Block-based Watermarking for Robust Authentication and Integration of GIS Data

Afaf Tareef
Faculty of Information Technology, Mutah University, Jordan
a.tareef@mutah.edu.jo (corresponding author)

Khawla Al-Tarawneh
King Abdullah II School for Information Technology, University of Jordan, Jordan
khawla_t@mutah.edu.jo

Azzam Sleit
King Abdullah II School for Information Technology, University of Jordan, Jordan
azzam.sleit@ju.edu.jo

Received: 21 June 2024 | Revised: 8 July 2024 | Accepted: 11 July 2024

Licensed under a CC-BY 4.0 license | Copyright (c) by the authors | DOI: https://doi.org/10.48084/etasr.8197

ABSTRACT

A Geographic Information System (GIS) is a computer system for gathering, storing, transmitting, and presenting data related to positions on Earth's surface. This research aims to authenticate the GIS data during transmission via internet based on transform-based invisible watermarking. The proposed framework makes use of the singular value decomposition and discrete cosine transformation in the frequency domain. The proposed framework is evaluated on National DEM images obtained from the Geospatial Information Agency's (Badan Informasi Geospasial—BIG) geoportal, under several types of attacks. Two performance metrics (Peak to Signal Noise Ratio (PSNR) and Mean Square Error (MSE)) were considered for the evaluation of the security of the designed framework. Likewise, Normalized Correlation (NC) was computed to assess the robustness by calculating the similarity between the original and the extracted images. The experimental outcomes show that the extracted logos are readable even if they are altered, which guarantees that the received DEM data are authentic.

Keywords-singular value decomposition; discrete cosine transform; watermarking; encryption; authentication; DEM; GIS

I. INTRODUCTION

Geographic Information Systems (GIS) attract increasing attention in the military because they offer the geographic information required to organize the deployment of military personnel. The army forces need precise and trustworthy data regarding the region they are deployed. Operation planners can use a computer network or a portable device to get geographic, such as DEM, data. It is critical that the parties using the DEM data have confidence in each other, that the source of the data is authentic, and that the data have not been altered during transmission [1]. Digital Elevation Model (DEM) is a 3-D visual representation of the earth's surface, created by a GIS. DEM data are an important component of the geospatial data infrastructure since they play a key role in many scientific studies and applications [2, 3]. With the growing expansion of web-based apps, DEM data may now be distributed considerably faster and more easily. This leads to the issue of illegal copying and redistribution of DEMs. Developing tools to prove ownership and authenticate the received data is crucial.

Digital watermarking was proposed as an effective solution to prevent illegal usage of DEM data. Watermarking is the process of encoding a hidden message into a digital signal, which may then be retrieved on the receiver side for integrity verification and ownership identification [4]. There are three critical requirements for a reliable watermarking system [5, 6]. First, the image's quality should not be affected after concealing the secret message. Second, the secret message must be strong enough to resist attacks, which are different image processing and geometric operations that may be applied on the images during transmission intentionally or unintentionally. Also, no one other than the image's owner should be able to simply remove or extract the hidden signature or logo. Third, communication security should be ensured by encryption mechanisms.

In general, digital watermarking can be classified into spatial domain watermarking and frequency domain watermarking. In spatial domain watermarking, the watermark is inserted directly in the image's pixels, without any transformation to the cover image, whereas the watermark is embedded into the frequency transform coefficients in frequency watermarking. Several transformations are used to enhance the imperceptibility and robustness of the watermarking, including Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), and Singular Value Decomposition (SVD) [7]. These transforms split the image into different components with different details. For example, DCT divides images into three frequency sub-bands, i.e. low, middle, and high frequency sub-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). Singular value decomposition decomposes an $n \times d$ rectangular matrix A into the product of three other matrices as defined by (1):

$$A = U\Sigma V^T = \sum_{i=1}^{n} \lambda_i \Sigma_i {v_i}^T \qquad (1)$$

where U is an $n \times n$ column-orthonormal matrix whose columns are called left singular vectors, Σ = diag ($\sigma 1$, $\sigma 2$, ..., σn) is an $n \times d$ diagonal matrix, whose diagonal elements are non-negative singular values sorted in descending order, and V is an $d \times d$ orthonormal matrix, whose rows are called right singular vectors, as shown in Figure 1.

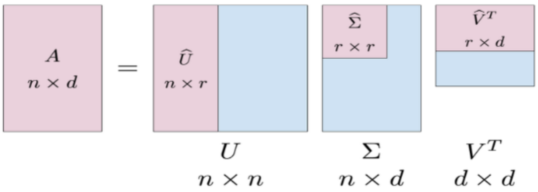


Fig. 1. Singular value decomposition of an n × d rectangular matrix A.

Watermarking has been widely used to ensure the integrity and validity of digital multimedia during transmission via electronic environments, including general, biometric, and medical data [8, 9]. For geographic data, several watermarking systems have been proposed in the past few years. For instance, authors in [10] proposed the blind watermarking method to protect vector geographic data based on coordinate mapping, Quantization Index Modulation (QIM), and matching detection technologies. The results prove high robustness against some attacks, including data compression, data adding, data deleting, and data cropping. The zero watermarking method proposed in [11] was based on the number of neighboring features in order to identify the features that resist data distortion. The zero watermarking method presented in [12] utilized the geometric invariance of the frequency domain transformation and mined the geometric statistical information in the spatial domain of vector maps. In [13], zero-watermarking and spatial domain watermarking were integrated making the watermark more robust against common attacks. In [14], two-level DWT and Complex Singular Value Decomposition (CSVD) were used to secure vector geographic data. According to this method, the watermark embedding domain is the ratio of the DWT–CSVD coefficients, which remains unaffected by geometric attacks. Authors in [15] proposed an encryption and watermarking scheme based on Minimum Bounding Rectangle (MBR) selected as geometric features and their initial vertex order. The encryption process is utilized by randomly shifting the features' coordinates, and the embedding process is performed by modifying the starting vertex order of the features. Despite the great improvements in watermarking applications, nevertheless, applications for protecting DEM data are still rarely employed, particularly in resisting attacks with considerable distortion. Few methods have been introduced to exploit watermarking in securing the DEMs. For instance, authors in [16] introduced a method for ownership identification of Dubai DEMs provided by the United States Geological Survey (USGS). In this method, dual watermarking was performed based on the scaled even/odd extraction algorithm. The dual watermark consists of the ownership signature which is concealed in the DCT-DWT coefficients, and key information concealed directly in the DEM pixels. In [17], frequency domain watermarking is performed based on different transformations, including DCT, DWT, and FFT, where the owner's logo is hidden in the frequency coefficients of the DEMs. The method proposed in [18] is based on DWT and DCT transformation. The method applies block-based transformation before embedding the watermark bits in the DEM blocks.

The above mentioned methods demonstrate a high imperceptibility level, however, they are not robust enough under common attacks occurring during data transmission, like image processing attacks (e.g. sharpening, blurring, compression, filtering, and noise addition). In this paper, a hybrid block-based SVD-DCT invisible watermarking method for DEM authentication and integration is introduced. The proposed system achieves a high imperceptibility level, as well as high robustness against the familiar image modification and attacks, and enables the legal owner of DEMs to prove their ownership even if the DEM is modified.

II. RESEARCH METHODOLOGY

The designed framework is performed in two phases: the encryption/embedding phase and the extraction/ decryption phase.

A. *Encryption and Embedding Phase*

Figure 2 displays the encryption and embedding procedure, where the color DEM images, the binary logo, and a security key are the procedure inputs to obtain the watermarked DEM image. To embed the watermark, the following steps are implemented:

Step 1: the green layer of the host DEMs image is chosen to carry the owner logo, due to its high weight in forming the most serious channel in the color image, i.e. the luminance plane.

Step 2: the binary logo is encrypted using Arnold transform in order to make the image visually unreadable and break the correlation between the neighboring pixels utilizing a specific key transferred to the receiver to be employed for the extraction process [19].

Step 3: the green layer is decomposed by singular value decomposition into three matrices. The singular matrix is chosen by the proposed method to meet the robustness and invisibility requirements.

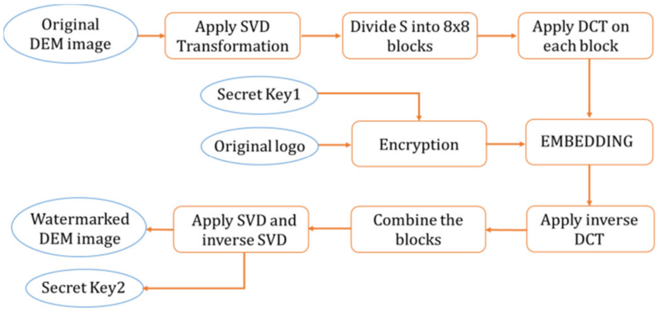


Fig. 2. The encryption and embedding phase of the proposed framework.

Step 4: the single matrix is divided into separate non-overlapping blocks, considering the following objectives: 1) maintaining the quality of the watermarked image, where a small block makes the watermarking more imperceptible; 2) improving the method's capacity by dividing the sub-band into small blocks; and 3) enhancing the robustness against various attacks, which is directly related to the block size. To obtain the optimal balance between the above requirements, the block size was experimentally driven to 8 by 8.

Step 5: each block is then transformed by DCT.

Step 6: embedding is performed. Particularly, the difference between the maximum and the minimum coefficient values of each block is calculated and scaled by a particular scaling constant C. An experimental value scaled by hiding factor is used if the computed difference is zero. Then, the difference value is subtracted from each coefficient less than the mean of the block if the logo bit is zero, and added to each coefficient greater than the mean of the block if the logo bit is one. In the other case, a small value (ϵ) is used instead of the difference value. Equations (2) and (3) describe the altering process.

$$I_w(i,j) = I(i,j) \mp C \times (\mathrm{Max} - \mathrm{Min}) \quad (2)$$

$$I_w(i,j) = I(i,j) \mp \epsilon \quad (3)$$

where I(i,j) is the coefficient value of the host block, $I_w(i, j)$ is the coefficient value of the corresponding watermarked block at (i,j) coordinates, and C is a constant used to control the tradeoffs between robustness and invisibility. To further increase the robustness, the minimum and maximum values of every block are modified by subtracting a small value from every maximum coefficient and added to every minimum coefficient in the block.

Step 7: the inverse DCT is utilized on each block, and then, the blocks are combined.

Step 8: SVD is applied again and the U and V matrices are stored as a secret key for the extraction phase. The remaining S matrix is then combined with the U and V before embedding.

Step 9: the watermarked green layer is finally concatenated with the cover red and blue layers to get the watermarked DEM.

B. Extraction and Decryption Phase

Figure 3 displays the extraction and decryption phase, where the watermarked DEM image and the keys are put into service to extract the hidden logo. To do this, the following steps are performed:

Step 1: the green layer of the watermarked image is extracted.

Step 2: SVD and the block-based DCT are performed on the green layer, as described in the embedding phase.

Step 3: the mean value of each block in the watermarked and host DEM images is calculated. If the mean value of the watermarked block is higher than the mean value of the corresponding host block, then, the embedded bit is one, else it is zero.

Step 4: the extracted logo is decrypted using the encryption key.

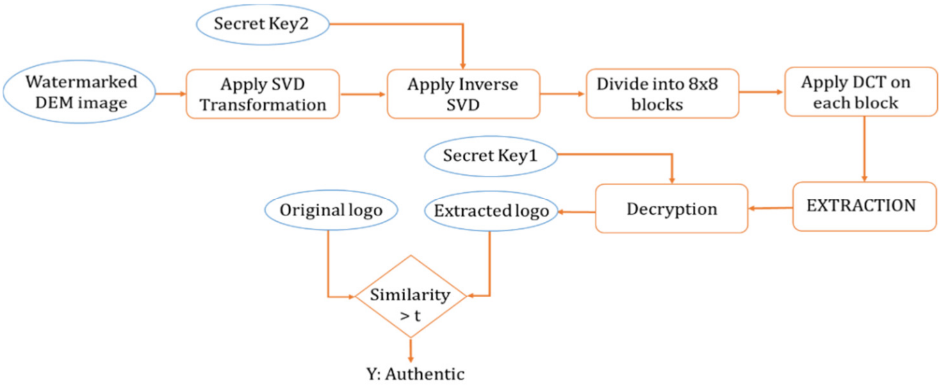


Fig. 3. The extraction phase of the proposed method.

III. EXPERIMENTAL RESULTS

In order to examine the algorithm, MATLAB functions for embedding and extraction are defined. For the performed implementation, the cover images are color DEM images of 256 × 256 pixels from the geoportal of the Geospatial Information Agency, i.e., Badan Informasi Geospasial (BIG) and DEMNAS Seamless Digital Elevation Model [20, 21].

Binary BIG and copyright logo of size (60 × 60) pixels were used as signatures. Figure 4 displays samples of DEM and logo images.

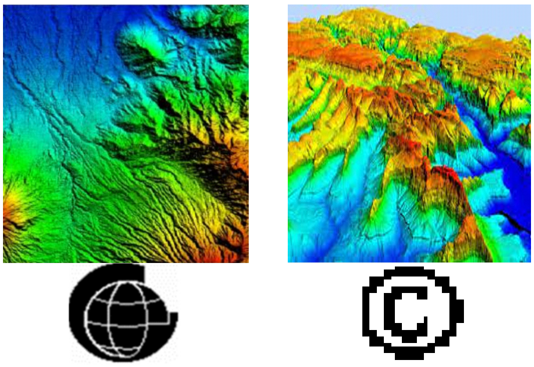


Fig. 4. Sample of host DEM images in the first row, and logo images in the second row.

The performance of the proposed framework was evaluated with Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) to assess the imperceptibility requirement, and Normalized Correlation (NC) to evaluate robustness. The PSNR, MSE, and NC are computed by:

$$\mathrm{PSNR} = 10 \times \log_{10}(255^2/\mathrm{MSE}) \quad (4)$$

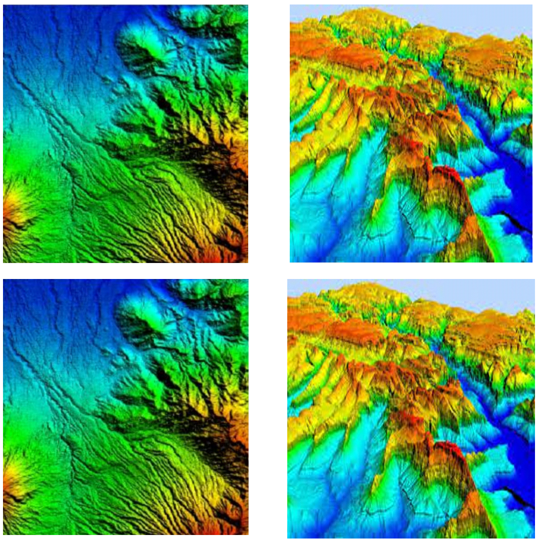
$$\mathrm{MSE} = \frac{1}{\mathrm{N} \times \mathrm{D}} \sum_{\mathrm{i}=1}^{\mathrm{N}} \sum_{\mathrm{j}=1}^{\mathrm{D}} (\mathrm{I}\,(\mathrm{i},\mathrm{j}) - \mathrm{I}'\,(\mathrm{i},\mathrm{j}))^2 \quad (5)$$

$$\mathrm{NC} = \frac{\sum_{\mathrm{i}} \sum_{\mathrm{j}} \mathrm{g} \times \mathrm{g}'}{\sqrt{\sum_{\mathrm{i}} \sum_{\mathrm{j}} \mathrm{g}^2 \times \sum_{\mathrm{i}} \sum_{\mathrm{j}} \mathrm{g}'^2}} \quad (6)$$

where I and I′ are the original and watermarked DEMs, respectively, N and D are the dimensions of the image, and g and g′ are the original and extracted logo, respectively. A PSNR value that is greater than 36 dB means that the concealed logo is invisible to the Human Visual System (HVS), whereas a NC value close to 1 means high similarity between the original and reconstructed logo images [22, 23].

The cover and watermarked DEMs, along with the corresponding PSNR and MSE values are depicted in Figure 5. It can be observed that the designed framework shows high invisibility indicated by the high PSNR values (higher than 42 dB), and the low MSE values. These values indicate a high similarity between the cover and watermarked DEM images. The reason behind these results is the use of the singular value decomposition along with the block-based DCT with this study's explained technique which preserves the original pixel values.

Additionally, the resistance of the designed framework to different attacks, i.e., signal processing and geometric operations, is evaluated. Table I presents the NC values between the original and extracted logos obtained by the proposed method and those attained by [18] under different types of operations, including filtering, noise addition, contrast adjustment, cropping, and compression. All NC values are greater than 0.93, and they are ideal for some attacks, such as contrast adjustment, Gaussian low-pass filter, and JPEG compression. The proposed framework exhibits higher robustness than [18]. This improvement is due to the utilization of SVD twice along with block-based DCT for logo embedding.



43.44	**42.33**
2.94	**3.81**

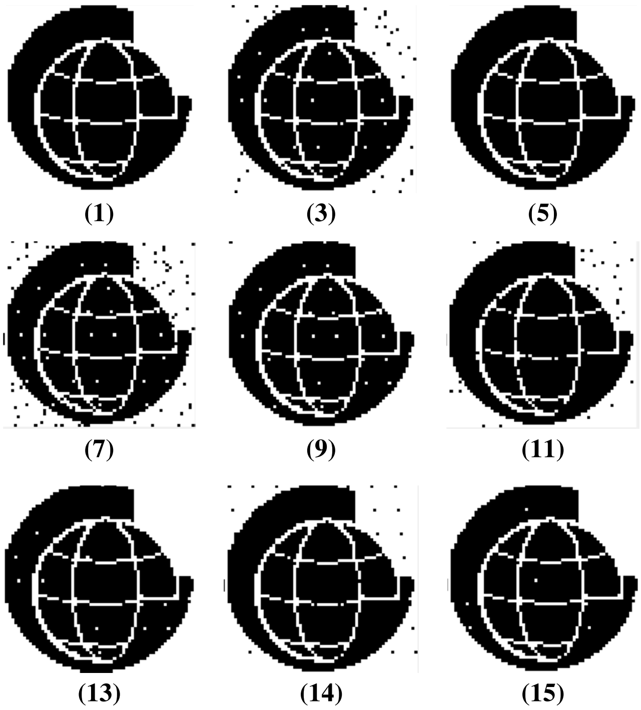
Fig. 5. Sample of host DEM images (first row), watermarked DEM images (second row), with the PSNR and MSE values in the third and fourth row.

TABLE I. NC COMPARISON OF THE EXTRACTED LOGO BY [18] AND THE PROPOSED FRAMEWORK UNDER SEVERAL ATTACKS

#	Attacks	[18]		Proposed	
		DEM1	DEM2	DEM1	DEM2
1	No attack	1	1	1	1
2	Average filter	0.89	0.88	0.95	0.93
3	Median filter	0.96	0.94	0.96	0.95
4	Weighted mean filter	1	0.99	0.99	0.99
5	Gaussian low pass filter	1	0.99	1	1
6	Gaussian noise	0.97	0.97	0.96	0.94
7	Salt & pepper	0.95	0.93	0.96	0.96
8	Speckle noise	0.99	0.99	0.98	0.96
9	Sharpening	1	1	1	1
10	Cropping	0.87	0.83	0.94	0.98
11	Blurring	0.95	0.94	0.99	0.94
12	Contrast adjustment	1	1	1	1
13	Histogram equalization	1	0.99	1	0.98
14	Gamma correction (0.5)	0.98	0.98	0.98	0.98
15	JPEG compression (30)	0.97	0.97	1	0.99

For further evaluation, Figure 6 provides samples of extracted and decrypted logos. The hidden logos can be successfully extracted with high similarity to the original one even when the DEM images are seriously corrupted.

The quantitative and qualitative results indicate that the concealed logo can successfully withstand many types of attacks and that the proposed hybrid SVD-DCT watermarking framework yields high robustness.



(1) (3) (5)

(7) (9) (11)

(13) (14) (15)

Fig. 6. The extracted logo after applying the respective attack number shown in Table I. It is clear that the extracted logo can be easily recognized by the human eyes.

IV. CONCLUSION

A hybrid watermarking method for DEM authentication and integration is introduced in this paper based on SVD and DCT. The frequency domain transformations are utilized in a manner making the watermark resistant to attacks, as well as preserving DEM quality. The proposed framework was implemented and tested under different type of image processing and geometric attacks and it showed high robustness. For most attacks, the average PSNR value was above 40 dB and the NC value above 0.93. The hidden authentic logo was restored with the key used during the encryption and embedding phase and the extraction process satisfied the security requirements.

REFERENCES

[1] I. I. Vulic *et al.*, "Protection of Digital Elevation Model—One Approach," *Applied Sciences*, vol. 12, no. 19, Jan. 2022, Art. no. 9898, https://doi.org/10.3390/app12199898.

[2] K. L. A. El-Ashmawy, "Vertical Accuracy of Google Earth Data," *Engineering, Technology & Applied Science Research*, vol. 14, no. 3, pp. 13830–13836, Jun. 2024, https://doi.org/10.48084/etasr.7121.

[3] A. M. Ali, "Making Different Topographic Maps with the Surfer Software Package," *Engineering, Technology & Applied Science Research*, vol. 14, no. 1, pp. 12556–12560, Feb. 2024, https://doi.org/10.48084/etasr.6525.

[4] A. Sleit and N. Fetais, "Watermarking: A Review of Software and Hardware Techniques," in *International Conference on Computational Science and Computational Intelligence*, Las Vegas, NV, USA, Dec. 2018, pp. 397–403, https://doi.org/10.1109/CSCI46756.2018.00081.

[5] L. Perez-Freire, P. Comesana, J. R. Troncoso-Pastoriza, and F. Perez-Gonzalez, "Watermarking Security: A Survey," in *Transactions on Data Hiding and Multimedia Security I*, Y. Q. Shi, Ed. New York, NY, USA: Springer, 2006, pp. 41–72.

[6] A. Tareef and A. Al-Ani, "A highly secure oblivious sparse coding-based watermarking system for ownership verification," *Expert Systems with Applications*, vol. 42, no. 4, pp. 2224–2233, Mar. 2015, https://doi.org/10.1016/j.eswa.2014.09.055.

[7] Y. S. Singh, B. P. Devi, and K. M. Singh, "A Review of Different Techniques on Digital Image Watermarking Scheme," *International Journal of Engineering Research*, vol. 2, no. 3, pp. 194–200, 2013.

[8] A. Tareef, A. Al-Ani, H. Nguyen, and Y. Y. Chung, "A novel tamper detection-recovery and watermarking system for medical image authentication and EPR hiding," in *36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, Chicago, IL, USA, Aug. 2014, pp. 5554–5557, https://doi.org/10.1109/EMBC.2014.6944885.

[9] E. B. Tarif, S. Wibowo, S. Wasimi, and A. Tareef, "A hybrid encryption/hiding method for secure transmission of biometric data in multimodal authentication system," *Multimedia Tools and Applications*, vol. 77, no. 2, pp. 2485–2503, Jan. 2018, https://doi.org/10.1007/s11042-016-4280-7.

[10] C. Yang, C. Zhu, Y. Wang, T. Rui, J. Zhu, and K. Ding, "A Robust Watermarking Algorithm for Vector Geographic Data Based on Qim and Matching Detection," *Multimedia Tools and Applications*, vol. 79, no. 41, pp. 30709–30733, Nov. 2020, https://doi.org/10.1007/s11042-020-08916-4.

[11] Q. Zhou, C. Zhu, N. Ren, W. Chen, and W. Gong, "Zero Watermarking Algorithm for Vector Geographic Data Based on the Number of Neighboring Features," *Symmetry*, vol. 13, no. 2, Feb. 2021, Art. no. 208, https://doi.org/10.3390/sym13020208.

[12] X. Xi, Y. Hua, Y. Chen, and Q. Zhu, "Zero-Watermarking for Vector Maps Combining Spatial and Frequency Domain Based on Constrained Delaunay Triangulation Network and Discrete Fourier Transform," *Entropy*, vol. 25, no. 4, Apr. 2023, Art. no. 682, https://doi.org/10.3390/e25040682.

[13] H. H. Le, V. T. Nguyen, H. A. Le, and D. H. Nguyen, "A Robust Integrated Watermarking Algorithm for Vector Geographic Data Copyright Protection." Jul. 13, 2023, https://doi.org/10.20944/preprints202307.0925.v1.

[14] C. Qu, X. Xi, J. Du, and T. Wu, "Robust Watermarking Scheme for Vector Geographic Data Based on the Ratio Invariance of DWT–CSVD Coefficients," *ISPRS International Journal of Geo-Information*, vol. 11, no. 12, Dec. 2022, Art. no. 583, https://doi.org/10.3390/ijgi11120583.

[15] S. Guo, S. Zhu, C. Zhu, N. Ren, W. Tang, and D. Xu, "A robust and lossless commutative encryption and watermarking algorithm for vector geographic data," *Journal of Information Security and Applications*, vol. 75, Jun. 2023, Art. no. 103503, https://doi.org/10.1016/j.jisa.2023.103503.

[16] M. Al-Saad, N. Aburaed, A. Panthakkan, S. A. Mansoori, and H. A. Ahmad, "Protection and Authentication of Dubai Digital Elevation Model using Hybrid Watermarking Technique," in *4th International Conference on Signal Processing and Information Security*, Dubai, United Arab Emirates, Nov. 2021, pp. 13–16, https://doi.org/10.1109/ICSPIS53734.2021.9652422.

[17] F. Amhar *et al.*, "Ownership Protection on Digital Elevation Model (DEM) Using Transform-Based Watermarking," *ISPRS International Journal of Geo-Information*, vol. 11, no. 3, Mar. 2022, Art. no. 200, https://doi.org/10.3390/ijgi11030200.

[18] A. Tareef, "Secure transmission and ownership identification of digital elevation model," *Science International (Lahore)*, vol. 35, no. 3, pp. 379–382, Jun. 2023.

[19] L. Wu, J. Zhang, W. Deng, and D. He, "Arnold Transformation Algorithm and Anti-Arnold Transformation Algorithm," in *First International Conference on Information Science and Engineering*, Nanjing, China, Dec. 2009, pp. 1164–1167, https://doi.org/10.1109/ICISE.2009.347.

[20] "Seamless Digital Elevation Model (DEM) dan Batimetri Nasional." https://tanahair.indonesia.go.id/demnas/.

[21] "Geoportal BIG." https://geoportal.big.go.id/#/.

[22] S. A. Kasmani and A. Naghsh-Nilchi, "A New Robust Digital Image Watermarking Technique Based on Joint DWT-DCT Transformation,"

in *Third International Conference on Convergence and Hybrid Information Technology*, Busan, Korea (South), Nov. 2008, vol. 2, pp. 539–544, https://doi.org/10.1109/ICCIT.2008.139.

[23] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: from error visibility to structural similarity," *IEEE Transactions on Image Processing*, vol. 13, no. 4, pp. 600–612, Apr. 2004, https://doi.org/10.1109/TIP.2003.819861.

AUTHORS PROFILE

Afaf Tareef received a B.Sc. degree in computer science from Mutah University, Jordan in 2008, an M.Phil. degree from the University of Jordan in 2010, and a Ph.D. degree from the University of Sydney, Australia in 2017. She is currently an Associate Professor in the Faculty of Information Technology at Mutah University, Jordan. She has many publications in several international conferences and journals. Her research interests include image processing and medical image analysis.

Khawla Al-Tarawneh received a B.Sc. degree in computer science from Mutah University, Jordan in 2015, an MSc degree from Mutah University in 2018, and has been a Ph.D. student at the University of Jordan from 2022 to present. She has been an Assistant Lecturer at Mutah University, Jordan from 2015 to present.

Azzam Sleit is a Former Minister of Information and Communications Technology (2013–2015). He is currently working as a Professor of Computer Science, King Abdulla II School for Information Technology, University of Jordan, where he functioned as the Dean (2015–2016) and the Assistant President/Director of the Computer Center (2007–2009). Dr. Sleit holds B.Sc, M.Sc. and Ph.D. in Computer Science. He received his Ph.D. in 1995 from Wayne State University, Michigan. He was the Chief Information Officer at Hamad Medical/Ministry of Public Health, Qatar. Before joining Hamad Medical, Dr. Sleit was the Vice President of Strategic Group and Director of Professional Services of Triada, USA, where he introduced the NGram Technology and Associative Memory Structures. He authored more than one hundred refereed research papers related to Cloud Computing, Imaging Databases, Data Mining, Health and Management Information Systems and Software Engineering, published in reputable journals and conferences.