Biometric Data Securement Using Visual Information Encryption

Sawsan D. Mahmood[1], Hadeel M Saleh[2], Asraa Y. Youssef [3], Lara Ahmad Ghasab Almashagba[4*], Fathiya Al Abri [5]

[1]College of Engineering, University of Diyala, Baqubah, Iraq

[2]Continuous education center, University of Anbar, Ramadi, Iraq

[3]Department of Soil Sciences and Water Resources, College of Agriculture, University of Diyala, Baqubah, Iraq

[4]School of Computer Sciences Universiti Sains Malaysia (USM) Penang, Malaysia

[5]Department of General Foundation programme, Al Zahra College for women, Muscat , Sultanate of Oman

Email: pcomp.sawsan.dheyaa@uodiyala.edu.iq; haddeel.mohammed@uoanbar.edu.iq; asraaalsady@uodiyala.edu.iq; laramashagba@student.usm.my; abrifathiya@gmail.com

Abstract

Biometric data is becoming increasingly valuable because of its uniqueness, and digital watermarking techniques are used to protect it. This paper presents a new method of hiding Palmprint images using wavelet decomposition and Encrypting Visual Information (EVI). EVI is a technique for securing Palmprint print images that has been extensively studied in this report. By embedding the Palmprint image in the cover image, and then using wavelet transformation, this output image can be decomposed into four segments (Segment $_{\text{Low Low}}$, Segment $_{\text{Low High}}$, Segment $_{\text{High Low}}$, and Segment $_{\text{High High}}$). A compressor is placed at the sender site to compress these four segments. DWT is obtained at the receiver side and then the bit-matching procedure is applied to obtain the original palmprint image. Using data concealing and EVI implementations on biometrics, palmprints, and related textual information can be protected from identity fraud. The watermarked cover images and palmprints, which could be used for authentication, have been improved from the existing approach. By reducing the segment size, quality is achieved along with higher security and bandwidth reduction. In addition, the three least significant bits are successfully applied to increase the length of a secret message while retaining palmprint quality.

Keywords: Encrypting Visual Information; Digital watermarking; Palmprint Image (MedImg)

1. Introduction

Based on physiological or behavioral characteristics, biometrics can identify or verify a person's identity. A biometric system is easier to use and more consistent than a traditional one. There are several biometric features that are commonly used: Face, Iris, Tongue, Fingerprint, Ear, Palmprint, Voice, posture, gait, and palmprint, hand geometry, etc [1]. A lifetime comparison of the palmprint with other biometric characteristics shows that it is the most stable and therefore the most reliable. Human palmprints are normally most noticeable by their vibrant texture [2].

There are still a number of issues to be resolved, especially in terms of the security of biometric systems and biometric data [3]. Considering that biometric templates are stored in databases, they may be altered by attackers because of security threats. The resource will not be accessible if the biometric template is altered [4]. Therefore, cryptography, stenography, and watermarking have all been used to protect biometric data [5]. EVI is one of the techniques among them. By providing the secret image as a share, EVI provides an independent method of sharing that does not divulge any information about the secret image. Such security needs are met by EVI, which provides an additional level of authentication [6]. The main contributions of this study are:

DOI: https://doi.org/10.54216/JCIM.160108
Received: October 30, 2024 Revised: January 23, 2025 Accepted: February 13, 2025

- The research presents EVI as an optimal palmprint image protection technique, which defends against identity theft and unapproved access attempts.
- DWT standards are used by the proposed approach to insert palmprint images into cover images before performing multi-stage decomposition, which improves security standards, preserves quality, and reduces bandwidth usage.
- The method enhances the ability to embed secret messages through use of three LSBs, which preserves both authentication-quality palmprint images.

The research follows a nine-section structure. Section 2 conducts an extensive literature evaluation, which explores previous work about biometric data protection and digital watermarking methods. The fundamental part of this section describes Discrete Wavelet Transform (DWT) together with its adoption within the proposed solution framework. The EVI technique serves as the method for protecting palmprint images through Section 4. The section defines a replacement algorithm that boosts data concealment performance. The methodological framework with implementation procedures forms Section 6 of the report. Section 7 explains implementation steps that show how the proposed system executes its functions. The results together with the analysis appear in Section 8 to evaluate experimentally the effectiveness of this approach. The study ends in Section 9 with an overview of important discoveries and proposals for upcoming research possibilities.

2. Related work

According to Anand et al. [4] DWT–SVD domain, watermarking provides improved security for medical records. Watermark noise is reduced by using the Hamming code. Chaotic-LZW (Lempel–Ziv–Welch) was considered the best encryption and compression scheme after testing two encryption and three compression schemes. Based on the concept of blind watermarking, Kahlessenane et al. [7] developed a robust method for incorporating EPR into computerized tomography scans. To select the subband of the wavelet transform, the Zigzag scanning method is used. Because of their research, they demonstrate that the method is effective against geometric and destructive attacks. In a paper [8], Fares et al. proposed a DCT-Schur and DWT-Schur combination-watermarking scheme. A robustness to conventional attacks is provided by their method results. According to Yuan et al. [9], DCT can be used as a tool for spatial image watermarking. Based on Lagrangian support vector regression (LSVR) and Lagrangian wavelet transform (LWT), a watermarking algorithm has been developed using the advantages of fast implementation, faster learning speed, and high generation capacity.

Using non-subsampled contourlet transforms, redundant discrete wavelet transforms, and SVD decomposition, Sing et al. [10] developed a semi-blind grayscale-watermarking scheme. The authors of Amit et al. [11] presented a study that used selective DWTs as watermarking systems that are spread spectrum-dependent. Amit et al. [12] presented a DWT, DCT, and SVD decomposition scheme. According to Amit et al. [13], DWT, DCT, and SVD decomposition techniques are combined into a hybrid multilevel watermarking scheme. DWT, DCT, and SVD methods were used in a paper presented by Chandan et al. [14]. An Arnold transform and set partitioning are used to enhance security. Based on homomorphic transform, RDWT, and SVD decompositions, Priyank et al. [15] proposed a watermarking scheme. Using principal components, watermarks are inserted into compressed images to protect against attacks where the region of interest (ROI) of the compressed image is hidden. In contrast to a watermark generated with a compressed image ROI, the ROI generated with a compressed image watermark is 100% reversible. It is proposed to watermark medical images in a way that is imperceptible and has zero affecting [16]. In this zero watermarking process, the imperceptible watermark detector retaliates against the imperceptible watermarking data in order to authenticate patient identity. In addition to embedding security, Kannammal et al. [17] developed an encryption algorithm using RSA and other algorithms based on 2-level security. Sharma et al. [18] developed a binary watermark embedding method based on digital multitoning [19].

The efficiency of LL is considered when selecting it. Once again, the LL subband is decomposed using DWT, and then the palmprint watermark is embedded in it. By combining these two elements, imperceptibility and robustness are improved. LWT coefficient magnitudes are used to satisfy imperceptibility requirements, while DWT coefficients are applied to improve robustness. Secret keys are used to embed the watermark into the coefficients of DWT.

3. Discrete wavelet transform (DWT)

DWT divides an image or signal into four subbands: S_{LL}, a lower resolution module, and S_{HL}, S_{LH}, and S_{HH}, both spatially oriented modules [16]. There is a great deal of consistency between the characteristics of DWT images' multi-resolution breakdown as well as the features of the images when it comes to selecting the spatial orientation [20]. A low-pass and high-pass resolver (Lo_D, Hi_D) will be used to apply filters to the DWT along rows and columns. A mathematical breakdown of the first level of the host signal S (a, b) is given in Equation (1). Figure 1 gives a representation of the decomposition of a signal into subbands and the decomposition of a sample X-ray image into one level [8].

DOI: https://doi.org/10.54216/JCIM.160108
Received: October 30, 2024 Revised: January 23, 2025 Accepted: February 13, 2025

$$LL(x,y) = K(m,n), \Psi^0\ (m - 2x, n - 2\,y)$$
$$LH(x,y) = K(m,n), \Psi^1\ (m - 2x, n - 2\,y)$$
$$HL(x,y) = K(m,n), \Psi^2\ (m - 2x, n - 2\,y)$$
$$HH(x,y) = K(m,n), \Psi^3\ (m - 2x, n - 2\,y) \quad (1)$$

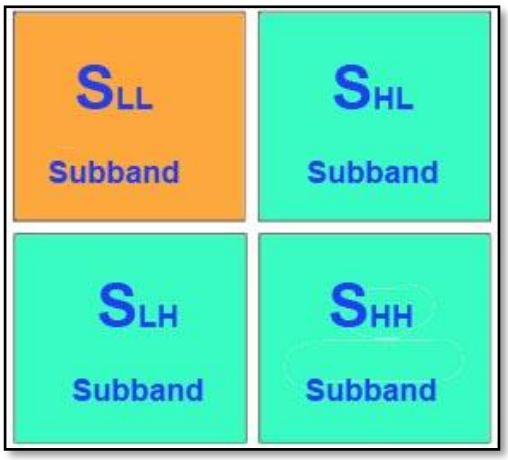


Figure 1. DWT Decomposed at the 1st level

4. Encrypting Visual Information (EVI)

A visual cryptography method called EVI uses simple mathematical algorithms to decrypt images without needing complex mathematical analysis. By using this method, the secret image is encoded into n random noise images known as sheets, such that decryption is only possible if k or more sheets are available and combined with a logical operator [21]. Combining less than sheets does not reveal the secret image. Data stored in a central database using raw digital biometrics has been protected using EVI. When both components of an input biometric image (or template) are simultaneously available, it is possible to recover the original data; when individual components are not easily matched to the original input data, the original input data is de-identified (obscured)[22][23].

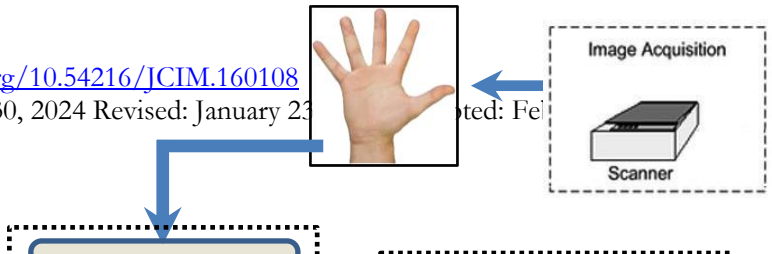
Verheul and Tilburg [17] introduced the concept of EVI to color images. The disadvantage was that the resulting image was of poor quality, making sharing impossible. A number of others were inspired by this work to create more advanced schemes ([4], [6], [15]). This work uses a technique wherein a colored image is hidden behind multiple meaningful cover images.

5. An Algorithm for Replacing Bits

As far as spatial data concealing is concerned, the best-known method is known as LSB (Least Significant Bit), where the least significant bits are replaced to hide the information [24]. In SLSB (Selected Least Significant Bit), a single color is chosen for each pixel of the cover image in order to hide the message. As a result, LSB hiding information performs better than it does in LSB hiding information. Two LSBs of the green pixels are used to store the secret message by the algorithm. Three planes make up a color image. For embedding, green planes are chosen because they appear dark in HSV, and red planes appear bright [16].

6. The Methodology

A legal patent can be authenticated by comparing it to those on file in a database of authorized users' information on a local operating system or a server used for authentication. Data, images, or whatever entities are authenticated to verify their real identity. The reason for this is primarily to make sure the message comes from the real user. Authentication is required as part of secure communication for security reasons. It serves as an authentication tool to provide the receiver with the data-hiding key. Images are embedded and encrypted in this scheme to provide authentication. Stegoimage remains the same size after embedding to avoid hackers recognizing it as an original image. This section presents the proposed methodology for implementing the proposed system. Moreover, it presents and analyzes the results of modules 1 and 2, module 3. Based on these results, it can be concluded that the DWT HAAR Filter is capable of providing good results and can be used as an embedding biometric.



DOI: https://doi.org/10.54216/JCIM.160108
Received: October 30, 2024 Revised: January 23 ted: Fe

Figure 2. Methodology of the Proposed System

The following steps describes the proposed method stages:

The 1st Part: The palmprint and cover image reading and secret message representation.

The purpose of this part is to display a cover and biometric image read from the cover. Pi, j corresponds to an integer in the range (0,255). The RGB scheme uses Ri, j, Gi, j and Bi, j as integers.

The 2nd Part: Analysis the Palmprint

A feature extraction process is performed on the palmprint image. A grayscale image of the palmprint is first created by converting it from RGB to grayscale. Palmprint shape can be created using Morphological Structuring. Using the previous 0 (black) and 1 (white) pixels as inputs, dilate the image to get pixels from the previous 0 (black). Next, pupils are detected.

The 3rdPart: DWT Transform implementation

Wavelet transforms reduce the number of pixels needed to represent a palmprint image. Four subbands have been formed from the palmprint image using wavelet transform, namely HH, HL, LH, and LL. The most information is found in HH, so it should be chosen. In terms of parameters such as the number of pixels needed to represent the HH subband, it has been compared to a grayscale palmprint image. Various filters will be used to decompose the palmprint image to embed in the cover for security, such as HAAR, Daubechies Orthogonal, and Biorthogonal filters. Comparison of Grayscale palmprint image with wavelet-decomposed palmprint is performed for performance evaluation.

Two parameters will be compared for this comparison [25].

1. Pixels number

DOI: https://doi.org/10.54216/JCIM.160108
Received: October 30, 2024 Revised: January 23, 2025 Accepted: February 13, 2025

2. PSNR (Peak Signal-to-Noise Ratio).

The 4th Part: Performing a Bit of Replacement

Each cover pixel contains two bits. Steganographic images are generated using MSBs, LSBs, and bit replacement processes. In this step, biometrics are embedded in these steganographic images by applying DWT transform and compressing them using JPEG compression. The decomposed DWT transform image is then applied to the watermark image and analyzed for its four bands. Once sent, it is received by the recipient.

The 5th Part: Results

A merger of all shares is conducted at the receiver side using IDWT. Implementing decompression. A de-watermarked version of this image is then used to create an image of the palmprint. Before and after compression of the cover image, the results are projected using MSE and PSNR. For various transforms such as DCT and Fast Walsh Hadamard Transform, a comparison is also made between the cover image after and before watermarking.

7. The Implementation

***Step One*. Authentication:**

Data, images, or whatever entities are authenticated to confirm their identities. For the most part, it ensures the message came from a real user. A secure communication system requires both transmitters and receivers to authenticate for security reasons. Receivers as authentication tools use data-hiding keys.

***Step Two*. Embedding**

There are two instances of some structure embedded within each other. An image of the cover and a secret image are captured here. Through a single bit least significant watermark insertion algorithm, the secret image will be hidden behind the cover image and a stego image will be generated. Their respective extensions are used to save both files.

***Step Three*. Generate shares.**

In this case, the stego image will be split into two parts. There will be a share of the same size and a blur share.

***Step Four*. Encryption**

A message or piece of information that is encrypted in a way that only authorized parties can access it. A simple image is encrypted using an encryption algorithm using an encryption scheme, creating an encrypted image that can only be decrypted to reveal the intended information. We will use the Permutation encryption algorithm to encode both generated shares. A receiver will then receive the shares. Encrypting data ensures that only authorized people can read it (for example, those authorized to view images, text messages, or files).

***Step Five*. Decryption**

When data is decrypted, it returns to its unencrypted state after having been made unreadable by encryption. By decrypting the data, the system extracts it from its garbled form into text and images that can be read by the reader and understood by the system as well. A series of keys or passwords may be used for decryption, either manually or automatically. Permutation decryption will be used on the receiver's side to receive and decrypt both encrypted shares.

***Step Six*. Putting a Stamp on Shares**

Images, text, or any data can be pressed onto a surface to create a stamp. The steno image will be recovered after both shares have been decrypted.

***Step Seven*. De-embedding (Embedding Removal)**

A de-embedding process removes the influence. A hidden image is subtracted or eliminated here from behind another image. It is designed to embed a watermark into the stem image using a least significant bit algorithm and to separate the signature and cover images.

Stego image Generation Algorithm

Initiate

Stage One: Create a secret image and a cover image.

Stage Two: Create a loop for embedding

a. Extract a pixel from a secret image

DOI: https://doi.org/10.54216/JCIM.160108
Received: October 30, 2024 Revised: January 23, 2025 Accepted: February 13, 2025

b. Produce an 8-bit binary representation of pixel

c . 1-LSB is extracted from the green plane of the cover image and 1-LSB is extracted from the secret image. Both images must be added together to complete the process

Stage Three: Generating Stego image.

Process Ending

8. Results and Discussion

Among various transforms like Hadamard, DCT, and DWT with Haar filter, we have concluded that the one with the lowest number of pixels provides the best average PSNR. Data concealing and watermarking are implemented after evaluating this result with various variations in parameters like DWT levels, palmprint resizing, and compression. Table 1, show the proposed technique with Biorthogonal Filter (PSNR), Daubechies Orthogonal Filter (PSNR), and HAAR Filter (PSNR).

Table 1: The proposed technique with Biorthogonal Filter (PSNR), Daubechies Orthogonal Filter (PSNR), and HAAR Filter (PSNR)

Dataset Sample		DWT					
		HAAR Filter (PSNR)		Daubechies Orthogonal Filter (PSNR)		Biorthogonal Filter (PSNR)	
		Palmprint Image	Cover Image	Palmprint Image	Cover Image	Palmprint Image	Cover Image
Phoenix Dataset	Palmprint_Image #1	31.0676	0.4137	0.4895	27.1181	0.3558	31.3732
	Palmprint_Image #2	31.0887	0.4455	0.3708	27.4355	0.5181	30.9077
	Palmprint_Image #3	31.0787	0.5089	0.3532	27.1296	0.3558	31.5975
	Palmprint_Image #4	30.0887	0.5059	0.3558	27.6651	0.3553	31.0364
	Palmprint_Image #5	31.0676	0.5084	0.3455	27.7306	0.3532	30.6866
	Palmprint_Image #6	31.0887	0.4455	0.3708	27.4355	0.5181	30.9077
	Palmprint_Image #7	31.0787	0.5089	0.3532	27.1296	0.3558	31.5975
	Palmprint_Image #8	30.0887	0.5059	0.3558	27.6651	0.3553	31.0364

When the decomposition level is increased to the second level, the palmprint image quality improves, but not the cover image quality. Using two levels of decomposition and resizing of the palmprint image, Table 2, shows the results obtained with the palmprint and cover image compression parameter removed.

Table 2: The 2nd Level Decomposition of HAAR Filter

DOI: https://doi.org/10.54216/JCIM.160108
Received: October 30, 2024 Revised: January 23, 2025 Accepted: February 13, 2025

Sample Databases		DWT	
		HAAR Filter (PSNR-2nd Level Decomposition)	
		Palmprint Image	Cover Image
Phoenix	Palmprint_Image #1	0.58271	40.87091
	Palmprint_Image #2	0.58361	40.49371
Phoenix	Palmprint_Image #3	0.58351	40.19371
	Palmprint_Image #4	0.58350	40.09371

Table 3: The PSNR of the Proposed Methodology

Sample Databases		PSNR	
		Palmprint Image	Cover Image
Phoenix	Palmprint_Image #1	32.15971	39.9802
	Palmprint_Image #2	31.54091	39.6028
Phoenix	Palmprint_Image #3	33.04251	39.3028
	Palmprint_Image #4	31.73961	39.2028

This method is discarded due to its bandwidth requirements, since quality requires less bandwidth. The best method, based on all results obtained, is to use two levels of DWT, resize but without compression of the final image in order to obtain best quality of palmprint and cover images. As part of the proposed work, two least significant bits are used as replacements for selected least significant bits. This method produces the same results as Stegnography when three least significant bits are used. Table 5.6 shows the results.

9. Conclusion

EVI is used to secure the biometric image embedded in the cover image. Using wavelet decomposition and sharing the subbands is an original feature of the scheme. A Stegnography method is implemented for embedding secret messages inside cover images based on Three Least Significant Bits (TLSB) instead of SLSB (Two Least Significant Bits). Using various wavelet transform filters, various images of different sizes can be obtained using the work that has been accomplished. The HAAR transform further reduces the number of pixels while maintaining quality of the image in comparison to the original palmprint image. In order to achieve the results, various parameters like compression, decomposition levels and palmprint size enhancements are considered along with SLSB techniques enhancements. With Two Levels of Wavelet Decomposition of palmprint with resize without compression of final watermarked image, best results could be obtained with high quality palmprint and cover image with a reduced bandwidth requirement. Additionally, Three Least Significant Bits replacement for Stegnography is successfully implemented, thereby allowing the size of secret messages to be embedded to be increased while maintaining palmprint's quality.

Reference

[1] S. M. Mohammed and O. Ali, "Human biometric identification: Application and evaluation," *IJECS*, vol. 6, no. 2, pp. 131-152, 2024.

[2] N. Obeid, "On the product and ratio of Pareto and Erlang random variables," *Int. J. Math. Stat. Comput. Sci.*, vol. 1, pp. 33-47, 2023, doi: 10.59543/ijmscs.v1i.7737.

[3] S. D. Mahmood, F. Drira, H. F. Mahdi, Y. Aribi, and A. M. Alimi, "Chaotic model-based blind watermarking with LSB technique for digital fundus image authentication," in *Proc. 2023 Int. Conf. Cyberworlds (CW)*, 2023, pp. 395-402, IEEE.

DOI: https://doi.org/10.54216/JCIM.160108
Received: October 30, 2024 Revised: January 23, 2025 Accepted: February 13, 2025

[4] A. Anand and A. K. Singh, "An improved DWT–SVD domain watermarking for medical information security," *Comput. Commun.*, vol. 152, pp. 72-80, 2020.

[5] S. D. Mahmood, Y. Aribi, F. Drira, and A. M. Alimi, "Secure blind medical image watermarking using hybrid feature extraction techniques," *Iraqi J. Comput. Sci. Math.*, vol. 5, no. 4, pp. 15, 2024.

[6] H. J. Hadi, Y. Cao, K. U. Nisa, A. M. Jamil, and Q. Ni, "A comprehensive survey on security, privacy issues and emerging defense technologies for UAVs," *J. Netw. Comput. Appl.*, vol. 213, p. 103607, 2023.

[7] F. Kahlessenane, A. Khaldi, R. Kafi, and S. Euschi, "A DWT-based watermarking approach for medical image protection," *J. Ambient Intell. Humaniz. Comput*, vol. 12, no. 2, pp. 2931–2938, 2021.

[8] K. Fares, A. Khaldi, R. Redouane, and E. Salah, "DCT&DWT based watermarking scheme for medical information security," *Biomed. Signal Process. Control*, vol. 66, p. 102403, 2021.

[9] Z. Yuan, Q. S. Liu, D. Zhang, and T. Yao, "Fast and robust image watermarking method in the spatial domain," *IET Image Process.*, vol. 14, no. 15, pp. 3829–3838, 2020.

[10] S. Singh, V. S. Rathore, R. Singh, and M. K. Singh, "Hybrid semi-blind image watermarking in redundant wavelet domain," *Multimed. Tools Appl.*, vol. 76, no. 18, pp. 19113–19137, 2017.

[11] A. K. Singh, B. Kumar, M. Dave, and A. Mohan, "Multiple watermarking on medical images using selective discrete wavelet transform coefficients," *J. Med. Imaging Health Inform.*, vol. 5, no. 3, pp. 607–614, 2015.

[12] A. K. Singh, M. Dave, and A. Mohan, "Hybrid technique for robust and imperceptible multiple watermarking using medical images," *Multimed. Tools Appl.*, vol. 75, no. 14, pp. 8381–8401, 2016.

[13] A. K. Singh, "Improved hybrid algorithm for robust and imperceptible multiple watermarking using digital images," *Multimed. Tools Appl.*, vol. 76, no. 6, pp. 8881–8900, 2017.

[14] C. Kumar, A. K. Singh, and P. Kumar, "Improved wavelet-based image watermarking through SPIHT," *Multimed. Tools Appl.*, vol. 79, no. 15, pp. 11069–11082, 2020.

[15] P. Khare and V. K. Srivastava, "A secured and robust medical image watermarking approach for protecting integrity of medical images," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 2, p. e3918, 2021.

[16] M. Cedillo-Hernandez, A. Cedillo-Hernandez, M. Nakano-Miyatake, and H. Perez-Meana, "Improving the management of medical imaging by using robust and secure dual watermarking," *Biomed. Signal Process. Control*, vol. 56, p. 101695, 2020.

[17] A. Kannammal and S. Subha Rani, "Two-level security for medical images using watermarking/encryption algorithms," *Int. J. Imaging Syst. Technol.*, vol. 24, no. 1, pp. 111–120, 2014.

[18] R. Mehta, N. Rajpal, and V. P. Vishwakarma, "A robust and efficient image watermarking scheme based on Lagrangian SVR and lifting wavelet transform," *Int. J. Mach. Learn. Cybern.*, vol. 82, pp. 379–395, 2017.

[19] S. Sharma, J. J. Zou, and G. Fang, "Significant difference-based watermarking in multitoned images," *Electron. Lett*, vol. 56, no. 18, pp. 923–926, 2020.

[20] B. Yang, Z. Zhang, and J. Ma, "Wavelet-based normalized flow for anomaly detection in photovoltaic electroluminescent with non-stationary textures," *IEEE Sensors J.*, 2024, doi: 10.1109/JSEN.2024.3134567.

[21] K. M. Hosny and M. M. Darwish, "Invariant image watermarking using accurate polar harmonic transforms," *Comput. Electr. Eng.*, vol. 62, pp. 429–447, 2017.

[22] K. M. Hosny and M. M. Darwish, "Robust color image watermarking using invariant quaternion Legendre–Fourier moments," *Multimed. Tools Appl.*, vol. 77, no. 19, pp. 24727–24750, 2018.

[23] K. M. Hosny, M. M. Darwish, "New geometrically invariant multiple zero-watermarking algorithm for color medical images," *Biomed. Signal Process. Control*, vol. 70, p. 103007, 2021.

[24] K. M. Hosny, M. M. Darwish, K. Li, and A. Salah, "Parallel multi-core CPU and GPU for fast and robust medical image watermarking," *IEEE Access*, vol. 6, pp. 77212–77225, 2018.

[25] F. H. Al-Rubbiay, A. Y. Youssef, and S. D. Mahmood, "Medical image authentication and restoration based on mCloud computing: Towards reliant medical digitization era," in *Doctoral Symp. Comput. Intell.*, Singapore: Springer Nature, 2023, pp. 487-500.

DOI: https://doi.org/10.54216/JCIM.160108
Received: October 30, 2024 Revised: January 23, 2025 Accepted: February 13, 2025