SECURE TRANSMISSION AND OWNERSHIP IDENTIFICATION OF DIGITAL ELEVATION MODEL

Afaf Tareef
Faculty of Information Technology, Mutah University, Jordan
Corresponding email: a.tareef@mutah.edu.jo

ABSTRACT: *In this paper, a semi-blind invisible image watermarking method is proposed for the purpose of protecting Digital Elevation Model (DEM) data from piracy or counterfeiting. The proposed method embeds invisible logo by decomposing the DEM image with 2D discrete wavelet and cosine transforms and modifying the frequency coefficients using different equations. The proposed method is evaluated under several attacks, and the results demonstrate that the DEMs altered by serious attacks can still be identified. The proposed method shows a high performance in terms of imperceptibility, robustness, and security.*

Keywords: data protection; digital elevation model (DEM); discrete wavelet transform; discrete cosine transform; ownership; watermarking

1. INTRODUCTION

Geospatial data are collected to serve national interests, such as tidal simulation [1], tsunami modeling [2], and hydrodynamic modeling of tidal flooding and its affect salt production [3]. The term "geospatial information" refers to data displaying an item or event's position and status in a specific coordinate system underneath above the Earth's surface. These data have distinctive forms, such as georeferenced data and information, geodata, and geoinformation. A Digital Elevation Model (DEM) is a visual representation of the Earth's surface generated by a Geographic Information System (GIS).

With the rapid growth of open geospatial data and the ease of transmission, data protection and ownership verification become essential to maintain the integrity of geographical data and prevent it from being altered illegally through copying. In general, copyright protection, authentication and proof of ownership are the major problems associated with transmission of digital multimedia over internet where it can be easily copied and modified. To this context, watermarking was emerged as one of effective solutions to those issues. Watermarking is the process of embedding a secret message into digital multimedia, hence, it can be extracted in the receiver side for integrity verification and ownership identification [4].

There are three important requirements for the reliable watermarking system [5]. First, the quality of the image should not be degraded after hiding the secrete message. Second, the hidden message must be robust enough to resist malicious and un-malicious attacks. Also, the hidden signature or logo should not be easily removable or extractable by anyone except the owner of the image. Third, message security should be guaranteed using encryption techniques.

2. Background

In the literature, several transformations are used to enhance imperceptibility and robustness of the watermarking, including Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), and Discrete Fourier Transform (DFT) [6]. These transforms divide the image into different bands with different details. For instance, DCT divides images

into three frequency bands, i.e., low, middle, and high frequency bands, while DWT divides image into four sub-bands in a single level: Low-Low (LL). Low-High (LH), High-Low (HL) and High-High (HH) frequency sub-bands, where LL sub-band presents a soft approximation of image and the other three sub-bands show horizontal, vertical and diagonal details.

Despite the wide use of watermarking for assuring the integrity and maintain authenticity of digital multimedia, it is still rarely used for DEM data. In [7], different transformations (i.e., DCT, DWT, and FFT) are performed to hide a logo on DEM files. This method shows that DCT technique is better than DWT and FFT, and it is able to resist cropping attack. Another method is introduced in [8] for protection and authentication of Dubai Digital Elevation Model provided by United States Geological Survey (USGS). This method performs dual watermarking using the scaled odd/even extraction technique. Specifically, the ownership signature is embedded in coefficients of DCT-DWT domain, while a key information is embedded in the spatial domain pixels.

These methods show an acceptable invisibility level, however, they are not evaluated under serious attacks, such as sharpening, blurring, compression, filtering, and noise addition.

3. The proposed Methodology

The proposed scheme consists basically of two phases: the embedding phase and the extraction phase.

A. The embedding phase

The inputs of the embedding process are the watermark, the host DEM image, and the security key. The output is the watermarked image, as shown in Figure 1. First, the binary signature is encrypted using Arnold transformation [9] in order to enhance the security of the watermarking algorithm. This key is saved for the extraction process. On the other hand, the green channel of the host color DEMs image is extracted to be the host part.

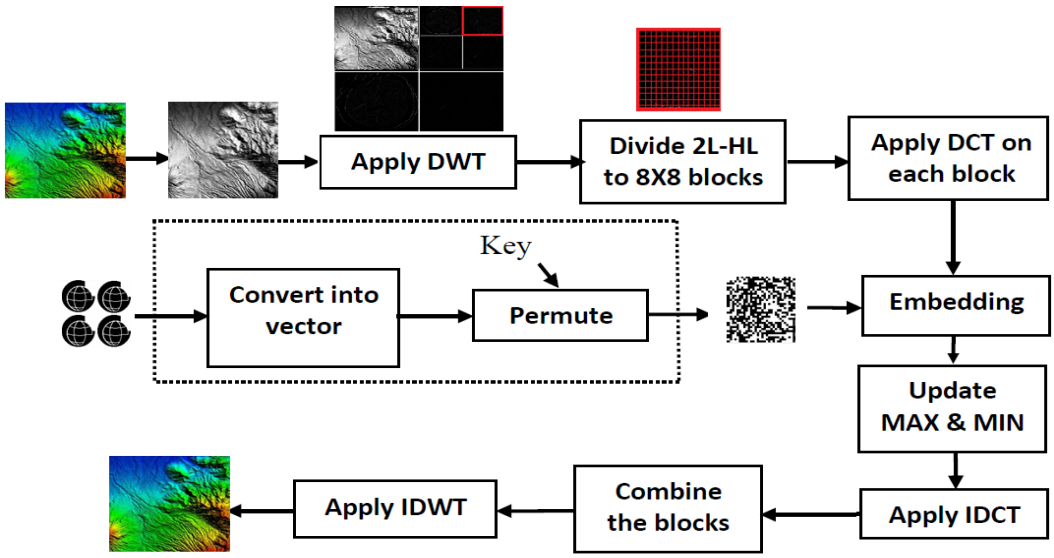


Figure 1: The embedding phase of the proposed method

This selection is due to the high weight of the green layer in forming the most important component in the colored image, i.e., luminance component. Then, it is transformed into wavelet domain by applying two level DWT using a haar wavelet filter. In order to choose the most suitable sub-band for carrying the signature, two facts are taken into consideration: 1) the Human Visual System (HVS) is more sensitive to small perturbation in the lower frequency bands than the higher ones, and 2) many attacks, such as image compression, eliminate high frequency components. Thus, the high-low frequency sub-band is chosen by our method to meet the transparency and robustness requirements.

Next, the chosen sub-band is divided into non-overlapping blocks, taking into consideration three factors, which are 1) preserving the quality of the watermarked image, where the small block increases the watermarking imperceptibility, 2) increasing the capacity of our method by dividing the sub-band into small blocks, and finally 3) improving the robustness against different attacks which is proportional to the block size. Therefore, the size of block was driven experimentally into 8x8 to achieve the best balance between these factors.

After dividing process, DCT is applied on each block. For signature embedding, the difference between the maximum and the minimum coefficient values of each block is computed and scaled by certain experimental factor α to be used as the embedding factor. In case where the difference is zero, experimental value scaled by scaling factor is used instead. If the signature bit is zero, the difference value is subtracted from every coefficient that is less than the mean of the block. In contrary, this value is added to every coefficient greater than the mean of the block if the corresponding signature bit is one. In the other case, a small value (ϵ) is used instead of the difference value. Equations (1) and (2) describe the altering process.

$$B_w(i,j) = B(i,j) \mp \alpha \times (Max - Min) \quad (1)$$

$$B_w(i,j) = B(i,j) \mp \epsilon \quad (2)$$

where, $B_w(i,j)$ represents the coefficient value of the watermarked block at (i,j) coordinate, $B_w(i,j)$ represents the coefficient value of the host DEM block, and α is the scaling factor controlling the tradeoffs between the robustness and the perceptual transparency. α is set experimentally to (0.2) in our method. To further increase the robustness, the minimum and maximum values in each block are altered by subtracting a small value from each coefficient equal to the maximum value and added to each minimum coefficient in the block.

After embedding process, watermarked channel is reconstructed by applying inverse DCT and combining the blocks, followed by inverse DWT. Finally, the watermarked green channel is combined with the host red and blue channels to get the watermarked DEM.

B. The extraction phase

The extraction phase is summarized in Figure 2. For extraction process, the transformations applied in the embedding phase (i.e., 2L DWT, 8x8 Block dividing, and DCT) are applied again to obtain the watermarked high-low frequency sub-band. Then, the mean value is computed for each block in the watermarked and host DEM image. If the mean of the watermarked block is greater than the mean of the corresponding host block, then, the hidden signature bit is one, else it is zero. Finally, the security key is used to decrypt the extracted signature.

4. EXPERIMENTAL RESULTS

For performance evaluation, three measures are used, which are Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) to assess the imperceptibility requirement, and Normalized Correlation (NC) to assess the robustness requirement of the proposed watermarking method. The PSNR, MSE, and NC can be calculated by equation (3-5), respectively.

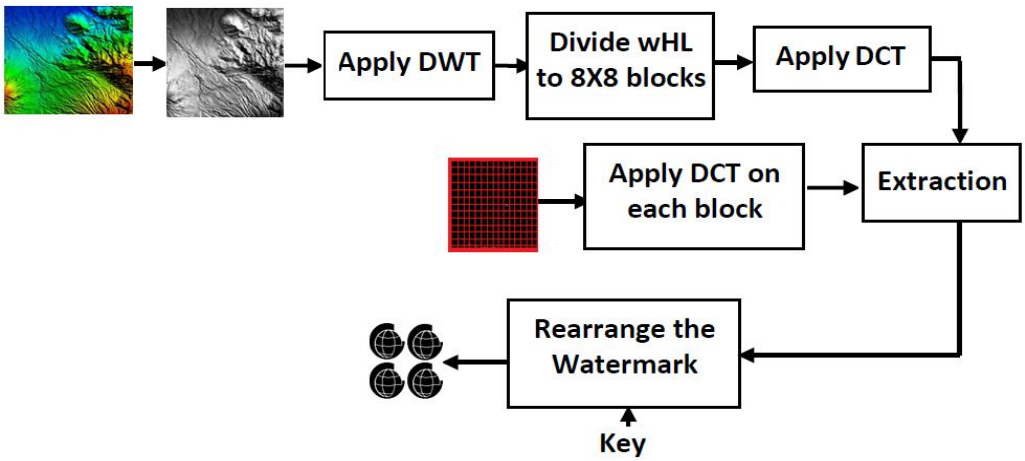
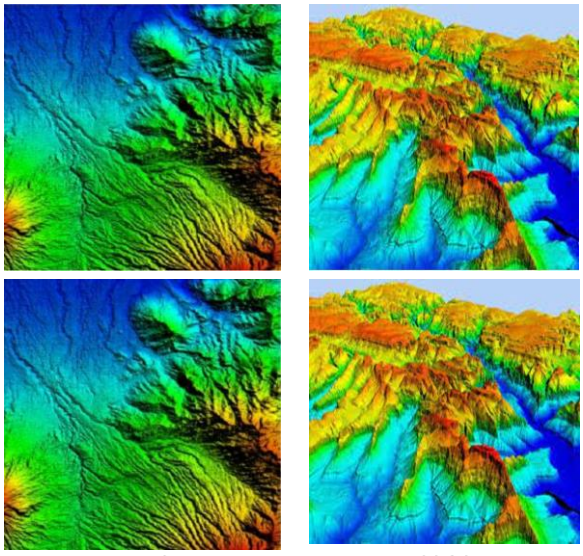


Figure 2: The extraction phase of the proposed method

$$PSNR = 10 \times log_{10}(255^2/MSE) \quad (3)$$

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (f(i,j) - g(i,j))^2 \quad (4)$$

$$NC = \frac{\sum_i \sum_j S \times S'}{\sqrt{\sum_i \sum_j S^2 \times \sum_i \sum_j S'^2}} \quad (5)$$



57.16	**66.36**
0.1250	**0.0349**

Figure 3: Sample of host DEM image (first row), watermarked DEM images (Second row), with the PSNR (third row), and SSIM values (Fourth row).

.Where f and g are the original and watermarked image, respectively. M and N are the dimensions of the image. S and S' are the original and extracted signature, respectively.

The acceptable degradation level in the watermarked image is achieved when the obtained PSNR value is greater than 36dB, which means that the hidden message is almost invisible to Human Visual System (HVS) [10,11].

The used data for our evaluation include DEMNAS Seamless Digital Elevation Model (DEM), and a National DEM file downloaded from the geoportal of the Geospatial Information Agency (Badan Informasi Geospasial—BIG). BIG logo is used as a signature.

Figure 3 shows the host and watermarked DEM, along with the corresponding PSNR and MSE values. It is obvious that the proposed method obtains a good imperceptibility between the host and watermarked DEM. All PSNR values obtained by our method are higher than 55dB, with an average PSNR of 62.70 dB, compared with an average PSNR of 57.40 obtained by [8]. Moreover, the MSE values are very low. These values indicate invisible degradation to the watermarked images.

The robustness of the proposed method is also evaluated by applying several signal processing operations and common attacks. The results are presented in Table 1. As shown, all NC vales are higher than 0.88, and it is almost one after applying sharpening, histogram equalization, and contrast adjustment on the watermarked image. These results demonstrate that our proposed DWT-DCT watermarking method has a high resistance to different type of attacks.

Table 1. Psnr And Nc Results Of Extracted Signature Under Several Attacks

Attacks	DEM1	DEM2
Without attack	1	1
Average filter	0.93	0.88
Median filter	0.98	0.89
Weighted mean filter	1	0.99
Gaussian low pass filter	1	0.99
Gaussian Noise	0.97	0.97
Salt & Pepper	0.99	0.99
Speckle Noise	0.99	0.99
Sharpening	1	1
Cropping	0.87	0.83
Contrast adjustment	1	1
Histogram equalization	1	0.99
Gamma Correction (0.5)	0.98	0.98
JPEG Compression (QF=30)	0.98	0.99

5. CONCLUSION

This paper introduces a hybrid DWT-DCT watermarking method to confirm the integrity and ownership of DEM images by embed a binary logo in the images. In our method,

DWT and DCT are performed to enhance the robustness against attacks in a lower complexity time than other transforms, such as Fourier transform. The proposed method is evaluated under different type of attacks and it shows a high fidelity and ability to extract the hidden signature. The average PSNR value is above 60 dB, and NC value is above 0.95 for most attacks. Finally, it has been demonstrated that our proposed technique can be successfully used for secure transmission and ownership identification of digital elevation model.

REFERENCE

[1] Nuraghnia, A., Windupranata, W., Hakim, A. R., & Nusantara, C. A. D. S. (2021, May). Modeling of tide in the Java sea coastal area between Jakarta and Cirebon, Indonesia: bathymetric data source and sensitivity tests due to bottom roughness and boundary condition. In *IOP Conference Series: Earth and Environmental Science* (Vol. 777, No. 1, p. 012034). IOP Publishing.

[2] Cummins, P. R., Pranantyo, I. R., Pownall, J. M., Griffin, J. D., Meilano, I., & Zhao, S. (2020). Earthquakes and tsunamis caused by low-angle normal faulting in the Banda Sea, Indonesia. *Nature Geoscience*, *13*(4), 312-318.

[3] Nirwansyah, A. W., & Braun, B. (2019). Mapping impact of tidal flooding on solar salt farming in Northern Java using a hydrodynamic model. *ISPRS International Journal of Geo-Information*, *8*(10), 451.

[4] Mohanty, S. P. (1999). Digital watermarking: A tutorial review. *URL: http://www. csee. usf. edu/~ smohanty/research/Reports/WMSurvey1999Mohanty. pdf*.

[5] Perez-Freire, L., Comesana, P., Troncoso-Pastoriza, J. R., & Perez-Gonzalez, F. (2006). Watermarking security: a survey. In *Transactions on data hiding and multimedia security I* (pp. 41-72). Springer Berlin Heidelberg.

[6] Singh, Y. S., Devi, B. P., & Singh, K. M. (2013). A review of different techniques on digital image watermarking scheme. *International Journal of Engineering Research*, *2*(3), 194-200.

[7]Amhar, F., Giri, E. P., Silalahi, F. E. S., Neyman, S. N., Anggrahito, Ramdani, D., ... & Murdaningsih. (2022). Ownership protection on Digital Elevation Model (DEM) using transform-based watermarking. *ISPRS International Journal of Geo-Information*, *11*(3), 200.

[8] Al-Saad, M., Aburaed, N., Panthakkan, A., Al Mansoori, S., & Al Ahmad, H. (2021, November). Protection and authentication of Dubai digital elevation model using hybrid watermarking technique. In *2021 4th International Conference on Signal Processing and Information Security (ICSPIS)* (pp. 13-16). IEEE. [26] Kasmani, S.

[9] Wu, L., Zhang, J., Deng, W., & He, D. (2009, December). Arnold transformation algorithm and anti-Arnold transformation algorithm. In *2009 first international conference on information science and engineering* (pp. 1164-1167). IEEE.

[10] A., & Naghsh-Nilchi, A. (2008). A new robust digital image watermarking technique based on joint DWT-DCT transformation. In *International Conference on Convergence and Hybrid Information Technology (ICCIT)*. (Vol. 2, pp. 539-544). IEEE.

[11] Wang, Z., Bovik, A. C., Sheikh, H. R., & Simoncelli, E. P. (2004). Image quality assessment: from error visibility to structural similarity. *IEEE transactions on image processing*, *13*(4), 600-612.