CORRECTED VERSION: A System of Human Biometric-Fusion Authentication Security Improvement Using Hybrid Technique

Salwa Mohammed Nejrs[1], Azmi Shawkat Abdulbaqi[2,*]
[1]University of Mustansiriya, College of Art, Baghdad, Iraq
[2]Renewable Energy Research Center, University of Anbar, Ramadi, Iraq
Emails: qsalwaaa@uomustansiriyah.edu.iq; azmi_msc@uoanbar.edu.iq

Abstract

The collected information from the environment in WSN continuously sends from one node to another until it reaches the main collector or server, where processing is done. The transferred data volume will be greater when the network grows. Medical images will also contribute to network traffic. To alleviate this challenge, this research has developed an interlayer transmission protocol for WSNs. This protocol uses the construction of medical images with pixel-based data. In the analysis, a gray-scale medical image 512x512 in size, provided by Brain, is utilized. The image was compressed by the protocol from 256 KB to 192 KB with a percentage of 25%. As a result, the structural similarity index measure showed the SSIM at 51.1365, while the PSNR is at 0.9976; therefore, the quality of the medical image remains unchanged. The protocol uses the AES encryption method for strong data protection to improve security during transmission. Results show that this protocol reduces data transmission in WSNs by 12.5 to 25% without affecting the integrity of the medical image, which is indicative of the efficiency of the protocol in enhancing network performance while ensuring data safety.

Keywords: Cover Image (Cov_Img) Discrete Cosine Transformation (DCT); Practical Linear Algebra Technique (PLAT); Normalized Cross-Correlation (NCC) Discrete Wavelet Transformation (DWT)

1. Introduction

Along with conventional physical and knowledge-based identification techniques, biometric technology will be quite important in future society. Biometric verification is the automated verification of one's identity utilizing their physiological and/or traits of behavioral [1]. Typical biometric examples technologies including hand shape measurements, iris scanning, fingerprint analysis, facial recognition, and voice validation. Token and knowledge-based identification methods have many drawbacks, such as the possibility of losing items like identification cards or stealing them, or even forgetting passwords or PINs [2]. On the contrary, biometrics ensures that only authorized persons can access services and information, which significantly reduces fraud and costs related to its counteraction. One of the most critical strengths of biometric technology is its dependency on unique, immutable biometric traits. Compared to other personal identification methods, biometrics has some very definite advantages [3]. Nevertheless, biometric data are not secure in themselves and have to be protected from a number of threats. The protection of biometric templates, both when stored and in transmission is one way of protecting individual privacy through encryption [4]. Encryption alone cannot guarantee the security that users expect. Although encryption is an important part of information security, its strength and proper use will determine whether it is effective. Weak encryption or the absence of encryption during data transmission, especially after decryption, exposes information. Using digital watermarking, users can embed recognizable information in an image, called a "watermark," without altering the image's visual content, according to the Digital Watermarking Group, 2009 [5]. This method can hide the biometric data like fingerprints by embedding it directly in the spatial domain or by transforming it into an image in the frequency domain. Sometimes, watermarking considers a hybrid approach in which both spatial and frequency domains are utilized together to give more robustness and security. These developments have contributed a great deal to the development of multi-modal biometric authentication systems. The most common multi-modal systems, using face and fingerprints as their base biometric modality, have better recognition performance compared to unimodal biometric systems [6]. A robust watermarking technique can

DOI: https://doi.org/10.54216/FPA.180106
Received: June 24, 2024 Revised: September 22, 2024 Accepted: December 25, 2024 Corrected: December 11, 2025

enhance the security and efficiency of multimodal biometric authentication systems. This study introduces a new hybrid biometric authentication system integrating cutting-edge encryption and watermarking techniques to enhance biometric-fusion authentication security and effectiveness. The findings of this study are reported as follows:

1. *Multimodal hybrid biometrics:*

Developed is a dynamic watermarking method that straight inserts distinctive identifiers—such as encrypted biometric features—into the multi-modal biometric images. The outcome of this could also guarantee traceability and integrity against unauthorized access or manipulation of the biometric data.

2. *Dynamic watermarking's data integration:*

A dynamic watermarking technique has been created to intrinsically introduce uniqueness into multimodal biometric photographs by embedding unique identifiers encrypted via biometric features, for example. This safeguards biometric data and assures traceability and integrity in case of unlawful access or interference..

3. *Security of Template Utilizing advanced encrypting:*

To protect the storage and transmission of biometric templates, the research suggests an optimized encryption framework, such as the blending of AES and ECC. This two-tier encryption guarantees the confidentiality and security of user data.

4. *Assessing resilience to assaults and performance:*

Many investigations have been conducted to verify the system's capacity to withstand frequent security threats including template reversal, spoofing, and brute force attacks. With little decrease in image quality, the hybrid approach maintains excellent identification accuracy.

5. *Feasibility and Scalability in Real-Time:*

The proposed system will be able to handle large-scale authentication scenarios efficiently and hence is suitable for real-time applications in high-security environments such as banking, healthcare, and border control.

2. Literature Review

Authors in [7] have developed an effective 2D Gabor filter for palm recognition. Using the Gabor function on hand images, Gabor features are computed as Hamming codes at the pixel level. Authors in[8] utilized SMCC for enhanced feature extraction, by focusing on Gabor second derivatives at different scales and orientations. Gabor-based systems are less effective when hand images are displaced and rotated [9]. Even though Gabor is resistant to brightness and contrast, altering image brightness can still affect system accuracy negatively. Authors in [10] proposed a method of directional image displacement to address this issue. Hamming distances were determined individually for every case and the smallest was chosen. Kong's method had the issue of only considering displacement within a restricted range, as well as the added workload of more calculations. Other authors utilized Gabor function to categorize palm texture with turn invariant features [11]. The texture features of an image were determined by applying a filter and calculating its mean and variance. This method utilizes a circular shift of the feature components to achieve rotational invariance in all images. The technique is limited to regular images and cannot be utilized on irregular hand images. With the help of WEF, Wu and colleagues could differentiate between different palm textures [12]. Wavelet transform (WT) was utilized to divide the palm into various scales, and local energy coefficients of the WT were assessed across various directions and scales to determine the WEF value. Different wavelet functions were examined at different scales. In addition to wavelet function type and composition stage, authentication accuracy varied significantly. Authors in [13] utilized modified haar energy (MHE) to recognize palm trees. The modified haar transform was utilized to normalize MHE values. Using MHE values calculated at various levels combined with accuracy coefficients, they calculated the characteristic vector.

WT-dependent techniques are negatively impacted by variations in displacement, rotation, and brightness. Researcher in[14] propose a statistical approach to detect palm textures unaffected by rotation. Principal line coefficients were determined by directional context modeling using wavelet amplitudes. The context value was calculated using its neighboring coefficients. Our analysis utilized directional context values to determine the center of mass, density, distance propagation, and energy of the palm. Finger wrinkles can be utilized to authenticate. Genes control this region’s line patterns before birth. In [15], authors was developed a biometric authentication method using the inner surface of the fingers. Using a CCD digital camera, 1423 images were taken of 73 individuals. According to the study, the image resolution was 1792 x 1200, but after pre-processing, it dropped to under 70 dpi. Furthermore, only the middle finger was utilized for authentication [16]. A feature extraction method uses spatial and line characteristics, such as the finger's length in the first method and the middle phalanx in the second method. Phalanx line thresholds and morphological operators were extracted using a specific mask. A local binary pattern (LBP) was utilized by [17] to resolve the displacement issue. Consideration of the

DOI: https://doi.org/10.54216/FPA.180106
Received: June 24, 2024 Revised: September 22, 2024 Accepted: December 25, 2024 Corrected: December 11, 2025

finger characteristics improved the neighbors of the LBP operator. The prominent lines on the fingers run vertically, so 8 adjacent pixels around the center pixel are chosen in a horizontal orientation. Compared to the original LBP operator, the new method detects horizontal displacement more effectively because it has 8 circular pixels surrounding the central pixel. Individual identification was achieved using both palms and faces in a biometric system developed by [18]. Feature extraction from palm and face images was performed using the Gabor-Wigner transform (GWT). An image of a biometric is analyzed simultaneously in terms of both its spatial and frequency components. Particle Stream Optimization (PSO) was utilized to select the prominent characteristics. In terms of precision, multimodal systems perform better than unimodal systems.

The PerRam biometric system was created using hand and finger images. The back lines of each finger were initially removed. Differential features were extracted using Scale Invariant Feature Transform (SIFT) and Speeded-Up Robust Features (SURF). When keypoints are analyzed in an image, SIFT patterns can be seen. SURF feature vectors are also derived using local patterns surrounding key points. Moreover, the EMD determines what the frequency range of every image is. It is a biometric system developed by Anitha and Rao that uses the internal surface characteristics of the middle, ring, and index fingers. Distance between specific points can be used to evaluate hand geometry using the LBP algorithm, whereas finger quality can be assessed using the LBP algorithm. The multimodal system Arulalan and his team suggested should use iris and middle finger images. Researchers in [19] merged their veins to prove the authenticity of the hand and palm. Wavelet coefficients were used for iris analysis while line-based features were used for middle finger analysis. Besides palm images, research was also done on the backside of the hand. Sizes of the masks were compared with those of conventional edge detectors like Sobel. In [20], fingerprints, palm prints, and facial images were used to verify identities. One-mode palm images were found to be more effective than both other techniques in this study. The acceptance rate increases to 92% if all biometric techniques are combined, a 10% increase over relying on only one biometric. Watermarking of the palm and retina improves the accuracy and security of biometric systems. An enhanced level of security and authenticity can be achieved by watermarking biometric information (like fingerprints, facial recognition, or iris patterns). The following is a brief overview:

Biometric watermarking embeds the biometric data into the digital content to create a unique identifier for it. This allows identification on the part of the user or owner of such information.

Its primary objectives include user authentication, data integrity, and intellectual property protection. Tracking digital content helps to stop unauthorized access [21].

Process:

Extracting: From a user's biometric sample, biometric characteristics are extracted.
Embedding: Employing several algorithms, the watermark is incorporated into digital content to guarantee it is undetectable to people.
Detecting: Watermarks can be extracted and examined to confirm ownership or identity.

Applications:

- Safeguarding of copyrighted content via digital rights management (DRM).
- Authentication of IDs is necessary for a secure transaction.
- Examining digital content for forensic reasons: Following and finding the source [21] [22].

Advantages:

- More security and privacy.
- Original material cannot be changed or deleted without losing its quality.
- The technique offers a strong approach to establish ownership confirmation [23].

Challenges:

- Extraction of biometric information has to be precise.
- Balancing the strength of the watermark with the quality of the original material.
- Concerns about privacy arise from the storage and use of biometric data.
- Biometric watermarking can improve digital authenticity and security [22][23].

Integrating several types of biometric authentication to verify people, multimodal biometrics improves account security by combining strong identification verification techniques. This approach can include a range of biometric characteristics to boost security measures, such as voice recognition and facial authentication inside a mobile application to improve customer experience.[14]. To successfully deploy biometric authentication features, companies are advised to work with a reputable vendor providing enterprise-grade security and scalability solutions. Customers should thereafter be asked to register their biometric data during account sign-up, so enabling

DOI: https://doi.org/10.54216/FPA.180106
Received: June 24, 2024 Revised: September 22, 2024 Accepted: December 25, 2024 Corrected: December 11, 2025

them to authenticate themselves by submitting a selfie or recording a pass phrase for comparison with their saved biometric template upon log in [15].

Direct minutiae matching is circumvented as the database is big and the minutiae-based matching algorithm meets the high-performance speed requirements. Spectral minutiae representations substitute the minutiae sets.

Watermarking is the act of embedding information into items like images, films, or sound clips to verify their authenticity. Security can be achieved by later finding and removing the data hidden within these elements. An image is watermarked after it has been designed, embedded, and detected or retrieved [16]. In cases where security is a top priority, the embedded watermark needs to be long lasting, inconspicuous, and have a high capacity. Watermarks are mainly utilized to safeguard copyright, allowing for the tracing of content source, identification of unauthorized sharing, and thwarting of unauthorized content access. The particular demands for watermarks change based on the situation. Typically, placing one watermark at the distribution source is enough to identify the original content. To monitor unauthorized copies, a unique watermark is required that corresponds to the recipient's identity or position in the network. Non-blind schemes are best suited for this, as watermark extraction or detection is only required in situations involving ownership disagreements. The watermark on each authorized consumer device is checked as part of semi-blind or blind access control. DCT and DWT have recently been utilized to develop many watermarking methods. An overview of how watermarks are embedded and extracted is shown in Figure 1[6][19].

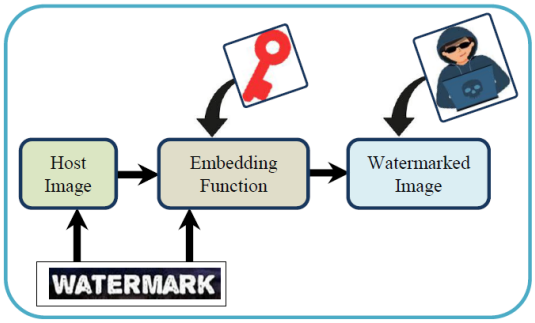


Figure 1. Embedding Model for Watermarks

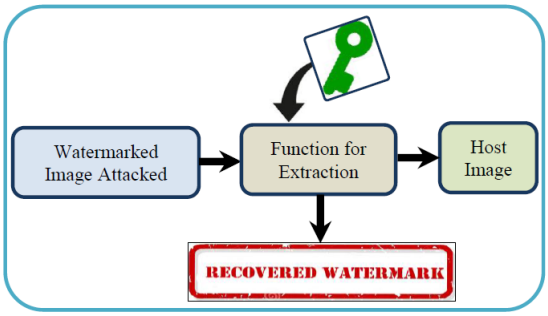
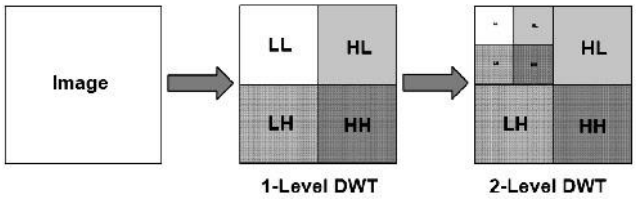


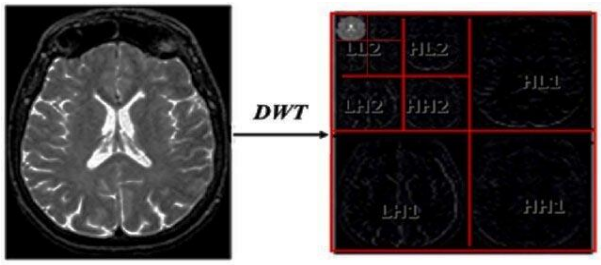
Figure 2. Extraction Model for Watermarks

Through the use of a confidential key and embedding function, an embedded module creates a complex pattern of marking between the host image and the message image. There are several ways in which watermarked images can be compromised, including storing them securely in databases or transmitting them over networks. Using a potentially compromised watermarked image and a confidential key, a watermark or message image can be extracted [3][20]. One of the key components of DWT involves splitting a one-dimensional signal into its high and low frequencies. The low-frequency band is continuously split into smaller segments until the intended level of decomposition is achieved. When dealing with M*N 2-D images, it is necessary to apply 2-D filters in both dimensions, which results in three sets of coefficients for two dimensions. LL1 is a lower-resolution approximation image, HL1 is a horizontal high-frequency band, and LH1 is a vertical high-frequency band. In the lower frequency range, there is an image similar to the original [11][21]. Signals input to DWT analysis must be multiples of 2^n. DWT analysis requires input signals that are multiples of 2 raised to the power of n. In addition to reducing computation time, DWT provides abundant data for examination and reconstruction of the initial signal. A two-level DWT is utilized to decompose the image in Figure 2 [7][22].

DOI: https://doi.org/10.54216/FPA.180106
Received: June 24, 2024 Revised: September 22, 2024 Accepted: December 25, 2024 Corrected: December 11, 2025



(A)



(B)

Figure 3. A and B, Decomposition of DWT on 2_Levels, and 3_Levels

DCT is commonly utilized as a linear transformation function in the digital signal-processing realm. It changes signals from spatial or time domain to frequency domain, leading to images being transformed into an even function. Compared to spatial domain techniques, DCT techniques exhibit greater resilience [9][24]. Using DCT-based algorithms, images can resist resizing, blurring, changing brightness, applying low pass filters, and adjusting contrast. Speech waveforms can be effectively processed using one-dimensional DCT. Images, which are two-dimensional signals, require a 2-D DCT. Matrix coefficients are provided by a two-dimensional DCT of a given matrix. Top left corner of the matrix contains the lowest frequency coefficients, while bottom right corner contains the highest frequency coefficients [5][23]. Formula for 2-D DCT:

$$F(m,n) = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} C(m)C(n)\, f(i,j)\, cos\left[\frac{\pi(2i+1)m}{2N}\right] * cos\left[\frac{\pi(2j+1)m}{2N}\right] \quad (1)$$

Formula for 2-D inverse DCT:

$$F(i,j) = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} C(m)C(n)\, f(m,n) \cos\left[\frac{\pi(2i+1)m}{2N}\right] * cos\left[\frac{\pi(2j+1)m}{2N}\right] \quad (2)$$

$$\text{Where, } C(m), C(n) = \begin{Bmatrix} \sqrt{\frac{1}{N}} & |m,n=0 \\ \sqrt{\frac{2}{N}} & |m,n=1\ upto\ N-1 \end{Bmatrix} \quad (3)$$

Linear algebra is at the core of PLAT, which is an effective method for altering images. According to this theorem, a rectangular matrix A can be broken down into three matrices: U (which is orthogonal), S (which is diagonal), and V (which is a transpose of an orthogonal matrix). Theorems such as this are often referred to as [2][24]:

$$A_{m*n} = U_{m*m}\, S_{m*n}\, V^T_{n*n} \quad (4)$$

where

$$U^T\ \ U = I;\ \ V^T\ \ V = I \quad (5)$$

The U columns are eigenvectors that are orthonormal to AA^T, the V columns are eigenvectors that are orthonormal to A^TA, and a diagonal matrix S consists of square roots of eigenvalues from U or V in decreasing order [6][24].

3. Proposed Scheme

In the innovative proposal, a hybrid-watermarking scheme based on PLAT is utilized to embed one biometric data within another. Specifically, the face image serves as the cover image (Cov_Img) or host image for watermarking with the fingerprint image. This unique watermarking technique is visually and algorithmically represented in the proposal. The DWT is initially utilized on the Cov_Img, resulting in the decomposition into four subbands: LL, HL, LH, and HH [9]. The DCT and PLAT algorithms process the high-frequency bands to generate the matrices

DOI: https://doi.org/10.54216/FPA.180106
Received: June 24, 2024 Revised: September 22, 2024 Accepted: December 25, 2024 Corrected: December 11, 2025

SH1_I, SH2_I, and SH3_I. Watermarked images undergo DWT, which decomposes them into LL1, HL1, LH1, and HH1 bands. Images with watermarks are processed using DCT and SVD to derive their associated matrices [14]. Singular values in the Cov_Img are adjusted by manipulating those in the Watermark image. Watermarked images are formed by applying Inverse DCT and inverse DWT to the altered SVD matrix. As shown in Figure 3, watermarking is represented diagrammatically.

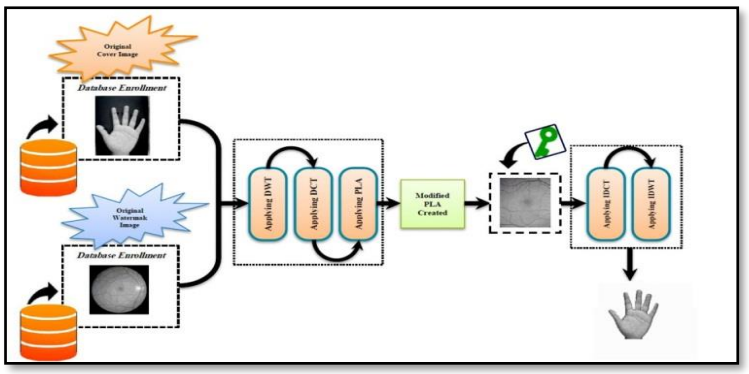


Figure 4. The Embedding of Watermarks Stages

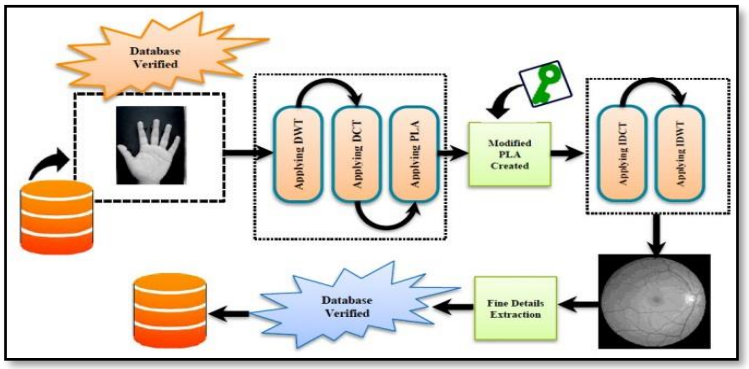


Figure 5. The Extraction of Watermarks Stages

Watermark image W_I.DWT is applied to the original Watermarked image W_I to obtain the Four sub-bands. The original Watermarked image W_I yields four sub-bands when applied to Watermarked image W_I DWT. By transforming all high-frequency bands, DCT generates SH1_WI, SH2_WI, and SH3_WI matrixes, which are then generated by PLA [14]. PLAT matrix is altered when these matrices are modified. By using inverse DWT, the watermark image is retrieved once the high-frequency bands have been converted back with inverse DCT. As shown in Figure 2, the process of extracting the watermark can be visualized [24].

4. Implementation and Results

Two factors determine the effectiveness of a watermarking algorithm: stealth and durability. Using objective criteria, NCC evaluates the similarity between the original watermark and the retrieved watermark. The formula for Normalized Cross-Correlation (NCC) is

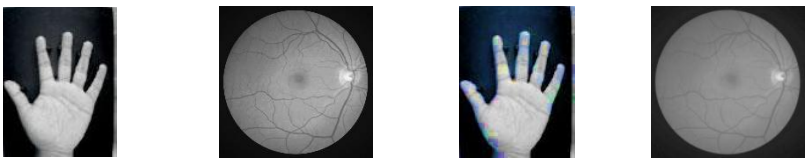
$$NCC = \sum_i \sum_{ij} \frac{w(i,j)w\prime(i,j)}{\sum_i \sum_j |(i,j|^2} \quad (6)$$

A greater NCC value means the watermark's robustness is enhanced; the value varies from -1 to 1. Peak Signal to Noise Ratio (PSNR) is used as a numerical measure of concealment capability :

$$PSNR = 10log_{10}\left(\frac{255^2}{MSE}\right) \quad (7)$$

Decibels (dB) measure the invisibility of a watermark. Better watermark invisibility is indicated by an improved Peak Signal-to-Noise Ratio (PSNR). MATLAB 2012a is used to do simulations to assess the algorithm. Both the main image and the watermark image in this simulation are a 256x256 grayscale image. The initial cover, the watermark image, and the removed watermark are shown in Figure 5.

DOI: https://doi.org/10.54216/FPA.180106
Received: June 24, 2024 Revised: September 22, 2024 Accepted: December 25, 2024 Corrected: December 11, 2025



Original Cov_Img | Oiginal Watermark Image | Watermaked Image | Extracted Watermark

(A) (B)

Figure 6. (A) Watermark and Original Cov_Img (B) Extracted Watermarked and Watermarked Image

Depending on the Human Visual System, the visual similarity of the watermarked photograph to the original image varies; the two images seem very identical, therefore implying that the algorithm effectively obscures the watermark. The two images appear quite similar, therefore demonstrating that the algorithm successfully hides the watermark. With an NCC value of 0.9727, the extracted watermark images with their respective values of NCC in Figure 6 present the outcomes from testing the algorithm's resilience to various attack forms. A PSNR of 46.041 dB between the original Cov_Img and the watermarked image is considered as outstanding.

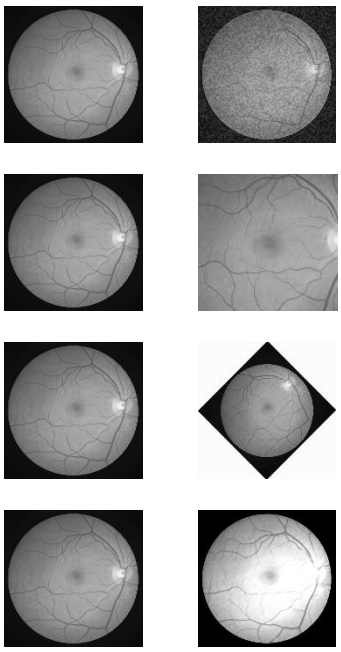
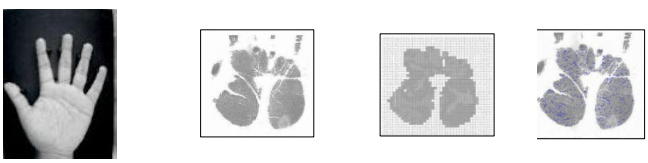


Figure 7. (A) Watermark image original (B) Image with watermark attacked



A B C D

Figure 8. (AImages of original palmprints (B) processing of the mage (C) Image Direction (D) Feature Extraction of the Image

Simulated data indicate that even if the watermark is under assault, the watermarked image can yet be extracted successfully. The watermark technique also prevents salt noise addition, filtering, photo compression, sharpening, crop ping, and rotations among many often used assaults.

DOI: https://doi.org/10.54216/FPA.180106
Received: June 24, 2024 Revised: September 22, 2024 Accepted: December 25, 2024 Corrected: December 11, 2025

Table 1: Biometric Image Parameters Measuement

Image ID	PSNR	MSE	NCC	Time of Steganography (in second)
Img_of_Palm 1	62.882	5.1498e-07	1	0.0261
Img_of_Palm 2	62.915	5.1111e-07	1	0.0250
Img_of_Palm 3	63.853	4.118e-07	1	0.0313
Img_of_Palm 4	59.649	1.0843e-06	1	0.0348
Img_of_Palm 5	56.157	2.4226e-06	1	0.0182
Img_of_Palm 6	60.812	8.2945e-07	1	0.0233
Img_of_Palm 7	59.844	1.0366e-06	1	0.0186
Img_of_Palm 8	56.664	2.1558e-06	1	0.0181
Img_of_Palm 9	62.08	6.1945e-07	1	0.0208
Img_of_Palm 10	61.87	6.5009e-07	1	0.0185

Biometric modalities each have their own advantages and disadvantages and include:

Fingerprint recognition:

Though their superb accuracy, challenges might present themselves while working with low-quality images. The complexly crafted ridges and valleys on our fingers function as a special identification mark [11].

Face recognition:

The system finds a match by contrasting the given image with stored data on personal devices or in large databases or cloud servers. Although it is widely used, mostly in the smartphone industry, facial recognition is vulnerable to fluctuations in lighting, aging, or the use of accessories like glasses or makeup [17].

Retina Recognition:

Though getting good-quality images may be challenging, the application of this sophisticated technique depends on the precise patterns observed in the iris [21].

Voice recognition:

Typically during first interaction with a voice assistant, account holders must record their voice so that algorithms may create biometric templates. From the captured sample, the engine produces an "enrollment" voice template, also known as a "voiceprint," which then serves for future login voice captures. Though voice biometrics provide great convenience, noise or voice variations caused by disease might impair them [14][18].

Behavioral biometrics:

Like other biometric techniques, there are privacy issues regarding the gathering of data from online behavior; platforms for behavioral biometrics use consumers' digital actions and online login behavior to create a distinctive behavioral signature that can stop fraudsters [22].

Liveness detection:

To confirm that the submission comes from a live subject rather than being created or altered by artificial intelligence, a selfie or voice recording is compared to an indexed photo or voice print. This approach is regarded as a really efficient means of authentication, therefore improving security measures against possible spoofing incidents [18][24].

5. Conclusion

Combining DWT and DCT methods, this study presents a new way of watermarking biometric data. Through PLAT, signals of watermark are embedded into the bands of the high-frequency of the WT domain. Prior to embedding, the watermark image is treated with DWT as well as DCT to prepare it for integration. Simulation results demonstrate that the suggested watermarking approach successfully preserves image quality while providing durability against several image-processing algorithms. The algorithm is incredibly efficient at embedding signals and shows strong resilience against outside threats, ensuring secure and consistent watermarking for biometric data.

DOI: https://doi.org/10.54216/FPA.180106
Received: June 24, 2024 Revised: September 22, 2024 Accepted: December 25, 2024 Corrected: December 11, 2025

References

1. M. R. Jomaa, H. Mathkour, Y. Bazi, and M. S. Islam, "End-to-end deep learning fusion of fingerprint and electrocardiogram signals for presentation attack detection," *Sensors*, vol. 20, p. 2085, 2020. DOI: https://doi.org/10.3390/s20072085.
2. D. Yaman, F. I. Eyiokur, and H. K. Ekenel, "Multimodal soft biometrics: combining ear and face biometrics for age and gender classification," *Multimedia Tools and Applications*, vol. 81, pp. 22695–22713, 2022. DOI: https://doi.org/10.1007/s11042-021-10630-8.
3. M. A. M. El-Bendary, H. Kasban, A. Haggag, et al., "Investigating nodes and personal authentications utilizing multimodal biometrics for medical application of WBANs security," *Multimedia Tools and Applications*, vol. 79, pp. 24507–24535, 2020. DOI: https://doi.org/10.1007/s11042-020-08926-2.
4. M. Singhal and K. Shinghal, "Recent advances in online signature verification and face recognition," *Test Engineering and Management*, vol. 82, pp. 11371–11377, 2020.
5. S. B. Jadhav, N. K. Deshmukh, and V. T. Humbe, "HDL-PI: hybrid deep learning technique for person identification using multimodal fingerprint, iris, and face biometric features," *Multimedia Tools and Applications*, 2022. DOI: https://doi.org/10.1007/s11042-022-14241-9.
6. S. R. Saeed, et al., "The study of deep learning for automotive logo recognition and classification," *Periodicals of Engineering and Natural Sciences (PEN)*, vol. 11, no. 3, p. 255, 2023. DOI: https://doi.org/10.21533/pen.v11i3.3641.
7. V. C. Kagawade and S. A. Angadi, "VISA: a multimodal database of face and iris traits," *Multimedia Tools and Applications*, vol. 80, pp. 21615–21650, 2021. DOI: https://doi.org/10.1007/s11042-021-10650-4.
8. A. Arora and R. Miri, "Cryptography and Tay-Grey wolf optimization-based multimodal biometrics for effective security," *Multimedia Tools and Applications*, vol. 81, pp. 44021–44043, 2022. DOI: https://doi.org/10.1007/s11042-022-11993-2.
9. S. Chandra and V. Kumar, "A novel approach to validate online signatures using dynamic features based on locally weighted learning," *Multimedia Tools and Applications*, vol. 81, pp. 40959–40976, 2022. DOI: https://doi.org/10.1007/s11042-022-13159-6.
10. K. Bibi, S. Naz, and A. Rehman, "Biometric signature authentication using machine learning techniques: Current trends, challenges, and opportunities," *Multimedia Tools and Applications*, vol. 79, pp. 289–340, 2020. DOI: https://doi.org/10.1007/s11042-019-08022-0.
11. T. Dhieb, H. Boubaker, S. Njah, et al., "A novel biometric system for signature verification based on score level fusion approach," *Multimedia Tools and Applications*, vol. 81, pp. 7817–7845, 2022. DOI: https://doi.org/10.1007/s11042-022-12140-7.
12. M. Leghari, S. Memon, L. D. Dhomeja, A. H. Jalbani, and A. A. Chandio, "Deep feature fusion of fingerprint and online signature for multimodal biometrics," *Computers*, vol. 10, p. 21, 2021.
13. P. S. Chanukya and T. K. Thivakaran, "Multimodal biometric cryptosystem for human authentication using fingerprint and ear," *Multimedia Tools and Applications*, vol. 79, pp. 659–673, 2020.
14. S. Minaee, A. Abdolrashidi, H. Su, M. Bennamoun, and D. Zhang, "Biometric recognition using deep learning: A survey," *arXiv*, arXiv: 1912.00271, 2019.
15. W. Kong, D. Zhang, and W. Li, "Palmprint feature extraction using 2-D Gabor filters," *Pattern Recognition*, vol. 36, no. 10, pp. 2339–2347, 2003.
16. W. Kong and D. Zhang, "Competitive coding scheme for palmprint verification," *Proceedings of the 17th International Conference on Pattern Recognition (ICPR)*, 2004.
17. —, "Sequential Modified Haar Wavelet Energy," *2008 International Conference on Signal Processing, Communications and Networking*, 2008.
18. L. Zhang, L. Zhang, D. Zhang, and H. Zhu, "Online finger-knuckle-print verification for personal authentication," *Pattern Recognition*, vol. 43, no. 7, pp. 2560–2571, 2010.
19. L. Zhang and D. Zhang, "Characterization of palmprints by wavelet signatures via directional context modeling," *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol. 34, no. 3, pp. 1335–1347, 2004.

DOI: https://doi.org/10.54216/FPA.180106
Received: June 24, 2024 Revised: September 22, 2024 Accepted: December 25, 2024 Corrected: December 11, 2025

20. P. Recobos Rodriguez and J. Landa Silva, "Biometric identification by dermatoglyphics," *Proceedings of the 3rd IEEE International Conference on Image Processing*.

21. I. Fatima, N. K. Mehra, and N. K. Nishchal, "Optical image encryption using equal modulus decomposition and multiple diffractive imaging," *Journal of Optics*, vol. 18, no. 8, p. 085701, 2016.

22. I. H. Abdalla and R. F. Yaser, "WSN recruitments for encrypted medical image transmission securely," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 26, no. 7, pp. 1981–1990, 2023. DOI: https://doi.org/10.47974/jdmsc-1838.

23. 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 Symposium on Computational Intelligence*, Singapore: Springer, 2023, pp. 487–500.

24. 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 *2023 International Conference on Cyberworlds (CW)*, IEEE, 2023, pp. 395–402.

DOI: https://doi.org/10.54216/FPA.180106
Received: June 24, 2024 Revised: September 22, 2024 Accepted: December 25, 2024 Corrected: December 11, 2025