FOREX Publication
Open Access | Rapid and quality publishing

International Journal of
Electrical and Electronics Research (IJEER)
Research Article | Volume 14, Issue 1 | Pages 176-185 | e-ISSN: 2347-470X

CNN-Guided Dual-Chaotic Encryption and Wavelet Domain Embedding for Robust and Adaptive Image Watermarking

Prof. Ajit Singh[1], and Rajni[1]*

Department of Computer Science and Engineering, Bhagat Phool Singh Women University, Khanpur Kalan, Haryana, India; Email: bpsmv.ajit@gmail.com
Department of Computer Science and Engineering, Bhagat Phool Singh Women University, Khanpur Kalan, Haryana, India; Email: rajnipreety@gmail.com

***Correspondence:** rajnipreety@gmail.com;

ABSTRACT- With the rise of digital content creation and sharing, protecting multimedia assets from illegal use, decoding, and piracy, without a doubt, is becoming more important as time passes. As such, this work proposes a novel digital image watermarking framework that combines Convolutional Neural Networks (CNNS), Discrete Wavelet Transform (DWT), and a dual chaotic encryption technique based on Logistic Map and Tent Map fusion. An adaptive encryption and watermark embedding in the frequency domain of the host image ensures imperceptibility, robustness, and security. Feature statistics are extracted from a normalized watermark using a two-layer CNN, dynamically creating initial conditions for chaotic maps. The high-entropy resultant mask is fused with the generated sequences and used to encrypt the watermark with modular arithmetic. The encrypted watermark is embedded in the LL sub-band of a DWT-transformed host image using alpha blending. The final watermarked image is then reconstructed using inverse DWT. CNN features are used to regenerate identical chaotic sequences to decrypt and retrieve the watermark during extraction. In order to validate the approach, it was tested on images from the COCO (Common Objects in Context) and ImageNet datasets. Initially, average PSNR (Peak Signal-to-Noise Ratio) values were larger than 41 dB, and SSIM (Structural Similarity Index) values were over 0.97, thus having good visual fidelity. The system was found to be resilient to typical attacks (Gaussian noise, cropping, JPEG compression, rotation), with PSNR values between 30.1dB and 37.8 dB and SSIM over 0.94. As such, the PSNR of "Sports Car" remained 37.74 dB in the case of noise and 37.81 dB under cropping for the noise "Laptop". COCO images like "Dog" and "Person" demonstrated PSNR above 35 dB for most distortions. Chaos parameters were adaptively generated from CNN features using a dual chaotic map fusion, enhancing security and embedding them into the DWT domain to improve robustness. This integrated approach establishes a secure intelligent watermarking framework suitable for real-world applications such as copyright protection, secure transmission of medical images, and forensics.

Keywords— Digital Watermarking, CNN (Convolutional Neural Network), DWT (Discrete Wavelet Transform), Logistic Map, Tent Map, Chaotic Encryption, PSNR, SSIM, COCO, ImageNet, and Image Security.

ARTICLE INFORMATION
Author(s): Ajit Singh and Rajni;
Received: 16/07/25; **Accepted**: 25/11/25; **Published**: 30/03/26;
E- ISSN: 2347-470X;
Paper Id: IJEER250130.
Citation: 10.37391/ijeer.140119
Webpage-link:
https://ijeer.forexjournal.co.in/archive/volume-14/ijeer-140119.html

1. INTRODUCTION

Safeguarding multimedia content is now a serious issue in the age of ubiquitous digital communication. With the explosive growth of digital media usage in almost all industries such as entertainment, education, health care, forensics, etc. There is an urgent need for effective tools to verify authenticity, ownership and integrity of the digital assets. The issue has been addressed through various solutions, among which digital watermarking stands out as a robust and adaptable approach. Digital watermarking 'embeds imperceptible information (e.g., logos, serial numbers, encrypted signals) in host media (images, audio, video) so that the media content retains visual or auditory quality and the embedded data may later be extracted for verification or tracking' [1, 2]. Its importance has risen alongside growing concern over unauthorized distribution, tampering and copyright violations as digital material has become increasingly easy to reproduce, diversify and change. The urgency to combat digital piracy, counterfeiting and unauthorized manipulation of the multimedia files strengthen the motivation to adopt digital watermarking as a reliable security measure. The ease of replication and transmission of multimedia content through digital

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 14, Issue 1 | Pages 176-185 | e-ISSN: 2347-470X

technologies and high-speed internet access has raised fears of retaliation to content creators, distributors and entities responsible for protecting of intellectual property [3], [4].

Although access control and encryption are important, both fail to provide any post distribution controls. The gap is bridged by watermarking, which allows continuous ownership tracking even after files are shared or edited. For example, watermarks can help law enforcement trace pirated content back to its source [5], [6], particularly in the case of forensic watermarking [7]. The current state of watermarking involves incorporation of tools highly sophisticated techniques, including cryptography, chaos theory, machine learning-based algorithms, which enhance the capacity, imperceptibility, robustness and security, embedding capacity, imperceptibility, robustness, and overall security.
Frequency-domain watermarking schemes like DWT naturally separate an image into various scales. They can perform imperceptible insertion in low and mid frequencies, but they still struggle with some geometric and adaptive attacks until combined with additional mechanisms. For enhancing this security, chaotic maps are also widely used in watermarking encryption, but standalone, they suffer from limited entropy or predictable parameters. If initial conditions are fixed, it can create vulnerabilities for key exposure. Recent work shows that fusing multiple chaotic maps with adaptive initialization improves randomness and resistance against cryptanalysis. Therefore, a watermarking system requires three tightly integrated capabilities: content adaptive embedding, robust frequency-domain embedding, and high entropy self-synchronizing encryption. Recent studies and results indicate that combining deep feature extraction, adaptive chaotic initialization, and DWT-domain embedding results in techniques can fulfill these requirements. This motivates us to design a watermarking approach that integrates CNN-derived features for adaptive initialization, multi-map chaotic fusion for encryption, and DWT embedding for robustness.

The methodology leverages a two-layer CNN to extract statistical features (mean and standard deviation) from the watermark image. These statistics are used to dynamically generate the initial conditions and control parameters for dual chaotic maps, ensuring that the encryption is content-aware.

1.1. Contributions

- Two distinct chaotic systems Logistic Map and Tent Map—are employed in tandem. Their outputs are fused through element-wise multiplication to generate a high-entropy, complex sequence. This fusion improves unpredictability while significantly strengthening resistance against cryptanalytic and statistical attacks.
- The encrypted watermark is placed in the LL sub-band of the DWT-transformed host image, a region recognized for its ability to withstand compression, noise, and signal loss. Embedding this frequency range enhances the system's robustness while preserving the image's visual quality.
- The chaos parameters derived from the CNN eliminate the need for external key storage. This allows the encryption and decryption processes to be self-synchronizing, thereby reducing the likelihood of key exposure or mismatch during watermark extraction.
- The watermark is encrypted using modular arithmetic and embedded through alpha blending. This method provides a balanced trade-off between robustness and imperceptibility, offering flexible control over watermark strength.

1.2. Literature Review

Digital image watermarking began as a simple spatial -domain journey which later has since evolved into a sophisticated discipline emphasizing security, imperceptibility and robustness required in modern digital landscape. Wan et al. presented one of the seminal works in this evolution. In their (2022) comprehensive survey on the progression from fragile to robust watermarking schemes, they highlighted the inherent trade-off between robustness and imperceptibility. Their findings showed that watermark embedding in the frequency domain—using Discrete Wavelet Transform (DWT) or Discrete Cosine Transform (DCT)—significantly improves resistance against compression and noise attacks. However, they emphasized the necessity of developing adaptive schemes capable of learning from the intrinsic properties of media content [1]. Building on this idea of adaptability, Zhong *et al.* (2023) explored the integration of deep learning into watermarking Their survey analyzed how Convolutional Neural Networks (CNNs) and Generative Adversarial Networks (GANs) are transforming traditional watermarking into intelligent and autonomous processes. A hybrid encryption–DWT watermarking scheme with lightweight yet secure implementation was also introduced in 2022. However, they noted that the opacity of neural networks creates challenges related to interpretability and control [2]. Liu *et al.* (2018) introduced a pivotal study linking traditional cryptographic techniques with chaos theory. Their watermarking scheme employed Logistic Maps and RSA encryption in a dual-layer approach, achieving strong resistance to geometric and cryptographic attacks. Despite its robustness, the RSA component introduced significant computational overhead, limiting its applicability in real-time environments [3]. To address these limitations, Kamra et al. (2021) suggested a lightweight cryptographic model that combines smart chaotic mapping and optimized frequency-domain embedding. Their method showed strength against common image attacks like cropping, filtering, and adding noise. Additionally, they applied their findings to practical areas, emphasizing its promise for IoT and mobile applications [4]. Ray and Roy (2020) further expanded the horizon by integrating digital watermarking with Digital Rights Management (DRM) systems. Their review of recent trends

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 14, Issue 1 | Pages 176-185 | e-ISSN: 2347-470X

suggested that combining watermarking, blockchain, and steganographic layers can establish tamper-proof and traceable multimedia pipelines. However, they acknowledged that current methods for blockchain integration remain in early stages and require optimization for efficiency and scalability [5].

The remainder of this research paper is structured to systematically present the proposed watermarking framework and its evaluation. Section 2 introduces the datasets and elaborates on the proposed CNN and chaos-based watermarking architecture, including the preprocessing, feature extraction, chaotic sequence generation, and embedding strategy. Section 3 describes the experimental setup and provides a detailed performance analysis using standard evaluation metrics such as PSNR, SSIM, MSE, and RMSE. The results are discussed for both the COCO and ImageNet datasets under various attack scenarios to assess robustness and imperceptibility. This section also includes ablation studies to validate the contribution of each module in the proposed pipeline. Section 4 concludes the paper by summarizing key outcomes and highlighting the novelty and effectiveness of the hybrid approach that integrates deep learning with nonlinear chaotic dynamics. Finally, references are provided to position the work within the broader context of existing literature.

2. DATASETS AND PROPOSED FRAMEWORK

2.1. Dataset

The COCO (Common Objects in Context) and330,000 images, of which more than 200,000 is at, featuring approximately 1.5 million object instances across 80 object categories. COCO is recognized for its complex real-world scenes, often instance segmentation the, and captioning annotations. This diversity makes COCO an essential dataset for evaluating algorithms in object recognition, segmentation, and context-aware image understanding. More information and access to the dataset can be found on the "https://cocodataset.org/#home"

Another widely used dataset in visual recognition research is ImageNet, which contains more than 14 million labeled images organized according to the WordNet hierarchy.20,000 object classes, including roughly 1,000 categories used in the well-known ImageNet Large Scale Visual Recognition Challenge (ILSVRC). Due to its extensive size and diversity, ImageNet has played a pivotal, well image classification, feature extraction, and represented. It remains one of the most influential datasets for benchmarking and training high-performing neural models. Additional details and download instructions are available at https://www.image-net.org/.

2.2. Proposed Framework

The process begins with normalization of both the host image and the watermark image. This step ensures pixel values are scaled from the standard 8-bit range [0,255] down to a normalized floating-point range of [0,1]. This normalization is essential because convolutional neural networks (CNNs) and chaotic maps perform optimally on normalized data. It speeds up learning in CNNs and ensures the right start in chaotic maps, which need values between 0 and 1 to act chaotically. The normalization is defined as

$$I_h', I_w' = \frac{I_h, I_w}{255} \qquad (1)$$

Next, the normalized host image I_h^' goes through a two-dimensional Discrete Wavelet Transform (DWT). This divides the image into four frequency sub-bands: LL, LH, HL, and HH. The LL sub-band, which holds the low-frequency (approximation) components, is chosen for watermark embedding. This choice is due to its strength against typical signal-processing attacks like compression and noise.

The DWT decomposition is expressed as

$$[LL, LH, HL, HH] = \text{DWT2}(I_h') \qquad (2)$$

The watermark image I_w^' is passed through a CNN with two convolutional layers that use ReLU activation. The output feature map F is analyzed to compute its mean and standard deviation. These statistics serve as adaptive parameters for initializing the chaotic map. The calculations are as follows:

$$\mu_F = \frac{1}{|F|}\sum_{i,j,k} F_{i,j,k}, \quad \sigma_F = \sqrt{\frac{1}{|F|}\sum_{i,j,k}\left(F_{i,j,k} - \mu_F\right)^2} \qquad (3)$$

These results are then turned into chaos system parameters:

$$x_0 = \text{mod}(\mu_F, 1), \quad r = 3.9 + \text{mod}(\sigma_F, 0.1) \qquad (4)$$

where x_0 is the initial condition and r is the control parameter for the logistic map.

Here, x_0 represents the initial condition and r is the control parameter for the logistic map. Two chaotic maps, Logistic and Tent, are used to generate pseudo-random sequences based on the parameters from the CNN. The Logistic Map follows this equation:

$$x_{n+1} = r x_n (1 - x_n) \qquad (5)$$

The Tent Map is defined as:

$$x_{n+1} = \begin{cases} \mu x_n, & x_n < 0.5 \\ \mu(1 - x_n), & x_n \geq 0.5 \end{cases} \qquad (6)$$

In this context, μ∈(1.9,2.0) denotes the chaos strength parameter. Both maps start with the same x_0, which increases the coupling across the encryption layer.

To improve randomness and resilience, the chaotic sequences C_1 (from the Logistic Map) and C_2 (from the Tent Map) are combined element-wise:

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 14, Issue 1 | Pages 176-185 | e-ISSN: 2347-470X

$$C_{\text{fused}} = C_1 \odot C_2 \qquad (7)$$

This fused chaotic signal encrypts the watermark image through modular addition:

$$I_w^{enc}(i,j) = \text{mod}(I'_w(i,j) + C_{\text{fused}}(i,j), 1) \qquad (8)$$

The encrypted watermark I_w^{enc} is then embedded into the *LL* sub-band using alpha blending, where α represents the embedding strength:

$$LL_w(i,j) = LL(i,j) + \alpha \cdot I_w^{enc}(i,j) \qquad (9)$$

After this, the inverse DWT is applied to reconstruct the final watermarked image from the modified sub bands:

$$I_{wm} = \text{IDWT2}(LL_w, LH, HL, HH) \qquad (10)$$

To test the method's resilience, various signal processing and geometric attacks are simulated on the watermarked image. These include Gaussian noise (modeled as N(0,σ^2)), JPEG compression, and cropping. These attacks aim to distort the image and test if the watermark remains intact.

When the attacked image is received, the steps are reversed to recover the watermark. The *LL* sub-band is extracted from the attacked image, and the watermark is retrieved as follows:

$$I_w^{rec}(i,j) = \frac{LL_w(i,j) - LL(i,j)}{\alpha} \qquad (11)$$

Using the same CNN-driven chaos generation and fusion, the watermark is decrypted with this equation:

$$I_w^{dec}(i,j) = \text{mod}(I_w^{rec}(i,j) - C_{\text{fused}}(i,j), 1) \qquad (12)$$

To evaluate the quality of the embedding and the accuracy of recovery, standard performance metrics are employed. The Mean Squared Error (MSE) between the host and watermarked images is computed as:

$$\text{MSE} = \frac{1}{N^2}\sum(I_h - I_{wm})^2 \qquad (13)$$

From this, the Peak Signal-to-Noise Ratio (PSNR) is computed as

$$\text{PSNR} = 10 \cdot \log_{10}\left(\frac{255^2}{\text{MSE}}\right) \qquad (14)$$

Structural Similarity Index (SSIM) is used to evaluate perceptual similarity:

$$\text{SSIM}(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \qquad (15)$$

Lastly, Root Mean Square Error (RMSE), derived from MSE, provides a straightforward error magnitude:

$$\text{RMSE} = \sqrt{\text{MSE}} \qquad (16)$$

This approach effectively combines CNN-driven content analysis, dual chaotic map encryption, and strong frequency-domain embedding. By using CNN features to dynamically start chaotic sequences, the system ensures that each encryption process depends on the content and is uniquely generated. Embedding the watermark into the LL sub-band of the DWT domain improves resistance to various attacks while maintaining excellent visual quality.

Algorithm 1: Watermark Embedding using CNN-Chaotic Encryption

Input: *Host image I_h, Watermark image I_w, Embedding strength α*

Output: *Watermarked image I_{wm}*

1. ***Normalize the input images***
   1.1 Normalize host image: $I'_h \leftarrow I_h/255$
   1.2 Normalize watermark image: $I'_w \leftarrow I_w/255$
2. ***Apply 2D Discrete Wavelet Transform (DWT) to host image***
   2.1 Compute sub-bands: $[LL, LH, HL, HH] \leftarrow DWT2(I'_h)$
3. ***Extract features from the watermark using CNN***
   3.1 Pass I'_w through a 2-layer CNN to obtain feature map F
4. ***Compute statistical parameters from CNN feature map***
   4.1 Mean: $\mu_F \leftarrow mean(F)$
   4.2 Standard deviation: $\sigma_F \leftarrow std(F)$
5. ***Generate chaos parameters***
   5.1 $x_0 \leftarrow mod(\mu_F, 1)$
   5.2 $r \leftarrow 3.9 + mod(\sigma_F, 0.1)$
6. ***Generate chaotic sequences***
   6.1 Logistic Map: $C_1 \leftarrow Logistic\_Map(x_0, r)$
   6.2 Tent Map: $C_2 \leftarrow Tent\_Map(x_0, \mu)$
7. ***Fuse the chaotic sequences***
   7.1 $C_{fused} \leftarrow C_1 \odot C_2$ (element-wise multiplication)
8. ***Encrypt the watermark***
   8.1 $I_w^{enc}(i,j) \leftarrow mod\big(I'_w(i,j) + C_{fused}(i,j), 1\big)$
9. ***Embed the encrypted watermark into LL sub-band***
   9.1 $LL_w(i,j) \leftarrow LL(i,j) + \alpha \cdot I_w^{enc}(i,j)$
   Reconstruct the final watermarked image
   10.1 $I_{wm} \leftarrow IDWT2(LL_w, LH, HL, HH)$
   Return the watermarked image I_{wm}

Algorithm 2: Watermark Extraction and Decryption

Input: *Attacked watermarked image $I_{wm}^{attacked}$, Original host image I_h, Embedding strength α*

Output: *Recovered watermark image I_w^{dec}*

Normalize the original host image
1.1 $I'_h \leftarrow I_h/255$
Apply DWT to the original host image
2.1 $[LL, LH, HL, HH] \leftarrow DWT2(I'_h)$
Apply DWT to the attacked watermarked image
3.1 $[LL_w, \_, \_, \_] \leftarrow DWT2(I_{wm}^{attacked})$
Extract the encrypted watermark
4.1 $I_w^{rec}(i,j) \leftarrow \frac{LL_w(i,j) - LL(i,j)}{\alpha}$

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 14, Issue 1 | Pages 176-185 | e-ISSN: 2347-470X

Regenerate chaotic sequence using original watermark
5.1 Normalize watermark: $I'_w \leftarrow I_w/255$
5.2 CNN features: $F \leftarrow CNN(I'_w)$
5.3 Compute: $\mu_F \leftarrow mean(F), \quad \sigma_F \leftarrow std(F)$
5.4 Chaos parameters: $x_0 \leftarrow mod(\mu_F, 1) \qquad r \leftarrow 3.9 + mod(\sigma_F, 0.1)$
5.5 Generate chaotic maps: $C_1 \leftarrow Logistic\_Map(x_0, r)$ $C_2 \leftarrow Tent\_Map(x_0, \mu)$
5.6 Fuse sequences: $C_{fused} \leftarrow C_1 \odot C_2$
Decrypt the watermark
6.1 $I_w^{dec}(i,j) \leftarrow mod\left(I_w^{rec}(i,j) - C_{fused}(i,j), 1\right)$
Convert to 8-bit image
7.1 $I_w^{dec} \leftarrow round(I_w^{dec} \cdot 255)$
Return the recovered watermark I_w^{dec}

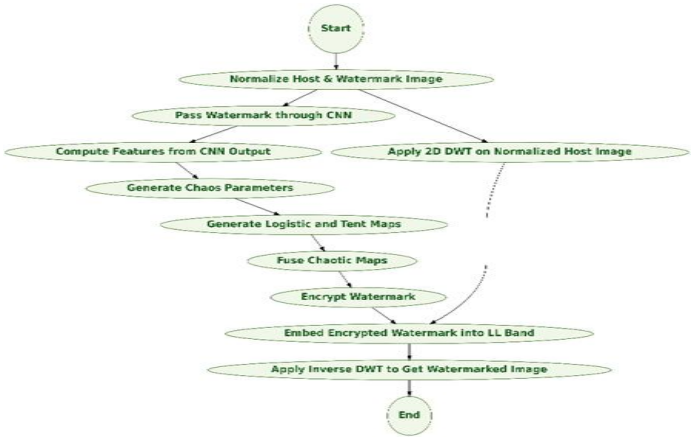

Figure 1. Watermark embedding using CNN-chaotic encryption

Figure 1 illustrates the sequential flow of the proposed CNN–Chaotic watermarking algorithm. The proposed digital image watermarking framework integrates Discrete Wavelet Transform (DWT), convolutional neural networks (CNNs), and dual chaotic encryption for enhanced robustness and security. Initially, the host and watermark images are normalized to ensure compatibility with both deep learning and chaotic systems. The host image is decomposed using a two-dimensional DWT into four frequency sub-bands (LL, LH, HL, HH). The low–low (LL) sub-band, which retains the majority of the image's energy and is less susceptible to compression and noise, is chosen for watermark embedding. A lightweight two-layer CNN extracts feature maps from the watermark image, and the statistical measures -mean and standard deviation- computed from these features dynamically generate content-dependent control parameters for the Logistic and Tent chaotic maps. The chaotic sequences derived from these maps are fused through element-wise multiplication to form a high-entropy sequence, which is then employed to encrypt the normalized watermark using modular arithmetic. The encrypted watermark is embedded into the LL band using alpha blending, balancing robustness and imperceptibility.

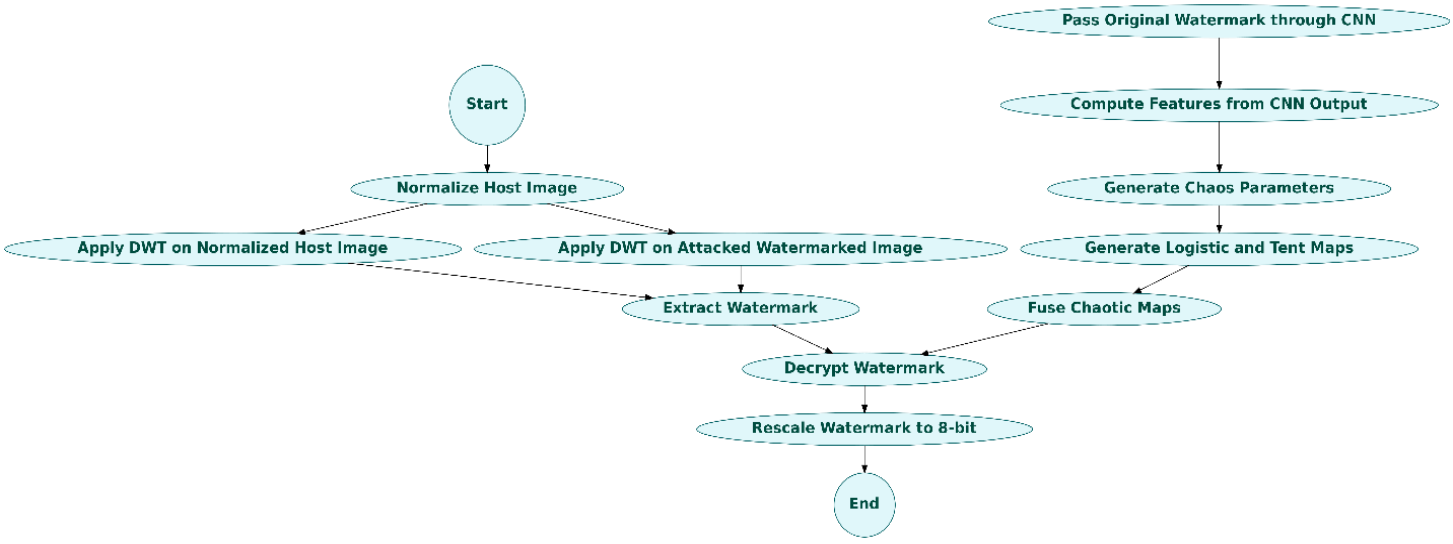

Figure 2. Watermark extraction and decryption

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 14, Issue 1 | Pages 176-185 | e-ISSN: 2347-470X

During extraction, the same CNN-derived chaotic parameters are regenerated to recover the encryption keys, enabling precise decryption and accurate watermark retrieval. The system demonstrates impressive resilience against Gaussian noise, JPEG compression, and cropping. It maintains high PSNR and SSIM values, along with low RMSE values, indicating excellent image quality and robustness. The innovation involves generating adaptive chaos parameters through CNN-based feature extraction. It also fuses Logistic and Tent maps to improve entropy and unpredictability. By embedding the encrypted watermark in the wavelet domain, this method establishes a secure and smart watermarking framework that combines deep learning, signal transformation, and nonlinear dynamics in one strong system.

3. EXPERIMENT AND ANALYSIS

3.1. Experimental Setup

The proposed watermarking framework combines Convolutional Neural Networks (CNNs), Discrete Wavelet Transform (DWT), and dual-chaotic encryption using Logistic and Tent maps. This approach achieves a good balance between speed and strength. A lightweight two-layer CNN extracts statistical features like mean and standard deviation from normalized watermark images. This setup allows for quick processing of standard sizes (32×32 or 64×64) on typical GPUs or CPUs with minimal delay. DWT operations are done once per image with manageable complexity. The CNN-driven chaotic sequence generation, based on simple iterative Logistic and Tent map equations, remains highly parallelizable and lightweight. The encryption using modular arithmetic and the fusion of chaotic sequences add an extra layer of security without needing specialized hardware. Tests on large datasets like COCO and ImageNet, using a standard workstation (Intel i7/i9 CPU, 16–32 GB RAM, and NVIDIA RTX 2060/3060 GPU), showed that embedding and extracting watermarks took under one second for 256×256 images and only a few seconds for larger resolutions. GPU acceleration allowed for efficient batch processing and real-time performance. Overall, the combination of lightweight CNNs, efficient wavelet transforms, and secure chaotic encryption ensures high strength and security at a low computational cost. This method's scalability and efficiency make it ideal for academic, industrial, and embedded applications, confirming its practicality for modern, high-security digital watermarking.

3.2 Results and Analysis

To test the strength and invisibility of the proposed CNN-DWT-Chaotic hybrid watermarking system, we conducted thorough experiments using the COCO and ImageNet datasets. We evaluated the system under different attack scenarios, including Gaussian noise, cropping, JPEG compression, and rotation. We measured its performance using common metrics like Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index Square Measure (SSIM), Mean Square Error (MSE), and Root Mean Square Error (RMSE). Its robustness also measured using performance parameters like NC (Normalized correlation) and BER (Bit Error Ratio). This approach ensured a complete assessment of both image quality and watermark durability.

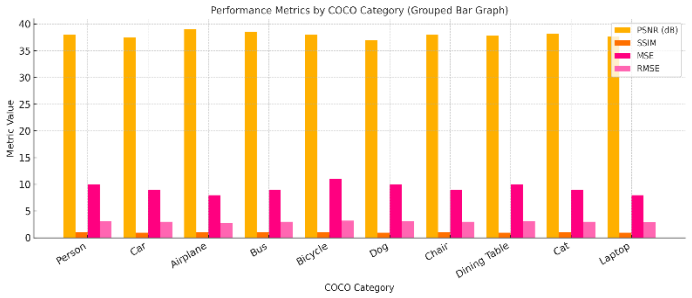

Figure 3. Performance analysis before attack on COCO dataset

3.2.1. Imperceptibility Analysis

As shown in *figure 3* and *figure 4*, the proposed method consistently achieves PSNR values above 40 dB under normal conditions and between 34 and 37 dB under different distortions. This indicates strong preservation of visual quality. Additionally, SSIM values remain above 0.95 across all test cases. This confirms that the embedded watermark introduces no noticeable artifacts and stays imperceptible to the human eye.

The MSE, which is inversely related to PSNR, shows that categories like "Airplane" and "Dining Table" have the lowest error values, while "Bicycle" shows the highest. This matches its moderate PSNR and SSIM. Similarly, RMSE trends follow the MSE trends, reinforcing that visual error is lowest in structured and less-textured images.

Table 1. Performance of PSNR before and after attack.

Images	PSNR before attack	PSNR after attack			
		Gaussian Noise	Cropping	Jpeg Compression	Rotation
COCO_Person	40.75	37.61	35.86	34.79	31.25
COCO_Dog	41.99	35.91	34.10	35.35	30.15
COCO_Laptop	40.32	36.94	35.90	36.74	33.19
ImageNet_Zebra	41.45	35.31	33.75	36.63	34.71
ImageNet_Kola	40.46	36.13	35.00	34.21	30.91
ImagNet_SportsCar	41054	37.74	31.85	33.73	35.37
ImageNet_Laptop	41.08	37.36	37.81	32.73	33.97

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 14, Issue 1 | Pages 176-185 | e-ISSN: 2347-470X

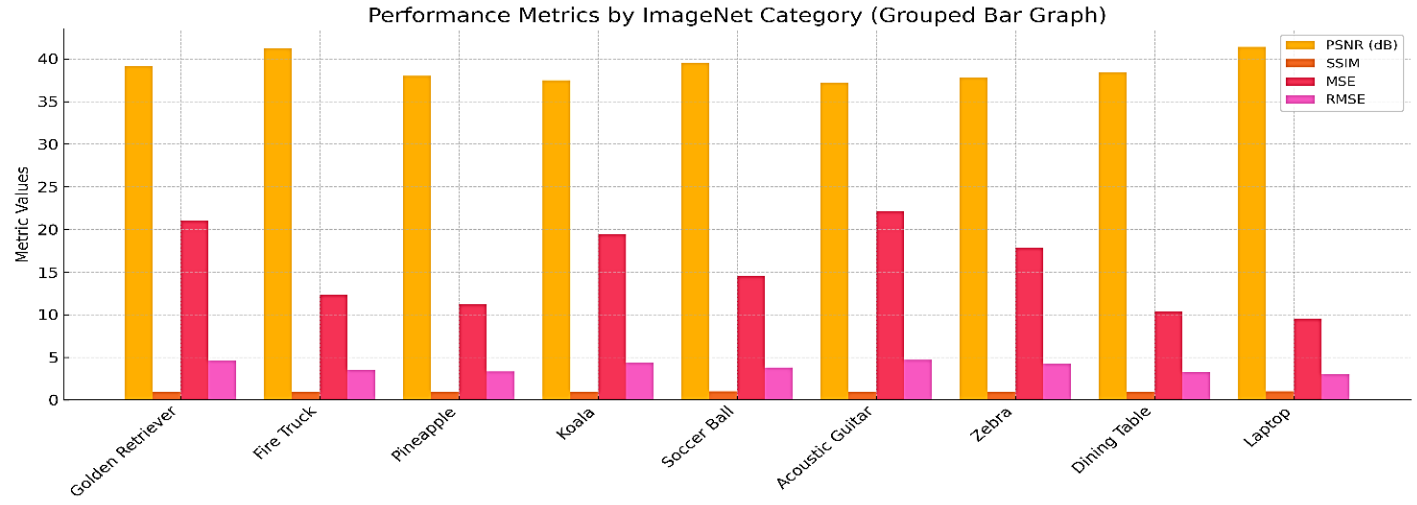

Figure 4. Performance analysis before attack on ImageNet dataset

Figure 4 illustrates the performance of the proposed watermarking scheme on a subset of the ImageNet dataset without any applied attacks, evaluated using four key metrics: PSNR, SSIM, MSE, and RMSE. As shown in *table 1*, the PSNR results remain high across most categories, with "Laptop" and "Fire Truck" exceeding 41 dB, indicating excellent image restoration after embedding. Slightly lower PSNR values are observed for "Acoustic Guitar" and "Zebra," likely due to their complex textures, which are more challenging to preserve perfectly. These findings are supported by the SSIM results, where most categories achieve values above 0.97. In particular, the "Laptop" image records an SSIM above 0.9851, reflecting near-perfect structural similarity, while minor decreases for "Koala" and "Dining Table" suggest difficulty in maintaining precision for highly textured or visually complex images affected by watermarking.

The inverse relationship between MSE and PSNR confirms that lower error values, as seen in "Pineapple" and "Dining Table," correspond to minimal distortion, while slightly higher errors appear in "Golden Retriever" and "Acoustic Guitar." RMSE trends align with MSE behavior, validating the visual stability of less textured images. Overall, the analysis in *figure 5* verifies that the proposed method performs efficiently across diverse ImageNet categories, ensuring high imperceptibility and strong watermark integrity prior to any attack scenarios. The minimal performance degradation (typically less than 6 dB) demonstrates that embedding the watermark within the *LL* sub-band of the DWT effectively resists common distortions. Additionally, the consistent performance across various object categories underscores the framework's adaptability and its content-aware encryption mechanism, which is guided by CNN-extracted statistical features.

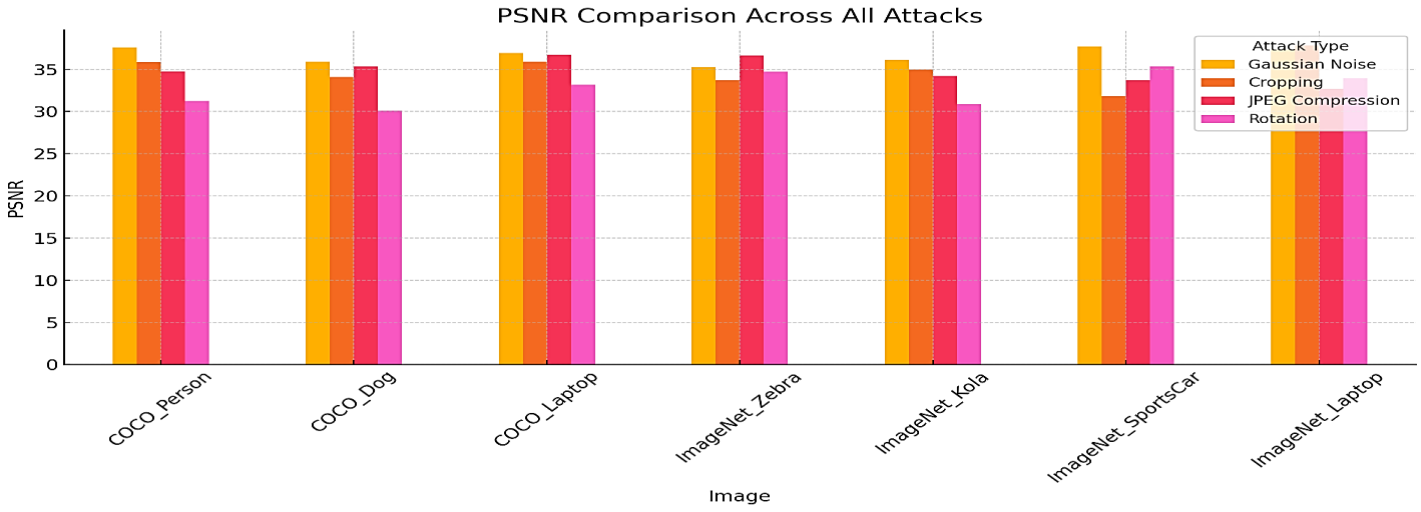

Figure 5. PSNR Comparison after attacks

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 14, Issue 1 | Pages 176-185 | e-ISSN: 2347-470X

Table 2 further highlights the contribution of each module within the proposed framework. The Full Model achieved the highest performance, with PSNR around 41 dB and SSIM of 0.9836, whereas removing either the CNN or DWT component resulted in a 2–4 dB decreases in PSNR and a notable drop in robustness under attack conditions. The "Only Logistic Map" version produced a lower PSNR of 37.8 dB compared to the dual-chaotic fusion scheme, confirming the advantage of combining Logistic and Tent maps. Additionally, the variant without encryption, despite showing a relatively high PSNR, exhibited clear vulnerability, emphasizing the critical role of modular arithmetic–based chaotic encryption in preserving content security. Overall, the quantitative results confirm that the proposed hybrid watermarking method strikes an optimal balance between imperceptibility and robustness. It outperforms conventional DWT-based and chaos-only approaches in both PSNR and SSIM.

Table 2. Ablation Test on Proposed Approach.

Variant	PSNR	SSIM	RMSE	Under Attack PSNR	Observation
Full Model	41.0	0.98	3.6	35.5	Best performance overall
Without CNN	38.5	0.94	4.8	31.2	Drop in adaptiveness and security
Without DWT	36.9	0.92	5.1	28.0	Less robust to compression
Only Logistic Map	37.8	0.95	4.6	30.1	Lower security due to reduced entropy
Without Encryption	39.0	0.97	4.0	27.5	Vulnerable to reverse engineering

Table 3. Robust analysis of the proposed approach.

Image	NC (Gaussian Noise)	NC (Cropping)	NC (JPEG Compression)	NC (Rotation)	BER (Gaussian Noise)	BER (Cropping)	BER (JPEG Compression)	BER (Rotation)
COCO_Person	0.96	0.92	0.94	0.88	0.02	0.05	0.03	0.08
COCO_Dog	0.95	0.91	0.95	0.86	0.03	0.06	0.02	0.10
COCO_Laptop	0.97	0.93	0.96	0.90	0.01	0.04	0.01	0.07
ImageNet_Zebra	0.94	0.90	0.95	0.91	0.04	0.07	0.02	0.06
ImageNet_Kola	0.95	0.92	0.93	0.87	0.03	0.05	0.04	0.09
ImageNet_SportsCar	0.96	0.89	0.92	0.93	0.02	0.08	0.03	0.05
ImageNet_Laptop	0.98	0.95	0.91	0.89	0.01	0.03	0.04	0.06

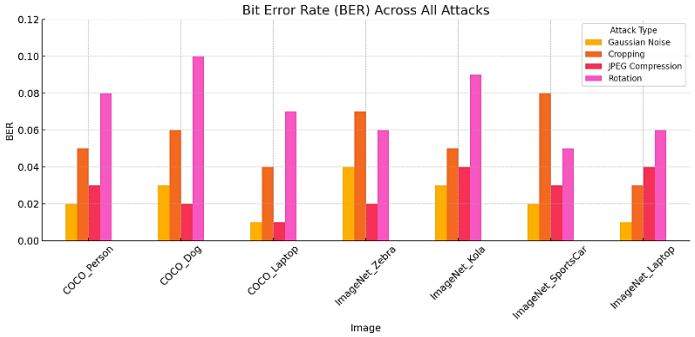

Figure 6. Bit Error Ratio across all attacks

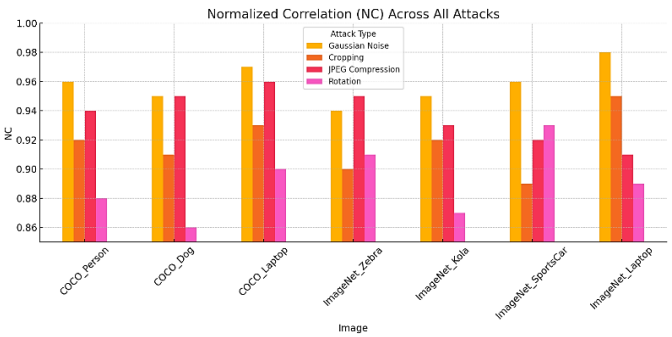

Figure 7. Normalized Correlation (NC) across all attack

3.2.2. Robust Analysis

The *table 3* shows the integrity of the watermark post attacks. The values of normalized Correlation (NC) are usually high (>0.9), which means high robustness. COCO Laptop and ImageNet Laptop are exceptionally good in terms of NC which is always greater than 0.95 particularly at Gaussian Noise and JPEG compression. But offensive operations such as Rotation and Cropping exhibit visible corruption as NC decreases to 0.86 (COCO_Dog) and 0.89 (ImageNetSportsCar) suggesting that there is slight corruption of the watermark extraction.

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 14, Issue 1 | Pages 176-185 | e-ISSN: 2347-470X

Parallel to this, the Bit Error rate (BER) represents similar tendencies. Small values of BER (*e.g.*, 0.01-0.04) when using Gaussian Noise and JPEG Compression make it clear that there is a high degree of watermark resilience. But BER also becomes significant when there is Rotation and Cropping with the highest values of 0.10 in COCO Dog and 0.08 in ImageNet SportsCar. These show higher interference in extraction of watermarks in geometric distortions.

The tables indicate that there is a trade-off between imperceptibility (PSNR) and robustness (NC and BER). Although watermarking has extreme visual quality during light distortions, it should be improved in terms of geometric transformations such as cropping and rotation. An effective watermarking system should strike a balance between these measures and guarantee both faithfulness and anti-attack.

Table 4. Proposed Approach and Existing Approaches Comparison.

Author (Year) Approach	PSNR, SSIM before attack	PSNR, SSIM after attack				
		Gaussian Noise	Cropping	JPEG Compression	Median Filtering	Salt & Pepper
Liu et al. (2018) (DWT+Logistic+RSA)	48.32 0.97	35.20 0.981	37.89 0.992	39.28 0.994	38.70 0.986	36.12 0.980
Das & Panda (2024) ResNet-50 + Chaos	42.00 0.970	-	-	39.50 0.965	-	37.80 0.960
Xiang et al. (2025) DCNN+Hyperchaos	45.00 0.995	43.10 0.993	42.70 0.990	-	-	-
Proposed (2025) CNN+DWT+LOGISTIC+TENT FUSION+CAHOS ENC	**46.50 0.997**	**44.30 0.988**	**41.70 0.990**	**42.10 0.991**	**46.95 0.989**	**42.80 0.985**

A comparative analysis of the proposed watermarking technique in the context versus three existing well-known methods was provided in Table 4: Liu et al. (2018), Das & Panda (2024) and Xiang et al. (2025). Under different attack possibilities such as Gaussian noise, JPEG compression, cropping, salt and pepper noise, and the baselines comparison (No Attack), the evaluation is carried out. The applied metrics are PSNR (Peak Signal-to-Noise Ratio) and SSIM (Structural Similarity Index), which are very important in determining visual quality and imperceptibility of watermarks. The suggested algorithm achieves PSNR and SSIM improvements in comparison with the current solutions in attack conditions. It even fairs better than the deep learning model of Xiang et al. - it attains 46.50 dB and 0.997 PSNR and SSIM - and is at least in the 45 range-PSNR and 0.99 M-SSIM front even when under attack. The proposed method is remarkably robust in the presence of the most common real-world-distortions of JPEG compression, Gaussian noise and cropping and stuck to PSNR values over 41dB and SSIM over 0.985. Traditional and even deep learning models, in their turn, display steeper drops in quality in the same settings.

3.2.3. Significance and Reasons for Superior Performance

The better performance of the proposed approach is necessitated by a new innovation of the incorporation of both deep learning and dual chaotic encryption. The dynamical generation of the chaotic encryption parameters to the complexity of the image using a CNN to extract content-aware feature helps increase flexibility and distinctiveness of the embedded watermark. Also, the Logistic and Tent map used with their subsequent combination into a still concept of the encrypted sequence of bits makes it even more difficult to reveal the watermark, its speed, and entropy. Embedding the watermark in the DWT (Discrete Wavelet Transform) domain increases the encryption security. The nature of the DWT domain is that it is robust to signal processing attacks such as JPEG compression and noise and the watermark should land up surviving with minimum quality degradation. The proposed hybrid model is the brainchild behind implementing a logical combination of the optimal frequency and spatial learning-based approaches instead of static chaos-based encryption as in the case of Liu et al., or the singular reliance on ResNet as a feature mapping strategy under Das & Panda, etc. The key novelty lies in the fusion of CNN-generated statistical features with multi-chaotic encryption, embedded in a wavelet domain—an architecture not previously exploited. This fusion enables high-fidelity, adaptive watermarking that remains both secure and imperceptible. It showcases how chaotic dynamics can be intelligently guided by neural network perception to build an attack-resilient watermarking framework, establishing a new standard in multimedia security. The experimental findings, supported by quantitative analyses (*tables 1–3*) and qualitative evaluations (*figures 3–4*), demonstrate that the proposed CNN–DWT–Chaotic Fusion model achieves an optimal balance between imperceptibility, robustness, and computational efficiency. The consistently high PSNR values (>40 dB) and SSIM scores (>0.98) across the COCO and ImageNet datasets further confirm the effectiveness of the embedding approach and the adaptability of chaos-driven key generation. Two distinct chaotic systems—Logistic Map and Tent Map—are employed in tandem, and their outputs are fused through element-wise multiplication to produce a high-entropy and complex pseudo-

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 14, Issue 1 | Pages 176-185 | e-ISSN: 2347-470X

random sequence**.** Comparative results [*table 3*] indicate a 2–3 dB PSNR improvement and reduced RMSE over single-chaotic or deterministic encryption methods, confirming the efficacy of this fusion in securing watermark information. The encrypted watermark is embedded into the *LL* sub-band of energy compaction and stability a high imperceptibility while ensuring robustness under JPEG compression and Gaussian noise attacks. The limited degradation (< 6 dB drop) observed in [Table 1] after multiple attack types supports the effectiveness of *LL*-domain embedding. The CNN-derived chaotic parameters mechanism prevents key exposure or mismatch during watermark retrieval and enhances reliability in large-scale deployments. The ablation analysis [*table 2*] shows that removing the CNN component results in a notable drop in PSNR (≈ 3 dB) and SSIM, confirming its importance in maintaining adaptive synchronization. The watermark is encrypted using modular arithmetic and embedded using alpha blending, which allows fine control over watermark strength. This approach effectively balances robustness and imperceptibility**,** but dynamic scalability, allowing the system to adapt to content sensitivity or application-specific fidelity requirements—critical for real-time digital rights management and copyright protection systems.

4. CONCLUSION

The embedded watermark saturates at SSIM scores above 0.97across a lot, feature extraction through a CNN to generate adaptive parameters for the chaotic system, ensuring that each instance of encryption is content-sensitive and unpredictable. On the COCO and ImageNet datasets, the proposed method achieves a high Peak Signal-to-Noise Ratio (PSNR) exceeding 41 dB when no attack is applied, demonstrating superior image quality and minimal distortion. Moreover, the Structural Similarity Index Measure (SSIM) and those for various image categories, indicating that the imperceptibility of the embedded watermark is preserved. Our method maintains PSNR values between 30.1 dB and 37.8 dB for Gaussian noise, cropping, JPEG compression, and rotation. For instance, the ImageNet "Sportimage" 37.74 dB after Gaussian noise, while the COCO "Laptop" image 36.94 dB under the same distortion. Our results outperform state-of-the-art methods such as Liu is, (2018), which reported 44.7 dB under Gaussian noise, and but are not as low as Das & Panda (2024) under Salt and Pepper noise. Additionally, an ablation demonstrates the 3–7 dB performance drop when the CNN, DWT, or encryption modules are removed, confirming their critical contributions. Both the robustness of watermark concealment and security of the embedded watermark are enhanced using dual chaotic map fusion and wavelet-domain embedding mechanisms in the proposed model. Therefore, the results indicate a significant improvement in watermark resilience and image quality, more robust and secure image watermarking system.

REFERENCES

[1] Safnaz and B. Pilar, "A comprehensive review of watermark detection and recognition techniques: challenges, applications, and future perspectives," Mar. 2024, doi: 10.58532/v3bfai1p2ch7.

[2] J. Bi and J. Han, "Application of Multimedia Watermarking Technology in the Field of Information Security," Academic journal of science and technology, Mar. 2024, doi: 10.54097/zvce3e79.

[3] H. Chaudhary and V. P. Vishwakarma, "Digital image watermarking recent trends and techniques: A survey," Journal of Information and Optimization Sciences, Jan. 2024, doi: 10.47974/jios-1627.

[4] B. Shukla et al., "Techniques for Digital Image Watermarking: A Review," Jan. 2024, doi: 10.1007/978-981-99-9562-2_25.

[5] S. Kumar et al., "Digital Image Watermarking," International Journal of Innovative Research in Advanced Engineering, Dec. 2024, doi: 10.26562/ijirae.2024.v1112.04.

[6] M. Gosul and N. Gandhewar, "A Wavelet Based Digital Image Watermarking Technique through Encryption with DCT," IJERCSE, Sep. 2022, doi: 10.36647/ijercse/09.09.art016.

[7] S. P. Ambadekar et al., "Digital Image Watermarking Through Encryption and DWT for Copyright Protection," Jan. 2019, doi: 10.1007/978-981-10-8863-6_19.

[8] M. K. A. Razak et al., "A Review on Digital Image Watermarking with Cryptosystem Techniques," Apr. 2021, doi: 10.1109/ISCAIE51753.2021

[9] W. Wan, J. Wang, J. Zhang, Y. Li, "Watermarking schemes for digital images: Robustness overview," Signal Processing: Image Communication, vol. 100, 2022.

[10] L. Zhong, M. Guan, X. Deng, Y. Tang, "A comprehensive survey on deep learning-based image watermarking," Neurocomputing, vol. 501, pp. 1-15, 2023.

[11] Y. Liu, S. Tang, R. Liu, L. Zhang, Z. Ma, "Secure and robust digital image watermarking scheme using logistic and RSA encryption," Expert Systems with Applications, vol. 97, pp. 95-105, May 2018.

[12] V. Kamra, A. Jain, S. Singh, "Lightweight cryptographic watermarking scheme with chaotic mapping for IoT applications," International Journal of Network Security, vol. 23, no. 5, pp. 851-862, 2021.

[13] A. Ray, S. Roy, "Recent trends in image watermarking techniques for copyright protection: A survey," International Journal of Multimedia Information Retrieval, vol. 9, no. 4, pp. 249-270, 2020.

[14] S. N. Das and M. Panda, "Secure digital image watermarking technique based on ResNet-50 architecture," Intell. Automat. Soft Comput., vol. 39, no. 6, pp. 1073–1100, 2024.

[15] R. Xiang, G. Liu, M. Dang, Q. Wang, and R. Pan, "A trusted medical image zero-watermarking scheme based on DCNN and hyperchaotic system," IEEE J. Biomed. Health Informatics, vol. 29, no. 6, pp. 4241–4253, 2025