Authentication Scheme Based on Principal Component Analysis for Satellite Images

Ashraf. K. Helmy and GH.S.El-Taweel

National Authority of Remote Sensing and Space Sciences, Cairo, Egypt
Faculty of Computers and Informatics, Sues Canal University, Ismailia, Egypt
akhelmy@narss.sci.eg, ghada_el11@hotmail.com

Abstract

This paper presents a multi-band wavelet image content authentication scheme for satellite images by incorporating the principal component analysis (PCA). The proposed scheme achieves higher perceptual transparency and stronger robustness. Specifically, the developed watermarking scheme can successfully resist common signal processing such as JPEG compression and geometric distortions such as cropping. In addition, the proposed scheme can be parameterized, thus resulting in more security. That is, an attacker may not be able to extract the embedded watermark if the attacker does not know the parameter.

In an order to meet these requirements, the host image is transformed to YIQ to decrease the correlation between different bands, Then Multi-band Wavelet transform (M-WT) is applied to each channel separately obtaining one approximate sub band and fifteen detail sub bands. PCA is then applied to the coefficients corresponding to the same spatial location in all detail sub bands. The last principle component band represents an excellent domain for inserting the water mark since it represents lowest correlated features in high frequency area of host image.

One of the most important aspects of satellite images is spectral signature, the behavior of different features in different spectral bands, the results of proposed algorithm shows that the spectral stamp for different features doesn't tainted after inserting the watermark..

Keywords: *Multi-band wavelet, principal component analysis.*

1. Introduction

The demand for remote sensing data has increased dramatically mainly due to the large number of applications capable to exploit remotely sensed data and images. Along with the widespread infusion of digital technologies, and the proportional ease of distribution of digital contents over the internet, digital rights management (DRM) is becoming an increasingly important issue in multimedia applications and services [1]. One significant advantage of the digital watermarking approach is that the protection is robustly integrated with the raw media data, independent of the specific representation format, which provides great flexibility that allows the protected content to be adapted or modified in the course of delivery without having to access the watermarking key for un-protection, adaptation, and reproduction.

Robustness and perceptual transparency are two fundamental issues in digital watermarking [2, 3]. Many existing watermarking techniques embed watermarks in the discrete dyadic wavelet transform (DWT) domain to take advantage of its unique characteristics. In terms of embedding strategy, most works propose that watermarks should be embedded in one or several selected detail frequency band coefficients because of the small impact on perceptual distortion [5]. Principle component analysis (PCA) has also been applied to non-overlapping spatial image blocks to achieve more robust watermark embedding [5], which nevertheless suffers from the common limitations of a rigid block based approach. This paper proposes a new approach that incorporates parameterized multi-band (M-band) wavelet transformation and PCA. By taking advantage of the strength of both MWT and PCA, the watermark energy is distributed to low correlated wavelet coefficients of every detail sub band thus achieve better robustness, perceptual transparency, and good localization.

2. Multi-band Wavelet Transformation

From conventional two-band wavelet (M = 2), there is a scaling function $\Phi(x) \in L^2(R)$ and (M-1) wavelet functions $\Psi_L(x)\ 1 <= L <= M-1, M > 2\}$. These functions satisfy the following equations respectively [6, 7]:

$$\Phi(x) = \sum_{k \in Z} h_0(k)\Phi(Mx-k) \quad (1)$$

$$\Psi(x) = \sum h_1(k)\Phi(Mx-k), 1 <= l <= M-1$$

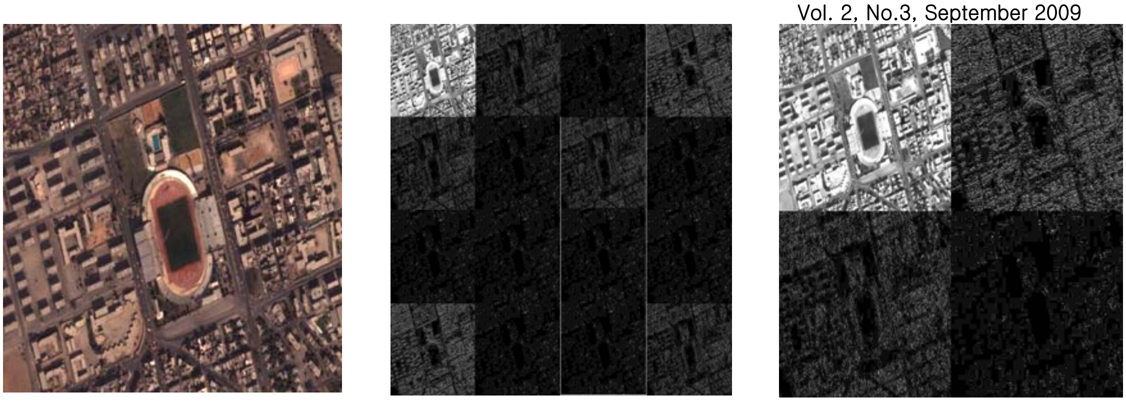
Where Z is the integer set and sequence $\{h_1(k), 1 <= l <= M-1\}$ has finite length. The one dimensional Mallat decomposition and reconstruction formulae of orthogonal multi-band wavelet are expressed in Equations (2) and (3) respectively [7]

$$C_{j+1}(k) = M^{1/2} \sum c_j(k')h_0(k'-Mk)$$
$$d_{j+,1,l}(k) = M^{1/2} \sum d_j(k')h_1(k'-Mk)\ 1 <= 1 <= \mathrm{M}-1 \quad (2)$$

$$C_j(k) = M^{-1/2} \sum_{k' \in Z} c_{j+1}(k')h_0(k'-Mk) + M^{-1/2} \sum d_{j+1}(k')h_1(k'-Mk), 1 <= l <= M-1 \quad (3)$$

Where $\{C_{j+1}(k), j=0, 1, 2\ldots\}$ is the approximation coefficients of the J+1 level M-band wavelet decomposition of one dimensional signal $C_o(k)$, and $\{d_{j+1}(k), j=0, 1, 2,\ldots\}$is the detail coefficient of the J+1 level M-band wavelet decomposition. For image signal, the above one-dimensional multi-band discrete wavelet transformation is easy to extend to two-dimensional multi-band discrete wavelet transformation (MWT) by applying one-dimensional multi-band wavelet transformation along the image rows then columns separately [7].

Figure 1 shows an example of two-dimensional MWT [6] and two-band discrete wavelet transform (DWT). In multi-band discrete wavelet transformation, one-level image decomposition is used, every wavelet coefficient is a band-pass filtering result of a local region of the original image at the same scale. Every wavelet sub band of MWT has the same number of coefficients (Figure 1b). This is different from the two-level DWT (Figure 1c), where the coefficients might belong to different scales the multi-band wavelet $\Psi(x)$ used in this paper is symmetric, parameterized by a parameter $\lambda \in R$. Modulo value t = $\mathrm{mod}(\lambda, 2\Pi)$ assumes a real value between 0 and 2Π [6]. Here mod denotes the signed remainder after division. Different values of t lead to different multi-band wavelets.



(a) (b) (c)

Figure 1. (a) Original image (b) one-level decomposition with 4-band wavelet with (multi- band WT) (c) two level decomposition 2-band DWT

3. Embedding Process

The proposed embedding algorithm based on MWT and PCA (Figure 2) is divided into the following steps:

1- The color image is transformed YIQ, thus decreasing the correlation among the three channels. Each channel is considered as an independent image, candidate for Watermarking.
2- One-level decomposition with MWT is applied to each channel. One approximate sub band and fifteen detail sub bands are obtained which provide a secure embedding domain and excellent space frequency localization.
3- PCA is used to transform a coefficients corresponding to the same spatial location in all detail sub bands. (PCA) [5] is applied as follows. Firstly, the covariance matrix $V=E\ (g_i \times g_i^T)$ is calculated, where vector g_i is the i^{th} one-dimensional data array, T denotes the matrix transpose operation, E denotes expectation operation. Secondly, the eigenvectors Φ (basis function) corresponding to the eigenvalues ζ of the covariance matrix V is considered. $V\Phi = \zeta\ \Phi$, where eigenvectors ζ are sorted in descending order, $\Phi = \{\varphi_1 \ldots \varphi_6)$. Lastly PCA components p_i is calculated as $\Phi^T g_i = (p_{i,1}, p_{i,1}, p_{i,1, \ldots,} p_{i,16})$, $1<i< N$ for each g_i respectively.
4- The full-frame DCT (Discrete Cosine Transform) of the one approximate sub band of wavelet coefficient is computed. The DCT coefficients are then quantized by using quantization matrix. The scaled values are then ordered through a zigzag scan and just a portion of them, the first ones that are likely to be the most significant, are selected.
5- The resulting coefficients are then embedded in the last principle component of all fifteen detail sub bands wavelet domain of the host image (one dimensional vector).
6- apply the inverse PCA on the modified PCA components to obtain the modified one-dimensional wavelet coefficients array
7- Performing inverse MWT (IMWT) on the modified image coefficients and finally perform the inverse color transform

The motivations of incorporating multi-band wavelet and PCA are as follows: parameterized multi-band wavelet which concentrates the energy of the wavelet coefficient vectors and distributes the watermark energy over all detail sub bands, resulting in enhanced watermark invisibility and/or robustness.

It is well known that even after the orthogonal wavelet decomposition, some correlations between the wavelet coefficients are still exist, especially those corresponding to the same spatially local region at the same scale. These correlations between the coefficients corresponding to different frequencies but the same spatial location are removed in the last band of PCA. More over the energy of the image could be further concentrated, leading to an embedding domain that permits the embedding of larger watermark energy, which in turn lead to better perceptual transparency, and improved robustness. This approach makes the watermark less visible or more robust to lossy compression than embedding watermarks in only one or several selected wavelet sub bands.

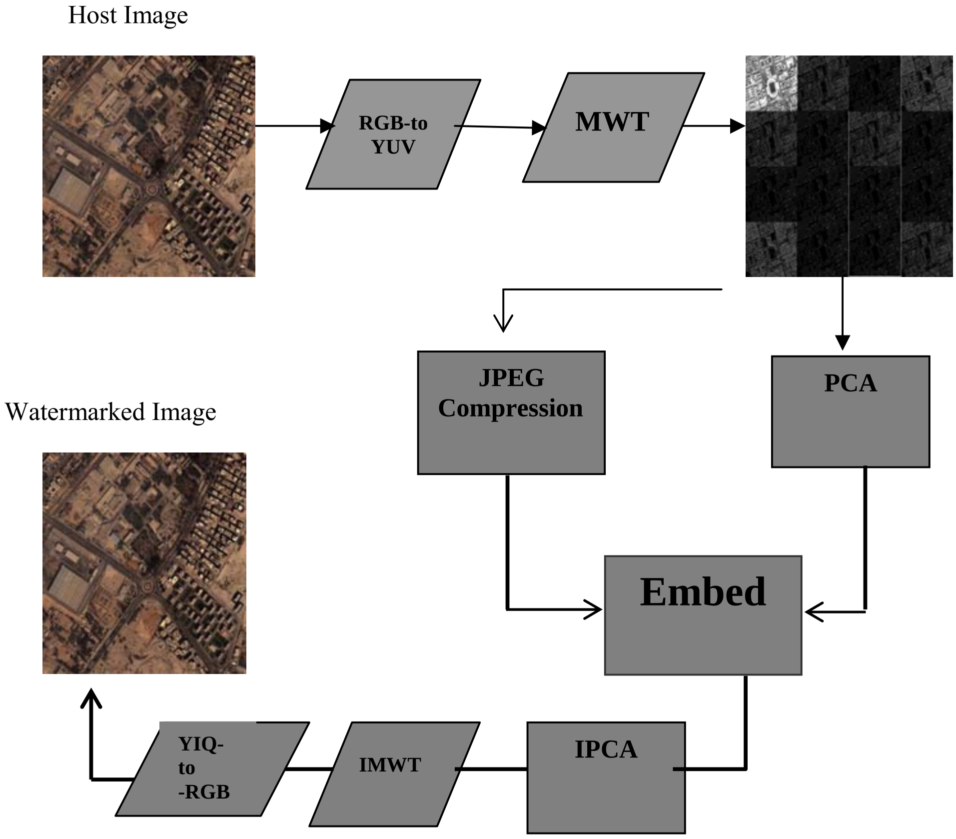


Figure 2. Block diagram of Embedding Process

4. Verification Process

The watermark extraction (figure 3) is the inverse process of watermark embedding. The watermarked image is decomposed by MWT, then PCA is applied, and the last principle components are obtained to form a 1-D array $C^*\{C^*(i), 1 < i < N\}, C^*(i)$ is the extracted principal component. An estimate of the original DCT coefficients is then obtained by averaging all the copies of the same coefficient extracted from principal component. This averaging operation is used to smooth possible modifications occurred to the image that are likely to produce different effects in the two sub-bands. Then a unique set of authentication data is obtained.

The inverse scaled coefficients are then replaced in their correct positions, by means of an anti-zigzag scanning, in such a way to obtain an estimate of the DCT of the reference image (missing elements are set to zero). These values are weighed back with the JPEG quantization matrix, and then inverse-DCT is applied to finally obtain an approximation of the original-reference image. The quality of this extracted image is very satisfactory and permits to make a good comparison with the checked image to understand if it is authentic or not, by verifying if some content has been altered or not and to localize manipulation.

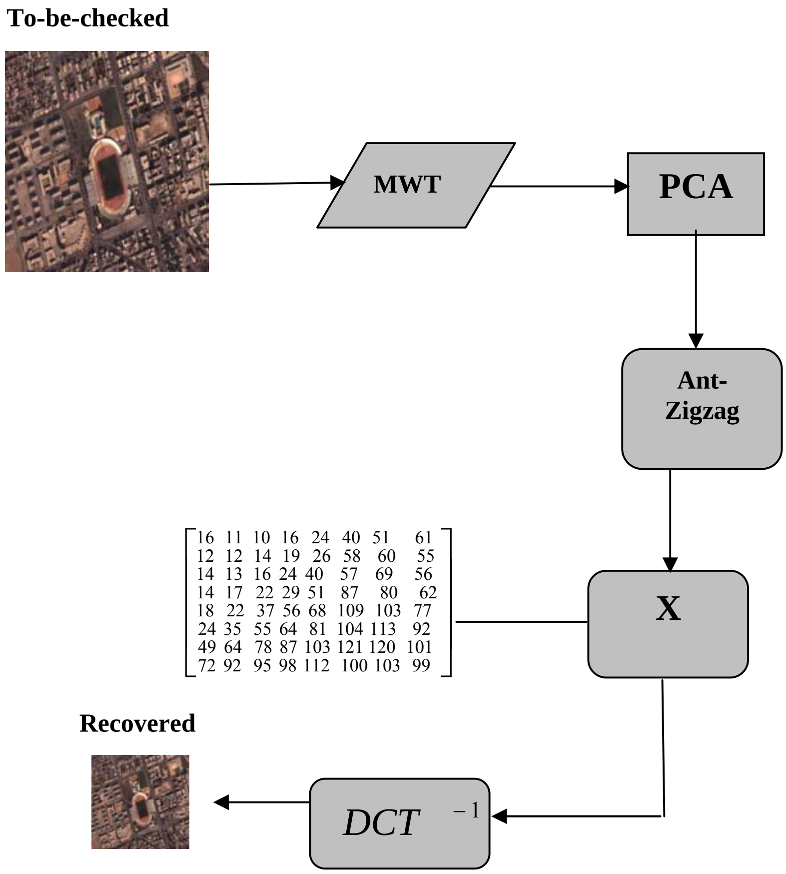


Figure 3. Block Diagram of Integrity Verification Process

5. Simulating Results

The proposed scheme for content authentication is applied to two sets of satellite images. Firstly, 512 x 512 11-bit quick -bird satellite image (figure 4-a). Secondly, 14000 x 9000 mosaiced TM satellite image (figure 4-b). Besides qualitative observations, visual quality of the watermarked images, Peak Signal-to-Noise Ratio “PSNR” (equation 4) which measures the difference between an original image and its modified version is used as a quantitative measure to evaluate the performance of proposed scheme.

In addition of the previous measures, spectral signature for different features in host and watermarked images are plotted against each other to show if any feature has been altered due to watermarking insertion. With the set of images produced. Firstly, we have obtained an average PSNR of 50.47 *dB*. Figure (5) clearly shows that the majority of the watermarked images are not perceptually different from the unprotected ones.

(a) (b)

Figure 4. Demonstrate input images (a) quick bird image (b) Mosaiced TM image

$$PSNR = 10 \, . \log \left[\frac{\max(I(i,j))^2}{\sum_{N,M} (I'(i,j) - I(i,j))^2} \right] \tag{4}$$

(a) (b)

Figure (5) Demonstrate watermarked images (a) quick bird image (b) TM image

Secondly, an important aspect of our scheme is its ability to localize image tampering (system is able to detect, the malicious modification of an image with the intention of adding or removing information). For this reason, we have tampered previously watermarked images, results of verification process show that the proposed system is robust against most common image processing such as an additive noise, cropping, median filtering, Gaussian filtering, and JPEG compression. Figure (6) shows samples of the tampering done, and table 1 summarizes the PSNR values for different attacks of the proposed scheme compared with DWT.

It can be pointed out that even when quality factor goes down to 70%, the PSNR is still quite high (around 25%), and could be satisfactory for particular applications in which data compaction is more important than image detail reconstruction. Table 2 shows values of PSNR of the recovered image after JPEG compression. For each PSNR value the corresponding JPEG quality factor and compression ratio are shown.

a) Additive-noise watermarked

(b) median filter Watermarked

Figure 6. sample of tampering applied to water marked image

Table 1. Comparison of watermarking performance Between Proposed Scheme and DWT

ATTACKS	PSNR of proposed scheme	PSNR of DWT scheme
Additive noise	71.4	64.7
Median Filter	68.5	53.3
Gaussian filtering	67	61.3
Cropping	82.3	79.5

Table 2. PSNR versus JPEG Quality Factor

PSNR	**Quality factor**	**Compression Ratio**
51.5	100	**1.8**
45.3	95	**3.3**
40.8	80	**7.1**
38.1	75	**8.2**
35.1	70	**9.2**
28.4	65	**10.2**
22.8	**60**	**11.3**

Finally, the spectral signature for different features (urban, vegetation, sand, water) for three bands before and after embedding the water mark are plotted against each other to show whether the signature stamp has been tainted. It can be shown from figure 7 that although the pixel values for different features has been slightly changed but it still preserves the overall trend of individual features. This means that the watermarked satellite image is still preserve its characteristics and ready for remote sensing processing (classification, transformation…)

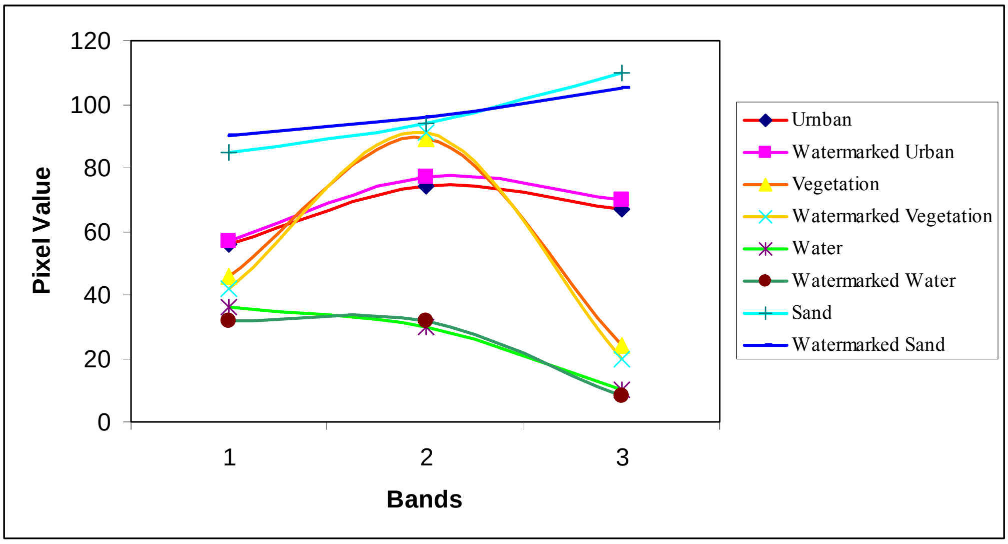


Figure 7. Changes of spectral signature after embedding watermark

6. Conclusions

In this paper, a new multi-band wavelet image content authentication based on principle component has been proposed. We have shown the efficacy and efficiency in applying PCA method for performing watermark embedding and verification.

MWT and PC provide an excellent domain for inserting water marked image since the correlations between the coefficients (derived from MWT) corresponding to different frequencies but the same spatial location are removed in the last band of PCA, More over the energy of the image could be further concentrated, leading to an embedding domain that permits the embedding of larger watermark energy, which in turn lead to better perceptual transparency, and improved robustness.

Experimental results have shown that the watermarked image with such a well-chosen embedding domain is robust against most image processing techniques (additive noise, filtering, cropping, and compression) and is more robust against JPEG compression than watermarks embedded in the DWT domain

Also, it has been proven that inserting a water mark into satellite image does not taint the spectral signature of satellite images; hence the satellite image is still ready for further remote sensing processing (classification, transformation…)

References

[1] W. Zeng, J. Lan, and X. Zhuang, "Network friendly media security: rationales, solutions, and open is- sues," in 2004 International Conference on Image Processing (ICIP), pp. 565- 568, Singapore, Oct. 2004.

[2] F. A. P. Petitcolas, "Watermarking schemes evaluation," IEEE Signal Processing, vol. 17, no. 5, pp.58-64, Sep. 2000.

[3] M. Wu, and B. Liu, "Data hiding in images and video: Part I: fundamental issues and solutions," IEEE Transactions on Image Processing, vol. 12, no. 6, pp. 685-695, Jun. 2003.

[4] M. J. Tsai, K. Y. Yu, and Y. Z. Chen, "Joint wavelet and spatial transformation for digital watermarking," IEEE Transactions on Consumer Electronics, vol. 46, no. 1, pp. 241-245, 2000

[5] T. D. Hien, Y.W. Chen, and Z. Nakao, "Robust digital watermarking based on principle component analysis," International Journal of Computational Intelligence and Applications, vol. 4, no. 2, pp. 183-192,2004.

[6] N. Bi, D. Huang, Q. Dai, and F. Li, “A class of orthogonal and symmetric 4-band wavelets with one parameter,” Mathematica Numerica Sinica, vol. 27, no. 2, pp. 1-10, May 2005.
[7] Q. Sun, N. Bi, and D. Huang, An Introduction to Multi-band Wavelets, Zhejiang University Press,2001.
[8] B. Chen and G. W. Wornell, “Quantization index modulation: A class of provably good methods for digital watermarking and information embedding,” IEEE Transactions on Information Theory, vol. 47, no. 4, pp. 1423- 1443, May 2001.
[9] I. Cox, J. Kilian, T. Leighton, and T. Shamoon, “Secure spread spectrum watermarking for multimedia, ”IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1673-1687, 1997.
[10] J. Huang, J. Hu, D. Huang, and Y. Q. Shi, “Improve security of fragile watermarking via parameterized wavelet,” in 2004 international Conference on Image Processing, pp. 721-724, Singapore, Oct. 2004.
[11] X. Kang, J. Huang, Y. Q. Shi, and Y. Lin, “A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression,” IEEE Transactions on Circuits and Systems for Video Technology, vol.13, no. 8, pp. 776-786, Aug.2003.