IJIRIS: International Journal of Innovative Research in Information Security
Volume 12, Issue 04, April 2026
E-ISSN: 2349-7017
P-ISSN: 2349-7009
https://www.ijiris.com/archives
https://doi.org/10.26562/ijiris.2026.v1204.07

Robust Zero-Water Marking of Medical Images Using Deep CNN-Based Feature Extraction for Secure Copyright Protection

N.Anand Babu
Assistant Professor, Department of CSE
Guru Nanak Institute of Technology, Hyderabad, Telangana, India
rekotesh@gmail.com
https://orcid.org/0009-0006-8221-9103
Bommu Kotesh, Amaravadi Pavan Reddy, Chinthala Nagasheshu
Students, Department of CSE
Guru Nanak Institute of Technology, Hyderabad, Telangana, India

Publication History
Manuscript Reference No: IJIRIS/RS/Vol.12/Issue04/ISAP26.ISAP10086
Research Article | Open Access | Double-Blind Peer-Reviewed| ArticleID: IJIRAE/RS/Vol.12/Issue04/ISAP26.ISAP10086
Received:02,March 2026, Revised: 29, March 2026, Accepted: 10,April 2026,Published Online: 22, April 2026.
https://www.ijiris.com/volumes/Vol12/iss-04/07.ISAP26.ISAP10086.pdf
Article Citation:Anand,Bommu,Amaravadi,Chinthala(2026),Robust Zero-Water Marking of Medical Images Using Deep CNN-Based Feature Extraction for Secure Copyright Protection. IJIRIS: International Journal of Innovative Research in Information Security, Volume 12, Issue 04 of 2026 pages 303-308
Doi:> https://doi.org/10.26562/ijiris.2026.v1204.07 **BibTeX Key: Anand@2026Robust**
IJIRIS papers should be cited as IJIRIS(International Journal of Innovative Research in Information Security, AM Publications, India 2026, ISSN 2349-7017, https://doi.org/10.26562/ijiris.2026.v1204.07 The journal's official abbreviation is IJIRIS. Orcid: https://orcid.org/0009-0004-9398-7488

Abstract: Medical imaging plays a vital role in modern healthcare systems for diagnosis, storage, and data sharing. However, ensuring the authenticity and integrity of such images remains a critical challenge due to the risk of unauthorized modifications. This work presents a zero-watermarking framework based on deep feature extraction using Convolutional Neural Networks. The proposed method extracts high-level feature representations from medical images and generates a unique watermark signature without altering the original image content. During verification, the extracted features are compared with the stored signature to identify authenticity and detect tampering. The approach demonstrates strong resistance to common image processing and geometric distortions, including noise, compression, scaling, and rotation. The results indicate that the system provides reliable and lossless protection while maintaining diagnostic quality. This framework is suitable for secure medical image management in modern healthcare environments.
Keywords: Zero-Watermarking, Convolutional Neural Networks, Deep Feature Extraction, Image Authentication, Tamper Detection, Digital Healthcare.

INTRODUCTION

The increasing use of digital technologies in healthcare has led to widespread reliance on medical imaging for diagnosis, storage, and data transmission. This growth raises significant concerns regarding image integrity, authenticity, and ownership, as any unauthorized modification can result in serious clinical and legal consequences. Ensuring secure and reliable protection of medical images has therefore become essential. Conventional watermarking techniques embed information directly into images, which may affect their diagnostic quality and limit their applicability in sensitive environments. In contrast, zero-watermarking generates watermark information from inherent image features without altering the original content. However, earlier approaches based on handcrafted features often lack robustness against geometric transformations and common image processing attacks. Recent advancements in Convolutional Neural Networks have enabled the extraction of more discriminative and stable features. This work utilizes such deep features to develop a zero-watermarking framework that enhances authentication accuracy and ensures robust medical image protection.

LITERATURE SURVEY

Han et al. (2021) presented a zero-watermarking approach for medical images using a pretrained VGG19 model to extract deep feature representations. These features capture both structural and semantic information and are further processed using frequency domain techniques and perceptual hashing to generate a compact watermark signature. The method preserves the original image without modification and demonstrates strong resistance to geometric distortions, improving authentication reliability.

Dongetal.(2023) proposed an improved zero-water marking framework by combining an optimized NasNet-Mobile network with discrete cosine transform. The extracted deep features are refined using frequency-based processing, while chaotic encryption is applied to enhance security. The system shows strong robustness against noise, compression, and geometric transformations while maintaining image quality.

E-ISSN: 2349-7017
P-ISSN: 2349-7009
https://www.ijiris.com/archives
https://doi.org/10.26562/ijiris.2026.v1204.07

Xiang et al. (2023) introduced a deep learning-based zero-watermarking scheme utilizing residual network architecture. The approach extracts both local texture and global structural features, leading to more stable representations. It improves detection accuracy and provides strong resistance to image processing and geometric attacks without altering the original image. Anand et al. (2024) developed a deep learning-driven zero-watermarking method for secure healthcare data protection. The frame work integrates multi-scale feature extraction with singular value decomposition to generate robust watermark signatures. A scrambling mechanism enhances security, and the system demonstrates strong resistance to noise, compression, and other attacks while maintaining image integrity.

EXISTING SYSTEM

The existing approaches for medical image protection mainly utilize zero-watermarking techniques based on handcrafted feature extraction methods, particularly orthogonal moments such as Fractional Racah Moments. In these methods, significant features are derived from the image and combined with a watermark to generate a unique security key without altering the original image content. This ensures that the diagnostic quality of the image remains unaffected while supporting ownership verification. However, such techniques rely heavily on predefined mathematical descriptors, which are often in sufficient for capturing complex spatial patterns and semantic details present in medical images. As a result, their performance is limited when dealing with diverse datasets and advanced image processing operations.

EXISTING SYSTEM DISADVANTAGES

- Limited resistance to geometric transformations such as rotation and scaling, which affects reliability under image distortions
- In adequate feature representation due to dependence on hand crafted descriptors that fail to capture complex image characteristics
- Poor generalization capability when applied to different types of medical image datasets
- Increased computational overhead caused by complex mathematical calculations involved in moment-based methods
- Decreased authentication accuracy when images are subjected to noise, compression, and other processing operations

PROPOSED SYSTEM

The proposed approach presents a deep learning-driven zero-watermarking framework for securing medical images using Convolutional Neural Networks. Unlike traditional methods that depend on handcrafted features, this system employs pretrained neural models to extract robust and discriminative feature representations. These deep features effectively capture both structural patterns and semantic information within the image. Based on these extracted features, a unique watermark signature is generated without modifying the original image content, thereby preserving its diagnostic quality. The generated watermark is stored securely for future reference. During the verification phase, features from a test image are re-extracted and compared with the stored signature using similarity measures. This process enables accurate authentication and reliable detection of any tampering or unauthorized modifications.

PROPOSED SYSTEM ADVANTAGES

- Strong resistance to geometric transformations and common image processing operations, ensuring reliable performance under distortions
- Ability to extract rich and meaningful features through deep learning, capturing complex structural and semantic information
- Maintains original image integrity by generating watermark signatures without modifying image content
- Enhances authentication accuracy and enables effective detection of tampered or manipulated images.

SYSTEM ARCHITECTURE

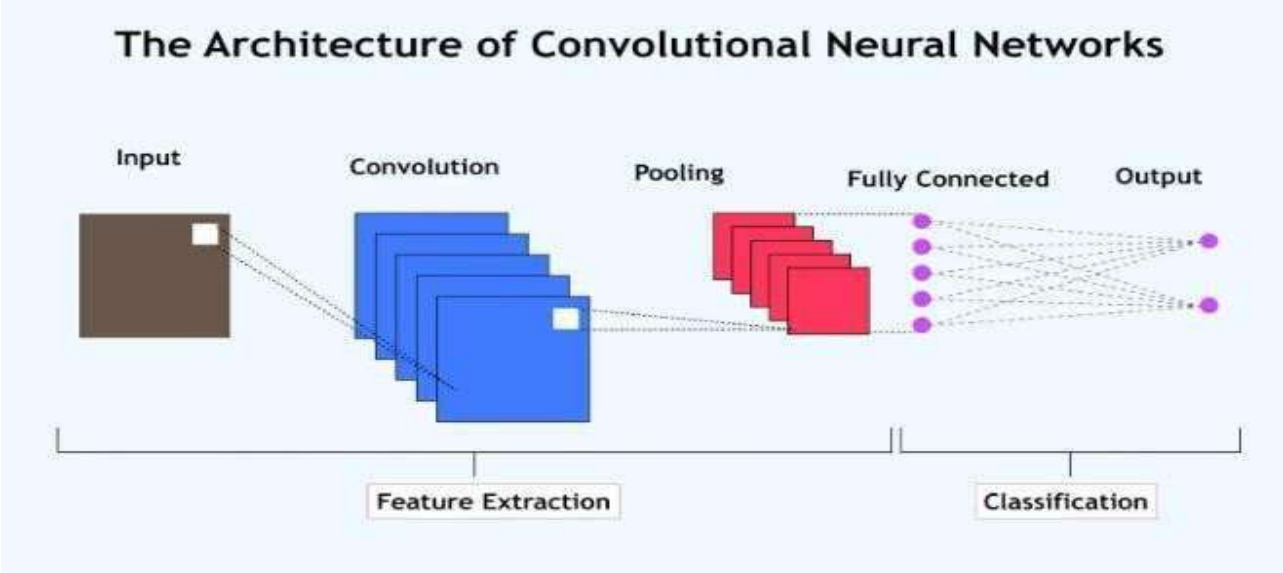

Figure 1: System Architecture

E-ISSN: 2349-7017
P-ISSN: 2349-7009
https://www.ijiris.com/archives
https://doi.org/10.26562/ijiris.2026.v1204.07

The architecture of the proposed zero-watermarking framework is designed to provide secure and loss less protection for medical images through deep learning techniques. Initially, the input image is subjected to preprocessing operations such as resizing, normalization, and noise reduction to ensure uniform quality. The preprocessed image is then fed into a Convolutional Neural Network, where deep features representing both structural and semantic characteristics are extracted. These features are combined with a predefined watermark to generate a distinct zero-watermark signature without modifying the original image. The generated signature is securely stored in a database for future reference. During the verification phase, features are re-extracted from a test image and compared with the stored signature using similarity measures. Based on this comparison, the system determines whether the image is authentic or has been tampered with.

METHODOLOGIES

The proposed methodology starts with the acquisition of medical images from reliable sources, followed by preprocessing steps including resizing, normalization, and noise reduction to ensure uniform input quality. The processed images are then fed into a Convolutional Neural Network to obtain deep feature representations that capture both structural patterns and semantic details. These extracted features are transformed into a binary format and combined with a predefined watermark using logical operations to produce a unique zero-watermark signature. This signature is securely stored for future use. During the authentication phase, features are re-extracted from the test image using the same process and compared with the stored signature. Similarity measures are applied to evaluate the match, allowing the system to accurately determine whether the image is original or has been tampered with.

MODULE NAMES:

- Image Acquisition
- Preprocessing
- Feature Extraction
- Zero-Watermark Generation
- Watermark Verification
- Attack Simulation
- Performance Evaluation

MODULES EXPLA0NATION:

1. Image Acquisition: Medical images such as MRI, CT, and X-ray are collected from datasets or healthcare systems. The data is verified and formatted to ensure consistency and reliability. These images serve as the input for the system.
2. Preprocessing: The input images are enhanced using operations like resizing, normalization, and noise reduction. This step ensures uniform quality and minimizes variations caused by different imaging conditions.
3. Feature Extraction: A Convolutional Neural Network is used to extract deep feature representations from the images. These features capture both structural patterns and semantic information effectively.
4. Zero-Watermark Generation: The extracted features are combined with a predefined watermark to generate a unique signature without modifying the original image. The generated watermark is securely stored.
5. Watermark Verification: Features from a test image are extracted and compared with the stored signature. Based on similarity, the system identifies whether the image is authentic or tampered.
6. Attack Simulation: Various distortions such as noise, compression, and rotation are applied to evaluate system robustness under different conditions.
7. Performance Evaluation: The system performance is analyzed using similarity and correlation measures, and results are compared with existing approaches.

IMPLEMENTATION
EXPERIMENTAL RESULTS

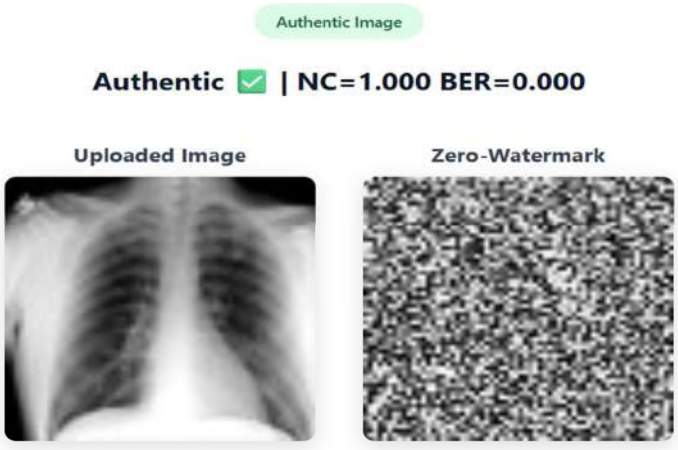

Figure2: Successful Authentication Result

E-ISSN: 2349-7017
P-ISSN: 2349-7009
https://www.ijiris.com/archives
https://doi.org/10.26562/ijiris.2026.v1204.07

The implementation of the proposed framework is developed using Python along with deep learning and image processing libraries such as TensorFlow, OpenCV, NumPy, and Matplotlib. The process begins with loading and organizing the medical image dataset, followed by preprocessing operations including resizing, normalization, and noise reduction to ensure uniform input quality. A pretrained Convolutional Neural Network is then employed for feature extraction by removing the final classification layers and obtaining feature evectors from intermediate layers. These features are transformed into a binary representation and combined with a predefined watermark using logical operations to create a unique zero-watermark signature. The generated signature is securely stored for later use. During verification, a test image undergoes the same processing steps, and its extracted features are compared with the stored signature using similarity measures to determine authenticity. The overall pipeline ensures efficient processing, reliable authentication, and strong resistance to various image distortions.

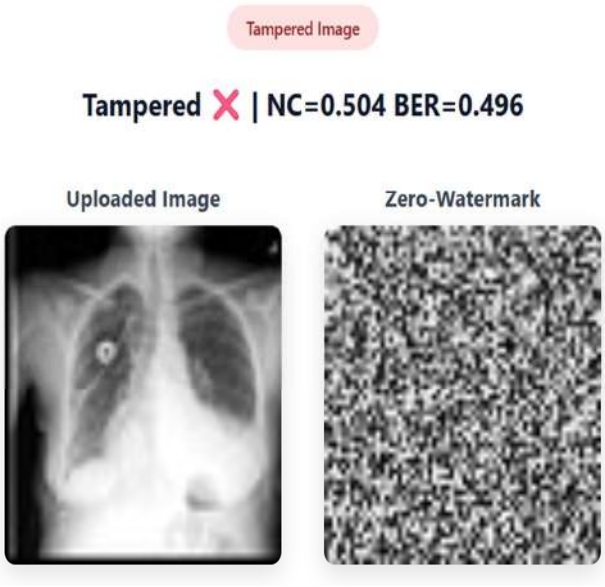

Figure 3: Tampered Image Detection

Figure 2 illustrates the successful authentication of an original medical image. The system extracts deep feature representations using the Convolutional Neural Network and compares them with the stored zero-watermark signature. As the features show a high level of similarity, the image is classified as authentic, confirming that no alterations have been made and ensuring reliable ownership verification. Figure 3 demonstrates the detection of a tampered image, where a modified input is provided. In this case, the extracted features differ significantly from the stored signature, resulting in a mismatch and classification of the image as tampered. These outcomes highlight the capability of the proposed system to effectively differentiate between genuine and altered images, ensuring accurate and reliable authentication.

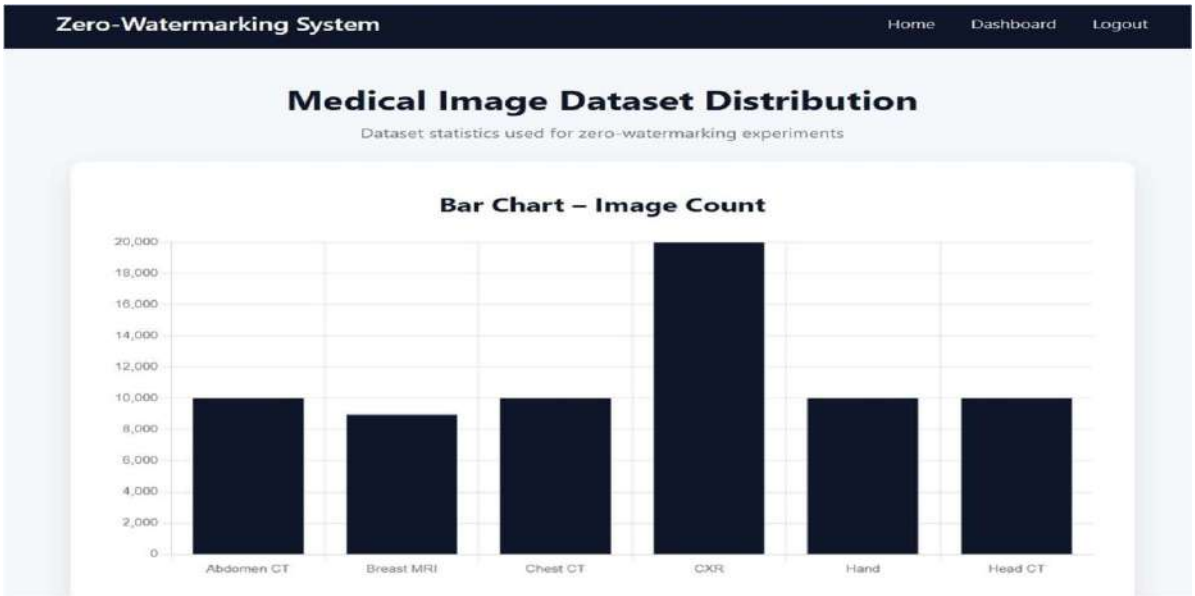

Figure 4: Bar Chart Visualization

E-ISSN: 2349-7017
P-ISSN: 2349-7009
https://www.ijiris.com/archives
https://doi.org/10.26562/ijiris.2026.v1204.07

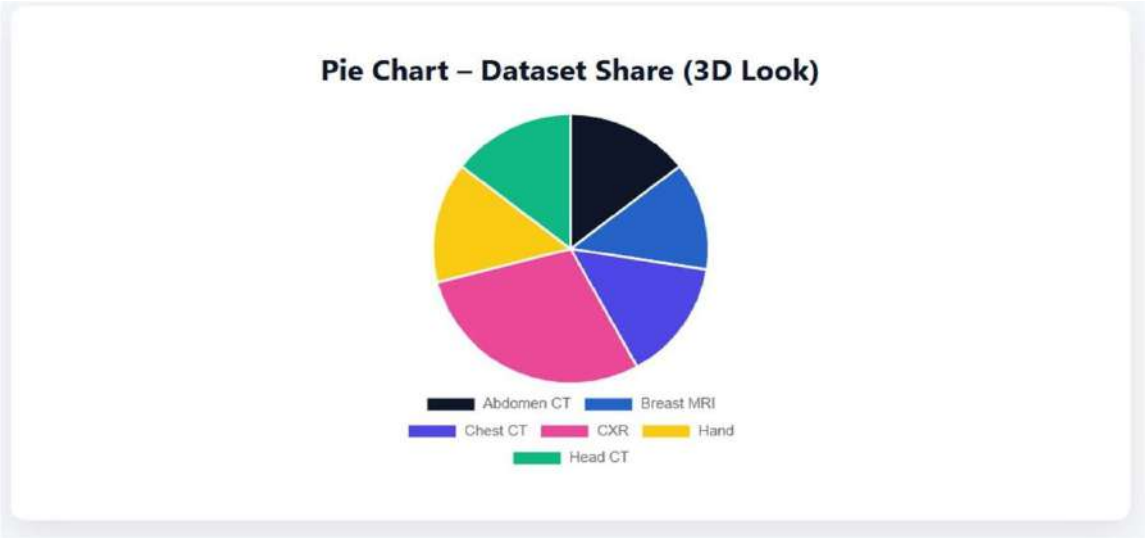

Figure 5: Pie Chart Visualization

Figure 4 illustrates a bar chart representing the overall performance behavior of the proposed system based on key factors such as accuracy, robustness, and reliability. The chart indicates stable performance across different conditions, highlighting the effectiveness of the framework in medical image authentication. Figure 5 presents a pie chart showing the distribution of system outcomes, including successful authentication and tamper detection. The results indicate a high proportion of correctly authenticated images along with accurate identification of altered inputs, demonstrating the reliability and practical applicability of the proposed approach.

CONCLUSION

The proposed system presents a secure zero-watermarking framework for medical image authentication using deep feature extraction. By leveraging Convolutional Neural Networks, it generates a unique watermark signature without modifying the original image, thereby preserving diagnostic quality. The system effectively distinguishes between authentic and tampered images through feature similarity comparison, ensuring reliable integrity verification. The results indicate consistent performance and robustness against common image processing and geometric distortions. Overall, the approach provides a practical solution for protecting medical images in modern healthcare environments. Future work can focus on improving scalability and incorporating advanced deep learning models to enhance accuracy.

FUTURE ENHANCEMENT

Future improvements can focus on enhancing accuracy, scalability, and real-time performance of the proposed system. Advanced deep learning techniques, including transformer-based models, can be integrated to obtain more robust feature representations. The framework can be extended to support real-time authentication in cloud-based and telemedicine environments. Incorporating secure storage solutions such as blockchain can further strengthen data integrity and watermark security. Additionally, optimization methods can be applied to reduce computational complexity and improve efficiency for large-scale datasets. The system can also be adapted to support various medical imaging modalities, increasing its applicability across different healthcare scenarios.

REFERENCES

1. Han,Y.,etal., “Zero-Water marking Algorithm for Medical Images Based on VGG19 Convolutional Neural Network,” IEEE Access, 2021.
2. Dong,L.,etal., “Robust Zero-Water marking Algorithm for Medical Images Based on Improved NasNet-Mobile and DCT,” Electronics, vol. 12, no. 16, 2023.
3. Sheng, Y., et al., “Zero Watermarking Algorithm for Medical Image Based on ResNet50 and DCT,” Multimedia Tools and Applications, 2023.
4. Shi,X.,etal., “A Novel Zero Watermarking Algorithm Based on Multimodal Fusion with VGG16 and Chaotic Encryption,” IEEE Transactions on Multimedia, 2023.
5. Li,Z.,etal., “Medical Image Zero Watermarking Algorithm Based on Dual-Branch Network,”Pattern Recognition Letters, 2024.
6. Arévalo-Ancona, R., et al., “Secure Medical Image Authentication Using Zero Watermarking Based on Deep Learning Context Encoder,” Journal of Healthcare Engineering, 2024.
7. Xiang,L.,etal., “Zero-Water marking Scheme for Medical Image Protection Based on Deep Residual Network,” Biomedical Signal Processing and Control,2023.
8. Wang,S.,etal., “Deep Learning-Based Image Water marking: A Comprehensive Survey, ”IEEE Access,2023.

E-ISSN: 2349-7017
P-ISSN: 2349-7009
https://www.ijiris.com/archives
https://doi.org/10.26562/ijiris.2026.v1204.07

9. Zhang,H.,etal.,"Deep Learning-Based Robust Image Water marking Techniques: A Review, "Multimedia Tools and Applications,2022.
10. Good fellow,I.,Bengio,Y.,and Courville, A.,Deep Learning, MITPress,2016.
11. He, K., et al., "Deep Residual Learning for Image Recognition," IEEE Conference on Computer Vision and Pattern Recognition, 2016.
12. Simonyan,K.,and Zisserman, A.,"Very Deep Convolutional Networks for Large-Scale Image Recognition," International Conference on Learning Representations,2015.
13. Howard,A.,etal.,"Mobile Nets: Efficient Convolutional Neural Networks for Mobile Vision Applications,"2017.
14. Zhu,H.,etal.,"Image Analysis by Discrete Orthogonal Racah Moments,"Signal Processing, 2007.
15. Xiao,B.,etal.,"Image Analysis by Fractional-Order Orthogonal Moments, "Information Sciences,2017.
16. Zhou,J.,etal.,"Robust Zero-Watermarking Scheme Based on Deep Feature Extraction for Medical Images,"IEEE Access, 2022.
17. Liu,Y.,etal.,"A Deep Learning-Based Image Water marking Frame work for Secure Medical Data Transmission," MultimediaTools and Applications,2022.
18. Nasrullah, N., et al., "Deep Learning for Medical Image Security and Authentication: A Survey, "Journal of Medical Systems, 2021.
19. Su,Q.,etal.,"A Robust Digital Image Water marking Method Based on DCT and SVD, "IEEE Transactions on Multimedia, 2020.
20. Chen, B., etal., "Robust Image Water marking Based on Deep Neural Networks and Feature Fusion," Signal Processing, 2023.