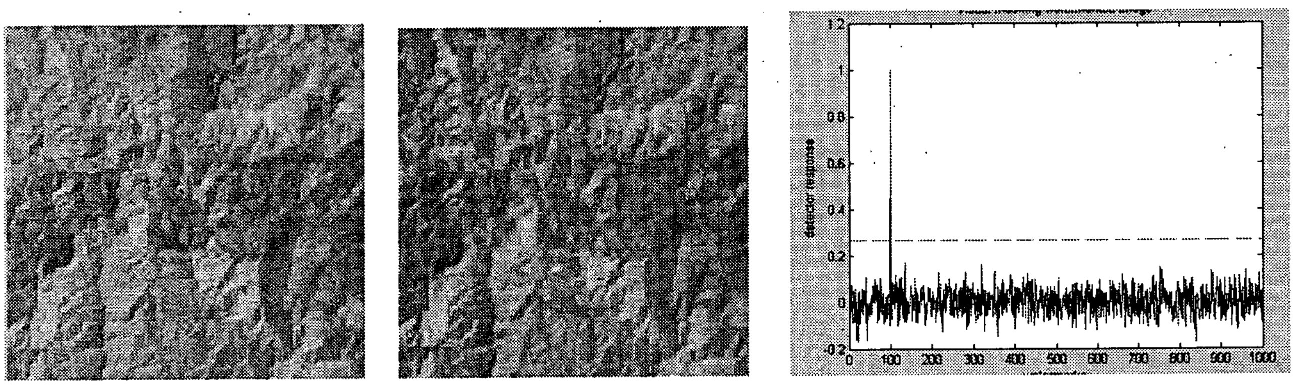


Fig. 4 Watermark detection process in wavelet domain



(a) (b) (c)

Fig. 5 Comparison between original image (a) and watermarked image (b) and the corresponding detector response (c)

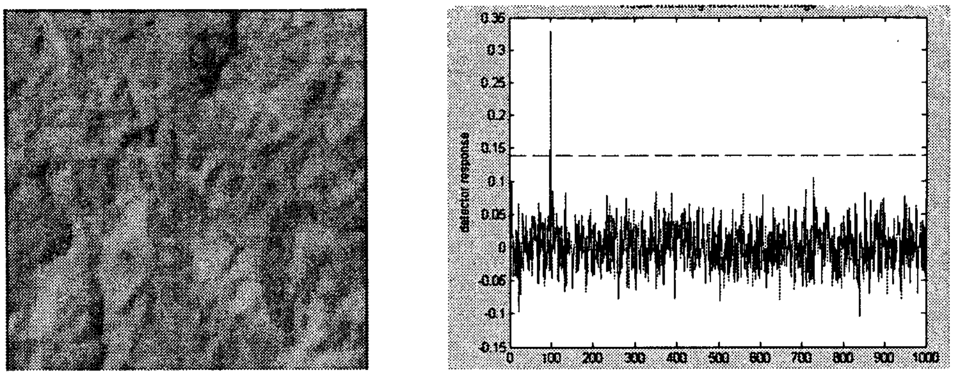


Fig. 6 Watermarked image after smoothing (*left*) and the corresponding detector response (*right*)

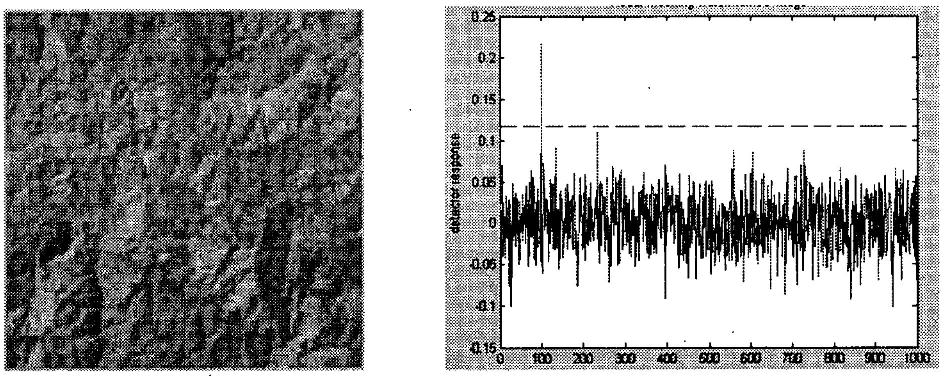


Fig. 7 JPEG image with quality at 50% (*left*) and the corresponding detector response (*right*)

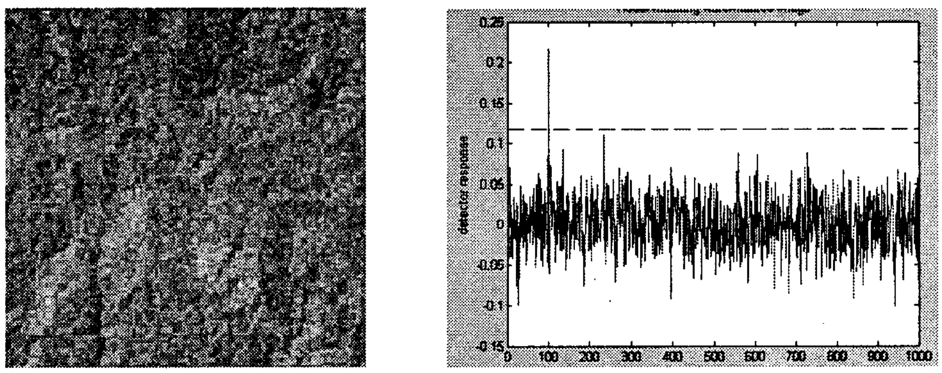


Fig. 8 Watermarked image disturbed by Gaussian noise (*left*) and the corresponding detector response (*right*)

4. CONCLUSIONS

In this paper, we have presented a digital watermarking technique of multispectral images. The proposed method is archived by applying a wavelet-based watermarking technique on the most principal component image resulted by PCA. The robustness against various attacks such as smooth with 3x3 median filter, JPEG compression and Gaussian noise are also presented.

REFERENCES

M.S. Hsieh, D.C. Tseng and Y.H. Huang, 2001, Hiding digital watermarks using multiresolution wavelet transform, *IEEE Trans. Ind. Electronics*, 48(5):875–882.

R. Tay and J.P. Havlicek, 2002, Image watermarking using wavelets, *45th Midwest Symp. Circuits and Systems*, 3:258-261.

Y.P. Wang, M.J. Chen and P.Y. Cheng, 2000, Robust image watermark with wavelet transform and spread spectrum techniques, *34th Asilomar Conf. Systems and Computers*, 2:1846–1850.

Z.H. Wei, P.Q. In and Y.Q. Fu, 1998, Perceptual digital watermark of images using wavelet transform, *IEEE Trans. Consumer Electronics*, 44(4):1267–1272.

G. Xie and H. Shen, 2004, Robust wavelet-based blind image watermarking against geometrical attacks, *IEEE Intl. Conf. Multimedia and Expo*, 3:2051–2054.