

A UNIFIED BIOMETRIC AND REVERSIBLE WATERMARKING FRAMEWORK FOR SECURE MEDICAL IMAGE AUTHENTICATION

Brahim Ferik, Lakhdar Laimeche, Abdallah Meraoumia, Abdelkader Laouid and Khaled Chait

Keywords and phrases: Blind Reversible Watermarking, Fingerprint Authentication, Improved BSIF, LWT, Spread-Spectrum, and Lightweight Encryption.

This manuscript is an extended and significantly improved version of a full paper entitled “Combining I-BSIF Fingerprints and FlexenTech for Reversible Medical Image Watermarking” presented at ICRAMI 2025 (Tunisia, November 2025). Compared to the conference version, this paper includes a substantially expanded related-work section, a more rigorous security analysis with threat model and key-management assumptions, and an extended methodology covering embedding capacity, blind extraction, biometric authentication, and reversible image reconstruction.

The authors would like to thank the reviewers and editor for their constructive comments and valuable suggestions that improved the quality of our paper.

Brahim Ferik acknowledges resources and support from the LAMIS laboratory of Larbi Tebessi University, Tebessa, Algeria.

Abstract The rapid adoption of digital medical imaging in telemedicine has heightened concerns about image authenticity, integrity, and patient privacy. Existing watermarking techniques often trade robustness for reliable patient authentication, limiting their suitability for clinical settings. To address this gap, this paper proposes a novel blind, reversible watermarking framework that tightly integrates biometric authentication with transform-domain watermarking. The framework uses orientation-guided Improved Binary Statistical Image Features (I-BSIF) to extract compact, rotation-invariant fingerprint signatures, which are then secured with lightweight FlexenTech permutation-based encryption. The encrypted biometric watermark is embedded in medical images via adaptive spread-spectrum modulation in the mid-frequency subbands of the Lifting Wavelet Transform, ensuring reversibility and blind extraction. The primary objective is to achieve secure, imperceptible, and identity-aware medical image authentication without compromising diagnostic quality. Experimental results show that the proposed approach preserves over 99% biometric similarity under 270° rotation, achieves an average PSNR exceeding 51 dB, and SSIM values close to 0.999. These findings confirm strong imperceptibility, robustness, and authentication reliability. Overall, the proposed framework offers a practical and balanced solution for secure telemedicine, ensuring trustworthy image exchange with high perceptual fidelity and robustness.

1 Introduction

Medical imaging is essential for diagnosis, treatment planning, and telemedicine [1]. However, its transmission over networks is subject to risks, including tampering and privacy breaches. Digital watermarking helps address these threats, but few methods achieve a balance among high perceptual fidelity, robustness to attacks, exact reversibility, and reliable patient authentication [2,3]. Although transform-domain spread-spectrum techniques can counteract signal-processing attacks and reversible methods enable flawless image recovery, integrating these with biometric watermarks that link images to their owners remains challenging [4,5,6]. Specifically, modern reversible methods often rely on computationally heavy transforms or large watermark sizes, which hinder their application in real-time medical devices with limited resources.

To address current limitations, we propose a lightweight, blind, reversible medical watermark that combines orientation-guided BSIF fingerprint features with spread-spectrum embedding in lifting wavelet (LWT) sub-bands [7, 8]. The encrypted biometric vector, secured by FlexenTech permutation [9], produces a compact key-dependent watermark. Each image was decomposed using a single-level integer LWT; mid-frequency LH/HL coefficients were modulated by key-driven pseudo-noise scaled to the local texture, preserving quality and robustness. This adaptive power control minimized visual distortion under compression, noise, rotation, and cropping attacks, validated through extensive experiments, blind extraction correlated coefficients with the same pseudo-noise and inverted permutations, restoring the watermark and image [10].

The core contributions of this research include three fundamental advances in medical image watermarking:

- **Orientation-guided improved BSIF operator:** Developing a novel feature extraction method that demonstrates exceptional rotation invariance while extracting compact and distinctive fingerprint features for enhanced biometric authentication.
- **Lightweight FlexenTech encryption:** Introducing a computationally efficient encryption scheme that provides robust biometric watermark security through iterative key-dependent permutations, significantly reducing computational overhead compared to traditional cryptographic approaches.
- **Adaptive spread-spectrum embedding:** Designing an embedding framework that utilizes the lifting wavelet transform to optimally balance watermark imperceptibility with extraction reliability in various medical imaging modalities.

This manuscript is an extended and significantly improved version of a full paper entitled “Combining I-BSIF Fingerprints and FlexenTech for Reversible Medical Image Watermarking” presented at ICRAMI 2025 (Tunisia, November 2025) [11]. Compared to the conference version, this paper includes a substantially expanded related-work section, a more rigorous security analysis with threat model and key-management assumptions, and an extended methodology covering embedding capacity, blind extraction, biometric authentication, and reversible image reconstruction. The experimental study has also been broadened through additional medical datasets, new biometric identification results based on ROC/AUC analysis, sensitivity analysis to orientation noise, FlexenTech security and efficiency evaluation, extended robustness testing, and more comprehensive comparisons with state-of-the-art watermarking and feature extraction methods. These additions provide a more complete validation of the proposed framework for secure, identity-aware, and real-time medical image authentication.

This paper presents a comprehensive evaluation of the performance and practical applicability of the method. Section 2 examines related work to establish the context of contributions. Section 3 provides background on improved BSIF, FlexenTech encryption, lifting wavelet transforms, and spread-spectrum embedding, which form the theoretical foundation. Section 4 details the proposed scheme, including the generation, embedding, and extraction processes. Section 5 presents experimental results that include imperceptibility measurements, robustness evaluations, comparative analysis, and clinical application considerations.

2 Related work

Robust watermarking has long been recognized as a fundamental mechanism for preserving the integrity and authenticity of medical images, particularly in environments where images are subject to compression, transmission noise, and malicious manipulation. Early research focused on transform-domain watermarking, in which watermark information is embedded in frequency components that are perceptually significant yet robust to common signal-processing operations. Spread-spectrum watermarking combined with multiresolution transforms such as the Discrete Wavelet Transform (DWT), Lifting Wavelet Transform (LWT), Stationary Wavelet Transform (SWT), and Integer Wavelet Transform (IWT) has been widely adopted due to its favorable tradeoff between imperceptibility and robustness. Chauhan et al. [12] employed adaptive spread-spectrum embedding in the DWT domain, while De et al. [13] and Novamizanti et al. [8] explored reversible and multibit spread-spectrum techniques using IWT and SWT. These

methods demonstrate strong resistance to noise, compression, and filtering; however, their authentication capability remains largely image-centric, and reversibility often comes at the cost of reduced robustness or embedding capacity, particularly under geometric distortions such as rotation and scaling.

To avoid any permanent alteration of diagnostic content, zero-watermarking and reversible watermarking schemes have been proposed as alternatives to conventional embedding-based methods. Dai et al. [14] introduced a hybrid reversible-zero watermarking approach that combines nearest-neighbor grayscale residual features with Slantlet-SVD-QIM embedding, enabling lossless recovery while maintaining robustness to signal-processing attacks. Similarly, Taj et al. [15] employed invariant local feature extraction with SURF, combined with SVD, to generate robust zero-watermark signatures without modifying pixel values. While these approaches successfully preserve visual quality and diagnostic reliability, authentication is limited to feature consistency and ownership verification, without explicit association to patient or clinician identity. As a result, authenticity is verified at the signal or content level rather than through identity-aware mechanisms.

Region-based reversible watermarking has further extended this line of research by explicitly accounting for clinical relevance. Bhalerao et al. [16] proposed an ROI/RONI-based reversible watermarking framework that embeds cryptographic authentication information within diagnostically important regions while storing recovery data in non-critical areas. This design enables accurate tamper localization and recovery with high imperceptibility. Despite these advantages, authentication relies on embedded hash values, and verification remains decoupled from patient or data-source identity, limiting its suitability for scenarios requiring end-to-end identity assurance.

Another research direction focuses on robust transform-domain watermarking to improve resistance to signal-processing and geometric attacks. Taj et al. [17] proposed a transform-domain watermarking framework enhanced with invariant feature analysis, achieving high imperceptibility and robustness across multiple medical imaging modalities; however, authentication remains image-centric and is not explicitly linked to patient or user identity. MD-FFT-based schemes, such as those proposed by Abo El-Soud et al. [18], integrate compression and encryption mechanisms to enhance payload efficiency, robustness, and blind detection capability. By combining LZW compression, Arnold scrambling, and LFSR-based encryption with frequency-domain embedding, these methods achieve high PSNR and strong resistance to joint attacks. Nevertheless, such schemes are primarily designed for copyright protection and signal-level security, and do not incorporate biometric or identity-aware authentication within the watermarking process.

Hybrid authentication strategies that combine watermarking with perceptual hashing have also been explored. Roy et al. [19] generated compact hash vectors using KAZE and LBP-HF features and embedded them into LWT subbands for integrity verification. These approaches improve robustness against content-preserving manipulations but still authenticate image similarity rather than identity, making them insufficient for patient-specific verification.

Security during image transmission has motivated the development of crypto-watermarking and lightweight encryption frameworks. Rajendran et al. [20] combined wavelet packet transform with AES encryption and bio-inspired optimization to improve confidentiality and imperceptibility, while Alsaraireh et al. [21] proposed selective encryption strategies tailored for IoT and resource-constrained healthcare systems. Nazari and Mehrabian [22] employed a chaotic logistic map in a blind IWT-LSB watermarking scheme, ensuring secure and flexible embedding with minimal computational cost. Similarly, Ferik et al. [4] applied chaotic scrambling and ECC to protect fingerprint vectors. The authors of [23] introduced a fast spatial-domain method for real-time use that encrypts a signature watermark using simple XOR operations and a Sudoku-based permutation. Chaotic-map-based watermarking and lightweight spatial-domain encryption further reduce computational overhead and latency. However, these approaches ensure authenticity primarily through cryptographic keys or authentication tags, rather than embedded identity information. Moreover, complex cryptographic primitives such as elliptic-curve cryptography (ECC) [24] may introduce scalability challenges for real-time or edge-based medical systems.

More recently, dual and AI-assisted watermarking frameworks have emerged to enhance robustness and usability. Taj et al. [25] proposed a lightweight dual-watermarking scheme that embeds both a QR code and an institutional logo using DWT-DCT embedding, with water-

Table 1: Summary of related work methods, limitations, and our contribution

Category	Representative Methods	Key Limitations	Our Contribution
Spread-spectrum and transform-domain watermarking	DWT/LWT/IWT/SWT-based schemes [8, 12, 13]	Image-centric authentication; limited robustness under geometric distortions	Identity-aware watermarking with biometric binding
Zero and reversible watermarking	Hybrid reversible-zero watermarking, SURF-SVD [14, 15]	Ownership and integrity verification without identity linkage	Biometric-linked authentication and integrity protection
ROI-based reversible watermarking	ROI/RONI tamper detection and recovery [16]	Hash-based authentication; no patient identity verification	Unified integrity and identity-aware verification
Robust transform-domain watermarking	Invariant feature-enhanced watermarking [17]	Signal-level authentication only	Integrated biometric verification within watermarking
Blind frequency-domain watermarking	MD-FFT-based blind schemes [18]	Copyright-focused; no biometric authentication	Blind watermarking with identity binding
Crypto-watermarking and encryption	AES, chaotic maps, ECC [20, 21, 22]	Cryptography-only authentication; scalability issues	Embedded biometric-based authentication
Dual and AI-assisted watermarking	QR/logo embedding with CNN extraction [25]	Metadata-centric authentication	Individual identity-aware authentication
Biometric watermarking	Fingerprint and BSIF-based methods [4, 26, 27]	High computational cost; non-blind extraction	Lightweight unified biometric-watermarking framework

mark extraction performed by a compact CNN. The framework achieves strong imperceptibility and real-time performance on embedded platforms. Despite these advantages, authentication is limited to metadata and institutional identifiers, and does not provide patient- or user-specific identity verification.

Efforts to directly integrate biometric information into watermarking represent an important step toward identity-aware authentication. Vaidya [26] embedded fingerprint images using a hybrid LWT-DWT scheme with adaptive scaling, while Ferik et al. [4] employed BSIF-based fingerprint vectors protected via chaotic permutation and elliptic-curve cryptography. Garg et al. [27] further explored entropy-guided DWT-SVD watermarking for biometric image protection. Although these approaches introduce identity-related data, they often involve high computational complexity, non-blind extraction, or large payloads, limiting their practicality in real-time and resource-constrained clinical environments.

As summarized in Table 1, existing medical image watermarking and encryption approaches predominantly focus on image-centric integrity, ownership, or confidentiality, with biometric identity either absent or loosely coupled to the authentication process. Robustness, reversibility, efficiency, and identity-aware authentication are rarely addressed simultaneously within a single framework. These limitations motivate the proposed work, which aims to unify biometric verification and watermarking to provide integrated medical image integrity protection and identity-aware authentication suitable for modern clinical workflows.

3 Background

This section outlines the theoretical principles underlying the proposed framework, covering orientation-aware feature extraction, lightweight encryption, wavelet-domain analysis, and spread-spectrum techniques for secure biometric watermarking.

3.1 Orientation-Adaptive Improved BSIF (I-BSIF)

The proposed **Improved Binary Statistical Image Features (I-BSIF)** framework enhances the standard BSIF descriptor [28] by integrating local ridge flow data to achieve rotation invariance, which is important for secure biometric authentication and remote identification applications [6, 29]. This method partitions the fingerprint into 16×16 -pixel blocks, $\mathcal{B}$, and computes a dominant orientation, θ , for each segment. This directional component is derived from the structural tensor of the image using Sobel gradients, G_x and G_y , as follows (3.1):

$$\theta = \frac{1}{2} \tan^{-1} \left(\frac{\sum_{\mathcal{B}} 2 G_x G_y}{\sum_{\mathcal{B}} (G_x^2 - G_y^2)} \right) \quad (3.1)$$

Rather than applying static ICA filters, the system dynamically realigns the filter bank $\{\mathbf{F}_k\}_{k=1}^N$ to match the local ridge angle. This is achieved by applying a rotation matrix $\mathbf{R}(\theta)$ to the kernels, ensuring the axes of the filters are synchronized with the fingerprint's topography (3.2):

$$\mathbf{F}_k^{(\theta)} = \mathbf{R}(\theta) \mathbf{F}_k \mathbf{R}(\theta)^\top, \quad \mathbf{R}(\theta) = \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix} \quad (3.2)$$

The convolution response, $r_k = \mathcal{B} * \mathbf{F}_k^{(\theta)}$, is subsequently thresholded to produce a binary bit $b_k = \text{sgn}(r_k)$. By aggregating these binarized responses across all filters and blocks, a robust and compact biometric signature is generated. This adaptive steering ensures that the extracted features remain consistent and distinctive even when the fingerprint image undergoes significant geometric rotation, as evidenced by the improved clarity shown in Figure 1.

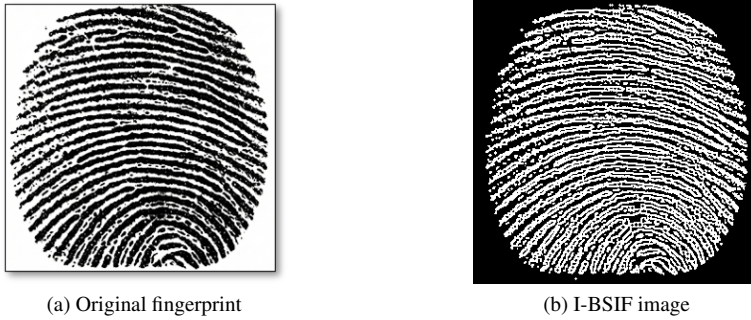


Figure 1: Improved BSIF for fingerprint feature extraction.

3.2 FlexenTech permutation encryption

FlexenTech is employed as a lightweight permutation-based encryption scheme [9] to secure the binary fingerprint features prior to watermark embedding. It is specifically designed to operate efficiently on variable-length biometric vectors, making it well-suited for medical imaging systems with limited computational resources. Given a feature vector of length n , FlexenTech generates a key-dependent permutation using a secret integer key K and block parameter B . The permutation indices are computed as (3.3):

$$v_i = (B \times (K - i)) \bmod K, \quad i = 1, 2, \dots, n. \quad (3.3)$$

Sorting the resulting index sequence defines a bijective mapping that rearranges the feature bits. This permutation process is iteratively applied over multiple rounds to enhance diffusion and obscure statistical relationships between the plaintext and ciphertext (Figure 2). Unlike conventional block ciphers, FlexenTech avoids substitution boxes and floating-point operations, achieving linear-time complexity. Decryption is performed by applying the inverse permutations in reverse order, ensuring exact recovery of the original biometric features when the correct key is available (Figure 3).

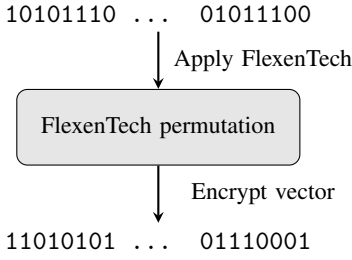


Figure 2: FlexenTech encryption process

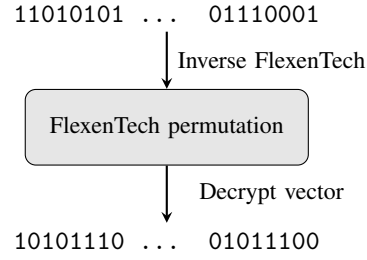


Figure 3: FlexenTech decryption process

Threat model and security assumptions

The threat model assumes a passive adversary capable of intercepting the encrypted biometric vector $\mathbf{C} \in \{0, 1\}^N$ during transmission, without access to the watermarking system's internal memory or the secret key K . The attacker's objective is to reconstruct the original feature vector by reversing the permutation process. Without knowledge of K , this requires solving an inverse permutation problem across multiple rounds, with computational complexity at least $\Omega(N!)$. After R rounds, each output index is determined by a composition of permutations,

$$j = \pi_{K,B}^{(R-1)}(\pi_{K,B}^{(R-2)}(\cdots \pi_{K,B}^{(0)}(i) \cdots)),$$

making statistical inference infeasible. The model assumes no chosen-plaintext access, consistent with embedded medical imaging environments.

Key management policy and practical deployment

In practical deployment, the secret key K is generated using a high-entropy source and securely provisioned during system initialization. While the block parameter B may be public, the secrecy of K is strictly maintained. A session-based key rotation strategy is adopted, assigning a new permutation key to each watermarking instance to limit long-term exposure. Keys are stored within secure hardware or trusted execution environments to prevent unauthorized access. Since FlexenTech relies solely on integer-based permutations with linear complexity, key updates introduce negligible overhead. This lightweight key management approach supports real-time medical imaging workflows while maintaining strong protection for sensitive biometric data.

3.3 Lifting Wavelet Transform (LWT)

The Lifting Wavelet Transform (LWT) provides a computationally efficient, fully reversible framework for multiresolution image analysis, making it well-suited for medical image watermarking applications [30]. In contrast to conventional wavelet implementations, LWT decomposes the signal through a sequence of simple operations—splitting, prediction, and updating—while preserving integer-valued coefficients [31]. This integer-to-integer mapping significantly reduces rounding errors and enables exact reconstruction.

For a discrete image signal $x[n]$, the lifting scheme separates the data into even and odd samples and generates detail and approximation components as follows (3.4).

$$d[n] = x_{\text{odd}}[n] - P(x_{\text{even}}[n]), \quad a[n] = x_{\text{even}}[n] + U(d[n]), \quad (3.4)$$

where $P(\cdot)$ denotes the prediction operator and $U(\cdot)$ represents the update function. Applying this process in two dimensions yields four subbands: LL , LH , HL , and HH , corresponding to different spatial-frequency components.

In the proposed framework, watermark embedding is restricted to the mid-frequency subbands LH and HL , which offer an effective compromise between visual transparency and resistance to signal-processing attacks. This selective embedding strategy enhances watermark robustness while preserving the diagnostic quality of medical images, as illustrated in Figure 4.

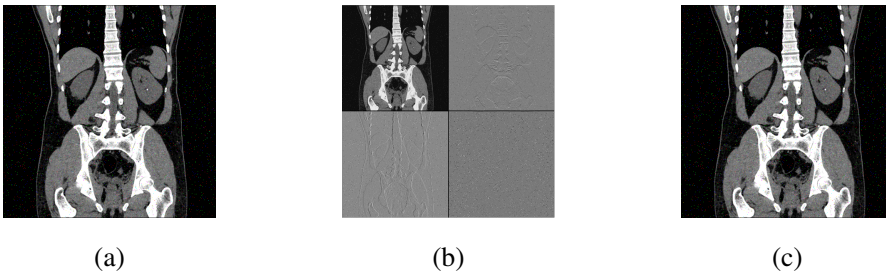


Figure 4: Single-Level 2D LWT decomposition and reconstruction of a medical image.

3.4 Spread-spectrum

Spread-spectrum watermarking embeds information by distributing a weak watermark signal across a large set of host coefficients, making the embedded pattern resemble noise and thereby reducing its detectability [5]. Let $\mathbf{s} \in \mathbb{R}^N$ be the host coefficient vector, $w \in \{\pm 1\}$ be a watermark bit, and $\mathbf{p} \in \{\pm 1\}^N$ be a key-dependent pseudo-random sequence. The watermark insertion is modeled as in Equation (3.5).

$$\mathbf{s}' = \mathbf{s} + \alpha w \mathbf{p}, \quad (3.5)$$

The gain factor α balances visual transparency and detection reliability. During extraction, the watermark bit is estimated by correlating the modified signal $\mathbf{s}'$ with the same pseudo-random sequence $\mathbf{p}$; the sign of the resulting correlation determines w without requiring access to the original image [32]. In the proposed scheme, this embedding strategy is applied to the *LH* and *HL* subbands obtained from the lifting wavelet transform, ensuring both robustness and imperceptibility.

4 Proposed watermarking scheme

This section presents a blind and reversible watermarking framework for securing medical images through biometric authentication. As shown in Figure 5, the method integrates fingerprint feature extraction, lightweight encryption, robust embedding, and lossless reconstruction. A compact biometric signature is generated using orientation-guided I-BSIF and protected via FlexenTech encryption. The encrypted watermark is embedded in mid-frequency LWT subbands using spread-spectrum modulation. Blind correlation-based extraction and inverse encryption recover the biometric data, while integer-to-integer LWT guarantees exact reconstruction of the original image.

4.1 Watermark generation

In the proposed framework, the watermark is generated from the patient's fingerprint using a three-step process summarized in Algorithm 1. Initially, a plain fingerprint image is acquired and divided into non-overlapping 16×16 blocks to capture the characteristics of the local ridge. Next, an orientation-guided I-BSIF operator is applied to each block, where the ICA-based filters rotate according to the dominant ridge orientation θ . The sign of the resulting filter responses is binarized, yielding a compact binary feature vector $\mathbf{W} = [b_1, b_2, \dots, b_N]^\top$, with N denoting the length of the resulting watermark.

To protect the extracted biometric features, FlexenTech permutation encryption is employed. Over R encryption rounds, the feature vector is iteratively permuted using a key-dependent mapping $\pi_{K,B}^{(r)}$, defined as

$$\mathbf{W}_{r+1} = \pi_{K,B}^{(r)}(\mathbf{W}_r),$$

resulting in the encrypted watermark $\mathbf{C} = \mathbf{W}_R$. This design enables flexible watermark sizing, providing an effective balance between authentication accuracy and imperceptible embedding.

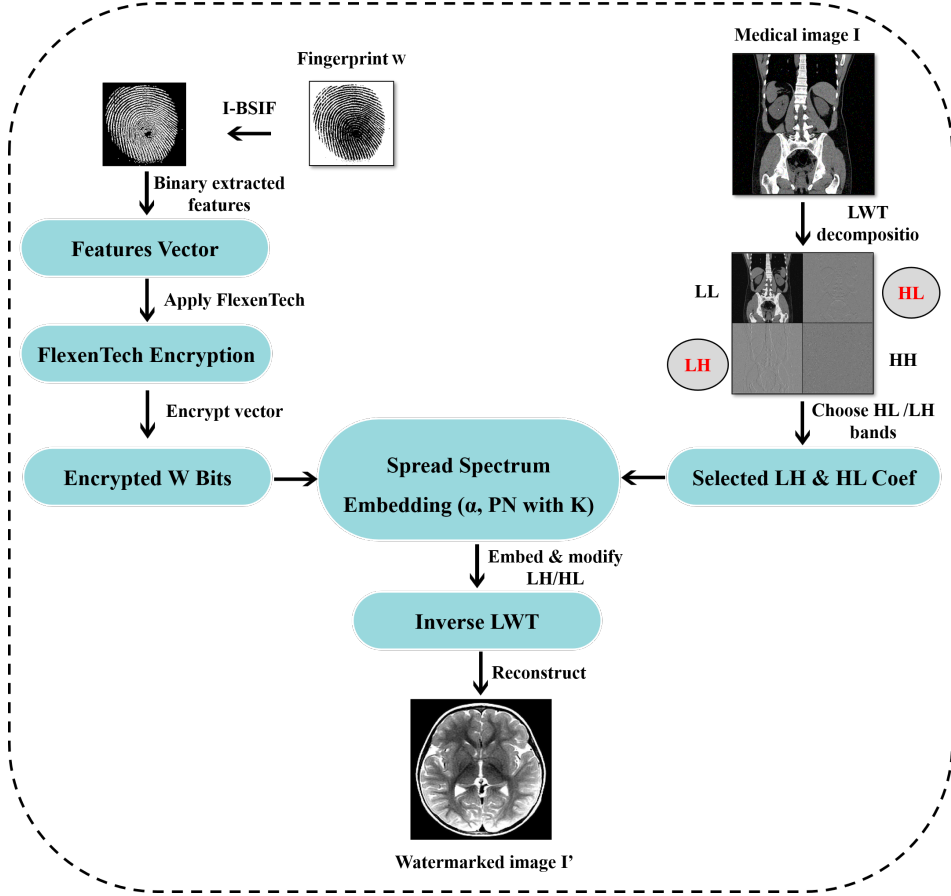


Figure 5: Workflow of the biometric feature embedding process.

4.2 Embedding process

Following FlexenTech encryption, the resulting binary sequence $\mathbf{C} = \{c_i\}_{i=1}^N$ is embedded into the host medical image through a structured multistage procedure. First, the input image $\mathcal{I}$ of size 512×512 is decomposed using a single-level lifting wavelet transform (LWT), yielding four subbands of dimension 256×256 , namely LL , LH , HL , and HH . To achieve a balance between visual transparency and robustness, watermark insertion is restricted to mid-frequency detail subbands LH and HL .

Each encrypted bit c_i modulates a corresponding block of wavelet coefficients via spread-spectrum embedding, expressed as

$$\mathbf{s}'_{(i)} = \mathbf{s}_{(i)} + \alpha c_i \mathbf{p}_{(i)}, \quad \mathbf{p}_{(i)} \in \{\pm 1\}^m,$$

where α denotes the embedding gain and $\mathbf{p}_{(i)}$ is a pseudo-random sequence generated from the secret key. The modified subbands are subsequently recombined using the inverse LWT

Algorithm 1 Watermark Generation

Require: Fingerprint image $\mathcal{W}$; key K ; block size B ; rounds R

Ensure: Encrypted watermark $\mathbf{C}$

- 1: Acquire fingerprint image $\mathcal{W}$
 - 2: Compute orientation map and extract I-BSIF bits to form $\mathbf{W}_0$
 - 3: **for** $r = 0$ **to** $R - 1$ **do**
 - 4: $\mathbf{W}_{r+1} \leftarrow \pi_{K,B}^{(r)}(\mathbf{W}_r)$
 - 5: **end for**
 - 6: **return** $\mathbf{C} \leftarrow \mathbf{W}_R$
-

to produce the watermarked image $\mathcal{I}'$. By distributing the watermark energy across multiple coefficients, the method ensures high imperceptibility while enabling reliable blind extraction. The complete embedding procedure is summarized in Algorithm 2, with N representing the watermark length derived from the fingerprint feature vector.

Algorithm 2 Watermark Embedding

Require: Medical image $\mathcal{I}$, encrypted bits $\mathbf{C}$, key K , strength α

Ensure: Watermarked image $\mathcal{I}'$

- 1: $(LL, LH, HL, HH) \leftarrow \text{LWT}(\mathcal{I})$
 - 2: **for** $i = 1$ **to** $|\mathbf{C}|$ **do**
 - 3: Generate pseudo-random block $\mathbf{p}_{(i)}$ with key K
 - 4: Select corresponding coefficient blocks $\mathbf{s}_{LH,(i)}, \mathbf{s}_{HL,(i)}$
 - 5: $\mathbf{s}_{LH,(i)} \leftarrow \mathbf{s}_{LH,(i)} + \alpha c_i \mathbf{p}_{(i)}$
 - 6: $\mathbf{s}_{HL,(i)} \leftarrow \mathbf{s}_{HL,(i)} + \alpha c_i \mathbf{p}_{(i)}$
 - 7: **end for**
 - 8: $\mathcal{I}' \leftarrow \text{InvLWT}(LL, LH, HL, HH)$
 - 9: **return** $\mathcal{I}'$
-

4.3 Embedding capacity

The embedding capacity of the proposed scheme is the total number of payload bits that can be embedded in the host medical image and subsequently extracted without error. Because each watermark bit modulates a pseudo-random block of length L distributed across the LH and HL subbands of the lifting wavelet transform, the capacity C (in bits) for an image of size $H \times W$ is given by

$$C = \frac{H \times W}{4L}. \quad (4.1)$$

For a typical 512×512 medical image and a spreading factor $L = 128$, the capacity is 512 bits. This comfortably accommodates the compact I-BSIF fingerprint signature while preserving high imperceptibility and robust extraction.

4.4 Watermark extraction and authentication process

The watermark extraction procedure, formalized in Algorithm 3, follows a blind recovery paradigm, requiring only the secret key K rather than the original host image. The process begins by applying a single-level LWT to the watermarked image $\mathcal{I}'$, isolating the mid-frequency LH and HL subbands. Using K , the receiver regenerates the same pseudo-random sequences $\mathbf{p}_{(i)}$ used during embedding.

Detection is achieved by computing the correlation between these sequences and the corresponding coefficient blocks. The sign of the sum of the correlations, $\rho_{LH} + \rho_{HL}$, determines the estimated bit c_i , effectively reversing the spread-spectrum modulation. Once the encrypted vector $\mathbf{C}$ is reconstructed, it undergoes FlexenTech decryption via R rounds of inverse permutation. This process reverses the cryptographic confusion and diffusion layers, restoring the original biometric fingerprint template $\mathbf{W}$ for patient authentication.

Algorithm 3 Watermark Extraction**Require:** Watermarked image $\mathcal{I}'$, key K , block size B , rounds R **Ensure:** Recovered watermark $\mathbf{W}$

- 1: Apply single-level LWT to the watermarked image:
- 2: $(LL, LH, HL, HH) \leftarrow \text{LWT}(\mathcal{I}')$
- 3: **for** $i = 1$ **to** N **do**
- 4: Regenerate pseudo-random sequence $\mathbf{p}_{(i)}$ using key K
- 5: Select corresponding coefficient blocks $\mathbf{s}_{LH,(i)}, \mathbf{s}_{HL,(i)}$
- 6: Compute correlation values:

$$\rho_{LH} = \langle \mathbf{s}_{LH,(i)}, \mathbf{p}_{(i)} \rangle, \quad \rho_{HL} = \langle \mathbf{s}_{HL,(i)}, \mathbf{p}_{(i)} \rangle$$

- 7: Estimate embedded bit:

$$c_i = \begin{cases} +1, & \text{if } (\rho_{LH} + \rho_{HL}) \geq 0 \\ -1, & \text{otherwise} \end{cases}$$

- 8: **end for**
- 9: Form encrypted watermark vector $\mathbf{C} = \{c_i\}_{i=1}^N$
- 10: Decrypt $\mathbf{C}$ using FlexenTech inverse permutation:
- 11: **for** $r = R - 1$ **to** 0 **do**
- 12: $\mathbf{C}_r \leftarrow \pi_{K,B}^{-1}(\mathbf{C}_{r+1})$
- 13: **end for**
- 14: $\mathbf{W} \leftarrow \mathbf{C}_0$
- 15: **return** $\mathbf{W}$

Following extraction, authentication is performed at the point of care by comparing the recovered template $\mathbf{W}$ with a live biometric scan or a secure HIS token $\hat{\mathbf{W}}$. This verification is independent of the host image, ensuring security throughout the transmission channel. Authenticity is confirmed by calculating the normalized correlation ρ :

$$\rho = \frac{\langle \mathbf{W}, \hat{\mathbf{W}} \rangle}{\|\mathbf{W}\| \cdot \|\hat{\mathbf{W}}\|} \quad (4.2)$$

A decision threshold τ (typically $\tau = 0.85$) is applied, so that if $\rho > \tau$, the patient's identity and image integrity are validated as authentic.

4.5 Reversible image reconstruction

The LWT lifting scheme utilizes rounding operators $\lfloor \cdot \rfloor$ to ensure that any signal $x[n] \in \mathbb{Z}$ decomposes into integer-valued subbands (LL, LH, HL, HH) , thereby preventing the numerical drift typically associated with floating-point arithmetic.

Formal reversibility is predicated on the exact inversion of the embedding modification $\delta_i = \alpha c_i \mathbf{p}_{(i)}$. Let $\mathcal{S}$ represent the original mid-frequency coefficients and $\mathcal{S}' = \mathcal{S} + \delta$ represent the watermarked state. Upon extracting the bit $\hat{c}_i$ via correlation, the restoration of the host coefficients is defined as (4.3):

$$\hat{\mathcal{S}} = \mathcal{S}' - \alpha \hat{c}_i \mathbf{p}_{(i)} \quad (4.3)$$

Under the condition of error-free extraction ($\hat{c}_i = c_i$), it follows that $\hat{\mathcal{S}} \equiv \mathcal{S}$. Because InvLWT is a deterministic mapping of these lifting steps, the reconstructed image $\hat{\mathcal{I}} = \text{InvLWT}(LL, \hat{LH}, \hat{HL}, HH)$ remains bit-identical to the original source image $\mathcal{I}$. The theoretical error bound remains zero ($MSE = 0$) provided that $\mathcal{S}'$ does not exceed the bit-depth dynamic range, effectively avoiding overflow or underflow truncation during the integer mapping phase.

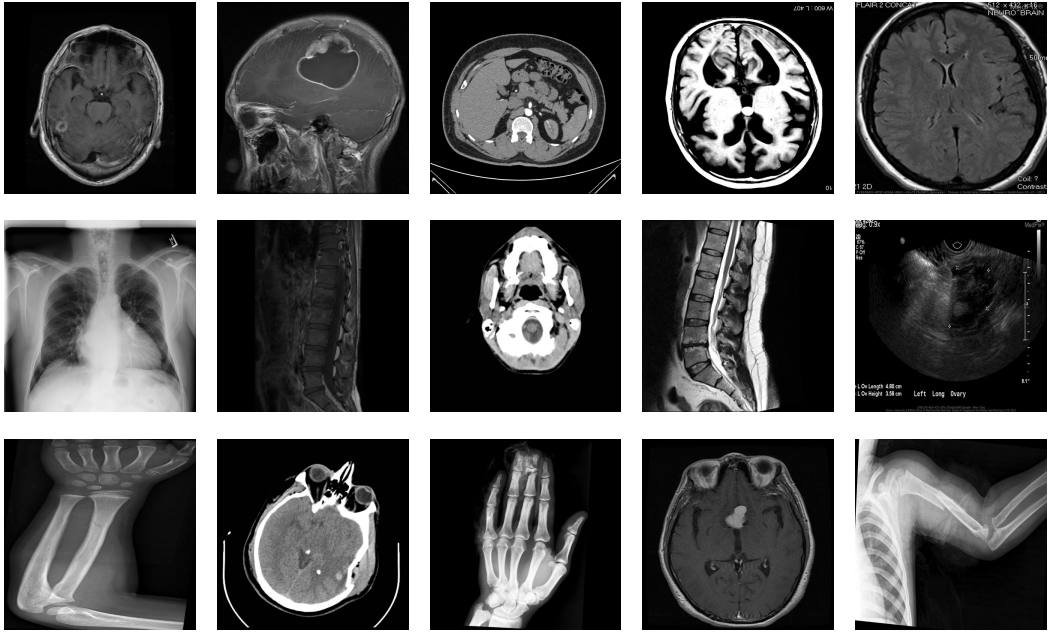


Figure 6: Illustrative examples of CT, MRI, and X-ray images from the benchmark datasets.

5 Results and discussion

To validate the versatility of our framework, we used five diverse medical datasets spanning multiple modalities and anatomical structures. First, Kaggle CT-to-MRI CycleGAN [33, 34] provided axial brain cross-sections 512×512 for cross-domain evaluation. For lower-contrast testing, we used the NIH Chest X-ray [35], a large-scale collection of 112,120 thoracic images. To assess performance on complex structural densities, the Human Bone Fractures Multi-modal Image Dataset (HBFMID) [36] contributed X-ray and MRI scans of various skeletal regions. Finally, the Lumbar Coordinate [37] provided images of the sagittal spine with key vertebral points, offering specialized geometric orientations.

This selection confirms that our watermarking approach is robust in high-resolution scans, noisy radiographs, and diverse clinical textures, demonstrating its broad applicability in telemedicine.

The FVC2002 DB3 dataset [38], captured with the Precise Biometrics 100 SC capacitive sensor at 500 dpi, consists of 300×300 pixel grayscale fingerprint images. These images serve as a benchmark for evaluating fingerprint recognition algorithms. Our study used this dataset to extract fingerprint features with the Improved BSIF method. Furthermore, we tested watermarking techniques with watermark sizes of 64×64 , 128×128 , and 256×256 pixels to assess the impact of watermark dimensions on the robustness and imperceptibility of the embedded watermarks [39]. Implemented in Python 3.14 on an i7 with 16GB RAM and Google Colab, the system leveraged OpenCV, NumPy, and scikit-image for image processing, numerical operations, and feature extraction.

5.1 Evaluation of rotation invariance in improved BSIF

Table 2 and Figure 7 demonstrate the enhanced rotation robustness of the I-BSIF method. Unlike standard BSIF, which suffers significant performance degradation under rotation, I-BSIF maintains over 99% similarity and minimal Hamming distance. This is achieved by integrating orientation maps that adapt filter alignment to local ridge directions, ensuring stable feature extraction. Such robustness is vital for watermarking, enabling secure and reliable embedding despite geometric variations in fingerprint images during medical imaging.

Table 2: Rotation robustness of improved vs. standard BSIF.

Method	Rotation	Similarity (%)	Hamming Distance
BSIF	0°	100.00	0
I-BSIF	0°	100.00	0
BSIF	90°	64.64	2897
I-BSIF	90°	99.85	12
BSIF	180°	65.09	2860
I-BSIF	180°	99.90	8
BSIF	270°	64.80	2880
I-BSIF	270°	99.88	10



Figure 7: Fingerprint image rotated at 0°, 90°, 180°, and 270°.

Biometric identification performance

The recognition accuracy of the proposed I-BSIF features was rigorously evaluated across multiple rotation angles (0° to 270°) to assess practical utility. By comparing rotated probe images with upright templates, we generated ROC curves that plot the True Positive Rate (TPR) against the False Positive Rate (FPR), as illustrated in the accompanying Figure 8.

The experimental results demonstrate exceptional rotational stability, with the AUC consistently above 0.9691 in all test orientations. This performance, characterized by an EER of less than 0.02, confirms that orientation-guided kernels establish a rotation-invariant coordinate system. This stability ensures reliable patient identification at the point of care, regardless of the biometric sensor’s initial alignment.

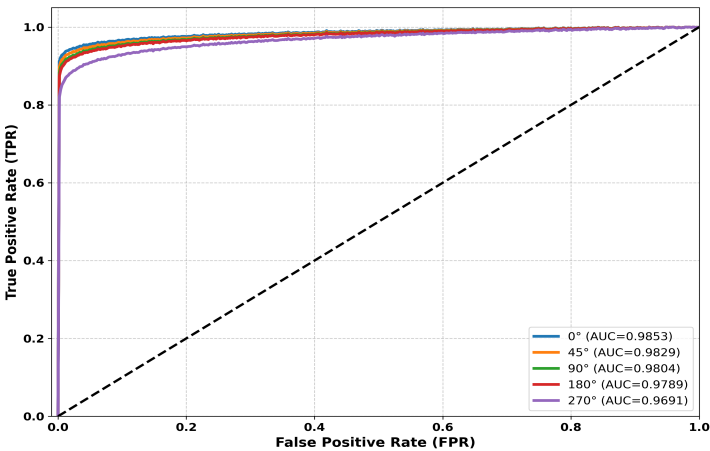


Figure 8: ROC curves showing rotational stability of I-BSIF.

Sensitivity to block-wise orientation noise

The precision of the I-BSIF operator depends on the precision of the dominant orientation θ calculated in Equation (3.1). To assess the robustness of our method against estimation errors, we added synthetic Gaussian noise to the orientation map. As illustrated in Figure 9, the experimental results indicate that the similarity index remains above 95% even when the orientation estimate has a standard deviation of up to 10° . This resilience is primarily attributed to local averaging within the 16×16 blocks and the inherent redundancy of the BSIF filter responses. These properties ensure that the watermarking framework remains operational and secure even in low-quality fingerprint scans where the ridge flow may be partially obscured by moisture, scarring, or sensor inaccuracies.

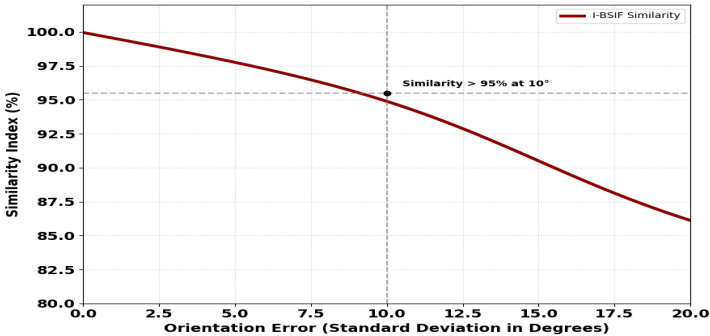


Figure 9: I-BSIF similarity index vs. orientation estimation noise.

5.2 Security and efficiency analysis of FlexenTech encryption

The security of the FlexenTech layer is validated through statistical tests and computational complexity analysis. We evaluate its performance using information entropy, correlation analysis, and Brute-Force resistance.

Table 3: Security and performance metrics of FlexenTech encryption for I-BSIF features.

N (bits)	Entropy (P)	Entropy (E)	Correlation	Bit Balance	Enc (ms)	Dec (ms)
128	0.9887	0.9887	-0.04762	0.488	0.093	0.060
256	1.0000	1.0000	0.01093	0.504	0.189	0.130
512	0.9989	0.9989	-0.00153	0.520	0.332	0.241
1024	0.9995	0.9995	-0.03202	0.486	0.349	0.388
2048	0.9999	0.9999	0.01156	0.494	0.396	0.482

As shown in Table 3, FlexenTech encryption exhibits ideal permutation characteristics when applied to I-BSIF features. Because the scheme uses key-dependent bit permutations, the global bit distribution is preserved, resulting in identical Shannon entropy before and after encryption. The near-zero correlation coefficients confirm strong diffusion, and the balanced ciphertext bit ratio of approximately 0.5 indicates strong statistical uniformity. From a computational perspective, both encryption and decryption times scale linearly with the feature length and remain below 0.9 ms even for 2048-bit vectors, supporting real-time deployment in medical systems. FlexenTech’s security relies on the secrecy of the integer key K and the round-based permutations. Regarding brute-force resistance, the permutation space increases factorially with feature length; for a 1024-bit I-BSIF vector, the keyspace exceeds 5.4×10^{2639} , rendering exhaustive inversion computationally infeasible. In the passive-adversary model, these results validate FlexenTech as a secure and efficient encryption layer for biometric watermarking in medical imaging applications.

5.3 Imperceptibility analysis

The visual fidelity of the watermarked image is a critical performance metric, particularly in medical informatics, where preserving diagnostic features is non-negotiable. To evaluate the imperceptibility of the proposed framework, we use a suite of full-reference metrics, including Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM), Mean Square Error (MSE), and Average Difference (AD). Table 4 summarizes these metrics across a diverse dataset comprising standard test images and clinical cancer scans, and the experimental results demonstrate a high degree of transparency. Specifically, the PSNR consistently exceeds 50.51 dB across all samples, reaching a peak of 52.34 dB for the Baboon image, indicating that the quantization noise introduced during watermark embedding is negligible. Furthermore, structural integrity is maintained as SSIM values remain remarkably close to unity, ranging from to, indicating that the I-BSIF-guided embedding process successfully preserves the luminance, contrast, and structural textures essential for clinical interpretation. Finally, the low MSE and AD distortion metrics further confirm that pixel-wise deviations are minimal, ensuring that the global statistical properties of the medical images remain intact.

Table 4: Imperceptibility metrics of the watermarked images

Image	PSNR	SSIM	MSE	AD
Baboon	52.3402	0.9900	0.1416	0.2095
Pepper	51.7180	0.9997	0.1378	0.2068
Eight	50.7325	0.9948	0.2493	0.3879
Cameraman	51.5614	0.9992	0.1539	0.2180
Cancer(11)	50.5138	0.9780	0.5777	0.5046
Cancer(108)	51.1837	0.9993	0.1951	0.2474
Cancer(110)	51.3621	0.9946	0.4752	0.4327
Cancer(1000)	50.5380	0.9976	0.2745	0.3010
Not(1013)	50.8683	0.9979	0.3324	0.2727
NotCancer(1023)	50.8990	0.9994	0.2287	0.2705
NotCancer(1036)	51.1735	0.9998	0.1963	0.2473
NotCancer(1077)	51.6418	0.9996	0.1455	0.2117

Qualitative assessment corroborates these quantitative findings. As illustrated in Figure 10, the watermarked Baboon image exhibits no discernible perceptual degradation compared to the original. The amplified difference map highlights the sparse, localized nature of the watermark embedding, thereby avoiding interference with high-variance regions. Furthermore, the comparison of the intensity histogram in Figure 11 shows virtually overlapping distributions between the original and watermarked states. This statistical transparency is vital for thwarting histogram-based steganalysis attacks and maintaining the diagnostic validity of pixel data.

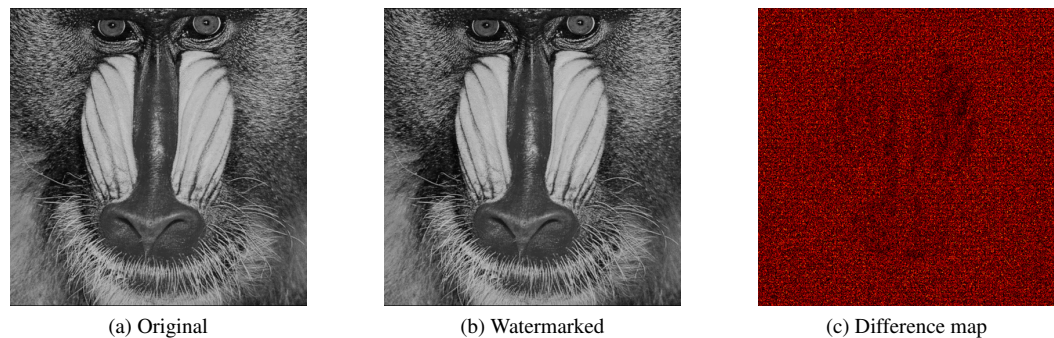


Figure 10: Visual comparison between the original, watermarked, and difference map images.

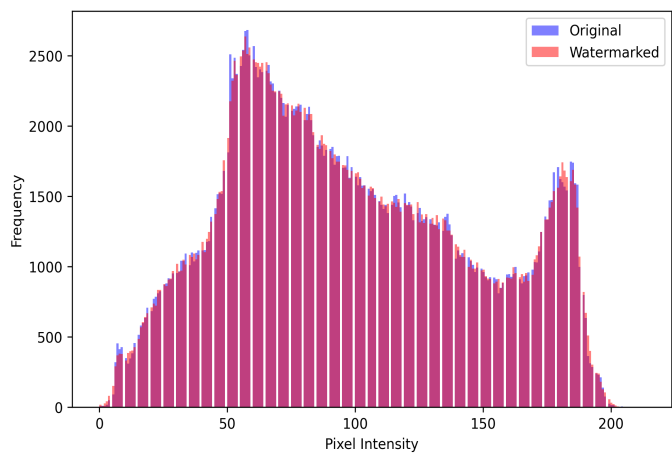


Figure 11: Histogram comparison of pixel intensities between the original and watermarked images.

Table 5: Robustness metrics of the watermarked images

Image	BER	NCC
Baboon	0.0469	0.9991
Pepper	0.0781	0.9990
Eight	0.0869	0.9951
Cameraman	0.0469	0.9991
Cancer (11)	0.0000	1.0000
Cancer (108)	0.0000	1.0000
Cancer (110)	0.0856	0.9984
Cancer (1000)	0.0625	0.9993
Not(1013)	0.0781	0.9992
NotCancer(1023)	0.0312	0.9688
NotCancer(1036)	0.0741	0.9996
NotCancer(1077)	0.0312	0.9998

5.4 Robustness measurements

The robustness of the proposed watermarking framework is first evaluated under ideal conditions, without applying any intentional attacks. As reported in Table 5, the extracted fingerprint feature vectors exhibit consistently low Bit Error Rate (BER) values, frequently approaching zero, while Normalized Cross-Correlation (NCC) values remain close to unity. These results confirm the accurate recovery of the encrypted biometric watermark after decryption and demonstrate the inherent stability of the embedding and extraction processes. Such near-perfect performance under attack-free conditions establishes a reliable baseline for subsequent robustness evaluation.

To assess resilience under practical conditions, a diverse set of signal-processing and geometric distortions is applied to the watermarked images, as illustrated in Figure 12. These manipulations include affine and bending transformations, noise addition, filtering, JPEG compression, rotation, and cropping. Together, these distortions simulate common image degradations encountered during storage, transmission, and processing in medical imaging systems, providing a comprehensive and realistic robustness assessment framework.

Quantitative results under these attacks are summarized in Table 6. The proposed method demonstrates strong robustness against common signal-processing attacks, including JPEG compression (BER = 0.035, NCC = 0.999) and Gaussian blurring (BER = 0.045, NCC = 0.996).

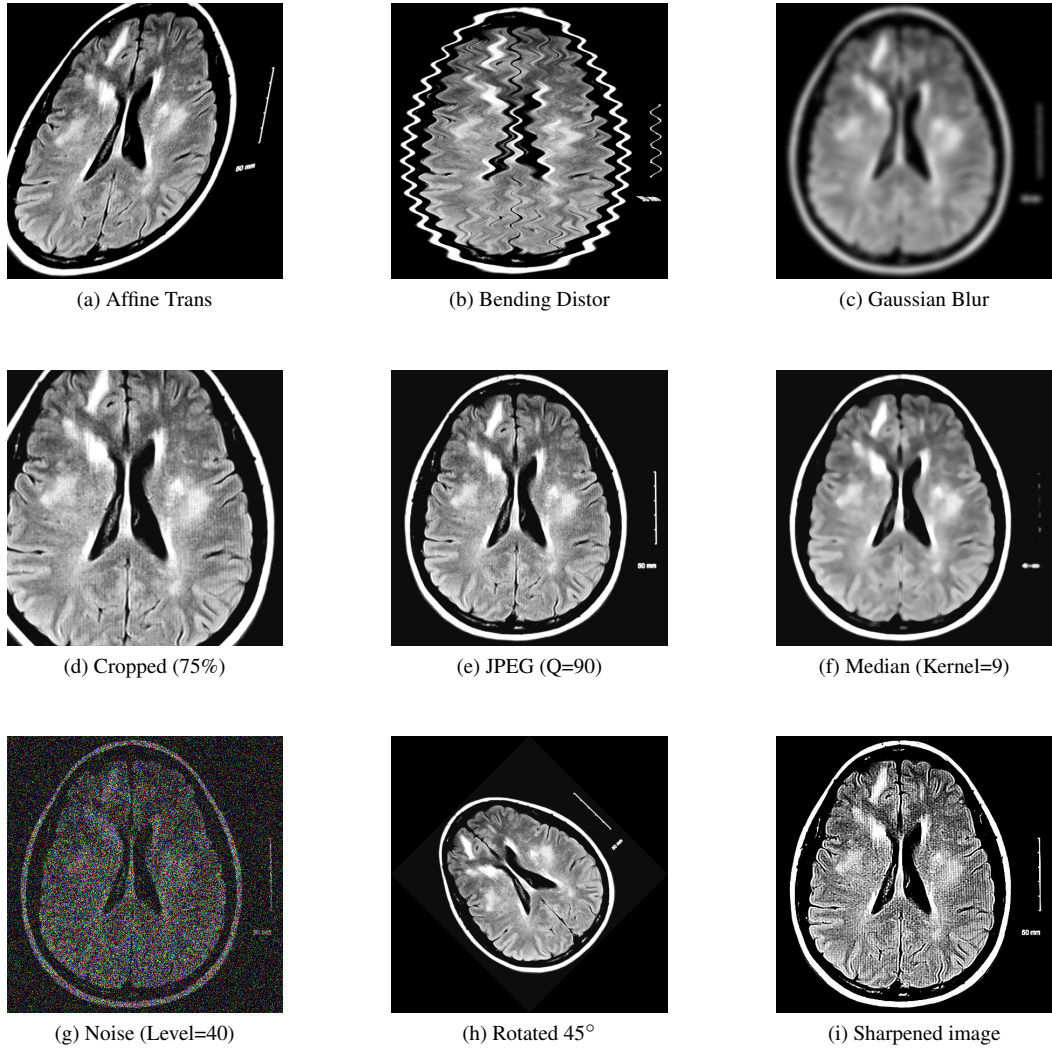


Figure 12: Simulated medical image variations for watermark robustness testing.

Moderate degradation is observed under filtering and noise, whereas more pronounced performance loss occurs under severe geometric transformations, such as a 45° rotation and 75% cropping. This degradation is primarily attributed to coefficient desynchronization and partial watermark loss in the transform domain. Overall, the results confirm that the proposed scheme achieves a favorable balance between robustness and imperceptibility for medical watermarking applications.

5.5 Computational complexity analysis

The computational cost of the proposed watermarking framework is primarily governed by the LWT transform, which performs a linear-time decomposition with complexity $O(M \times N)$ for a host image of dimensions $M \times N$. Subsequent processing stages, including orientation-adaptive I-BSIF feature extraction and FlexenTech permutation encryption, operate on compact binary feature vectors and therefore incur negligible additional overhead. As a result, the overall computational burden remains dominated by the wavelet decomposition stage, ensuring scalability for high-resolution medical images.

Empirical timing analysis further confirms the efficiency of the proposed framework. The lightweight FlexenTech module performs encryption and decryption in $91 \mu s$ and $62 \mu s$, respectively, making it suitable for resource-constrained environments. The complete watermark embedding procedure, including LWT decomposition and spread-spectrum modulation, requires

Table 6: Robustness metrics of the watermarked images under various attacks

Attack Type	BER	NCC
Affine Transform	0.1650	0.8750
Bending Distortion	0.0900	0.9550
Gaussian Blur	0.0450	0.9960
Cropping (75%)	0.1300	0.9100
JPEG Compression (Q=90)	0.0350	0.9990
Median Filter (Kernel=9)	0.0800	0.9600
Noise (Level=40)	0.0900	0.9500
Rotation (45°)	0.1600	0.8850
Sharpening	0.1400	0.9250

only 19.45 *ms*, while the blind watermark extraction process completes in 9.89 *ms*. These results demonstrate that the proposed method meets the real-time performance requirements of clinical imaging workflows while maintaining strong security and robustness guarantees.

5.6 Comparative study

A comparative evaluation was conducted to benchmark the proposed watermarking framework against several representative methods reported in the literature. As summarized in Table 7, the proposed approach achieves a PSNR of 51.64 dB, substantially exceeding the performance of existing techniques by 8–17 dB. In addition, the method attains an NCC of 0.9998, indicating highly accurate watermark recovery. These results highlight the effectiveness of integrating orientation-adaptive I-BSIF feature extraction with spread-spectrum embedding in the wavelet domain for medical image watermarking.

Table 7: Comparative performance analysis

Method	PSNR (dB)	NCC
Proposed Approach	51.6418	0.9998
[8]	41.5081	0.9283
[31]	35.47	0.9150
[30]	34.60	0.9989
[12]	43.9986	0.9953

Table 8: Comparative performance analysis of fingerprint feature extraction methods

Method	Extraction Time (seconds)	Reference
I-BSIF (Proposed)	0.011402	-
LBP	0.407516	[26]
SIFT	0.530149	[40]
Gabor	0.950701	[41]

The orientation-guided I-BSIF descriptor extracts features from a 300×300 fingerprint in only 11.4 ms, which is approximately $36\times$ faster than LBP, and $46\times$ faster than SIFT, illustrated in Table 8. This linear-time complexity and negligible overhead over standard BSIF confirm its suitability for real-time clinical workflows while preserving rotation invariance.

The lightweight FlexenTech cipher encrypts and decrypts a compact biometric vector in $91\text{ }\mu\text{s}$ and $62\text{ }\mu\text{s}$, respectively, which is at least an order of magnitude faster than the chaotic watermark encryption reported by the selective AES module employed by Alsaraireh et al. [21] ($\approx 1.2\text{ ms}$) and Nazari and Mehrabian [22] ($\approx 2.1\text{ ms}$). This linear-time permutation scheme thus incurs virtually no latency overhead in the complete pipeline.

The robustness of the proposed scheme under lossy compression was further investigated by varying the JPEG quality factor, as illustrated in Figure 13. The NCC values remain consistently high across a wide range of compression levels, decreasing to approximately 0.91 at severe compression (quality factor $Q = 20$) and approaching unity as the quality factor increases. This stable behavior demonstrates that the embedded watermark remains reliably detectable even under aggressive compression, reinforcing the suitability of the proposed framework for secure medical image storage and transmission.

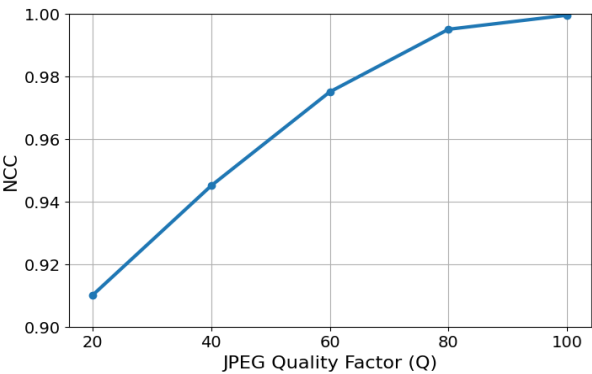


Figure 13: NCC vs. JPEG compression quality factor.

The results in Table 9 indicate that the proposed scheme achieves consistently high NCC in various attacks, compared to the recent literature. Notably, the scheme maintains an NCC of 0.9100 under 75% cropping, significantly outperforming Zear et al. [30], who reported an NCC of 0.6370 for the same intensity. Furthermore, while the methods of Zear et al. and Chauhan [12] are vulnerable to minor rotations that yield NCC values of approximately 0.6295 at just 5° , the proposed system achieves a robust 0.8850 under a severe 45° rotation. Although Taj et al. [15] and El-Soud et al. [18] achieve near-perfect scores under minor perturbations, the proposed approach offers a more balanced trade-off, ensuring survival against aggressive spatial transformations, which are critical for maintaining biometric integrity in clinical telemedicine environments.

Table 9: Robustness comparison: Normalized Cross-Correlation (NCC) performance against state-of-the-art methods

Method	Rotation	Cropping	Noise	Gaussian Blur	JPEG (Q)
Proposed Method (NCC)	0.8850 (45°)	0.9100 (75%)	0.9500 (L40)	0.9960	0.9990 (90)
[30]	0.6295 (5°)	0.6370 (75%)	0.9201 (S&P)	0.9539	0.9965 (80)
[15]	0.9900 (10°)	1.0000 (10%)	0.9980 (5%)	1.0000	0.9990 (90)
[12]	0.6295 (5°)	—	1.0000 (v0.01)	—	0.9953 (90)
[18]	0.9991 (Avg)	—	1.0000 (5%)	1.0000	0.9965 (80)

The latency from receiving a watermarked image to making an authentication decision remains below 20 ms on conventional computing hardware. This performance is well within the acceptable delay for interactive teleradiology and PACS/DICOM workflows [2]. The combination of integer-only LWT and key-dependent permutations also makes the framework suitable for resource-constrained edge devices (e.g., ultrasound scanners or portable X-ray machines) that lack dedicated cryptographic accelerators. Because FlexenTech relies exclusively on integer arithmetic and avoids substitution-box lookups, it can be implemented with a minimal memory footprint, further supporting deployment in IoT-based healthcare environments [21].

6 Conclusion

Secure transmission and authentication of medical images are fundamental requirements in modern telemedicine, where diagnostic integrity and patient privacy must be preserved simultaneously. This work addresses the challenge of achieving robust, imperceptible, and identity-aware authentication by proposing a unified blind reversible watermarking framework that tightly integrates biometric verification with transform-domain watermarking.

The proposed methodology combines orientation-guided Improved Binary Statistical Image Features (I-BSIF) for extracting compact and rotation-invariant fingerprint signatures with FlexenTech permutation-based encryption to secure the biometric template. The encrypted biometric vector is then embedded using adaptive spread-spectrum modulation within mid-frequency subbands of the LWT, ensuring reversibility, blind extraction, and computational efficiency. This synergistic design enables strong security guarantees while maintaining compatibility with real-time medical imaging workflows.

Extensive experimental results demonstrate that the framework achieves excellent imperceptibility, with PSNR values consistently exceeding 51 dB and SSIM values approaching unity. These results confirm that the embedded watermark introduces negligible visual distortion and does not compromise diagnostic content, both of which are essential for clinical acceptance.

From a security and robustness perspective, the system exhibits strong resilience to signal-processing and geometric attacks. High NCC values are preserved even under severe conditions, including 75% cropping (NCC = 0.9100) and 45° rotation (NCC = 0.8850). Moreover, FlexenTech encryption achieves near-zero correlation, balanced bit distributions, and brute-force resistance at a factorial scale, effectively protecting the biometric watermark against statistical and cryptanalytic attacks.

Clinically, this balanced performance, combining high security, robustness, and imperceptibility, makes the proposed framework well-suited for secure Electronic Health Record (EHR) systems, teleconsultation, and remote diagnostics. Future work will focus on enhancing resistance to severe geometric desynchronization, exploring robustness against deep-learning-based attacks, and optimizing the framework for mobile and edge-based mHealth applications.

Code availability

The source code implementing the proposed biometric watermarking framework, including all evaluation scripts and experimental configurations, is available at:

<https://github.com/FerikBrahim/BioRevMark>.

References

- [1] S. Sharma, R. Rawal and D. Shah, *Addressing the challenges of AI-based telemedicine: Best practices and lessons learned*, Journal of Education and Health Promotion, **1**, 338, (2023).
- [2] S. Gull and S. A. Parah, *Advances in medical image watermarking: A state of the art review*, Multimedia Tools and Applications, **83**(1), 1407–1447, (2024).
- [3] B. Ferik, L. Laimeche, A. Meraoumia, A. Laouid, K. Chait and M. AlShaikh, *A blind digital watermarking approach using palmprint-embedded local binary patterns and arnold cat map transformations*, in *2024 6th International Conference on Pattern Analysis and Intelligent Systems (PAIS)*, (2024), pp. 1–8. doi: 10.1109/PAIS62114.2024.10541138
- [4] B. Ferik, L. Laimeche, A. Meraoumia, O. Aldabbas, M. AlShaikh, A. Laouid and M. Hammoudeh, *A multi-layered security framework for medical imaging: integrating compressed digital watermarking and blockchain*, IEEE Access, (2024).
- [5] Z. Huang, B. Feng and S. Xiang, *Robust reversible image watermarking scheme based on spread spectrum*, Journal of Visual Communication and Image Representation, **93**, 103808, (2023).
- [6] Y. Belhocine, A. Meraoumia, H. Bendjenna and M. Saiga, *Empowering biometric security: A paradigm shift in remote identification*, Systems and Computing, **1**(1), (2025). doi: 10.64409/sycom.v1.i1.4.
- [7] P. Pal, P. Chowdhuri and T. Si, *A novel watermarking scheme for medical image using support vector machine and lifting wavelet transform*, Multimedia Tools and Applications, **82**(26), 41187–41206, (2023).
- [8] L. Novamizanti, A. B. Suksmono, D. Danudirdjo and G. Budiman, *Robust reversible watermarking using stationary wavelet transform and multibit spread spectrum in medical images*, International Journal of Intelligent Engineering & Systems, **15**(3), (2022).

- [9] S. Medileh *et al.*, *A flexible encryption technique for the internet of things environment*, *Ad Hoc Networks*, **106**, 102240, (2020).
- [10] Z. Makhoulouf, A. Meraoumia, L. Laimeche and M. Y. Haouam, *Enhancing medical data security in e-Health systems using biometric-based watermarking*, *Applied Computer Science*, **20(1)**, 28–55, (2024).
- [11] B. Ferik, L. Laimeche, A. Meraoumia, A. Laouid and K. Chait, *Combining I-BSIF fingerprints and Flex-enTech for reversible medical image watermarking*, in *2025 International Conference on Recent Advances in Mathematics and Informatics (ICRAMI)*, (2025), pp. 1–8. doi: 10.1109/ICRAMI64946.2025.11472704.
- [12] D. S. Chauhan, A. K. Singh, A. Adarsh, B. Kumar and J. P. Saini, *Combining Mexican hat wavelet and spread spectrum for adaptive watermarking and its statistical detection using medical images*, *Multimedia Tools and Applications*, **78**, 12647–12661, (2019).
- [13] S. De, S. Maity, J. Bhaumik, P. Pal and D. Giri, *Spread-spectrum based a new secured robust image watermarking scheme*, *International Conference on Network Security and Blockchain Technology*, 73–87, (2024).
- [14] Z. Dai, C. Lian, Z. He, H. Jiang and Y. Wang, *A novel hybrid reversible-zero watermarking scheme to protect medical image*, *IEEE Access*, **10**, 58005–58016, (2022).
- [15] R. Taj, F. Tao, S. Kanwal, A. Almogren and A. U. Rehman, *A SURF and SVD-based robust zero-watermarking for medical image integrity*, *PLoS One*, **19(9)**, e0307619, (2024).
- [16] S. Bhalarao, I. A. Ansari and A. Kumar, *A reversible medical image watermarking for ROI tamper detection and recovery*, *Circuits, Systems, and Signal Processing*, **42**, 6701–6725, (2023).
- [17] R. Taj, F. Tao, S. Kanwal *et al.*, *A reversible-zero watermarking scheme for medical images*, *Scientific Reports*, **14**, 17320, (2024).
- [18] M. W. El-Soud, M. M. Eltoukhy, M. M. Abdel-Aziz, A. Alourani and K. M. Hosny, *Robust blind watermarking to secure color medical images using multidimensional-FFT fusing LFSR-encryption and LZW compression*, *IEEE Access*, **13**, 46054–46069, (2025).
- [19] M. Roy, D. M. Thounaojam and S. Pal, *A perceptual hash based blind-watermarking scheme for image authentication*, *Expert Systems with Applications*, **227**, 120237, (2023).
- [20] M. Rajendran, G. Chandrasekaran, M. Subramaniam and S. Subramaniam, *Optimal crypto-watermarking system for medical image protection*, *Traitement du Signal*, **41(6)**, 3327–3334, (2024).
- [21] S. Alsaraireh, A. Ahmad and Y. AbuHour, *New step in lightweight medical image encryption and authenticity*, *Mathematics*, **13**, 1799, (2025).
- [22] M. Nazari and M. Mehrabian, *A novel chaotic IWT-LSB blind watermarking approach with flexible capacity for secure transmission of authenticated medical images*, *Multimedia Tools and Applications*, **80(7)**, 10615–10655, (2021).
- [23] M. Mehrabi, V. Zarei and M. Ghanbari, *A highly robust medical image watermarking method for medical real-time applications*, *Journal of Medical Signals & Sensors*, **13(3)**, 199–207, (2023).
- [24] F. Castro, D. Impedovo and G. Pirlo, *A medical image encryption scheme for secure fingerprint-based authenticated transmission*, *Applied Sciences*, **13(10)**, 6099, (2023).
- [25] R. Taj, S. Kanwal, A. Alsirhani *et al.*, *Lightweight dual-watermarking framework for medical image authentication and integrity preservation*, *Scientific Reports*, **16**, 1018, (2026).
- [26] S. P. Vaidya, *Fingerprint-based robust medical image watermarking in hybrid transform*, *The Visual Computer*, **39(6)**, 2245–2260, (2023).
- [27] P. Garg and A. Jain, *A robust technique for biometric image authentication using invisible watermarking*, *Multimedia Tools and Applications*, **82(2)**, 2237–2253, (2023).
- [28] N. E. Chalabi, A. Attia, A. Bouziane and Z. Akhtar, *Face based person recognition mechanism using monogenic binarized statistical image features*, *Multimedia Tools and Applications*, **81(18)**, 25657–25674, (2022).
- [29] D. Muthusamy and R. Ponnusamy, *An efficient approach for finger vein verification to solving the biometric recognition technique*, *Pattern Recognition*, **164**, 111563, (2025).
- [30] A. Zear and P. K. Singh, *Secure and robust color image dual watermarking based on LWT-DCT-SVD*, *Multimedia Tools and Applications*, **81(19)**, 26721–26738, (2022).
- [31] S. Jaiswal and M. K. Pandey, *Robust digital image watermarking using LWT and Random-Subspace-1DLDA with PCA based statistical feature reduction*, *Proceedings of ICCSEA*, 1–6, (2022).
- [32] J. You and Y. Zhou, *Two-stage watermark removal framework for spread spectrum watermarking*, *IEEE Transactions on Multimedia*, (2024).
- [33] pkdarabi Tumor, *Brain Tumor Dataset*, Available: <https://www.kaggle.com/datasets/darren2020/ct-to-mri-cgan/data>, (2026).
- [34] Y. Cai, M. Li, S. Liu and C. Zhou, *CycleGAN-based image translation from MRI to CT scans*, *Journal of Physics: Conference Series*, **2646(1)**, 012016, (2023).

- [35] NIH Clinical Center, *ChestX-ray14 Dataset*, Available: <https://www.kaggle.com/datasets/nih-chest-xrays/data>, (2026).
- [36] Orville, *Human Bone Fractures Multi-modal Image Dataset (HBF MID)*, Available: <https://www.kaggle.com/datasets/orville/human-bone-fractures-image-dataset-hbfmid>, (2026).
- [37] B. Artley, *Lumbar Coordinate Pretraining Dataset*, Available: <https://www.kaggle.com/datasets/brendanartley/lumbar-coordinate-pretraining-dataset>, (2026).
- [38] N. Singh, *FVC2002 Fingerprints Dataset*, Available: <https://www.kaggle.com/datasets/nageshsingh/fvc2002-fingerprints>, (2024).
- [39] J. K. Appati, P. K. Nartey, E. Owusu and I. W. Denwar, *Implementation of a transform-minutiae fusion-based model for fingerprint recognition*, International Journal of Mathematics and Mathematical Sciences, **2021**(1), 5545488, (2021).
- [40] J. Dong, J. Chen, X. Xie, J. Lai, and H. Chen, "Survey on adversarial attack and defense for medical image analysis: Methods and challenges," *ACM Computing Surveys*, vol. 57, no. 3, pp. 1–38, 2024.
- [41] M. Ahsan, M. A. Based, J. Haider, M. Kowalski, et al., "An intelligent system for automatic fingerprint identification using feature fusion by Gabor filter and deep learning," *Computers and Electrical Engineering*, vol. 95, p. 107387, 2021.

Author information

Brahim Ferik, Laboratory of Mathematics, Informatics and Systems (LAMIS), University of Larbi Tebessi, Tebessa, Algeria.

E-mail: brahim.ferik@univ-tebessa.dz

Lakhdar Laimeche, Laboratory of Mathematics, Informatics and Systems (LAMIS), University of Larbi Tebessi, Tebessa, Algeria.

E-mail: lakhdar.laimeche@univ-tebessa.dz

Abdallah Meraoumia, Laboratory of Mathematics, Informatics and Systems (LAMIS), University of Larbi Tebessi, Tebessa, Algeria.

E-mail: ameraoumia@univ-tebessa.dz

Abdelkader Laouid, Artificial Intelligence and its Applications Laboratory (LIAP), University of El Oued, El Oued, Algeria.

E-mail: abdelkader-laouid@univ-eloued.dz

Khaled Chait, Artificial Intelligence and its Applications Laboratory (LIAP), University of El Oued, El Oued, Algeria.

E-mail: chait-khaled@univ-eloued.dz