A Lightweight and Robust APBT–LBP Deep Feature Zero-Watermarking Framework with DNA Encryption for Medical Images

Ranjan Kumar Senapati[1], Prasanth Mankar[2], B Padmaja[3],
Chilamakuru Nagesh[4], Pradeep Kumar*[5]*, Gandikota Ramu[6], Gandharba Swain[7]
Department of ECE, VNR VJIET, Hyderabad, Telangana, India, 500018[1]
Department of ECE, Vasavi College of Engineering, Ibrahimbagh, Hyderabad, Telangana, India, 500031[2]
Department of CSE (AI & ML), Institute of Aeronautical Engineering, Hyderabad, Telangana, India, 500043[3]
Department of CSE, Srinivasa Ramanujan Institute of Technology, Anantapur, Andhra Pradesh, India, 515405[4]
Department of ECE, VNR VJIET, Hyderabad, Telangana, India, 500018[5]
Department of CSE, Aditya University, Surampalem, Andhra Pradesh, 533437, India[6]
Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, 522302, Guntur, Andhra Pradesh, India[7]

***Abstract*—The protection of medical images in healthcare services has become important due to the adoption of telemedicine and cloud-based healthcare services. Conventional watermarking methods embed information directly into the host image, which may introduce subtle distortions and potentially affect diagnostic accuracy. This paper addresses the problem by introducing a robust zero-watermarking scheme that preserves the original medical image without any modification. The proposed approach is designed on a hybrid feature extraction scheme. Initially, desired regions of interest are identified using variance-based analysis. Local Binary Pattern (LBP) is then applied to capture fine texture details. Further, the All-Phase Biorthogonal Transform (APBT) is used to obtain stable low-frequency information. These features are subsequently pipelined through the lightweight VGG16 convolutional neural network to extract high-level semantic representations. The resulting features are fused, normalized, encrypted, and converted into binary form using Quantization Index Modulation (QIM). DNA encryption is applied to the watermark to produce a secure zero-watermark key that is stored externally. Extensive experiments conducted under a wide range of signal processing and geometric attacks show the effectiveness of the proposed method. The results show high normalized correlation above 0.99, bit error rates ($\leq 0.1\%$), and complete preservation of higher image quality, making the approach suitable for medical image authentication and copyright protection.**

***Keywords*—Zero watermarking; medical image authentication; deep learning; APBT transform; local binary pattern; CNN feature extraction; robust watermarking**

I. Introduction

The rapid growth of telemedicine and cloud-enabled healthcare platforms has significantly changed how medical images are stored, accessed, and exchanged. Today, clinicians can review patient data and collaborate with specialists across different locations almost instantly, which has greatly improved the speed and quality of diagnosis and treatment. At the same time, this increased digital connectivity brings new challenges. Medical data is now more vulnerable to unauthorized access, manipulation, and misuse. Since medical images are directly involved in clinical decisions, ensuring their authenticity and rightful ownership is critical. Even a small modification in an image can result in incorrect diagnosis, potentially affecting patient safety and raising serious legal concerns.

Conventional watermarking methods secure digital images by embedding ownership information within the host image. These approaches work well for general multimedia data. However, such an approach is not always appropriate for medical images [1], [2], [3], [4]. This is due to the fact that any modification, even if it is not perceived by the human eye, can influence diagnostic evaluation. To circumvent this deficiency, zero-watermarking has gained attention as a safe side alternative. It derives a watermark from the inherent characteristics of the image. Instead of altering the original image. Hence, preserve its quality entirely.

However, the effectiveness of zero-watermarking strongly depends on how reliably image features can be retrieved. In a practical scenario, medical images often undergo operations such as signal processing and geometric transformations. These processes can distort image features and, hence, make it difficult to regenerate a good-quality watermark. Therefore, developing feature extraction mechanisms that are stable and distinctive under attack conditions remains an important research challenge.

Among various feature descriptors, texture-based methods like Local Binary Pattern (LBP) have shown good performance in capturing fine local details [5]. LBP is simple to compute and relatively robust against illumination and noise. This makes it suitable for medical imaging applications. It focuses on local patterns, which means it may overlook the overall structure of the image. To address this gap, it is important to combine LBP with other techniques that can capture more global and stable information.

Transform-domain methods offer an additional advantage by representing image content in terms of frequency components, where low-frequency information is generally more resistant to common image processing operations. At the same time, deep learning models have demonstrated remarkable

*Corresponding author.

capability in extracting meaningful and highly discriminative features. In particular, convolutional neural networks such as VGG16 can learn complex image representations that traditional methods may fail to capture. However, deep features alone may not always remain consistent under severe distortions.

Motivated by these observations, this work introduces a hybrid zero-watermarking framework that integrates multiple feature extraction strategies. Initially, stable regions of interest (ROI) are selected based on variance analysis, ensuring that features are derived from reliable portions of the image. LBP is then used to capture local texture characteristics, while the same regions are processed using the All-Phase Biorthogonal Transform (APBT) to obtain robust low-frequency information. These combined features are further refined using the VGG16 network to extract higher-level representations. By merging handcrafted and deep features, the proposed approach aims to improve both robustness and consistency.

Finally, the extracted features are used to generate a secure zero-watermark key, which enables ownership verification without modifying the original image. Through this multi-layered feature integration, the proposed method attempts to overcome the limitations of existing techniques and offers a more reliable solution for protecting medical image ownership in modern healthcare environments.

The major contributions of this work are as follows:

- A hybrid deep learning-based zero-watermarking framework is proposed for medical image authentication without modifying the original image.
- Stable ROI blocks are selected using variance analysis to ensure robust feature extraction.
- LBP, APBT, and CNN (VGG16) are combined to extract complementary texture, frequency, and deep features.
- QIM is used to binarize features into a compact and discriminative sequence.
- ORB-based alignment is applied to handle geometric distortions.
- Robustness is validated against 42 signal processing and geometric attacks.

II. Related Work

Conventional feature extraction algorithms such as SIFT, SURF, and KAZE, are often combined with transformed domain watermarking to achieve robustness to rotation, scale, and translation asserts. Binary feature extraction algorithms such as BRIEF, ORB, and BRISK have faster run time, making them suitable for real-time applications. These algorithms also combine with transformed domain watermarking techniques. Several works have been reported with these combinations.

In this context, Senapati et al. [6] combined the SIFT feature with DTT to improve the robustness to RST attacks. Similarly, Gao and Chen [7] applied a fusion technique, which includes DWT-SVD with SURF, RANSAC and improved ABC algorithms to improve security, robustness, and imperceptibility of the watermark scheme. Further, Soualmi et al. [8] proposed a medical image watermarking approach for tamper detection that combines SURF keypoints, Weber descriptors, and the Arnold transform. The method identifies salient points within the ROI using SURF and embeds the watermark in their surrounding regions, while Weber descriptors are used for reliable watermark embedding and extraction. Another work carried by Ray et al. [9] utilizes KAZE features to construct a perceptual hash of the watermark, which is then embedded using transform-domain techniques (LWT-SVD). The approach improves robustness and flexibility by removing size constraints on the watermark and enhancing resistance to attacks.

In contrast to the above methods, which embed watermark information into the host image, zero-watermarking methods generate a watermark signature based on extracted image features. Several studies have used moment invariants, texture descriptors, and transform-domain coefficients for zero watermark generation [10], [11]. Orthogonal moments zero-watermarking, such as Zernike [12], Tchebichef [13], Legendre-Fourier [14], etc. have been proposed because these are inherently invariant to scaling, translation, and rotation. These approaches construct a feature matrix by computing significant moment parameters.

Based upon these moment-based techniques, a multiple-zero-watermarking framework for protecting medical images in IoMT applications is reported in [15]. It uses multi-channel fractional Legendre Fourier moments (MFrLFM) due to its high stability, accuracy, and geometric invariance. The scheme is realized on a Raspberry Pi board to evaluate its aptness for IoMT applications. However, the method is evaluated under a few attack scenarios.

To further enhance robustness and resolve the computational issues, a zero-watermarking scheme based on fractional-order radial harmonic Fourier moments (FoRHFMs) is proposed by [16]. The authors tackle the issue of numerical instability, which is inherent in continuous orthogonal moments, by proposing integer-order radial harmonic Fourier moments (IoRHFMs) to their fractional-order counterparts (FoRHFMs). This improves the computational stability and reliability. The experimental results show that this algorithm is resistant to lossless copyright protection of medical images and robust to all kinds of attacks.

In addition to moment-based approaches, hybrid feature-based schemes have also been investigated. Gharib et al. [17] presented a zero-watermarking method for color images. LBP and VGG-19 features are fused to generate a feature matrix. DWT and DCT improve the feature representation. The encrypted watermark is XORed with the improved feature matrix to generate a zero-watermark. Higher robustness and imperceptibility are achieved for a set of 12 images. However, this method has no stable ROI, and geometric alignment robustness is missing. In contrast to zero-watermarking approaches, embedding-based methods are still being investigated for improved performance. Anand et al. [18] proposed a multimodality image fusion scheme using NSST and DTCWT to generate a watermark image. The combination of NSST, BEMD, and MSVD conceals the generated mark in the host image. Weighted HOG-based optimization is applied to trade off between imperceptibility and robustness. The method shows an improvement of 47.65% compared with a standard

baseline scheme. Unlike [18], which embeds a watermark using NSST–BEMD–MSVD, our proposed method avoids modifying the host image and ensures higher medical data integrity.

To overcome the limitations of handcrafted and transform-based features, recently, deep learning-based watermarking has become popular among researchers. This is due to the fact that many pretrained models can be directly used for extracting the deep semantic features. The encrypted watermark can be embedded with the deep features. Further, deep learning can adapt to different image features to enhance higher robustness and imperceptibility. However, the unique nature of medical imaging data poses significant challenges, including limited availability of large-scale annotated datasets and the high cost associated with expert labeling. These constraints make it difficult to train deep neural networks from scratch for reliable feature extraction. These limitations are circumvented using transfer learning, where knowledge from a pre-trained model is used. The pre-trained model is trained on a large dataset and adapted to a target domain with limited data. This improves generalization performance and reduces training requirements.

Based on these advancements, several deep learning-based watermarking algorithms have been proposed. Fan et al. [19] extract image features using Inception V3 CNN and then encrypt the hidden watermark using the chaotic map. The method shows robustness to a wide range of geometric assertions. However, it is less robust to common attacks. Similarly, Dong et al. [20] used an enhanced NasNet-mobile CNN. It also used DCT features to embed watermarks. The scheme shows strong resistance to most of the assaults. In addition, a multiwatermarking algorithm approach using GoogleNet transfer learning for medical images is proposed by Zhang et al. [21]. Henon chaos encryption is used to hide multiple pieces of watermark information. The deep semantic features XORed with the secret watermark, and the generated key is stored in a 3rd party authority. The framework provides good robustness to conventional and geometrical attacks. Similarly, Sheng et al. [22] used ResNet50 to extract deep features. Then DCT transformation and a perceptual hash function are used to generate a feature vector.

Recently, a Swin Transformer-based zero watermarking is suggested by Han et al. [23] to improve the security of medical images in the metaverse healthcare system. This Swin Transformer is pretrained. The deep features generated from the host medical images by the transformer show good generalization performance. A mean hashing algorithm is used to generate multiscale and binary feature vectors. The watermark is encrypted using a logistic chaotic encryption method, and it is XORed with the binary feature vector to create a zero-watermark. The scheme exhibits robustness against all kinds of attacks and provides privacy protection for medical image transmission in the metaverse.

In a related direction, another work by Han et al. [24] addresses the critical issue of protecting privacy and ensuring data security in teledermatology systems within the IoMT. The zero-watermarking method uses federated learning and sparse autoencoders to extract secure image features without altering the original medical image. By applying 2D-DCT on these features, the scheme creates a watermark that is robust to attacks while preserving image integrity and patient privacy.

Furthermore, a zero-watermarking algorithm using multiple circular statistical features of the medical image is proposed by Wang et al. [25]. It combines DCT and SVD for feature stability and uses Arnold transform with XOR operation to securely generate the zero watermark without modifying the original image. The method also includes a blind image correction technique and demonstrates strong robustness against noise, filtering, and geometric attacks.

Motivated by the above limitations and improvements, the proposed zero-watermarking framework, extracting stable and discriminative features from medical images is a critical step. Initially, a stable Region of Interest (ROI) is identified to ensure robustness against most of the attacks. The selected ROI is then transformed using the All-Phase Biorthogonal Transform (APBT) to obtain invariant frequency-domain representations. These transformed coefficients are subsequently fed into a pretrained VGG16 model, originally trained on the large-scale ImageNet dataset, to extract deep hierarchical features. To further adapt the model to the medical domain, fine-tuning is performed using the constructed medical image dataset, enabling the network to capture domain-specific characteristics more effectively. The resulting deep features are then quantized using Quantization Index Modulation (QIM) to generate a robust binary sequence, which serves as the zero watermark. This integration of ROI selection, APBT transformation, transfer learning-based deep feature extraction, and QIM-based encoding ensures improved resistance and stability of the proposed zero-watermarking scheme under various attacks.

III. Preliminaries

A. All-Phase Biorthogonal Transform

All-phase Biorthogonal Transform (APBT) can be understood as a sequency-filtered version of the DCT. The idea is that APBT modifies the conventional DCT basis through all-phase preprocessing and sequency filtering, which improves phase consistency and energy compaction [26]. The APBT has better energy compaction in low frequencies and attenuation characteristics at high frequencies.

Suppose χ is an image which is cropped into $B \times B$ image blocks. and A represents the APBT matrix of the block. The APBT transform coefficients 'Y' can be expressed as:

$$Y = A\chi A^T \tag{1}$$

where, A^T is the transpose matrix of χ. To reconstruct the image χ, we can write

$$\chi = A^{-1}Y(A^{-1})^T \tag{2}$$

A^{-1} is the inverse matrix of A.

The transform matrix A is set in different forms as specified in Eq. 3 and 4. The corresponding transforms are denoted as an APBT and its inverse, IAPBT, respectively.

$$A_1(p,q) = \begin{cases} \frac{B-p}{B^2}, & p = 0,1,..B-1, q = 0 \\ \frac{(B-p)cos\frac{pq\pi}{B} - csc\frac{q\pi}{B} sin\frac{pq\pi}{B}}{B^2}, & p = 1,2,....B-1, \\ & q = 1,2,....B-1. \end{cases} \tag{3}$$

$$A_2(p,q) = \begin{cases} \frac{1}{B}, & p = 0, q = 0,1,..B-1. \\ \frac{B-p+\sqrt{(2)}-1}{B^2}.cos\frac{p(2q+1)\pi}{B}, & p = 0,1,2.....B-1, \\ ; & q = 1,2,....B-1. \end{cases} \tag{4}$$

B. DNA Encryption and Decryption

DNA encryption is employed on VGG features and the watermark to enhance the security of the zero-watermark. The binary watermark is first encoded into a DNA chain using a predefined encoding algorithm coupled with logical operations such as complement and permutation. This strategy significantly increases the key space and ensures strong confusion and diffusion operation. This enhances the system's ability to prevent brute-force attacks. A brief description of the DNA encryption and decryption mechanism is as follows:

DNA is composed of four fundamental nucleic acid bases: Adenine (A), Cytosine (C), Guanine (G), and Thymine (T). These bases store genetic information in the form of coded sequences. According to the Watson–Crick pairing principle, Adenine pairs with Thymine (A–T) and Guanine pairs with Cytosine (G–C) [27].

In DNA-based data representation, binary information can be mapped to these bases by encoding every two bits into one nucleotide. Based on the encoding and decoding constraints governed by complementary pairing rules, eight valid encoding schemes can be defined, as illustrated in Table I.

TABLE I. DNA ENCODING RULE

Rules	Watson-Crick Complementary Rules							
	1	2	3	4	5	6	7	8
00	A	A	C	G	C	G	T	T
01	C	G	A	A	T	T	C	G
10	G	C	T	T	A	A	G	C
11	T	T	G	C	G	C	A	A

In addition to encoding and decoding, DNA sequences can perform several operations such as addition, subtraction, complementation, and XOR. Nevertheless, the XOR operation is widely used in encryption for its simplicity and reversibility. Table II shows the DNA-based XOR operation, where each nucleotide in a row is combined with a nucleotide in a column to produce a corresponding output.

TABLE II. DNA XOR OPERATION BETWEEN EACH ELEMENT IN ROW AND EACH ELEMENT IN COLUMN

XOR row/column	A	C	G	T
A	A	C	G	T
C	C	A	C	G
G	G	T	A	C
T	T	G	T	A

To illustrate the encoding and encryption process, consider a binary sequence "10101101". This sequence is first divided into 2-bit groups and encoded into DNA bases according to a selected rule from Table I. For example, using Rule 2, the sequence is converted into a DNA string. Next, a predefined DNA key (e.g., "ACGT") is applied, and a DNA XOR operation is performed between the encoded sequence and the key, resulting in a new DNA sequence. This sequence is then decoded back into a binary form using the same encoding rule, producing the encrypted binary output.

The decryption process follows the reverse steps, where the encrypted binary sequence is converted back to DNA bases, XORed with the same key, and finally decoded to recover the original binary data. The pseudocode for the DNA-based encryption process is provided in Algorithm 1.

Unlike conventional encryption methods such as AES and RSA, DNA provides biologically inspired encoding. The XOR-based operation is computationally simple and well-suited for binary feature encryption. It enhances the features' confusion and diffusion properties while maintaining a lightweight zero-watermark operation. In the proposed scheme, DNA encryption is applied only to compact binary features instead of the full image. The objective of selecting DNA scheme is not to replace other cryptographic algorithms, but to provide a lightweight security layer for processing in real-time.

Algorithm 1 DNA-Based Feature Encryption

Require: Binary feature vector F_b
Ensure: Encrypted DNA sequence E_{dna}
1: Convert binary vector F_b into DNA sequence F_{dna} using encoding rule R
2: Generate random DNA key sequence K_{dna} of the same length as F_{dna}
3: **for** $i = 1$ to length(F_{dna}) **do**
4: $E_{dna}(i) \leftarrow$DNA_XOR($F_{dna}(i), K_{dna}(i)$)
5: **end for**
6: **return** E_{dna}

C. Feature Extraction

Efficient feature extraction is a vital step to ensure resilience under various attacks. We have proposed two complementary methods to extract features from the host medical image. LBP extracts texture features from the image, while VGG16 extracts deep-level semantic features.

1) Local binary pattern: Local Binary Pattern (LBP) is known as a texture descriptor. It efficiently encodes the local structure of an image by comparing a pixel intensity with the neighboring pixel intensities [28]. The image is partitioned, and LBP values are estimated and finally combined into a global representation. The computation of the LBP value for a given pixel is as follows:

$$S(p,q) = \begin{cases} 1, \text{if } \ g(p) \geq g(q) \\ 0, \text{otherwise} \end{cases} \tag{5}$$

The $g(p)$ and $g(q)$ in Eq. 5 represent the pixel intensities of the neighboring and center pixel, respectively. This operation provides texture analysis while ensuring robustness across various illumination conditions. Fig. 1 shows the generated texture map from the host medical image.

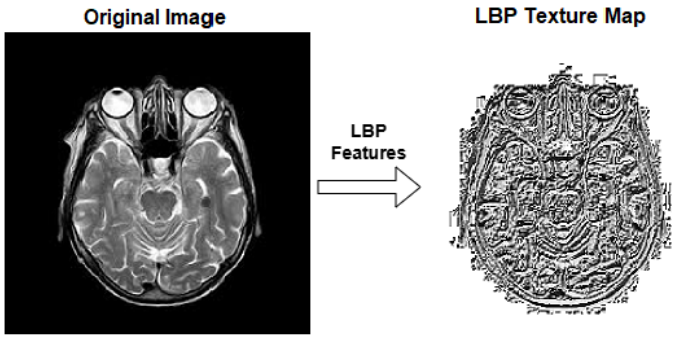


Fig. 1. LBP feature map of the "brain" image, showing pixel-wise texture encoding.

2) VGG-16 deep features: The VGG16 is a deep CNN that consists of 13 convolution layers and 2 fully connected (FC) layers. This gives a total of 15 layers. The output of the final FC is connected to a ReLU layer, which maps all the features to be positive. The VGG16 is a pretrained CNN that has weights and biases trained by ImageNet. It generates hierarchical features. The output feature map of the layer $X^{(l)}$ after convolution, activation, and pooling is fed to the next layer. In VGG16, the deep feature vector is obtained after the final convolution block and flattening.

The equation for deep features:

$$Z^{(l)} = W^{(l)} * X^{(l-1)} + b^{(l)} \tag{6}$$

$$A^{(l)} = \text{ReLU}\left(Z^{(l)}\right) \tag{7}$$

$$P^{(l)} = \text{MaxPool}\left(A^{(l)}\right) \tag{8}$$

$$X^{(l)} = P^{(l)} \tag{9}$$

$$f = \text{vec}\left(X^{(L)}\right) \tag{10}$$

$$F = \sigma(Wf + b) \tag{11}$$

where,

- $X^{(l-1)}$: Input feature map of layer $(l-1)$
- $W^{(l)}$: Convolution kernel weights
- $b^{(l)}$: Bias term
- $*$: convolution operation
- $\sigma(.)$: Nonlinear activation function (ReLU)
- $P^{(l)}$ Pooled feature map
- $X^{(l)}$: Output feature map of layer
- $X^{(L)}$: Denotes the output feature map from the final convolutional layer.
- f: Flattening operation,
- W: Contains the learned parameters that connect the input feature vector to the output neurons. These values are learned during the training phase of the CNN.
- F: Fxtracted deep feature descriptor used for watermark generation

$$f \in \mathbb{R}^{25088}, \text{and } F \in \mathbb{R}^{4096} \tag{12}$$

The number 25088 represents the total number of elements in the final convolution feature map of VGG16 before it enters the fully connected layers. This vector is passed to the fully connected layer (fc6) and then fc7, which are designed with 4096 neurons. fc7 output passes through ReLU, and the resulting 4096-dimensional vector is typically used as the deep feature descriptor.

Fig. 2 shows the VGG16 network used in the proposed method to extract deep semantic features at the output of the ReLU layer. The network learn increasing abstract visual representation at the output of each layer

Feature Fusion: The APBT, LBP, and VGG16 descriptors are integrated to form a unified feature representation, improving the discriminative capability of the system. LBP effectively characterizes local texture patterns, whereas VGG19 extracts high-level semantic and structural information from the image. The fused feature vector captures both regional texture details and global contextual information. This fused representation improves the robustness of the model against a wide range of image attacks.

IV. Proposed Zero Watermarking Framework

The proposed zero-watermarking system is depicted in Fig. 3. It consists of two major stages: registration and verification.

In the registration stage, the APBT and LBP feature sets are encrypted using a DNA algorithm before being fed to the VGG model for high-level semantic representation. After feature normalization and binarization, the watermark is encrypted separately using the same DNA encoding scheme. A hash derived from the host image is subsequently incorporated to bind the watermark to the host medical image. Finally, a zero-watermark key is generated and securely stored without altering the original image. Algorithm 2 presents the proposed zero-watermarking method.

The registration pipeline includes:

- Input medical image followed by preprocessing
- Stable ROI selection
- APBT-LBP feature extraction and Feature fusion
- DNA encryption
- CNN-based deep feature extraction
- Feature binarization using QIM
- Zero watermark generation
- Key storage
- Watermark verification

In the verification stage, the distorted test image is aligned with the original using ORB feature-based matching to handle

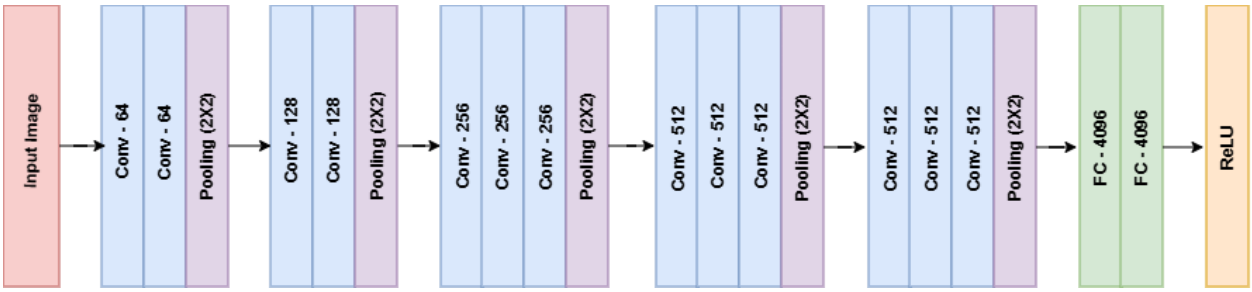


Fig. 2. VGG16 architecture used for feature map extraction.

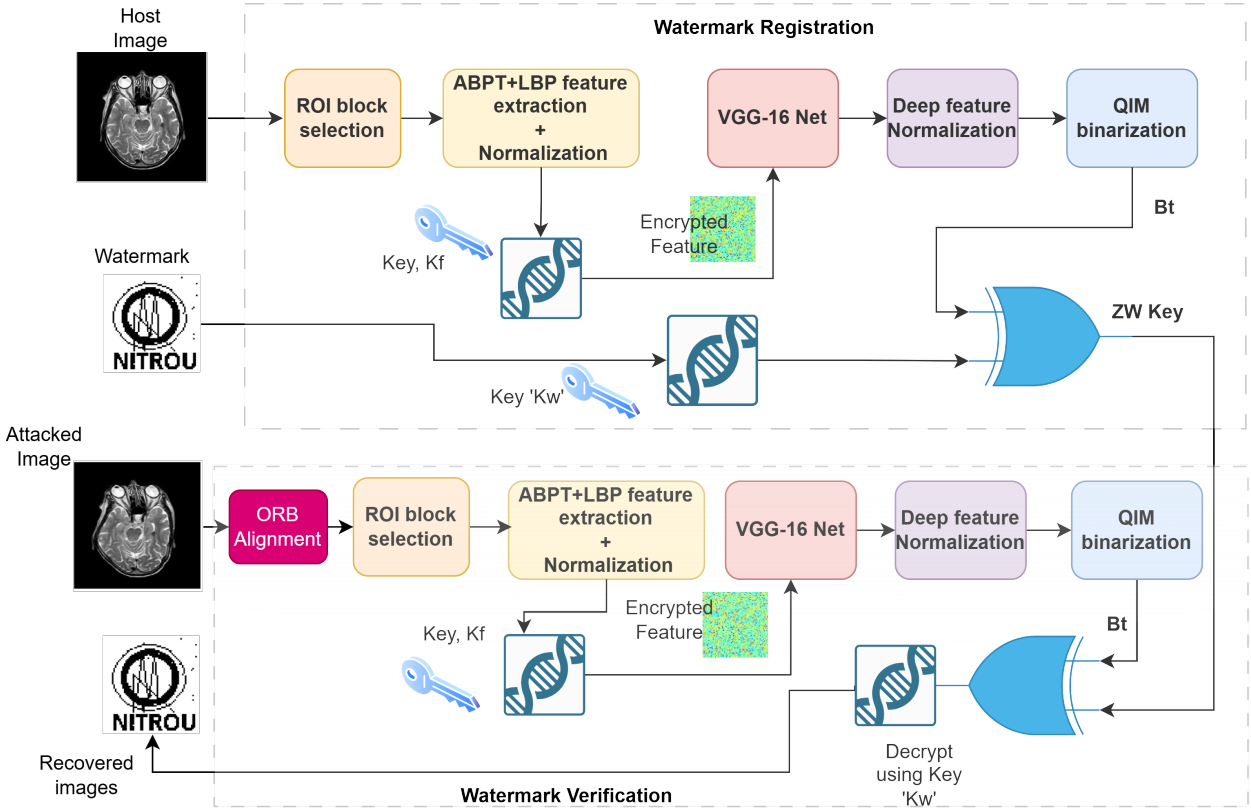


Fig. 3. Block diagram of the proposed scheme.

geometric imbalance. The same stable regions are then used to match feature consistency. The regions undergo the encoding, deep feature extraction, normalization, and binarization. The encrypted watermark is retrieved and decrypted using the stored zero-watermark key. Finally, the retrieved watermark is compared with the original watermark to evaluate robustness. Algorithm 3 presents the proposed watermark verification method.

The verification pipeline includes:

- Input attacked image
- Geometric alignment
- stable ROI extraction
- APBT+LBP Feature extraction
- Deep feature generation
- Binary feature generation using QIM
- Watermark recovery
- DNA decryption
- Recovered watermark

A. Stable ROI Block Selection

The input medical image is divided into non-overlapping blocks of size 8×8. For each block, the variance is computed:

$$Var(B) = \frac{1}{N} \sum_{i=0}^{N} (B_i - \mu)^2 \tag{13}$$

Blocks with variance greater than a predefined threshold are considered stable blocks. These blocks contain rich struc-

tural information and are less sensitive to image processing attacks.

B. APBT+LBP Feature Extraction

After the selection of stable ROI blocks based on variance, APBT, and LBP features of the ROI blocks are concatenated. APBT is effective in preserving signal energy and suppressing boundary artifacts. Only the low-frequency components of size (4×4) are retained in APBT because they are less sensitive to common signal processing operations and contribute to the stability of the feature representation against various attacks. LBP encodes the relationship between a pixel and its neighboring pixel to generate a compact representation of micro-patterns such as edges and textures. This enhances the robustness against illumination changes and noise variations. A combination of these features enables the algorithm to extract robust features. The features are then normalized and concatenated to form a unified feature vector. The aggregation of these features results in a comprehensive feature map, which is subsequently used for further processing in the zero-watermark generation. The details of the mathematical steps are developed below.

The low-frequency coefficients of APBT for each selected ROI block can be represented as:

$$F_{APBT} = \{c_1, c_2, \ldots, c_m\} \tag{14}$$

where, c_i denotes the normalized low-frequency APBT coefficients of the selected ROI blocks. The subsequent LBP texture features are computed from the same ROI regions and represented as

$$F_{LBP} = \{l_1, l_2, \ldots, l_n\} \tag{15}$$

where, l_i represents the normalized LBP histogram features.

The fusion of transform-domain and texture-domain features are concatenated to form a discriminative hybrid feature vector:

$$F = [F_{APBT}; F_{LBP}] \tag{16}$$

The fused feature vector is reshaped into a feature image and resized to 224×224 to be compatible with the pretrained VGG-16 network. Deep features are subsequently extracted from the fully connected layer ($fc7$) of VGG16 and expressed as:

$$F_d = \phi_{VGG16}(F) \tag{17}$$

The $\phi_{VGG16}(\cdot)$ denotes the nonlinear deep feature mapping function of the pretrained VGG16 model. Since the network parameters remain fixed during execution, the possibility of overfitting is reduced. The combination of ABPT-LBP and deep features improves feature generalization. In the subsequent operations, the features are normalized prior to QIM-based binarization and watermark generation.

C. Feature Normalization

The feature vector is normalized using z-score normalization:

$$F_n = \frac{F_d - \mu}{\sigma} \tag{18}$$

where, μ and σ represent the mean and standard deviation of the features.

D. Feature Binarization Using QIM

Quantization Index Modulation is used to convert deep features into binary form:

$$b_i = mod(\lfloor F_n/\Delta \rfloor, 2) \tag{19}$$

where, Δ is the quantization size.

E. Zero Watermark Generation

Let B = binary feature vector and ϑ = binary watermark. Then the zero watermark key is generated as

$$ZW = B \oplus \vartheta \tag{20}$$

The generated key and the associated encryption parameters are stored externally. In practical deployment, the key is securely maintained within hospital Picture Archiving and Communication System (PACS) servers, cloud storage systems, or blockchain-assisted authentication frameworks. In the proposed method, the extracted feature vector and watermark information are encrypted using DNA-XOR operations with random Keys K_f and K_w respectively. This makes the unauthorized reconstruction highly cumbersome. Moreover, the stored zero-watermark data contains only an encrypted bit string, not the image. This reduces the risk of sensitive medical data leakage.

F. Watermark Verification

During verification, the same feature extraction pipeline is applied to the test image. To compensate for geometric distortions, ORB-based feature matching and geometric transformation estimation are performed before feature extraction.

The recovered watermark is obtained as:

$$\vartheta_{enc} = B_t \oplus ZW_{key} \tag{21}$$

where, B_t is the binary feature vector extracted from the test image.

V. Experimental Setup

The experiment was carried out using MATLAB 2024a on a system equipped with an Intel i5 processor and 16GB of RAM. We have used different medical images of different sizes as host medical images (HMIs). These include COVID-19 chest X-ray sizes 3050×2539, 1698×1878, 1064×840 [29], MRI brain images of sizes 350×350, 210×240, 377×500, CT images of size 512×512 [30].

Algorithm 2 Proposed Zero Watermarking Framework

Require: Host medical image χ, watermark ϑ
Ensure: Zero-watermark key ZW_{key}
Resize χ to 256×256 and divide into 8×8 blocks
for each block $B_{i,j}$ **do**
  Compute variance $\sigma^2(B_{i,j})$
  if $\sigma^2(B_{i,j}) > T$ **then**
    Select block as Stable ROI
    Apply APBT transform
    Extract low-frequency coefficients
    Normalize coefficients
    Extract LBP texture features
    Normalize LBP vector
    Fuse features:

$$F = [F_{APBT}; F_{LBP}]$$

  end if
end for
Construct feature vector F_{map}
Convert feature vector to binary
Apply DNA encoding
Generate random DNA key K_f
Encrypt features using DNA-XOR
Convert encrypted features back to decimal
Reshape encrypted feature vector to image F_{img}
Resize F_{img} to 224×224 and replicate to 3 channels
Extract deep features using VGG16 layer $fc7$
Normalize deep features:

$$F_n = \frac{F - \mu}{\sigma}$$

Apply QIM binarization:

$$B = mod(\lfloor F_n/\Delta \rfloor, 2)$$

Convert watermark ϑ to binary vector
Apply DNA encoding to watermark
Generate random DNA key K_w
Encrypt watermark using DNA-XOR
Convert encrypted watermark back to binary
Generate zero watermark key:

$$ZW_{key} = B \oplus \vartheta_{enc}$$

Store $\{ZW_{key}, K_w, K_f, \mu, \sigma, \Delta\}$

Algorithm 3 Zero Watermark Verification

Require: Test image κ, stored data
Ensure: Recovered watermark ϑ_r
Apply attacks to κ
Align test image using ORB feature matching
Extract Stable ROI blocks using stored coordinates
for each selected block **do**
  Extract APBT + LBP fused features
end for
Construct feature vector F_t
Apply same DNA encryption using key K_f
Convert encrypted vector to feature image
Extract deep features using VGG16 ($fc7$)
Normalize using stored parameters
Apply QIM binarization to obtain B_t
Recover encrypted watermark:

$$\vartheta_{enc} = B_t \oplus ZW_{key}$$

Apply DNA decryption using key K_w
Convert binary to watermark image
Output recovered watermark ϑ_r

The COVID-19 chest X-ray images used in this study were originally acquired at high spatial resolution. Before embedding, the host images were resized to 224×224 pixels to ensure compatibility with the pretrained VGG-16 and to maintain computational efficiency. Resizing COVID-19 images introduces significant spatial downsampling. The proposed framework is designed for zero-watermark generation, which extracts stable and discriminative features rather than clinical diagnosis or lesion detection. Moreover, our scheme does not modify the original medical image, preserving its diagnostic integrity in practical deployment. The resizing operation primarily affects the feature extraction stage. It does not alter the actual medical image stored or used by doctors for diagnosis. Future work may investigate multi-scale feature extraction frameworks as a preprocessing stage to better preserve subtle pathological details.

A copyrighted image of size $64 \times 64$was employed. These HMIs and corresponding watermark images are illustrated in Fig. 4. To assess the visual quality of the watermarked images, Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index Measure (SSIM) were used. The algorithm's robustness was measured using metrics such as Normalized Correlation Coefficient (NCC) and Bit Error Rate (BER). PSNR and SSIM reflect the perceptual similarity between the original and watermarked images, while NCC and BER assess the strength and reliability of the embedded watermark. Ideally, NCC should be close to 1, indicating high similarity, and BER should be 0, reflecting superior robustness. The mathematical definitions of these evaluation metrics are presented below.

$$\text{PSNR}(\chi, \kappa) = 10log_{10}\frac{\chi^2_{peak}}{\Psi}, \tag{22}$$

where, Ψ is the mean square error between the test and host medical image. Evaluating image degradation through SSIM involves perceiving changes in structural information and considering perceptual phenomena such as luminance and contrast masking. SSIM addresses the limitations of PSNR and is expressed in Eq. (23) by:

$$\text{SSIM}(\chi, \kappa) = \frac{(2\mu_\chi\mu_\kappa + a_1) + (2\sigma_{\chi\kappa} + a_2)}{(\mu^2_\chi + \mu^2_\kappa + a_1)(\sigma^2_\chi + \sigma^2_\kappa + a_2)}, \tag{23}$$

where, μ_χ, μ_κ and σ_χ, σ_κ are the mean and variance of image χ and κ respectively. $\sigma_{\chi\kappa}$ is the covariance between χ and κ. a_1 and a_2 are +ve constants. For an watermark size $\vartheta = N_1 \times N_2$, the NCC between the ϑ and ϑ_r can be represented by [31]:

$$\text{NCC}(\vartheta, \vartheta_r) = \frac{\sum_{n_1=0}^{N_1}\sum_{n_2=0}^{N_2} \vartheta(n_1,n_2) \times \vartheta_r(n_1,n_2)}{\sum_{n_1=0}^{N_1}\sum_{n_2=0}^{N_2} \vartheta(n_1,n_2)^2}. \quad (24)$$

Similarly, the BER defines the percentage of error between ϑ and ϑ^*, which can be expressed by:

$$\text{BER}(\vartheta, \vartheta_r) = \frac{1}{S} \times \sum_{n_1=0}^{N_1}\sum_{n_2=0}^{N_2} [\vartheta(n_1,n_2) - \vartheta_r(n_1,n_2)] \quad (25)$$

VI. Results and Discussion

This section presents the robustness evaluation of the proposed scheme along with a comparative analysis against existing methods. Finally, the Wilcoxon signed-rank statistical test and the Friedman ranking test are conducted to evaluate the effectiveness of our method.

A. Robustness Evaluation

The robustness of the proposed framework was tested against 42 different attacks, including: Noise Attacks, Gaussian noise, Salt and pepper noise, Speckle noise, Filtering Attacks, Gaussian filtering, Median filtering, Average filtering, Compression Attacks, JPEG compression at different quality levels, Geometric Attacks: Rotation, Scaling, Translation, Cropping, Intensity Attacks, Histogram equalization, Gamma correction, Contrast stretching, Advanced Attacks: Motion blur, Poisson noise, Elastic distortion, Patch removal, Cut-and-paste manipulation, The watermark recovery performance remains high even under severe distortions.

Fig. 5 shows the various signal processing attacks applied to the test image and the corresponding recovered watermarks. The numerical values of NCC and BER are also listed under the recovered watermarks. The applied sets of combined attacks are 1) No attack 2) Average filtering (3x3), 3) Contrast stretch, 4) Gamma correction by (0.5 and 1.5), 5) Gaussian (0.01), 6) Histogram equalization, 7) Gaussian blur (σ=1), 8) Histogram compression, 9) Sharpen, 10) Salt and Pepper (0.02), and 11) JPEG (Q=50). A very high robustness is observed in all attack scenarios. The NCC values consistently above 0.99, indicating near-perfect watermark recovery. Correspondingly, BER remains very low, ranging from 0.05-0.3%. These quantitative results confirm that the proposed scheme maintains strong resilience against diverse signal distortions, including Noise, gamma corrections, histogram manipulations, Gaussian blur, compression, and sharpening operations. The retrieved watermarks are graphically illustrated in Fig. 5 under different attacks.

Fig. 6 shows the various geometrical, combined attacks applied to the test image and the recovered watermarks. The numerical values of NCC and BER are also listed. The applied sets of combined attacks are 1) Blur+noise, 2) Rotate by 5°+blur, 3) Rotate by 5°+noise, 4) Scale+JPEG, 5) Random bending, 6) Rotate by 5°, 7) Rotate by 10°, 8) Motion blur, 9) Cut-paste, 10) Elastic distortion, 11) Patch removal, and 12) scale by 0.8. A very high robustness is observed in all attack scenarios. The NCC values consistently above 0.99, indicating near-perfect watermark recovery. Correspondingly, BER remains very low, ranging from 0.05-0.3%. These quantitative results confirm that the proposed scheme maintains strong resilience against diverse geometric distortions, including arbitrary-angle rotation, elastic distortion, and scaling operations. The retrieved watermarks are graphically illustrated in Fig. 6 under different attacks.

Robustness to geometric attacks is closely related to ROI selection and ORB-based geometric alignment. The ROI selection improves feature consistency, and ORB feature matching compensates for rotation, scaling, and geometrical distortion prior to feature extraction. The higher NCC values in Fig. 6 demonstrate that the ORB alignment stage effectively preserves feature correspondence under geometric and combined attacks.

Fig. 7 shows the NCC and SSIM performance of the proposed method against 42 attacks. It is observed that NCC and SSIM are 1 under no attack case. The NCC is very close to 1 for all attacks irrespective of common, geometrical, or combined attacks. The average SSIM is above 0.7, considering all attacks. It indicates that the algorithm shows a good trade-off between imperceptibility and robustness. The robustness performance can be shown in the BER plot as shown in Fig. 8. The BER below 0.3% indicates perfect watermark recovery.

Both Gaussian Noise, Salt & Pepper Noise have robustness between (0.98–1.0), Hoever, SSIM drops significantly (0.3–0.8). This indicates that both noise deteriorates visual quality but do not impact the quality of the watermark. NCC remains 1.0, SSIM moderately high (0.8–0.95) for Gaussian blur, median, and average filter attacks, indicating filtering preserves structural content. High robustness and visual quality indicate effective use of low-frequency and structural features. NCC and SSIM are near 1.0 across all quality factors (Q) in JPEG attacks, showing robustness against real-world compression scenarios. NCC is approximately between (0.95 to 1.0), and SSIM is slightly reduced (0.8–0.95) in most of the geometrical attacks. This indicates the geometric distortion is successfully compensated by ORB-based alignment. A Minor SSIM drop may be due to interpolation and spatial misalignment. NCC is high (0.95–1.0), but SSIM drops abruptly (i.e., 0.3–0.6) on intensity-based attacks such as histogram equalization, gamma correction, and contrast stretching. This is due to the fact that these attacks alter the pixel intensity distribution. For combined and random bending cases, NCC remains significantly high (0.95+), whereas SSIM varies widely (0.4–0.9). This indicates that watermark detection is reliable even under complex distortions.

The PSNR plot in Fig. 9 illustrates the impact of various attacks on the perceptual quality of medical images, along with deviation (error bars). It provides both average performance and stability details. The PSNR for the no-attack case is between 24 and 25 dB. This confirms that no artificial distortion is introduced by the proposed algorithm. These values show inherent dataset variability instead of embedding loss. Under Gaussian Noise and Salt & Pepper Noise, PSNR drops to a range of 21–24 dB. This indicates moderate degradation, but it is still acceptable.

PSNR remains relatively higher (25–30 dB) under Gaussian blur, median filter, and average filter. This shows that the method preserves global structures. PSNR shows up to

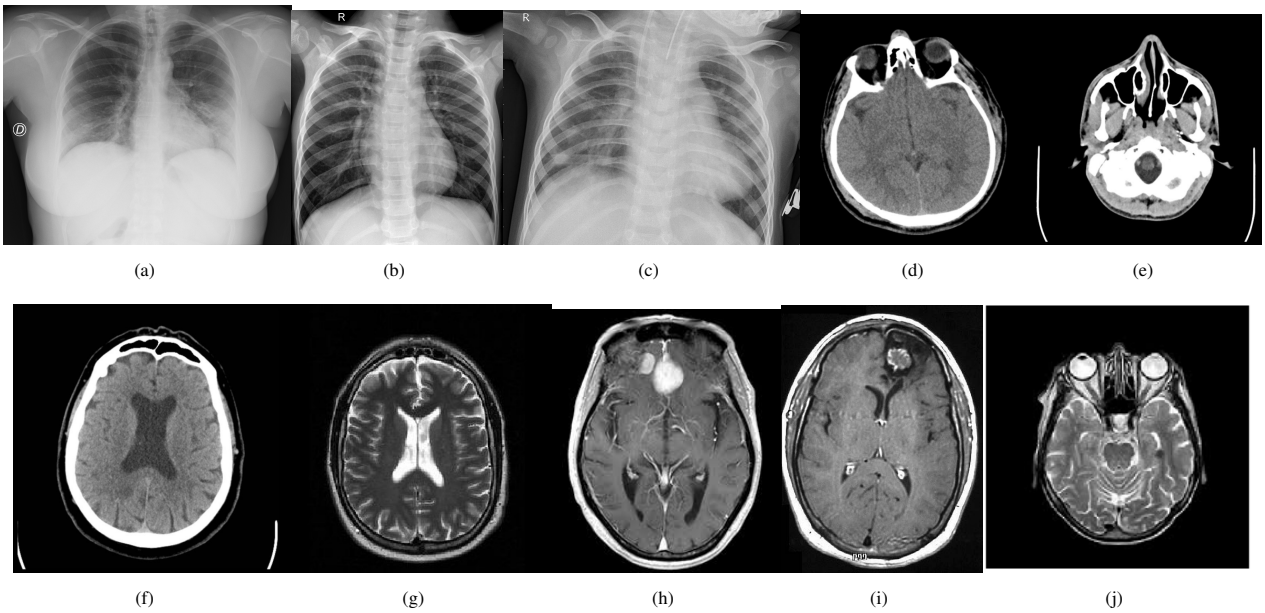


Fig. 4. Sample images used for experiment: (a), (b), (c) X-ray; (d), (e), (f) CT, and (g), (h), (i), (j) MRI images.

35–38 dB at higher quality (Q70) and drops gradually with compression strength. This indicates that compression removes redundancy but retains structural information. Therefore, the proposed algorithm leverages structure-based features. Moderate deviation in PSNR (26-34 dB) is observed in the rotation and scaling operations. This is due to ORB-based alignment. A significant PSNR drop (13–20 dB) occurs in histogram equalization and gamma correction as these attacks alter the global intensity distribution. This affects PSNR but not necessarily the watermark quality.

PSNR fluctuates widely (20–33 dB) in sharpening, motion blur, Poisson noise, and combined rotation with noise. Histogram compression/intensity scaling has the lowest PSNR (13–15 dB).

Large bar plots were observed in gamma correction, cropping, and combined attacks. This indicates performance relies on image content (edges vs smooth regions). This may be acceptable for medical images with varying textures.

The PSNR analysis demonstrates that the proposed framework preserves high perceptual quality under most signal processing and geometric attacks, while significant degradation is observed only under intensity-based transformations such as histogram equalization and gamma correction. This behavior confirms that the variations in PSNR are primarily due to attack severity rather than the watermarking process, making PSNR less indicative of robustness in zero-watermarking systems.

The performance of the proposed zero-watermarking algorithm is further analyzed using heat map visualization in Fig. 10, which provides an intuitive representation of spatial feature stability and robustness. The generated heat maps highlight the distribution of discriminative features extracted from the stable ROI using the APBT and deep features (VGG16).

From the heat map analysis, it is observed that:

- High-intensity regions correspond to structurally significant areas of the medical image, indicating that the algorithm effectively captures salient and invariant features.
- The feature concentration remains consistent across various attacks (e.g., noise, filtering, compression), demonstrating the strong robustness of the extracted watermark features.
- Minimal variation in heat distribution between the original and attacked images confirms the stability of the feature representation, which directly contributes to higher NCC values and lower BER.
- The use of stable ROI selection and ORB-based alignment ensures that the important regions retain their prominence in the heat maps even under geometric distortions.
- Compared to conventional methods, the proposed framework exhibits better localization of important features, reducing the influence of non-informative regions and improving watermark reliability.

Overall, the heat map visualization validates that the proposed method maintains spatial consistency, robustness, and discriminative feature preservation, which are critical for reliable zero-watermark generation and extraction.

B. Comparative Analysis

Table III shows the NCC comparison between the proposed method and other methods for conventional, geometrical, and combined attacks. It is observed that the proposed scheme outperforms the methods in [32] and [33] by a wide margin. Method [17] and [34] closely follows our method. The combined attack means that multiple image processing attacks are applied sequentially to the same image before extracting

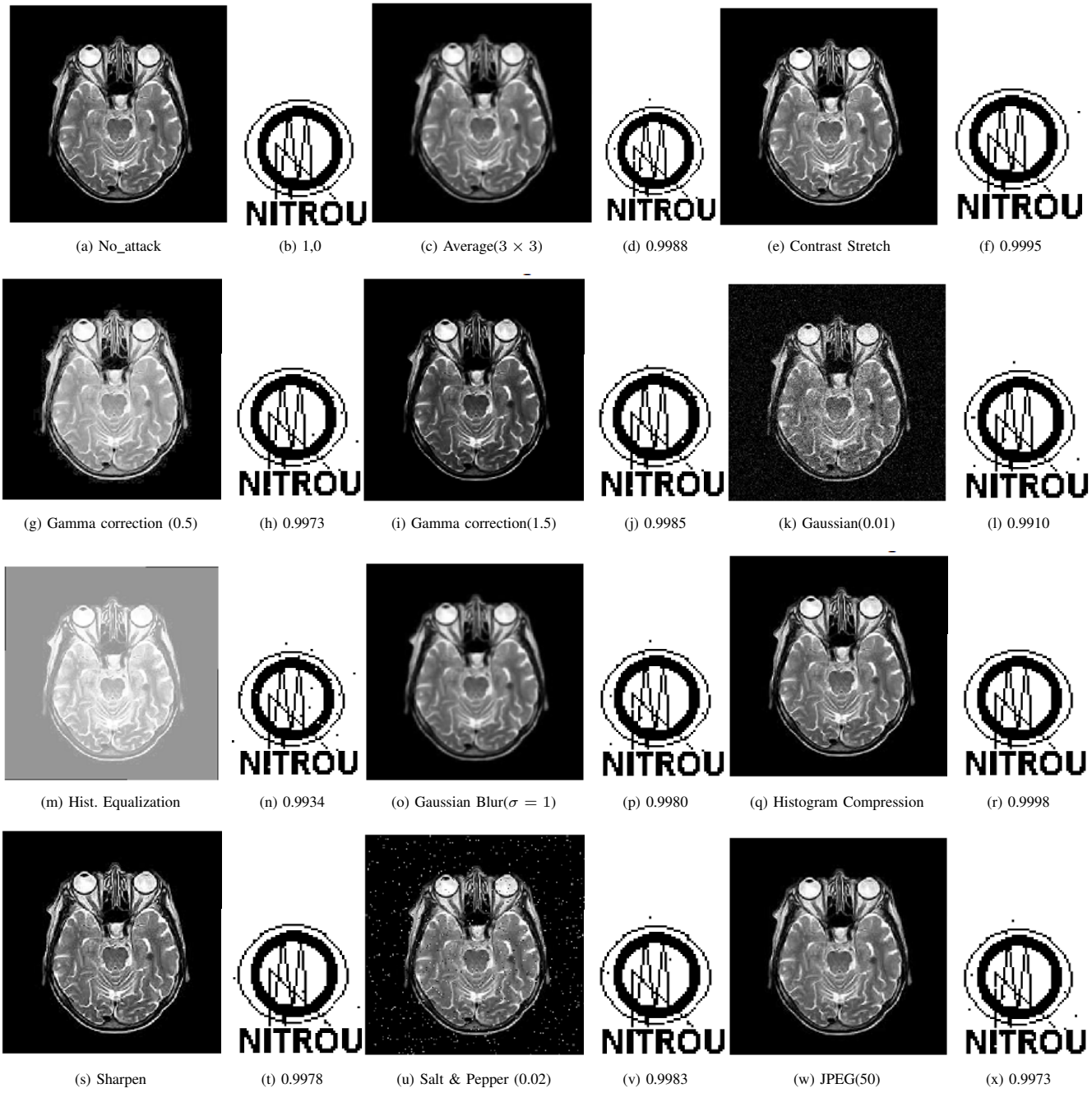
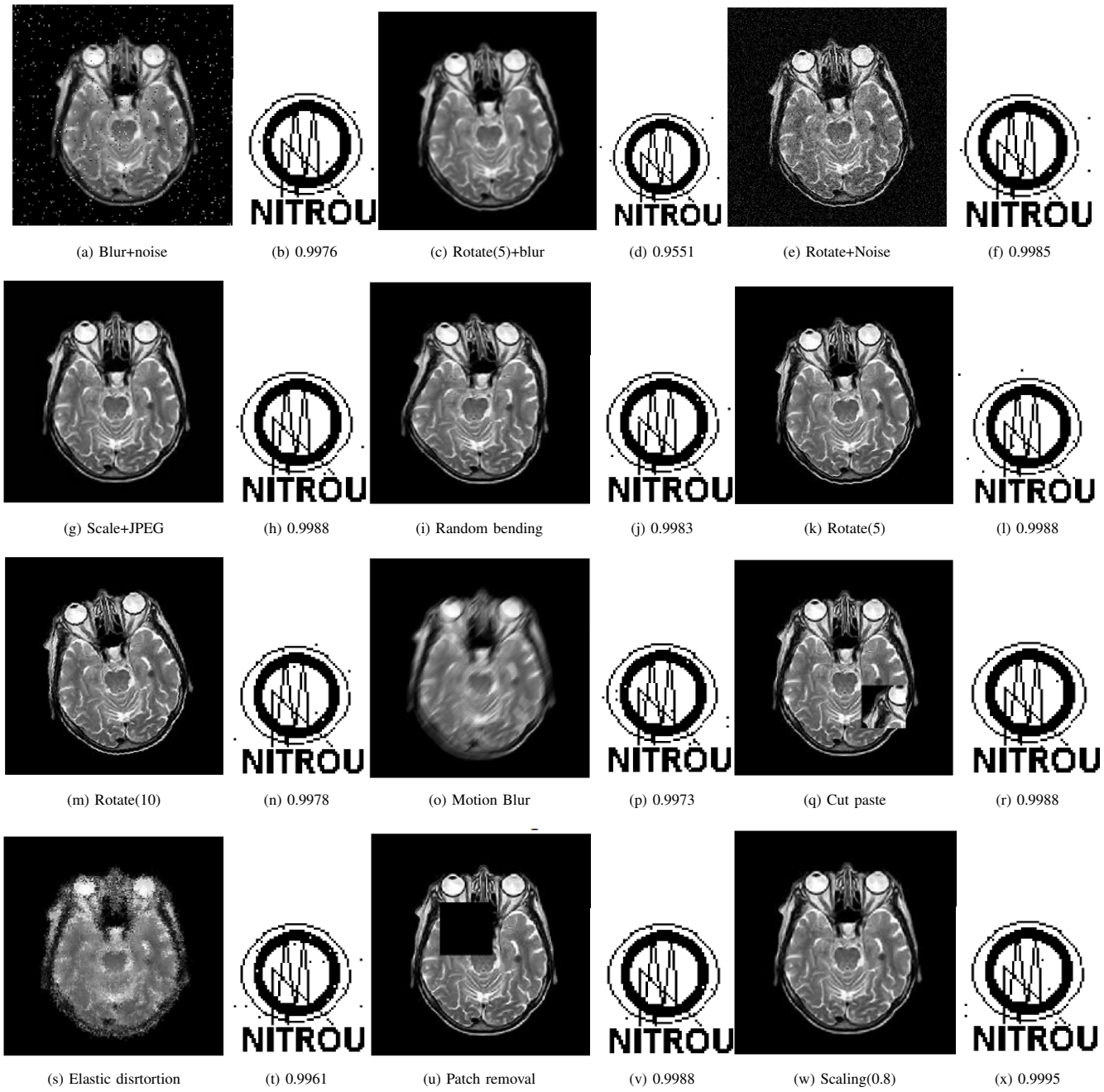


Fig. 5. Signal processing attacks on Brain Image. The SSIM and BER values of the Attacked image and extracted watermarks are calculated. (a) No attack, SSIM=1 (b) BER=0 , (c) Average filter(3×3), SSIM=0.9238 (d) BER=0.0017, (e) Contrast Stretch ,SSIM=0.9987 (f) BER=0.0005, (g) Gamma Correction (0.5), SSIM=0.8837 (h) BER=0.0007, (i) Gamma correction (1.5), SSIM=0.9429 (j) BER=0.0007 (k) Gaussian (0.01), SSIM=0.3045 (l) BER=0.0046, (m) Hist. equalization, SSIM=0.2505 (n) BER=0.0076, (o) Gaussian Blur ($\sigma = 1$), SSIM=0.9182, (p) BER=0.0029, (q) Hist. compression ,SSIM=0.8558 (r) BER=0.0005, (s) Sharpen, SSIM=0.9783, (t) BER=0.0010, (u) Salt & Pepper (0.02), SSIM=0.6746(v) BER=0.0.0020, (w) JPEG (Q=50), SSIM=0.9681, (x) BER=0.0024.

the watermark. This tests the worst-case robustness of the algorithm. Instead of applying one attack at a time, several attacks such as GN0.01, JPEG10, ROT5, and MedF are in a pipeline.

Similarly, a comparison on the imperceptibility test is depicted in Table IV for 10 types of images. It is observed that the PSNR of the proposed method outperforms by a large margin, $\geq$ 10 dB consistently than the other methods.

Fig. 11 shows a spider plot comparison of NCC values under fifteen types of image processing attacks. It is observed that the proposed method maintains NCC values close to unity across all distortions, indicating superior robustness compared with other methods. The scheme in [17] employs a complex feature-extraction process, comprising VGG19, LBP,



(a) Blur+noise (b) 0.9976 (c) Rotate(5)+blur (d) 0.9551 (e) Rotate+Noise (f) 0.9985

(g) Scale+JPEG (h) 0.9988 (i) Random bending (j) 0.9983 (k) Rotate(5) (l) 0.9988

(m) Rotate(10) (n) 0.9978 (o) Motion Blur (p) 0.9973 (q) Cut paste (r) 0.9988

(s) Elastic disrtortion (t) 0.9961 (u) Patch removal (v) 0.9988 (w) Scaling(0.8) (x) 0.9995

Fig. 6. Geometrical combined attacks on Brain image. The SSIM and BER values of the watermarked image and extracted watermarks using proposed scheme (a) Blur+Noise, SSIM=0.6008, (b) BER=0.0024, (c) Rotate (5°)+ Blur, SSIM=0.8962, (d) BER=0.0022, (e) Rotate (5°)+ Noise, SSIM=0.3616, (f) BER=0.0029, (g) Scale + JPEG, SSIM=0.8793 (h) BER=0.0020, (i) Random bending, SSIM=0.6965 (j) BER=0.0017 (k) Rotate (5°, SSIM=0.9728 (l) NCC=0.0010, (m) Rotate (10°), SSIM=0.9723 (n) BER=0.0029, (o) Motion blur, SSIM=0.7674 (p) BER=0.0.0032, (q) Cut and paste, SSIM=0.9539 (r) BER=0.0017, (s) Elastic distortion, SSIM=0.7003 (t) BER=0.0051, (u) Patch removal, SSIM=0.9386 (v) BER=0.0005, (w) Scaling (0.8), SSIM=0.9771, BER=0.0024.

DCT, and DWT. Whereas ZWNet [34] combines stationary wavelet transform (SWT), DarkNet53 deep feature extraction, and Fibonacci Q-matrix encryption. In contrast, our method uses only VGG16+LBP for feature extraction, reducing the complexity of implementation.

To statistically validate the performance improvement, the Wilcoxon signed-rank test was conducted between the proposed method and existing methods using NCC values obtained under fifteen attacks. The obtained p-values are less than 0.05, confirming that the proposed method achieves statistically significant improvements. A comparison of p-values is shown in Table V

To further validate the performance difference among multiple watermarking algorithms, the Friedman test was con-

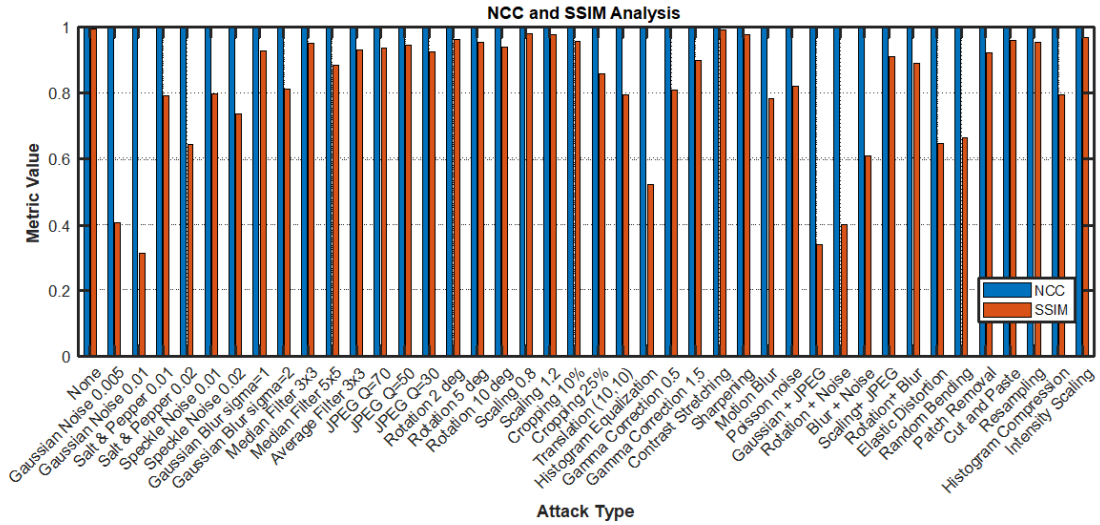


Fig. 7. NCC and SSIM performance under various attacks.

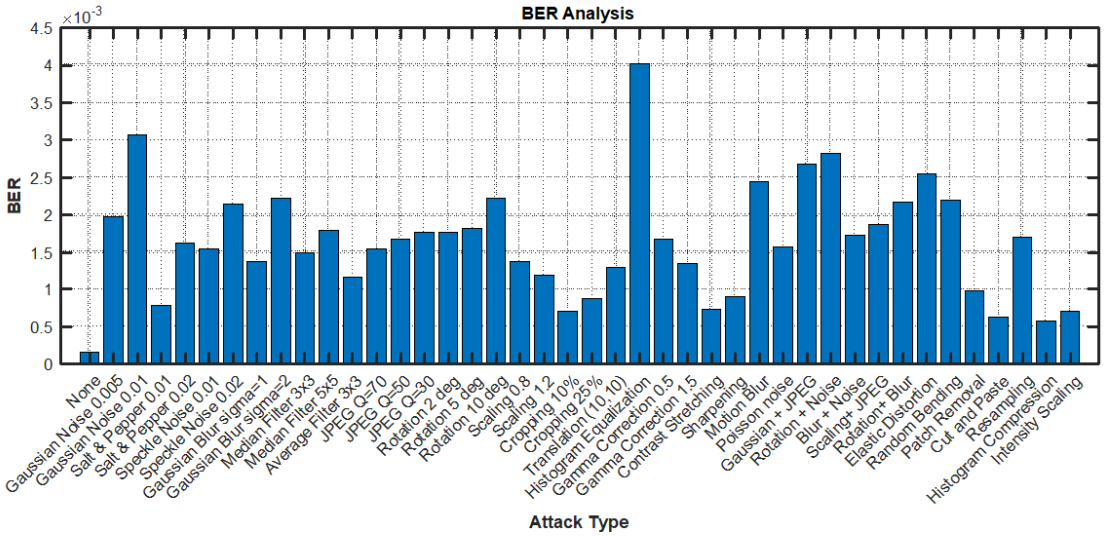


Fig. 8. BER plot under various attacks.

TABLE III. ROBUSTNESS COMPARISON USING NCC UNDER 15 DIFFERENT ATTACKS

Attack	Proposed	[17]	[32]	[33]	ZWNet [34]
GN0.01	0.998	0.995	0.90	0.83	0.992
GN0.05	0.997	0.994	0.89	0.82	0.989
SP0.01	0.997	0.994	0.90	0.83	0.991
SP0.03	0.996	0.993	0.88	0.82	0.988
AvgF	0.998	0.995	0.70	0.96	0.994
MedF	0.998	0.995	0.68	0.95	0.993
GaussF	0.998	0.995	0.69	0.95	0.993
JPEG10	0.996	0.995	0.90	0.92	0.989
JPEG30	0.996	0.995	0.89	0.92	0.990
JPEG50	0.995	0.994	0.88	0.91	0.988
Rot3	0.998	0.996	0.83	0.67	0.994
Rot5	0.998	0.995	0.82	0.66	0.992
Scale0.5	0.997	0.994	0.90	0.92	0.991
Scale1.5	0.997	0.994	0.89	0.91	0.990
Combined	0.998	0.993	0.80	0.90	0.987

TABLE IV. PSNR COMPARISON (DB) BETWEEN THE PROPOSED METHOD AND EXISTING METHODS

Medical Image	Proposed	[17]	[32]	[33]	ZWNet [34]
Brain MRI	58.72	46.31	41.85	39.74	55.92
Chest CT	57.94	45.88	40.92	38.63	55.37
Lung CT	58.21	46.05	41.13	39.22	55.64
Abdominal CT	57.63	45.41	40.55	38.91	55.11
Ultrasound	58.09	45.97	41.02	39.05	55.48

ducted using NCC values obtained under fifteen attacks. The p-value ($\leq$ 0.05) in Table VI indicates that the proposed framework significantly outperforms the compared methods.

Higher NCC under various attacks does not necessarily indicate overfitting or limited variability. The robustness is primarily attributed to 1) ROI selections, 2) APBT low coefficient calculations, 3) LBP feature extraction, and 4) ORB-based geometric alignment. The experiments are conducted across multiple image modalities, introducing variety into the experimental process under 42 different kinds of attacks. In addition, statistical evaluation using the Wilcoxon signed-rank

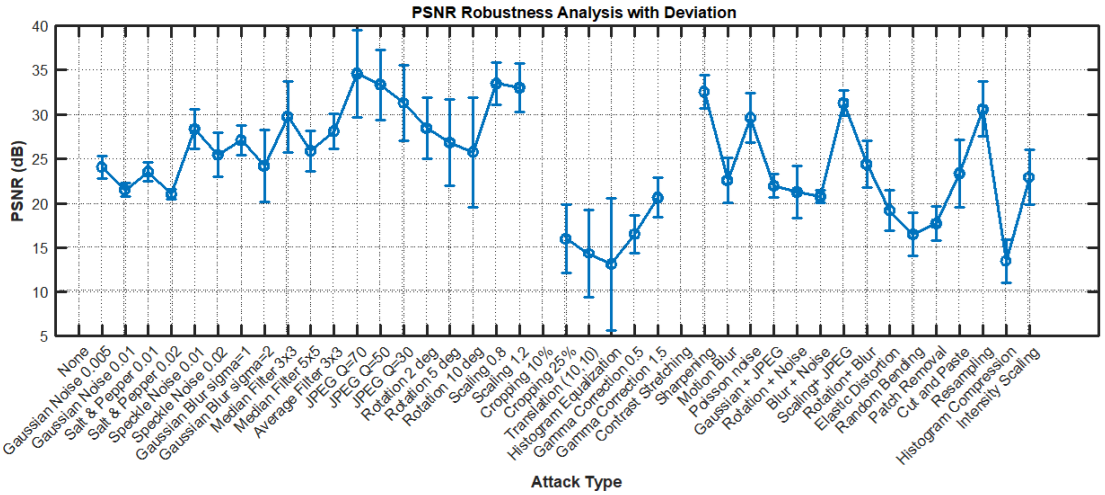


Fig. 9. PSNR performance under various attacks.

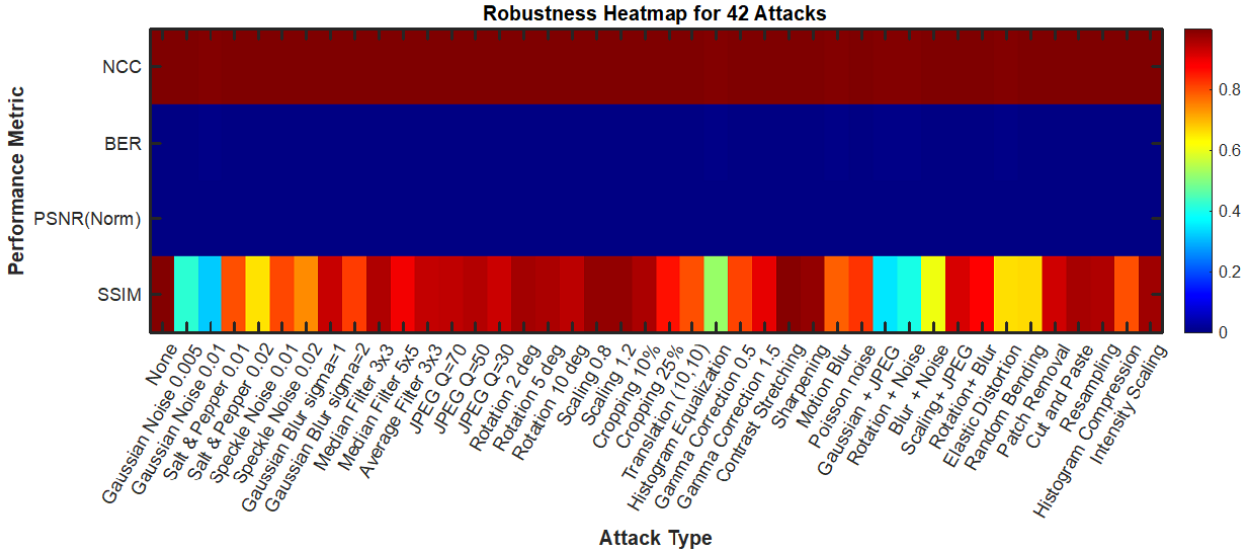


Fig. 10. Heat map plot under various attacks.

TABLE V. WILCOXON SIGNED-RANK AND FRIEDMAN RANK TEST COMPARISON

Comparison	p-value	Average Rank	Significant
Proposed vs [17]	1.2×10^{-3}	1.27	Yes
Proposed vs [32]	3.5×10^{-5}	1.13	Yes
Proposed vs [33]	2.8×10^{-5}	1.07	Yes
Proposed vs ZWNet [34]	8.6×10^{-4}	1.34	Yes

TABLE VI. FRIEDMAN RANKING COMPARISON BASED ON NCC VALUES UNDER 15 ATTACKS

Method	Average Rank
Proposed Method	1.00
Method in [17]	2.87
Method in [32]	3.74
Method in [33]	4.38
ZWNet [34]	2.01

test and the Friedman ranking test confirms that the observed performance improvement is not a consequence of overfitting.

C. Ablation Studies

Table VII illustrates the contributions of individual components of the proposed method towards the average NCC and average BER parameter calculation. The average NCC and BER are evaluated across 10 different image types using the same binary watermark. While the APBT contributes an average NCC of 0.9124, adding LBP yields a gain of 0.0363. The deep-level features of VGG16 only contribute an average NCC of 0.9315. Combining all the features in a single framework contributes a significant average NCC and average BER of approximately 1 and 0, respectively.

D. Computational Complexity and Execution Time

The computational overhead occurs primarily from the pretrained VGG-16 feature extraction, followed by the DNA

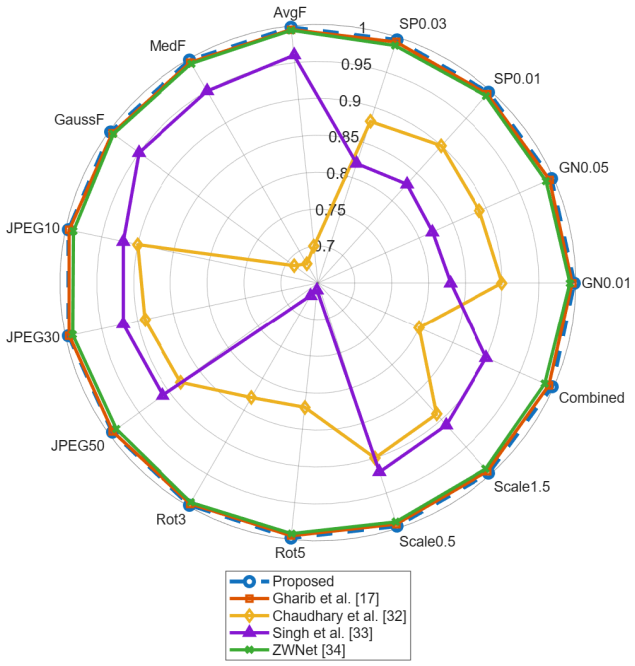


Fig. 11. Spider plot comparison of NCC values under 15 image processing attacks.

TABLE VII. ABLATION STUDY

Features Used	Avg. NCC	Avg. BER
APBT only	0.9124	0.0841
APBT + LBP	0.9487	0.0416
VGG16 only	0.9315	0.0563
APBT + LBP + VGG16	0.9982	0.0006

TABLE VIII. COMPUTATIONAL COMPLEXITY AND MEMORY USAGE COMPARISON

Method	Feature Extraction	Avg Time (s)	Memory (MB)	Complexity
Proposed	APBT+LBP+VGG16	1.24	118	Moderate
[17]	DWT+DCT+VGG19	3.25	214	High
[32]	DWT+HMD+SVD	2.51	176	High

encryption process. However, the proposed scheme is computationally more efficient than most of the existing deep-learning-based watermarking approaches because 1) only stable ROI blocks are selected rather than the whole image blocks, 2) dimensionality reductions are achieved due to low-frequency APBT coefficients, and 3) a pretrained VGG-16 is employed instead of full training. Finally, DNA encryption is applied to compact binary feature vectors rather than full-resolution images. This reduces encryption overhead.

Table VIII shows the average execution time and memory usage of the proposed method in comparison with the other methods. It is observed that the average execution time is nearly 33% and 50% less compared to methods in [17] and [32], respectively, while memory usage is proportionally less. The memory usage is calculated using the MATLAB profiling function by measuring the difference between before and after execution. The VGG16 is not the most lightweight architecture. VGG16 is chosen in our work for its strong feature representation capabilities, architectural simplicity, and widespread adoption. It is used only as a pre-trained feature extractor without end-to-end training. The fused ROI features are processed rather than the entire image, significantly reducing computation. The term 'lightweight' refers to a reduced feature-processing pipeline, achieved through compact fusion of APBT and LBP features rather than using ultra-lightweight architectures such as MobileNet, ShuffleNet, or EfficientNet. Compared with VGG19, ResNet, and Transformer architectures, VGG16 provides a favorable trade-off between memory usage and feature discrimination.

VII. CONCLUSIONS

This paper presented a robust medical image zero-watermarking framework that integrates transform-domain analysis with deep feature extraction. The proposed method employs the All Phase Biorthogonal Transform to capture stable frequency-domain characteristics and utilizes deep features obtained from VGG16 to enhance feature discrimination. Furthermore, ORB-based alignment improves robustness against geometric distortions. Experimental results show that the proposed framework achieves high robustness under various signal processing and geometric attacks. Additionally, the zero-watermarking strategy preserves the diagnostic quality of medical images by avoiding direct modification of the host medical image. Comparative analysis with existing methods and statistical validation using the Wilcoxon signed-rank statistical test and the Friedman ranking test confirm the effectiveness of the proposed approach. Future work will focus on further reducing computational complexity through lightweight deep learning architectures for higher-dimensional medical images.

REFERENCES

[1] M. Yang, J. Li, U. Bhatti, C. Shao, and C. Yen-Wei, "Robust watermarking algorithm for medical images based on non-subsampled shearlet transform and schur decomposition," *Computers, Materials, & Continua*, vol. 75, no. 3, p. 5539, 2023.

[2] R. K. Senapati, B. Biswal, S. Kautish, G. Swain, A. Altameem, A. S. Almazyad, and A. W. Mohamed, "Optimized video watermarking with entropy-aware block selection and modified hénon-map encryption," *IEEE Access*, 2024.

[3] A. M. Wagdarikar and R. K. Senapati, "Design and development of a multiobjective cost function for robust video watermarking using wavelet transform," *Journal of Intelligent Systems*, vol. 28, no. 5, pp. 873–891, 2019.

[4] B. Ahmaderaghi, J. M. Del Rincon, F. Kurugollu, and A. Bouridane, "Perceptual watermarking for discrete shearlet transform," in *European Workshop on Visual Information Processing*. Institute of Electrical and Electronics Engineers Inc., 2014, pp. 1–6.

[5] A. Hadid, "The local binary pattern approach and its applications to face analysis," in *2008 First Workshops on Image Processing Theory, Tools and Applications*, 2008, pp. 1–9.

[6] R. K. Senapati, S. Srivastava, and P. Mankar, "RST invariant blind image watermarking schemes based on discrete Tchebichef transform and singular value decomposition," *Arabian Journal for Science and Engineering*, vol. 45, pp. 3331–3353, 2020.

[7] H. Gao and Q. Chen, "A robust and secure image watermarking scheme using surf and improved artificial bee colony algorithm in dwt domain," *Optik*, vol. 242, p. 166954, 2021.

[8] A. Soualmi, A. Alti, and L. Laouamer, "An imperceptible watermarking scheme for medical image tamper detection," *International Journal of Information Security and Privacy (IJISP)*, vol. 16, no. 1, pp. 1–18, 2022.

[9] M. Roy, D. M. Thounaojam, and S. Pal, "A perceptual hash based blind-watermarking scheme for image authentication," *Expert systems with applications*, vol. 227, p. 120237, 2023.

[10] H. Chaudhary and V. Vishwakarma, "Digital image watermarking recent trends and techniques: A survey," *J. Inf. Optim. Sci*, vol. 45, no. 4, pp. 1051–1059, 2024.

[11] R. E. Arevalo-Ancona and M. Cedillo-Hernandez, "Zero-watermarking for medical images based on regions of interest detection using k-means clustering and discrete fourier transform," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 6, 2023.

[12] F. Li and Z.-X. Wang, "A zero-watermarking algorithm based on scale-invariant feature reconstruction transform," *Applied Sciences*, vol. 14, no. 11, p. 4756, 2024.

[13] M. Yamni, H. Karmouni, M. Sayyouri, and H. Qjidaa, "Color stereo image zero-watermarking using quaternion radial tchebichef moments," in *2020 International Conference on Intelligent Systems and Computer Vision (ISCV)*. IEEE, 2020, pp. 1–7.

[14] K. M. Hosny and M. M. Darwish, "Robust color image watermarking using invariant quaternion legendre-fourier moments," *Multimedia Tools and Applications*, vol. 77, no. 19, pp. 24 727–24 750, 2018.

[15] M. Magdy, N. I. Ghali, S. Ghoniemy, and K. M. Hosny, "Multiple zero-watermarking of medical images for internet of medical things," *IEEE Access*, vol. 10, pp. 38 821–38 831, 2022.

[16] Z. Xia, X. Wang, C. Wang, C. Wang, B. Ma, Q. Li, M. Wang, and T. Zhao, "A robust zero-watermarking algorithm for lossless copyright protection of medical images: Z. xia et al." *Applied Intelligence*, vol. 52, no. 1, pp. 607–621, 2022.

[17] H. A. Gharib, N. M. Abdelnapi, and K. M. Hosny, "Robust zero-watermarking for color images using hybrid deep learning models and encryption," *Scientific Reports*, vol. 15, no. 1, p. 28906, 2025.

[18] A. Anand, J. Bedi, and I. Rida, "Miwet: Medical image watermarking using encryption and fusion technique," *Computers and Electrical Engineering*, vol. 115, p. 109114, 2024.

[19] Y. Fan, J. Li, U. A. Bhatti, C. Shao, C. Gong, J. Cheng, and Y. Chen, "A multi-watermarking algorithm for medical images using inception v3 and dct." *Computers, Materials & Continua*, vol. 74, no. 1, 2023.

[20] F. Dong, J. Li, U. A. Bhatti, J. Liu, Y.-W. Chen, and D. Li, "Robust zero watermarking algorithm for medical images based on improved nasnet-mobile and dct," *Electronics*, vol. 12, no. 16, p. 3444, 2023.

[21] W. Zhang, J. Li, U. A. Bhatti, J. Liu, J. Zheng, and Y.-W. Chen, "Robust multi-watermarking algorithm for medical images based on googlenet and henon map." *Computers, Materials & Continua*, vol. 75, no. 1, 2023.

[22] M. Sheng, J. Li, U. Bhatti, J. Liu, M. Huang, and C. Yen-Wei, "Zero watermarking algorithm for medical image based on resnet50-dct," *Computers, Materials, & Continua*, vol. 75, no. 1, p. 293, 2023.

[23] B. Han, H. Wang, D. Qiao, J. Xu, and T. Yan, "Application of zero-watermarking scheme based on swin transformer for securing the metaverse healthcare data," *IEEE journal of biomedical and health informatics*, vol. 28, no. 11, pp. 6360–6369, 2023.

[24] B. Han, R. H. Jhaveri, H. Wang, D. Qiao, and J. Du, "Application of robust zero-watermarking scheme based on federated learning for securing the healthcare data," *IEEE journal of biomedical and health informatics*, vol. 27, no. 2, pp. 804–813, 2021.

[25] X. Wang, M. Wen, X. Tan, H. Zhang, J. Hu, and H. Qin, "A novel zero-watermarking algorithm based on robust statistical features for natural images," *The Visual Computer*, vol. 38, no. 9, pp. 3175–3188, 2022.

[26] Z.-X. Hou, C.-Y. Wang, and A.-P. Yang, "All phase biorthogonal transform and its application in jpeg-like image compression," *Signal Processing: Image Communication*, vol. 24, no. 10, pp. 791–802, 2009.

[27] L. Chu, Y. Su, X. Yao, P. Xu, and W. Liu, "A review of dna cryptography," *Intelligent Computing*, vol. 4, p. 0106, 2025.

[28] M. Pietikäinen, A. Hadid, G. Zhao, and T. Ahonen, *Computer vision using local binary patterns*. Springer Science & Business Media, 2011, vol. 40.

[29] J. P. Cohen, P. Morrison, and L. Dao, "COVID-19 Radiography Database," https://www.kaggle.com/datasets/tawsifurrahman/covid19-radiography-database, 2020, accessed: May 22, 2026.

[30] M. Nickparvar, "Brain Tumor MRI Dataset," https://www.kaggle.com/dsv/2645886, 2021, accessed: May 22, 2026.

[31] S. Kukreja, G. Kasana, and S. S. Kasana, "Extended visual cryptography-based copyright protection scheme for multiple images and owners using LBP–SURF descriptors," *The Visual Computer*, vol. 37, no. 6, pp. 1481–1498, 2021.

[32] H. Chaudhary, P. Garg, and V. P. Vishwakarma, "Enhanced medical image watermarking using hybrid dwt-hmd-svd and arnold scrambling," *Scientific Reports*, vol. 15, no. 1, p. 9710, 2025.

[33] K. N. Singh, O. P. Singh, A. K. Singh, and A. K. Agrawal, "Watmif: Multimodal medical image fusion-based watermarking for telehealth applications," *Cognitive Computation*, vol. 16, no. 4, pp. 1947–1963, 2024.

[34] M. M. Abdel-Aziz, N. A. Lashin, H. M. Hamza, and K. M. Hosny, "Zwnet: Darknet53-based zero watermarking method for authentication of medical images inspired by fibonacci q-matrix and stationary wavelet transform," *Biomedical Signal Processing and Control*, vol. 100, p. 107044, 2025.