

Paper Type: Original Article

## Robust Zero-Watermarking for Color Images Using VGG16 and Discrete Wavelet Transform

Amal Magdi <sup>1</sup> , Osama M. ElKomy <sup>1</sup> , Hanaa M. Hamza <sup>1</sup>  and Khalid M. Hosny <sup>1,\*</sup> 

<sup>1</sup>Department of Information Technology, Faculty of Computers and Informatics, Zagazig University, Zagazig 44511, Egypt.  
Emails: amal.magdi15@gmail.com; osamaelkomy@yahoo.com; hanaa\_hamza2000@yahoo.com; k\_hosny@zu.edu.eg.

Received: 10 Dec 2025

Revised: 10 Jan 2026

Accepted: 05 Feb 2026

Published: 07 Feb 2026

### Abstract

Classical watermarking systems have been created to protect images using spatial and transform domains. However, traditional watermarking systems are more vulnerable to various assaults. Deep learning-based watermarking has recently gained popularity for its contribution to image security. This work presents a zero-watermarking method for protecting color images using VGG16, the discrete wavelet transform (DWT), and chaotic encryption. DWT is applied to the input color image, and the resulting features are fed into the VGG16 pre-trained network for deep feature extraction. DWT decreases complexity by acting as a pre-feature extractor. The Henon chaotic map is applied to encrypt the binary watermark image. A zero watermark is produced by combining the derived image features with the encrypted binary watermark image via an exclusive OR operation. The experimental results show that our technique is effective and resilient against geometric and typical image-processing attacks.

**Keywords:** Deep Learning, Zero Watermarking, VGG16, Discrete Wavelet Transform.

## 1 | Introduction

Digital image security is crucial for protecting private and sensitive information about the content owner [1]. Watermarking is critical for securing sensitive digital images from unauthorized access, which can have significant consequences [2]. Image watermarking conceals copyright marks in cover images, making them less noticeable and more durable [3]. Watermarking schemes are categorized as blind or non-blind based on the extraction criteria. Blind watermarking allows extraction without the original image, whereas non-blind watermarking requires the original image [4].

Image watermarking systems are often classified as either spatial-domain or frequency-domain algorithms depending on where the embedding occurs [5]. Spatial-domain watermarking methods integrate the watermark directly into the pixel values. Although the algorithm is simple, it is not very robust [6]. In frequency domain approaches, the watermark is inserted by modifying the image's transform coefficients [7]. The discrete cosine transform (DCT) [8], discrete wavelet transforms (DWT) [9], and discrete Fourier transform (DFT) [10] are among the most widely used frequency-domain transformation methods.

DWT is an appropriate frequency-domain transform for watermarking because of its multi-level decomposition, which allows selection of subbands that provide both resilience and imperceptibility [11]. The discrete wavelet transform (DWT) is considered a very successful approach for extracting image features due to its multi-level decomposition [12]. DWT is ideal for real-time image processing and embedded systems due to its low complexity [13].



Corresponding Author: [k\\_hosny@zu.edu.eg](mailto:k_hosny@zu.edu.eg)



Licensee International Journal of Computers and Informatics. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0>).

Watermarking research employing deep learning is still in its early stages, although the number of studies has been expanding in recent years [14]. Deep learning is fundamentally based on artificial neural networks that mimic the structure and operation of the human brain [15]. Deep learning emerges as an important supporting technology to improve the robustness and adaptability of image watermarking [16]. Deep learning-based watermarking approaches, unlike traditional methods, may learn and grow over time [17].

CNNs are a significant deep learning architecture for processing visual data and are commonly used in applications such as image watermarking [18]. Among the several CNN architectures is the well-known VGGNet [19]. There are two types of VGGNet: VGG16 and VGG19 [20]. VGG16 comprises 16 layers (13 convolution layers, 3 fully connected layers), whereas VGG19 consists of 19 layers (16 convolution layers + 3 fully connected layers) [21]. VGG16 is simpler and quicker. VGG19 requires more computation and memory due to the additional convolutional layers [22]. VGG16 offers faster feature extraction and lower latency [23]. VGG16 is more efficient and often performs as well in real-world settings. VGG16 is usually the optimal choice for feature extraction [24].

A chaotic system is a cryptographic method that is often used in image encryption [25]. In the past 20 years, there has been a tremendous increase in the application of chaotic systems in cryptography. The great sensitivity of chaotic systems to initial values and parameter changes makes them an excellent candidate for improving image watermarking security [26]. Chaotic maps such as the Henon, logistic, and Arnold maps are commonly used for digital image watermarking [27]. The Henon map offers a better balance between complexity and computational efficiency [28]. Because the Henon map is two-dimensional, it produces two linked chaotic sequences, which improves unpredictability [29].

This study offers a novel semi-blind zero-watermarking method designed for color RGB images. The process begins by applying the DWT to the color image channels for feature extraction, and the extracted features are fed into the VGG16 pre-trained deep learning network to obtain deep features from the second fully connected layer. The second fully connected layer is more resilient because it collects global, high-level features that are less vulnerable to slight distortions. These extracted features are then combined with the chaotic-encrypted binary watermark via an XOR operation. The use of Henon-based encryption significantly enhances the security of the proposed zero-watermarking framework.

Our approach differs from previous DL-based zero-watermarking systems by combining DWT + VGG16 feature-level processing with Henon-based encryption. Our suggested method shows more robustness in terms of color photos and color medical imaging. Prior to applying vgg16, using DWT lowers noise and boosts important frequencies. As a result, the neural network has less computational load, leading to a quicker training model. The main contribution of this work can be outlined as:

- DWT and VGG16 are used to extract robust features from medical color images.
- The feature map and scrambled binary watermark image are combined to produce zero watermarking.
- The Henon chaotic map adds security to the watermarking technique.
- Experimental results indicate that the proposed strategy balances robustness with imperceptibility.

The article's remaining content is organized as follows: Section 2 provides preliminary information; Section 3 depicts the proposed deep learning watermarking technique; Section 4 presents experimental findings; and Section 5 provides a conclusion.

## 2 | Preliminaries

### 2.1 | VGG16

VGG16 belongs to the VGGNet family and comprises 13 convolutional layers followed by 3 fully connected layers, yielding a total of 16 hidden layers [30]. In this architecture, convolutional layers are organized into multiple blocks, each succeeded by a max-pooling operation and then connected to fully connected layers [31]. The architecture of VGG16 can be explained as seen in Figure 1:

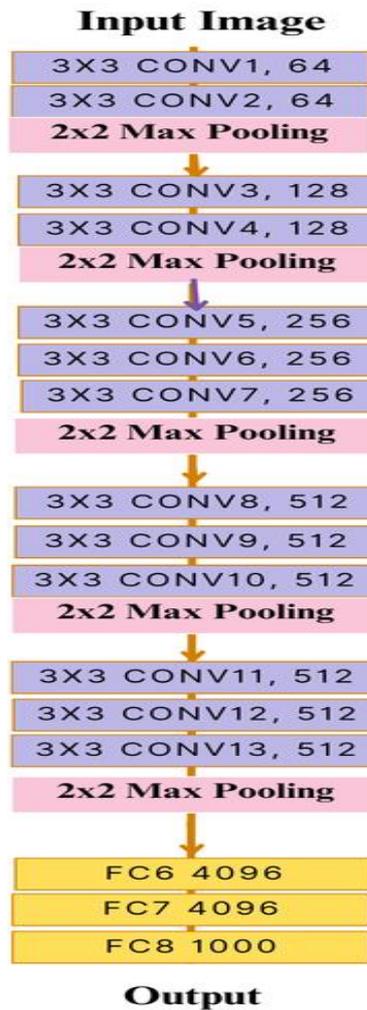


Figure 1. VGG16 architecture.

- The input is a 224x224x3 image.
- Convolutional Layers: There are multiple convolutional layers arranged in blocks. 3x3 convolutional kernels are used in each block. Following every convolution, max-pooling (2x2) is used to minimize the spatial dimensions, and ReLU is used as the activation function.
- Fully Connected Layers: Three fully connected layers are applied after the convolutional layers. 4096 units make up the first two fully connected levels, while the number of units in the final layer is equal to the number of classes in the classification task.
- Output Layer: Usually employed for classification (softmax output layer).

## 2.2 | Discrete Wavelet Transform (DWT)

DWT divides an image into four subbands: LL for approximation content and LH, HL, and HH for vertical, horizontal, and diagonal details [32]. The notation L represents low-pass filtering, whereas H indicates high-pass filtering performed on both rows and columns. The DWT offers a representation of an image in both spatial and frequency domains [33]. Its high energy compaction makes DWT-based techniques widely used in image processing applications, including watermarking [34]. The LL subband, carrying most of the image's energy, improves watermark robustness when used for embedding but can reduce invisibility [35]. The HH subband, rich in fine details, allows more hidden embedding but results in weaker robustness [36]. Therefore, watermarking is usually performed in the LH or HL subbands, which offer a more suitable trade-off [37]. The 2-level 2D DWT decomposition is depicted in Figure 2.

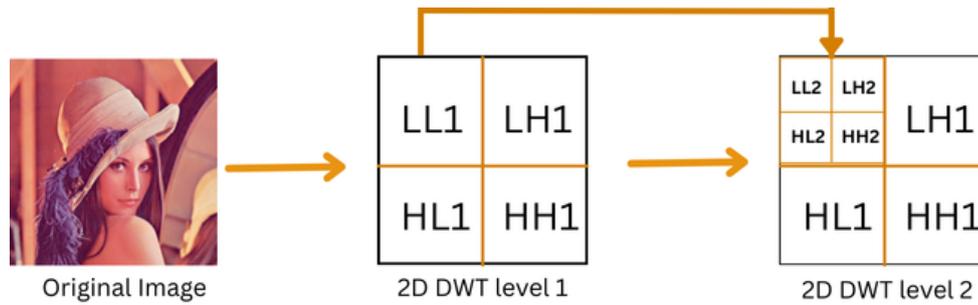


Figure 2. 2-level DWT decomposition.

### 2.3 | Henon Chaotic Map

The Henon map, first proposed by Michel Henon in 1969, is a two-dimensional nonlinear discrete chaotic system that depends on two input parameters and exhibits strong sensitivity to initial conditions. Because it operates with two independent parameters, it provides stronger security than one-dimensional chaotic methods, such as the logistic map. It is therefore effective for producing pseudo-random sequences in image encryption. It is mathematically described as:

$$x_{n+1} = 1 - ax_n^2 + y_n \quad (1)$$

$$y_{n+1} = bx_n \quad (2)$$

The map typically operates with chaotic parameters  $a=1.4$  and  $b=0.3$ . The system variables are denoted by  $x$  and  $y$ , and  $n$  represents the iteration number. Fig. 3 shows Henon chaotic behaviour.

The Henon map parameters and initial conditions expressed in double precision, make up the encryption key  $K = \{a, b, x_0, y_0\}$ . This results in a key space of around  $10^{60}$ , which is adequate to fend off brute-force assaults. These parameters are safely kept and exchanged via a secured key-management method, and they are utilized to construct the chaotic sequence for encryption and decryption.

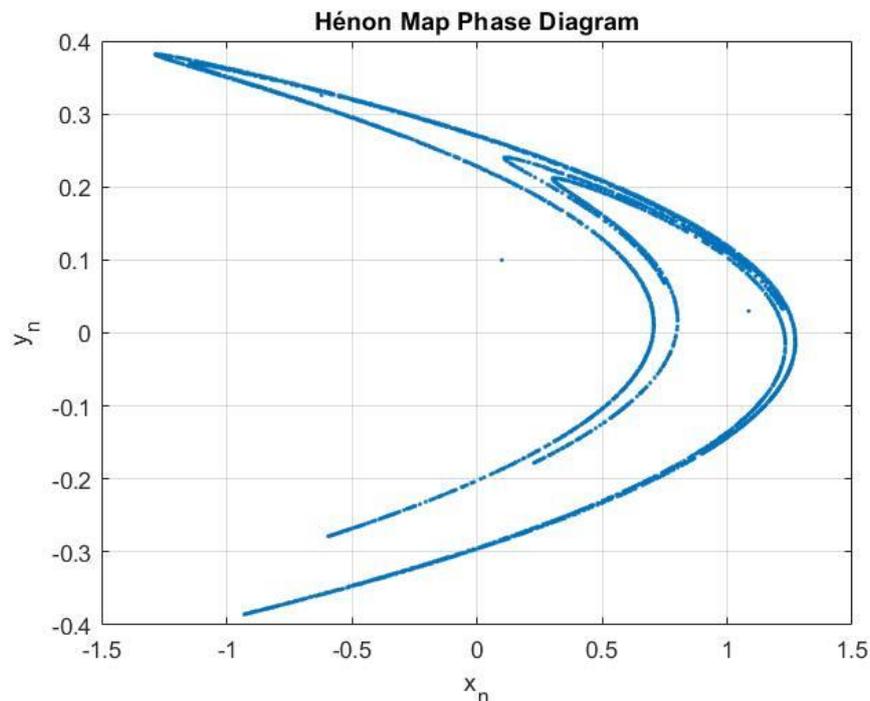


Figure 3. Henon map phase diagram.

## 3 | The Proposed Watermarking Algorithm

In this study, a zero-watermarking approach is used, in which the watermark is bound to the image's feature representation. Robust watermarking requires a stable feature vector, which is obtained using DWT and the

trained VGG16 network. The subsequent section details the embedding and extraction stages of the proposed method.

### 3.1 | Watermark Embedding

Figure 4 and 5 depicts the process of watermark embedding, which includes the following steps:

- Step 1: The original image is first processed using the DWT to extract its features. The image is decomposed into 4 subbands. LL subband features are extracted because they are more resilient to compression, noise, and filtering, and exhibit less visual distortion than other subbands.
- Step 2: The DWT-derived features are fed into a pre-trained VGG16 network to extract deep features and enhance the watermarking system's resilience. Before using a neural network, DWT reduces noise and enhances essential frequencies. This reduces computational strain on the neural network, resulting in a faster training model. The hybrid technique is more accurate and efficient than the standalone VGG16.
- Step 3: The binary watermark image is scrambled and encrypted using the Henon chaotic map. We begin by generating the chaotic sequence  $XY(n)$  based on the initial parameters  $X0$  and  $Y0$ . The resulting sequence is then quantized: values greater than or equal to zero are assigned a "1" and values less than zero are assigned a "0", producing a binary-encrypted sequence.
- Step 4: The FC2 layer of VGG16 generates a 4096-dimensional feature vector, which is binarized and reshaped into a  $64 \times 64$  map for XOR-based zero-watermark creation. Where binarized feature  $\text{map}(i) = 1$  when  $\text{feature map}(i) \geq \text{average feature map}$  chosen, and 0 otherwise.
- Step 5: The zero watermark is produced by applying an XOR operation between the binarized extracted feature vector and the encrypted watermark.

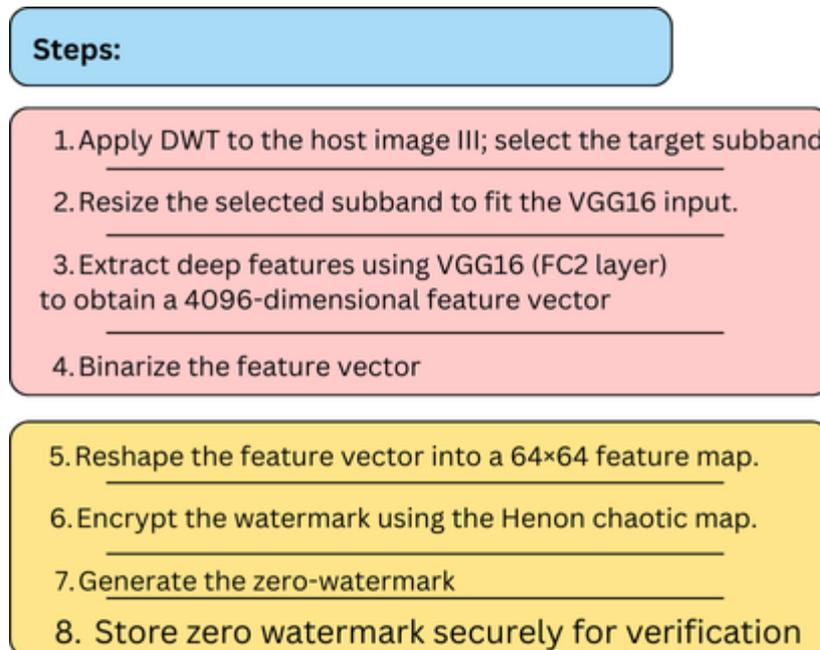


Figure 4. Watermark generation algorithm blocks.

### 3.2 | Watermark Extraction

Figure 6 depicts the process of watermark extraction, which includes the following steps:

- Step 1: The feature vector of the test image is extracted using the same procedure employed during the watermark embedding stage.

- Step 2: An XOR operation is performed between the feature vector and the zero watermark, enabling retrieval of the encrypted multi-watermark information.
- Step 3: Watermark decryption involves XORing the retrieved encrypted watermark with the binary encryption sequence to recover the watermark information.

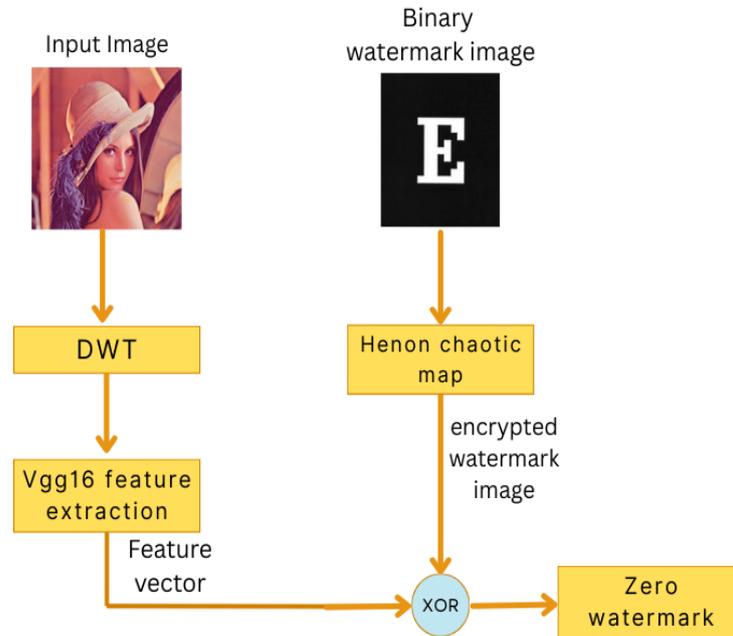


Figure 5. Watermark embedding procedure.

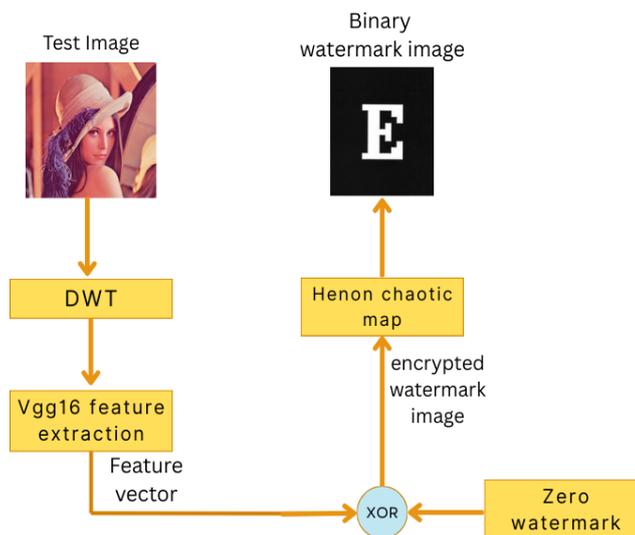


Figure 6. Watermark extraction procedure.

## 4 | Experimental Results

The experiments were conducted using MATLAB 2019a as the development environment and on a machine with an Intel Core i7 CPU (1.80–1.99 GHz) and 16 GB RAM. The primary objective of the experimental work is to evaluate the performance of the proposed watermarking algorithm under both conventional and geometric attacks. A diverse set of 512×512 color host images collected from multiple datasets was employed, along with binary watermark images of size 64×64. Standard benchmark pictures were sourced from the USC-SIPI Image Database and the MATLAB Image Processing Toolbox demo image collection. These images are presented in Figs. 7 and 8, respectively. The computation time, divided into zero-watermark creation and watermark image extraction, may be utilized to assess the complexity of

a watermarking process. Our proposed approach requires just 0.650391 and 1 seconds to generate and extract zero watermarks, respectively.



Figure 7. Samples of host color images.

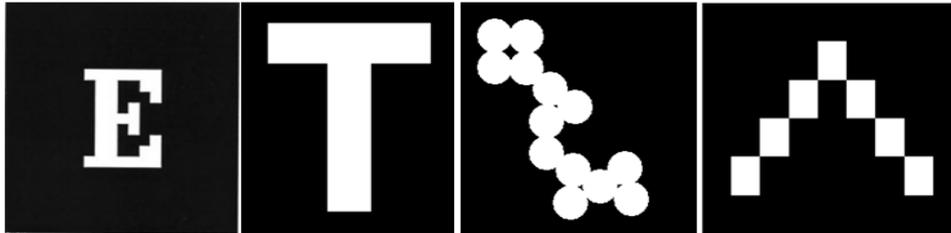


Figure 8. Samples of binary watermark images.

#### 4.1 | Metrics Used for Performance Assessment

Our experimental analysis relies on three performance measures: peak signal-to-noise ratio (PSNR), bit error rate (BER), and normalized correlation coefficient (NC). PSNR measures the amount of distortion in images after watermark embedding; a lower PSNR value indicates greater distortion. The PSNR formula is presented in Equation 3 between the attacked and original image. BER is the ratio of wrongly extracted bits to the total encoded bits, and a lower value reflects higher embedding performance.

$$PSNR = 10 \log_{10} \frac{MN \max(I(i, j))^2}{\sum_{i=1}^p \sum_{j=1}^q [I(i, j) - I'(i, j)]^2} \quad (3)$$

In addition, the normalized correlation coefficient (NC), defined in Equation 4, is used to evaluate the similarity between the original watermark and the extracted one. An NC value approaching 1 indicates a high degree of correlation, reflecting the algorithm's greater robustness against various attacks.

$$NC = \frac{\sum_{i=1}^p \sum_{j=1}^q [W(i, j) \times W_{\text{extracted}}(i, j)]}{\sum_{i=1}^p \sum_{j=1}^q [W(i, j)]^2} \quad (4)$$

#### 4.2 | Evaluation Results Against Attacks

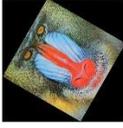
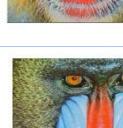
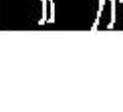
In this simulation study, we evaluated the effects of conventional, geometric, and hybrid attacks of varying intensities on a diverse set of color images. Additionally, a comparative analysis with existing watermarking algorithms was conducted. The experimental outcomes reported in the tables were generated using the Mandrill image as the reference host image. VGG16 requires a fixed input size of  $224 \times 224$ , therefore host images are scaled to this size before being fed into the network for feature extraction. Images with varied resolutions or non-square aspect ratios are preprocessed using uniform scaling, followed by resizing to  $224 \times 224$ .

##### 4.2.1 | Geometric Attacks

Since geometric robustness is crucial, the algorithm was tested against multiple geometric attacks—including rotation, scaling, and translation. As illustrated in Table 1, reliable watermark extraction was achieved under

all attack types. Experimental results indicate that the proposed approach maintains robustness under geometric attacks, including rotation, scaling, and translation.

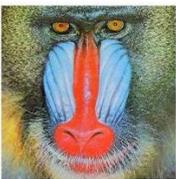
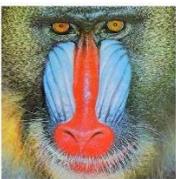
**Table 1.** Results against geometric attacks.

Attacks		PSNR	BER	NC	Attacked Image	Extracted Watermark
Rotation Attack (Bicubic interpolation)	20°	25.9566	0.0006	0.9990		
	40°	25.5233	0.0007	0.9989		
	60°	25.5924	0.0006	0.9990		
	80°	26.3856	0.0007	0.9989		
Scaling Attack (nearest scaling)	0.5	30.4058	0.0002	0.9996		
	1.5	35.8678	0	1		
	2	35.7239	0	1		
Translation Attack	(H2,V2)	29.1612	0.0002	0.9996		
	(H5,V5)	28.6450	0.0002	0.9996		
Cropping (Center)	32	48.1478	0.0002	0.9996		

## 4.2.2| Conventional Attacks

Conventional attacks refer to intentional manipulations that distort an image's pixel intensities without altering its geometric configuration. These attacks are often applied to test the resilience of image watermarking methods. We examined the algorithm's performance under three such attacks—JPEG compression, average filtering, and median filtering. Table 2 shows that the watermark remains recoverable, indicating that the proposed method offers strong resistance to conventional distortions.

**Table 2.** Results against conventional attacks

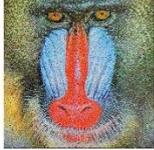
Attacks		PSNR	BER	NC	Attacked Image	Extracted Watermark
JPEG compression	40%	30.6521	0.0002	0.9996		
	70%	31.3743	0.0002	0.9996		
	90%	32.7037	0	1		
Average filter	3	30.5574	0.0002	0.9996		
	5	29.8525	0.0007	0.9989		
	7	29.5626	0.0010	0.9986		
Median filter	3	31.3107	0.0005	0.9993		
	5	30.1915	0.0005	0.9993		

	7	29.8868	0.0007	0.9989		
--	---	---------	--------	--------	--	---

### 4.2.3 | Hybrid Attacks

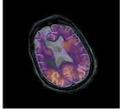
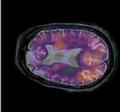
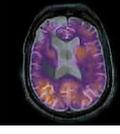
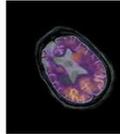
By combining two or more attack types, hybrid attacks create more severe distortion scenarios for evaluating the robustness of image watermarking and related systems. The cumulative effects of combined attacks make them a stringent benchmark for algorithm reliability. Table 3 confirms that the proposed scheme provides strong resistance to these hybrid distortions.

**Table 3.** Results against hybrid attacks

Attacks/images	PSNR	BER	NC	Attacked Image	Extracted Watermark
Salt & Pepper noise 0.1 + JPEG 90 %	29.7473	0.0002	0.9996		
Scaling 1.5 + JPEG compression 90 %	30.4432	0	1		
Rotation 35° + JPEG compression 90 %	25.5665	0.0007	0.9989		
Median filter 3+JPEG 90 %	30.7191	0.0002	0.9996		
Winner filter 5 + Salt & Pepper noise 0.01	30.3885	0.0002	0.9996		

The robustness of the proposed method is evaluated against attacks. Table 4 presents the resulting PSNR, BER, and NCC metrics obtained for a medical image. The experimental results indicate that the method is capable of reliably extracting the embedded watermark from medical images while maintaining robustness under a wide range of attack conditions. We also carried out experiments comparing VGG16 alone to DWT + VGG16 for our proposed zero-watermark approach in order to quantitatively support the usage of DWT as a pre-feature extractor. NC is calculated to gauge how resilient a watermark is to different types of assaults, and as table 5 illustrates, it increases when DWT preprocessing is used.

**Table 4.** Analysis Results on medical image

Attacks		PSNR	BER	NC	Attacked Image	Extracted Watermark
<b>Rotation Attack</b>	20°	28.8871	0.0002	0.9996		
	60°	28.6815	0.0005	0.9993		
	80°	29.3680	0.0005	0.9993		
<b>Scaling Attack</b>	0.5	47.0435	0	1		
<b>JPEG Compression</b>	40%	46.0856	0	1		
<b>Average filter</b>	3x3	44.6670	0	1		
<b>Median filter</b>	3x3	47.1573	0	1		
Rotation 35° + JPEG compression 90 %		28.5994	0.0005	0.9993		

**Table 5.** NC results without applying DWT.

Attacks		NC
<b>Rotation Attack</b>	20°	0.9973
<b>Scaling Attack</b>	0.5	0.9964
<b>JPEG Compression</b>	40%	0.9978
<b>Average filter</b>	3x3	0.9971
<b>Median filter</b>	3x3	0.9971

Additionally, we examined the stability of the features that our algorithm extracted. This implies that when the images are significantly altered—for example, by adding noise or rotating them—we investigated whether the features remain stable. Using NC, we assessed stability in a number of experiments. As table 6 illustrates, the findings demonstrate that our approach maintains the key features, indicating that it can function effectively even when images are somewhat modified.

**Table 6.** NC results for features stability.

Attacks	NC
No attack	1
Gaussian Noise 0.01	0.99999
Gaussian Noise 0.05	0.99994
JPEG 50	1
Rotation 5	0.99969
Cropping 10	0.99996

#### 4.2.4 | Comparison with other algorithms

Several experimental comparisons were conducted to assess the algorithm's resistance to various attacks. The results in Table 7 reveal that the proposed approach achieves marginally superior performance compared to the methods reported in [38–42]. Recent studies show a growing move toward deep learning and hybrid intelligent methods to strengthen watermarking security and robustness. Rai et al. [38] used an optimized fusion CNN to achieve strong imperceptibility and robustness against attacks. Sinhal et al. [39] proposed a lightweight ML-based blind watermarking technique. Jaiswal and Pandey [40] applied a deep ANN for blind color watermarking with improved robustness. Dwivedi et al. [41] enhanced security by combining redundant DWT, randomized SVD, and Henon chaos in a dual watermarking method. Li et al. [42] introduced ZWNET, a DL-based zero-watermarking approach that avoids modifying the host image. These works highlight the increasing success of deep learning and hybrid frameworks in watermarking.

**Table 7.** NC values comparison between different algorithms.

Attack	Ref. [38]	Ref. [39]	Ref. [40]	Ref. [41]	Ref. [42]	Proposed Method
JPEG compression 90	0.9362	1	-	0.9876	-	1
Rotation 90	0.9807	-	0.2344	0.2043	0.9063	0.9989
Scaling 0.7	0.9972	-	0.5195	-	-	0.9996
Salt & pepper 0.01	0.9784	0.998	0.8985	0.8465	0.9961	0.9996
Salt & pepper 0.02	0.9727	0.976	0.7852	-	0.9609	0.9996
Average filter 9x9	0.9975	-	0.2344	0.7284	0.9766	0.9982
Median filter 3x3	0.9771	0.72	-	0.835	0.9688	0.9993
Gaussian filter 3x3	0.9937	0.90	-	0.9803	0.9883	0.9989
Winner filter 2x2	1	0.964	-	-	-	1

### 4.2.5 | Henon Map Key Sensitivity

The Mandrill image is used to assess the Henon chaotic map's sensitivity to small changes in control parameters. Two cipher images are created with nearly identical parameter values, varying only by a little modification in one parameter. The resultant encrypted images are significantly different, as evidenced by high NPCR (Number of Pixel Change Rate) and UACI (Unified Average Changing Intensity) values. This behavior reveals the Henon map's high parameter sensitivity, confirming its applicability for secure image encryption.

The suggested zero-watermarking approach does not embed the watermark in the host image; instead, security is based on the stability of extracted features. An attacker can access the original or encrypted picture, but not the secret keys. While simple image alterations are allowed, the DWT + VGG16 features remain strong and restrict watermark removal. Furthermore, our key-sensitivity study of the Henon map reveals that even little changes in secret parameters result in dramatically different encrypted outputs, substantially protecting the system.

**Table 8.** Henon Map key sensitivity analysis.

Parameter Change	NPCR (%)	UACI (%)
$a = 1.4 \rightarrow 1.4000001$	99.62	33.41

## 5 | Conclusion

A zero-watermarking scheme combining DWT and VGG16 is proposed to address vulnerability to geometric attacks. DWT-based subband features and VGG16 deep descriptors are used to construct the zero watermark, and integrating DWT, neural networks, and zero-watermarking principles further enhances geometric resistance. The watermark is further protected through encryption using the Henon chaotic map. Experimental evaluation demonstrates that the method supports both watermark embeddings and extractions with high robustness. In future research, we aim to adapt and enhance the proposed method for medical imaging, as well as explore its potential for video authentication applications.

### Author Contribution

Amal Magdi: Conceptualization, Methodology, Software, Writing—original draft.

Osama ElKomy: Validation, Writing—review and editing.

Hanaa Hamza: Validation, Writing—review and editing.

Khalid M. Hosny: Conceptualization, Supervision, Writing—review and editing.

### Funding

This research has no funding source.

### Data Availability

The images used in this work are standard test images provided with MATLAB's Image Processing Toolbox and are publicly accessible for research and educational purposes

### Conflicts of Interest

The authors declare that there is no conflict of interest in the research.

## References

- [1] Singh, H. K., & Singh, A. K. (2024). Digital image watermarking using deep learning. *Multimedia Tools and Applications*, 83(1), 2979-2994.
- [2] Hatoum, M. W., Couchot, J. F., Couturier, R., & Darazi, R. (2021). Using deep learning for image watermarking attack. *Signal Processing: Image Communication*, 90, 116019.
- [3] Lee, J. E., Kang, J. W., Kim, W. S., Kim, J. K., Seo, Y. H., & Kim, D. W. (2021). Digital image watermarking processor based on deep learning. *Electronics*, 10(10), 1183.
- [4] Boujerfaoui, S., Riad, R., Douzi, H., Ros, F., & Harba, R. (2022). Image watermarking between conventional and learning-based techniques: a literature review. *Electronics*, 12(1), 74.
- [5] Ali, M., & Kumar, S. (2024). A robust zero-watermarking scheme in spatial domain by achieving features similar to frequency domain. *Electronics*, 13(2), 435.
- [6] Ali, M. (2023). Robust image watermarking in the spatial domain utilizing features equivalent to the SVD transform. *Applied Sciences*, 13(10), 6105.
- [7] Sanivarapu, P. V. (2022). Adaptive tamper detection watermarking scheme for medical images in transform domain. *Multimedia Tools and Applications*, 81(8), 11605-11619.
- [8] Gomez-Coronel, S. L., Moya-Albor, E., Brieva, J., & Romero-Arellano, A. (2023). A robust and secure watermarking approach based on Hermite transform and SVD-DCT. *Applied Sciences*, 13(14), 8430.
- [9] Zermi, N., Khaldi, A., Kafi, M. R., Kahlessenane, F., & Euschi, S. (2021). A lossless DWT-SVD domain watermarking for medical information security. *Multimedia Tools and Applications*, 80(16), 24823-24841.
- [10] Begum, M., & Uddin, M. S. (2021). Implementation of secured and robust DFT-based image watermark through hybridization with decomposition algorithm. *SN Computer Science*, 2(3), 221.
- [11] Chaudhary, H., & Vishwakarma, V. P. (2025). A Survey: Digital Image Watermarking-robustness and Imperceptibility. *Recent Advances in Electrical & Electronic Engineering*, 18(8), 1157-1175.
- [12] Hemdan, E. E. D. (2021). An efficient and robust watermarking approach based on single value decomposition, multi-level DWT, and wavelet fusion with scrambled medical images. *Multimedia Tools and Applications*, 80(2), 1749-1777.
- [13] Pacheco, J., Benitez, V. H., Pérez, G., & Brau, A. (2024). Wavelet-based computational intelligence for real-time anomaly detection and fault isolation in embedded systems. *Machines*, 12(9), 664.
- [14] Hosny, K. M., Magdi, A., ElKomy, O., & Hamza, H. M. (2024). Digital image watermarking using deep learning: A survey. *Computer Science Review*, 53, 100662.
- [15] Qamar, R., & Zardari, B. A. (2023). Artificial neural networks: An overview. *Mesopotamian Journal of Computer Science*, 2023, 124-133.
- [16] Zhong, X., Das, A., Alrasheedi, F., & Tanvir, A. (2023). A brief, in-depth survey of deep learning-based image watermarking. *Applied Sciences*, 13(21), 11852.
- [17] Ben Jabra, S., & Ben Farah, M. (2024). Deep learning-based watermarking techniques challenges: a review of current and future trends. *Circuits, Systems, and Signal Processing*, 43(7), 4339-4368.
- [18] Aberna, P., & Agilandeewari, L. (2024). Digital image and video watermarking: methodologies, attacks, applications, and future directions. *Multimedia Tools and Applications*, 83(2), 5531-5591.
- [19] Khan, A., Khan, A., Ullah, M., Alam, M. M., Bangash, J. I., & Suud, M. M. (2022). A computational classification method of breast cancer images using the VGGNet model. *Frontiers in Computational Neuroscience*, 16, 1001803.
- [20] Faghihi, A., Fathollahi, M., & Rajabi, R. (2024). Diagnosis of skin cancer using VGG16 and VGG19 based transfer learning models. *Multimedia Tools and Applications*, 83(19), 57495-57510.
- [21] Shah, S. R., Qadri, S., Bibi, H., Shah, S. M. W., Sharif, M. I., & Marinello, F. (2023). Comparing inception V3, VGG 16, VGG 19, CNN, and ResNet 50: a case study on early detection of a rice disease. *Agronomy*, 13(6), 1633.
- [22] Bansal, M., Kumar, M., Sachdeva, M., & Mittal, A. (2023). Transfer learning for image classification using VGG19: Caltech-101 image data set. *Journal of ambient intelligence and humanized computing*, 14(4), 3609-3620.
- [23] Zhenfei, W., Ali, M. M., Sahibzada, K. I., Maqsood, F., Rehman, N. U., Aftab, M., ... & Wei, D. Q. (2025). Hybrid feature extraction for breast cancer classification using the ensemble residual VGG16 deep learning model. *Current Bioinformatics*, 20(2), 149-163.
- [24] Bakasa, W., & Viriri, S. (2023). Vgg16 feature extractor with extreme gradient boost classifier for pancreas cancer prediction. *Journal of Imaging*, 9(7), 138.
- [25] Gilmolk, A. M. N., & Aref, M. R. (2024). Lightweight image encryption using a novel chaotic technique for the safe internet of things. *International Journal of Computational Intelligence Systems*, 17(1), 146.

- [26] Wang, K., Gao, T., You, D., Wu, X., & Kan, H. (2022). A secure dual-color image watermarking scheme based 2D DWT, SVD and Chaotic map. *Multimedia Tools and Applications*, 81(5), 6159-6190.
- [27] Kumar, V., Pathak, V., Badal, N., Pandey, P. S., Mishra, R., & Gupta, S. K. (2022). Complex entropy based encryption and decryption technique for securing medical images. *Multimedia Tools and Applications*, 81(26), 37441-37459.
- [28] Niu, S., Xue, R., & Ding, C. (2025). A dual image encryption method based on improved henon mapping and improved logistic mapping. *Multimedia Tools and Applications*, 84(11), 8651-8671.
- [29] SaberiKamarposhti, M., Sahlabadi, M., Lin, C. C., & Muniyand, R. C. (2024). Using 2d hénon map, cycling chaos and dna sequence for new secure color image encryption algorithm. *Arabian Journal for Science and Engineering*, 49(3), 4125-4137.
- [30] Sharma, S., Gulería, K., Tiwari, S., & Kumar, S. (2022). A deep learning based convolutional neural network model with VGG16 feature extractor for the detection of Alzheimer Disease using MRI scans. *Measurement: Sensors*, 24, 100506.
- [31] Younis, E. M., Ibrahim, I. A., Mahmoud, M. N., & Albarrak, A. M. (2025). Hybrid of VGG-16 and FTVT-b16 Models to Enhance Brain Tumors Classification Using MRI Images. *Diagnostics*, 15(16), 2014.
- [32] Hosseini, S. A., & Farahmand, P. (2024). An attack resistant hybrid blind image watermarking scheme based on DWT, DCT and PCA. *Multimedia Tools and Applications*, 83(7), 18829-18852.
- [33] Tang, M., & Zhou, F. (2022). A robust and secure watermarking algorithm based on DWT and SVD in the fractional order fourier transform domain. *Array*, 15, 100230.
- [34] Araghi, T. K., & Megías, D. (2024). Analysis and effectiveness of deeper levels of SVD on performance of hybrid DWT and SVD watermarking. *Multimedia Tools and Applications*, 83(2), 3895-3916.
- [35] Naem, S. A. S., & Hameed, S. M. (2025). Digital watermarking techniques, challenges, and applications: A review. *Mesopotamian Journal of CyberSecurity*, 5(2), 453-476.
- [36] Ferik, B., Laimeche, L., Meraoumia, A., Laouid, A., Alshaikh, M., Chait, K., & Hammoudeh, M. (2025). An efficient semi-blind watermarking technique based on ACM and DWT for mitigating integrity attacks. *Arabian Journal for Science and Engineering*, 1-21.
- [37] Singh, P., Devi, K. J., Thakkar, H. K., & Santamaría, J. (2021). Blind and secured adaptive digital image watermarking approach for high imperceptibility and robustness. *Entropy*, 23(12), 1650.
- [38] Rai, M., Goyal, S., & Pawar, M. (2023). An optimized deep fusion convolutional neural network-based digital color image watermarking scheme for copyright protection. *Circuits, Systems, and Signal Processing*, 42(7), 4019-4050.
- [39] Sinhal, R., Jain, D. K., & Ansari, I. A. (2021). Machine learning based blind color image watermarking scheme for copyright protection. *Pattern Recognition Letters*, 145, 171-177.
- [40] Jaiswal, S., & Pandey, M. K. (2023). Deep artificial neural network-based blind color image watermarking. In *Doctoral Symposium on Human Centered Computing* (pp. 101-112). Springer.
- [41] Dwivedi, R., Awasthi, D., & Srivastava, V. K. (2024). An optimized dual image watermarking scheme based on redundant DWT and randomized SVD with henon mapping encryption. *Circuits, Systems, and Signal Processing*, 43(1), 408-456.
- [42] Li, C., Sun, H., Wang, C., Chen, S., Liu, X., Zhang, Y., ... & Tong, D. (2024). ZWNET: A deep-learning-powered zero-watermarking scheme with high robustness and discriminability for images. *Applied Sciences*, 14(1), 435.