International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Robust Image Watermarking Using Lifting Wavelet Transform and Convolutional Neural Network

Thasleen Fathima J.[1*], Lekshmy P. L.[2], Srinivas S.[3], Jayakumari D.[4]

Submitted: 29/01/2024 **Revised**: 07/03/2024 **Accepted**: 15/03/2024

Abstract: The research introduces an innovative approach to resilient image watermarking, where the fusion of the Lifting Wavelet Transform (LWT) and the Convolutional Neural Network (CNN) forms the cornerstone. To refine the precision and resilience of the watermarking process, the study integrates the Adaptive Gazelle Optimization Algorithm (AGOA) into the LeNet-5 model. This integration lets AGOA fine-tune important hyperparameters like learning rate, batch size, and convolution kernel number without having to worry about the risks that come with doing it by hand. Overall, AGOA's main goal is to improve accuracy during the model training phase. This will make sure that the watermark can't be seen and is resistant to many possible attacks. Through the utilization of AGOA, the research endeavors to swiftly and efficiently pinpoint an array of optimal solutions, thus optimizing the watermarking process to its fullest potential. The performance of our AGOA-Improve-LeNet5 model is evaluated using 300 test images, with an average Peak Signal-to-Noise Ratio (PSNR) of 61.074 dB. The experimental outcomes demonstrate the effectiveness of our proposed methodology in achieving robust and high-quality image watermarking.

Keywords: *Lifting Wavelet Transform, Convolutional Neural Network, LeNet5, Adaptive Gazelle Optimization Algorithm, Peak Signal-to-Noise Ratio, Structural Similarity Index.*

1. Introduction

The way digital multimedia applications like audio, images, and videos are shared and communicated has changed dramatically as an outcome of social networks' and the Internet's rapid growth [1]. While this convenience has brought numerous benefits, it has also created significant challenges concerning copyright security, protection, and information integrity [2]. Digital content lacks robust security mechanisms, causing unauthorized usage and copyright violations. Techniques like digital watermarking have emerged to address these issues [3]. Watermarking is a technique that safeguards digital images from unlicensed use and ensures copyright protection by embedding additional data, called a watermark, into the images [4].

This study aims to create a watermarking method that is more resilient against various attacks, including statistical and geometric manipulations [5]. The research aims to investigate the vulnerability of watermarking to malicious and non-malicious attacks during content storage or distribution [6]. Whether the attacks are intentional or unintentional, they can result in damage to the embedded watermark data [7].

Traditionally, spatial domains have been used for watermarking, but they exhibit computational complexity and limited robustness against various attacks [8]. To overcome these limitations, this research proposes a reliable methodology for digital picture watermarking based on CNN-based LeNet5 [9] and discrete wavelet transform [10]. The proposed approach optimizes performance using meta-heuristic algorithms, evaluated using AGOA, image PSNR, watermarked performance, and time analysis for real-time applications [11]. Incorporating meta-heuristic optimization techniques has proven effective in solving the trade-off problem between watermarking quality and robustness [12].

The study is important because it focuses on enhancing the transform domain digital image watermarking approach while maintaining its blind nature [13]. The proposed approach aims to enhance the algorithm's resilience to various attacks, noises, and noises, thereby improving its overall performance [14-17]. Furthermore, special emphasis is placed on the algorithm's efficiency to ensure its applicability in real-time scenarios [18].

2. Literature Review

Singh et al [19] highlight the importance of watermarking techniques in digital image protection. Traditional schemes lack resilience, leading to the development of deep

[1]*Hajee karutha Rowther, howdia college, Tamilnadu, India.*
ORCID ID : 0009-0002-8203-1718
[2]*LBS Institute of Technology for Women, Kerala, India.*
ORCID ID : 0009-0000-4727-8788
[3]*CVR College of Engineering, Hyderabad, India.*
ORCID ID : 0009-0001-8971-5074
[4]*Sri Vasavi engineering college, Andhra Pradesh, India.*
ORCID ID : 0000-0002-1800-5745
Corresponding Author Email: profthaslleenit@gmail.com

learning-based watermarking techniques. CNNs offer imperceptibility and superior visual quality. Mellimi et al. (2021) [20] study reveals a powerful image watermarking technique utilizing a deep neural network and lifting wavelet transform, achieving high PSNR values and real-time application performance. Begum et al. (2022) [21] highlighted the need for efficient hybrid domain algorithms in watermarking, proposing a standard image watermarking system framework and evaluating recent techniques' performance. Sharma et al. (2020) [22] improved digital picture watermarking techniques by combining DWT and SVD techniques, and introduced a new adversarial attack using a Deep CNN-based Autoencoder, proving their robustness. Agushaka et al. (2023) [23] GOA, a metaheuristic algorithm, outperformed nine other algorithms in performance and competitiveness, focusing on gazelles' survival in predator-dominated environments. Overall, these studies highlight the continuous efforts to improve watermarking techniques' robustness and performance using deep learning approaches and metaheuristic algorithms.

3. Proposed Methodology

The proposed methodology introduces a blind watermarking approach, combining LWT and CNN for robust image watermarking, ensuring resilience against geometric and data removal attacks, without relying on host image availability.

3.1. Data Preprocessing

Digital images for watermarking undergo preprocessing to ensure consistency and compatibility. Attacks like speckle noise, salt and pepper noise, Gaussian noise, average filter, median filter, histogram equalization, image sharpening, gamma correction, JPEG compression, cropping, and scaling are applied. The Lifting Wavelet Transform (LWT) is used to break down the image into three levels, and the HL2 sub-band is split into 32x32 blocks. Each block is transformed into a 1x4 feature vector. Figure 1 illustrates the full process of extracting watermarks graphically.

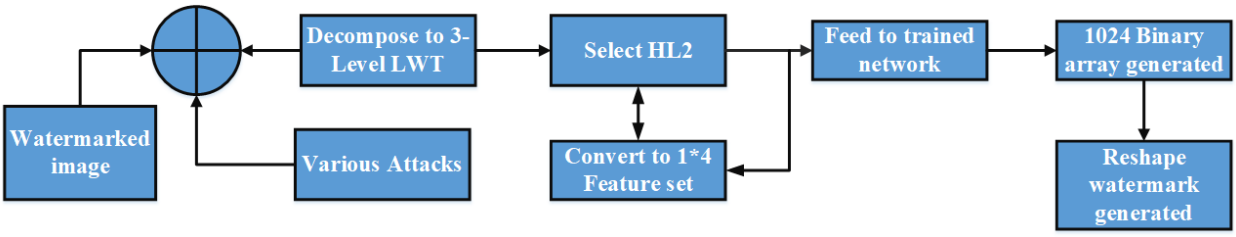

Fig. 1. Watermark extraction using CNN based lenet-5.

3.2. Lifting Wavelet Transform (LWT)

The LWT is a computationally efficient variant of the DWT that divides a cover image into sub-bands with different frequencies. It breaks the attacked watermarked image into three layers, partitioning the sub-band HL2 into 32x32 blocks, each 2x2, and transforming them into 1x4 feature vectors.

3.3. Watermark Embedding

The intended sub-band is attained by applying a 3-level LWT towards the host picture in the suggested watermarking approach [24]. The third level LWT component is represented by the Sub-Band LH/LH1/HL2, which is created by merging the LH, LH1, and HL2 Sub-Bands at the 1st, 2nd, and 3rd levels of the decomposition, namely.

The proposed plan enhances embedding performance by dispersing the insertion effect across the entire block, achieving better performance within a few altered block pixels [24]. The proposed watermarking scheme uses CNN-based feature selection to automate feature selection, resulting in a lower Bit Error Rate. The host image's 3-level LWT decomposition shows sample blocks with 2 × 2 size, allowing for 32 x 32 binary watermark pictures. This improved embedding and CNN-based feature selection enhance performance and robustness in protecting digital images from unauthorized use and copyright violations.

If watermark bit = 1

(1)

$$a_b(Z)=\begin{cases} a_b(z)+T/2 & \text{if } e_{b\max} < (g,T) \\ a_b(z)-T/2 & \text{otherwise} \end{cases} \quad (1)$$

If watermark bit = 0

$a_b(z) = a_b(z) - b_a(z)$ where, $e_{b\,max} = a_b(z) - b_a(z)$

$$g = \left[\frac{\sum_{z-1}^{H_w} e_{b\max}}{H_w} \right] \quad (2)$$

The subsequent formulas delineate the fundamental procedures involved in the watermark embedding procedure of the proposed scheme:

$a_b(z)$: Represents the largest coefficient of block z. $b_a(z)$: Represents the second-largest coefficient of block z. T: Denotes the threshold used in the embedding process. e_{bmax}: Refers to the maximum dissimilarity between the largest and second-largest coefficients of block z. g: Signifies the average value of ebmax for all non-overlapping blocks.

H_w: Represents the total number of non-overlapping blocks. The suggested plan is carefully examined for a range of threshold values, T, and the findings show that imperceptibility declines with T but robustness increases. After conducting experiments, it was found that a threshold value of T = 0.46 offers an advantageous compromise between imperceptibility and toughness. The sub-band LH/LH1/HL2 is used for the studies, and T = 0.46 is the embedding threshold that has been selected for various images. Utilizing Equation (1) and the embedding threshold T, the largest and second-largest coefficients in each non-overlapping 2 × 2 block are updated accordingly. The proposed embedding scheme has several steps, which can be seen in Figure 2. These steps are band selection, watermark insertion, three levels of LWT decomposition, and inverse LWT.

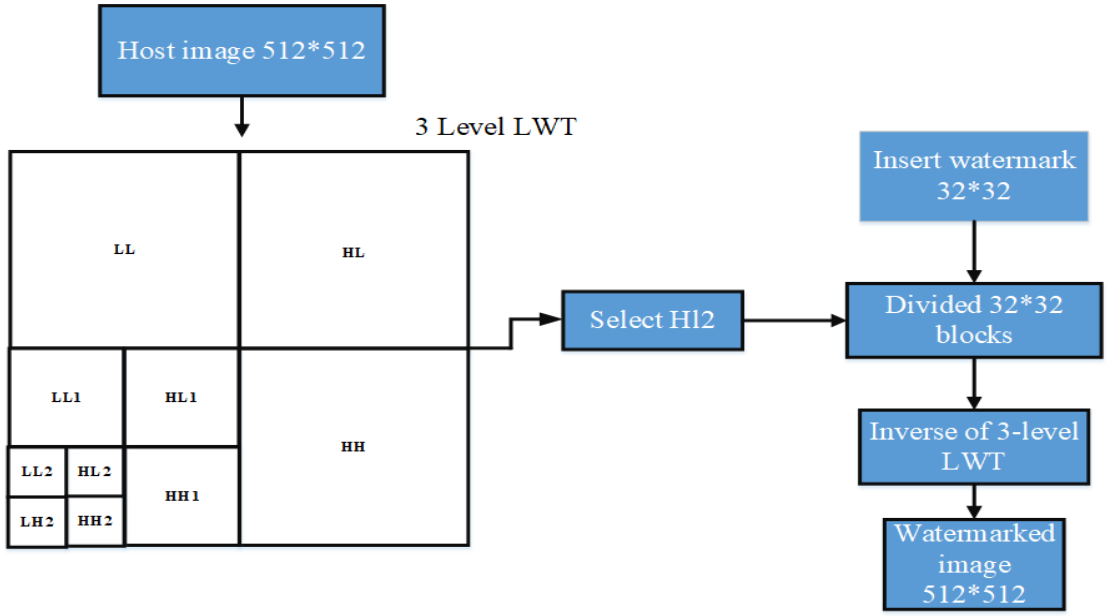

Fig. 2. Procedure of watermark embedding.

3.3.1. Watermark Embedding Steps

Step 1: On the host image, do 3-level LWT decomposition. Out of all the sub-bands that are accessible, choose LH/LH1/HL2.

Step 2: Further decompose the selected sub-band into non-overlapping 2 × 2 blocks and arrange them to form a 32 × 32 block matrix. Incorporate a 32 × 32 binary watermark into the designated sub-band by employing Equations (1) and (2).

Step 3: For binary watermark bit insertion:

a. For each block, find the two largest coefficients, as illustrated in Figure 2.

b. Modify the first and second largest coefficients according to Equation (1) based on the watermark bit value (1 or 0).

Step 4: Calculate the average variation among the two largest coefficients 'g' utilizing Equation (2).

Step 5: After the embedding procedure is finished, retrieve the watermarked image by performing the inverse LWT.

3.4. Convolutional Neural Network (CNN)

CNNs are deep learning architectures utilized for image processing and detection, including segmentation, object recognition, and image classification. They extract hierarchical features from unprocessed pixel input using layers like fully connected, pooling, and convolutional layers. Convolutional layers apply learnable filters to the input image, while pooling layers down sample feature maps to minimize computation. Fully linked layers process retrieved features for classification or other purposes.

3.4.1. The Improved-LeNet-5

The Improved-LeNet-5 is a modified version of the traditional LeNet-5 architecture, designed for handwritten digit recognition. It enhances performance and robustness, and is used in watermarking to identify changes caused by different attacks on watermarked images. It functions as a classifier to differentiate between the original and attacked watermarked images.

The Improved LeNet-5 is a classifier that can identify changes induced by various types of attacks on various frequency bands within watermarked images. It can discriminate between original watermarked and attacked images. The attack image is decomposed into three levels utilizing LWT, and the HL2 sub-band is partitioned into 32x32 blocks and transformed into 1x4 feature vectors. The trained Improved LeNet-5 classifies the attacked watermarked image into two classes: the original watermarked image or the attacked watermarked image. Its superior classification capability and high accuracy make it a preferred choice. Figure 3 displays every step that was taken throughout the network's training.

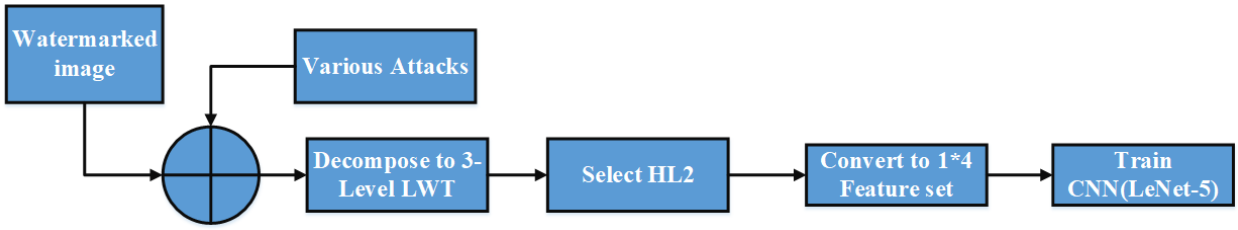

Fig. 3. Training CNN based lenet-5 for watermark extraction.

3.5. Integration of Adaptive Gazelle Optimization Algorithm (AGOA) for Finding Optimal Hyper parameters

The AGOA is a Meta heuristic optimization technique that efficiently solves real-world problems by combining exploration and exploitation phases, similar to how gazelles evade predators, focusing on peaceful grazing and outmaneuvering predators to safe havens. AGOA is integrated in Improved-LeNet-5 to automatically optimize network hyperparameters, reducing manual tweaking time and effectiveness, thereby enhancing the efficiency and effectiveness of the neural network architecture.

AGOA optimizes hyperparameters for Improved-LeNet-5, improving classification accuracy and performance under assault scenarios, enhancing watermarking process robustness and efficiency.

3.5.1. Initialization

The initial solution generation is crucial for identifying hyperparameters in the LeNet-5 architecture, and random initialization in AGOA allows for exploration of diverse configurations. GOA uses Gazelles (X) with randomly initialized search parameters, representing search agents as an n-by-d matrix. The method uses upper (U_pB) and lower (L_wB) boundary limitations to calculate possible values in a stochastic manner. According to equation (3), the search agents are represented by an n-by-d matrix of the potential solution.

$$X=\begin{bmatrix} X_{1,1} & X_{1,2} & \cdots & X_{1,j} & X_{1,1-d} & X_{1,d} \\ X_{2,1} & X_{2,2} & \cdots & X_{2,j} & X_{2,1-d} & X_{2,d} \\ \cdots & \cdots & \cdots & \vdots & \cdots & \cdots \\ \vdots & \cdots & \cdots & X_{i,j} & \vdots & \cdots \\ X_{n-1,1} & X_{n-1,2} & \cdots & X_{n-1,j} & \cdots & X_{n-1,d} \\ X_{n,1} & X_{n,2} & \cdots & \cdots & X_{n,d-1} & X_{n,d} \end{bmatrix} \quad (3)$$

where $X_{i,j}$ is the j^{th} randomly induced position of the i^{th} solution, d is the designated search space, n is the number of gazelles, and each location is stochastically produced by Equation (4).

$$X_{i,j}=rand*\left(\mathrm{U_pB}_j-L_wB_j\right)+L_wB_j \quad (4)$$

With rand being a random number, as stated in Equation (5), the optimal solution is designated as the top gazelle to produce an elite matrix (n × d). The purpose of this matrix is to investigate and identify the next iteration of the gazelle.

$$Elite=\begin{bmatrix} X'_{1,1} & X'_{1,2} & \cdots & X'_{i,j} & X'_{1,1-d} & X'_{1,d} \\ X'_{2,} & X'_{2,2} & \cdots & X'_{2,j} & X'_{2,1-d} & X'_{2,d} \\ \cdots & \cdots & \cdots & \vdots & \cdots & \cdots \\ \vdots & \cdots & \cdots & X'_{i,j} & \vdots & \cdots \\ X'_{n-1,1} & X'_{n-1,2} & \cdots & X'_{n-1,j} & \cdots & X'_{n-1,d} \\ X'_{n,1} & X'_{n,2} & \cdots & \cdots & X'_{n,d-1} & X'_{n,d} \end{bmatrix} \quad (5)$$

Where the top gazelle's places are indicated by X'i,j. The GOA considers predators and gazelles as search agents, with the elite shifting if superior gazelles take over. The iterative optimization process evaluates the fitness of each solution using a fitness function, such as Normalized Cross Correlation, to measure the performance of the LeNet-5 model.

3.5.2. Fitness Computation

AGOA uses NCC as a fitness function to evaluate the performance of a solution in explaining an optimization problem. Higher NCC values indicate better fitness. AGOA iteratively explores and updates candidate solutions, guiding its search towards high-fitness regions. This adaptive strategy enhances the algorithm's performance in finding suitable solutions, resulting in better convergence and optimization results.

$$NCC(A_1,B_1)=\frac{\sum\left[\left(A_1-\mu A_1\right)*\left(B_1-\mu B_1\right)\right]}{\left[\sqrt{\left(\sum\left(A_1-\mu A_1\right)^2\right)}*\sqrt{\left(\sum\left(B_1-\mu B_1\right)^2\right)}\right]} \quad (6)$$

Where, Equation (6) given by A_1 and B_1 are two signals or image regions being compared. μA_1 and μB_1 are the mean values of signals A_1 and B_1, respectively. $\sum$ represents the summation over all elements of the signals or image regions. The NCC value ranges from -1 to 1, with 1 indicating perfect match, 0 indicating no correlation, and -1 indicating perfect anti-correlation. Higher values indicate stronger similarity.

3.5.3. The Brownian motion

When the displacement fits into a typical (Gaussian) probability distribution function with a variance and median of $\sigma^2 = 1$ and $\mu = 0$, respectively, it appears to be random movement. The normal Brownian motion at position M is defined by equation (7) [23].

$$f_B(x;\mu,\sigma)=\frac{1}{\sqrt{2\mu\sigma^2}}\exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right)=\frac{1}{\sqrt{2\mu}}\exp\left(-\frac{x^2}{2}\right) \quad (7)$$

3.5.4. The Lévy Flight

The Lévy Flight is a stochastic process used in AGOA to update candidate solutions, allowing for long-distance jumps in the search space. This balances exploitation and exploration, enabling AGOA to explore distant regions and potentially find promising solutions.

The Lévy flight utilizes the Lévy distribution from Equation (8) to perform a random walk.

$$L(X_j)=\left|X_j\right|^{1-\alpha} \quad (8)$$

Where $\alpha = (1, 2)$ denotes the power law exponent and X_j denotes the flight space. Equation (9) represents the regular operation of Lévy.

$$f_L(x;\alpha,\nu)=\frac{1}{n}\int_{\infty}^{0}\exp\left(-\nu q^{\alpha}\right)\cos(qx)\delta q \quad (9)$$

An algorithm that produces a stable Levy motion was utilized in this work. Equation (10), where α is the distribution indexing handling the motion processes and v is the scale unit, represents the algorithm utilized over the range of 0.3–1.99.

$$Levy(\alpha)=0.05*\frac{x}{|y|^{\frac{1}{\alpha}}} \quad (10)$$

Where α, x, and y are defined as follows equation (11), (12), (13):

$$x=Normal\left(0,\sigma_x^2\right) \quad (11)$$

$$y=Normal\left(0,\sigma_x^2\right) \quad (12)$$

$$\sigma_x=\left[\frac{\Gamma(1-\alpha)\sin\left(\frac{\pi\alpha}{2}\right)}{\Gamma\left(\frac{1+\alpha}{2}\right)\alpha 2^{\frac{\alpha-1}{2}}}\right] \quad (13)$$

Where, $\sigma_y = 1$ and $\alpha = 1.5$.

3.5.5. Random walk

AGOA incorporates a Random Walk as an adaptive strategy for updating candidate solution updates, enhancing exploration capability and potentially discovering promising solutions beyond traditional updating strategies, involving a series of random steps. The definition of a random walk in mathematics is Equation (14)

$$W_N=\sum_{i=1}^{N-1}s_i, \quad (14)$$

where any random distribution can be utilized to produce the random step s_i. Any two successive RW's relationship, as described by Equation (15)

$$W_N=\sum_{i=1}^{N-1}s_i=\sum_{i=1}^{N-1}s_i+X_N=W_{N-1}+s_N \quad (15)$$

This connection states that the next state (WN) depends only on the current state (WN − 1) and the activity required to go from the current state to the next. Step size si can be fixed or can vary. Therefore, for a wolf that starts from point x0 and suppose its final location is xN, then RW can also be defined as Equation (16)

$$x_n=x_0+a_1s_1+a_2s_2+\cdots+a_N=x_0+\sum_{i=1}^{N}a_is_i, \quad (16)$$

Where, $\alpha_i > 0$ is a parameter that controls the step size s_i in each iteration.

Random Walk is a search algorithm that prevents local optima by adjusting step size distribution, enhancing search efficiency and robustness in the LeNet-5 architecture. Inspired by gazelle strategies, it encourages exploration of new areas and exploitation in immediate areas.

3.6. Watermark Extraction

The watermark extraction phase involves a trained AGOA-configured LeNet-5 neural network to accurately retrieve the embedded watermark from a watermarked image. The network optimizes its hyperparameters during training, allowing it to learn and capture intricate patterns and features within the watermarked image.

The AGOA-configured LeNet-5 analyzes watermarked images, distinguishing embedded watermark information from host image background. It uses adaptive strategies to

efficiently explore and identify relevant features, ensuring high accuracy in watermark retrieval, even in diverse attacks or distortions.

The AGOA configured LeNet-5 network efficiently processes watermarked images, performing complex calculations and decoding the embedded watermark. Its deep architecture and robustness to perturbations enable accurate and reliable watermark extraction, enabling copyright verification, authentication, and content protection. The combination of an adaptive optimization algorithm and a deep neural network is crucial for robust watermark retrieval, demonstrating the effectiveness of this approach.

4. Results and Discussion

Utilizing a test dataset of 300 gray scale images (512 × 512) that was distinct from the training set of images, the suggested LWT-DNN based image watermarking approach was assessed. Standard images, such as Lena, Barbara, Peppers, Boat, Fruits, Mandrill, Airplane, and Camera Man were also included in the evaluation. Figure 4 illustrates the original images, watermarked images (no attack), and the corresponding extracted watermarks. Figure 5 shows the watermarks that were taken out of the Barbara image and applied to the various attacks. The study used a MATLAB system with an i7 processor and 16 GB RAM for experiments on watermark embedding.

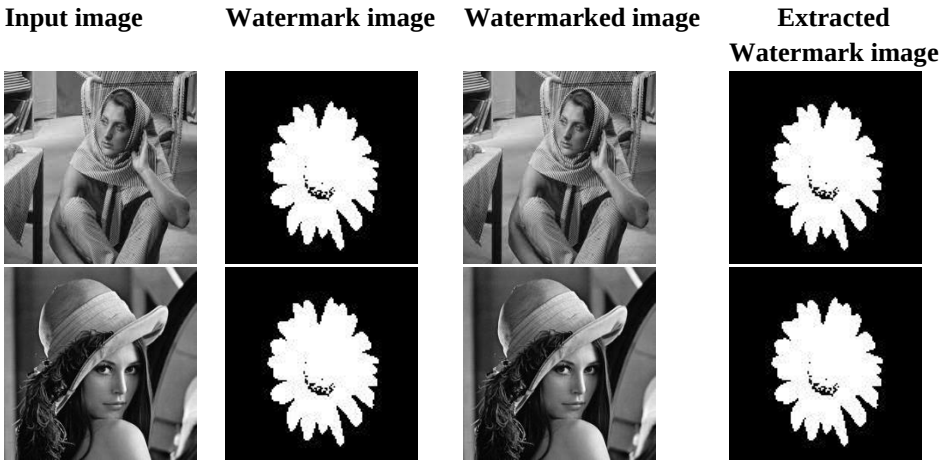

Fig. 4. Examples of standard images utilized in this research.

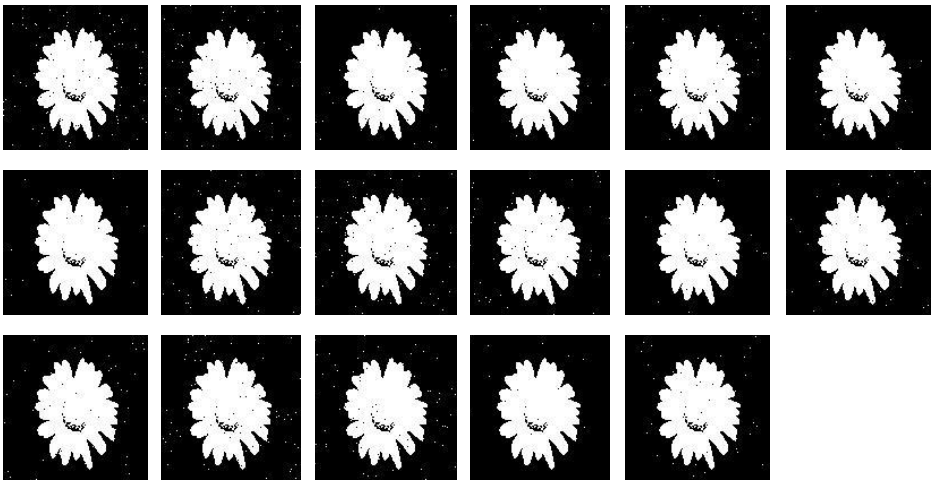

Fig. 5. Extracted watermarks from the Barbara image for the employed different attacks.

4.1. Bit Error Rate (BER)

BER is a performance metric for watermarking techniques, assessing the accuracy of retrieval. A lower BER indicates better robustness, indicating fewer errors in recovering the embedded watermark from the image, even under dissimilar attacks. The table 1 presents the BER results for each technique and attack combination, showcasing the performance of each method against various types of attacks.

Table 1. Bit Error Rate

Attacks	*SVM [24]*	*DNN [20]*	*lenet-5*	*PSO-lenet5*	*GOA-lenet-5*	*AGOA-lenet5*
SN(1%)	0.0548	0.2104	0.0512	0.0485	0.04589	0.0402
SPN(1%)	0.0778	0.1176	0.07568	0.07125	0.06584	0.06152
GN(0.5%)	0.1061	0.0505	0.0485	0.04568	0.03981	0.035246
AF(3x3)	0.1477	0.0503	0.04985	0.04625	0.04102	0.03652
MF(3x3)	0.1265	0.0835	0.07854	0.0758	0.0721	0.0652
GF(3x3)	0.0043	0.0006	0.00056	0.00052	0.0005	0.00045
IS	0.0066	0.0001	0.0000984	0.000054	0.0000423	0.00004
HE	0.0531	0.0231	0.0201	0.0195	0.018596	0.01785
CR(25%)	0.1354	0.0006	0.00056	0.0005	0.000475	0.000412
CR(10%)	0.0534	0.0001	0.000094	0.00009	0.0000854	0.000074
JPEG 20	0.0124	0.0054	0.0051	0.0046	0.0042	0.0036
JPEG 30	0.029	0.0118	0.0102	0.009582	0.00854	0.00745
JPEG 40	0.0357	0.0119	0.0105	0.00962	0.00812	0.00624
JPEG 50	0.0078	0.0057	0.0042	0.0032	0.0026	0.0012
GC(1.6)	0.0044	0.001	0.00094	0.00085	0.000745	0.000632
SCL(65%)	0.0575	0.0178	0.012	0.00958	0.00842	0.0071
SCL(75%)	0.0045	0.002	0.00152	0.001	0.00085	0.00062

4.2. Normalized Cross Correlation (NCC)

AGOA-lenet-5, when combined with LeNet-5, is an efficient and resilient method for watermark extraction, consistently achieving superior NCC values, making it a promising approach for digital image watermarking. Table 2 provided shows the NCC values for various watermark extraction techniques under dissimilar types of attacks.

Table 2. Normalized Cross Correlation

Attacks	*SVM [24]*	*DNN [20]*	*lenet-5*	*PSO-lenet5*	*GOA-lenet-5*	*AGOA-lenet5*
SN(1%)	0.8903	0.4073	0.8941	0.902	0.9085	0.912
SPN(1%)	0.8648	0.6736	0.8754	0.882	0.8895	0.8965
GN(0.5%)	0.7894	0.804	0.8125	0.8256	0.8295	0.8348
AF(3x3)	0.7241	0.8078	0.8167	0.8265	0.8352	0.8395
MF(3x3)	0.7474	0.7152	0.7584	0.7698	0.7785	0.7854
GF(3x3)	0.9913	0.9979	0.9978	0.9979	0.9982	0.9986
IS	0.9868	0.9995	0.9995	0.9996	0.9997	0.9998
HE	0.8971	0.9256	0.953	0.9584	0.9684	0.9745
CR(25%)	0.7573	0.9977	0.998	0.999	0.9992	0.9996
CR(10%)	0.8979	0.9998	0.99985	0.99989	0.99991	0.99996
JPEG 20	0.9753	0.9964	0.9967	0.9971	0.9975	0.9983
JPEG 30	0.9424	0.961	0.965	0.967	0.969	0.975

JPEG 40	0.055	0.9626	0.9635	0.9714	0.9753	0.9812
JPEG 50	0.964	0.9807	0.9812	0.9835	0.9854	0.9895
GC(1.6)	0.9753	0.9964	0.9971	0.9978	0.9985	0.9992
SCL(65%)	0.8846	0.9353	0.9378	0.9395	0.9421	0.9521
SCL(75%)	0.9851	0.993	0.995	0.996	0.9968	0.998

4.3. Peak Signal-to-Noise Ratio (PSNR)

In order to evaluate the quality of compressed or processed images in comparison to their original, untreated versions, PSNR is a commonly used metric in image and video processing. PSNR is computed utilizing the following Equation (17) – (18).

$$PSNR = 10\log_{10}\frac{MAX^{2}}{MSE} \quad (17)$$

$$MSE = \frac{\sum_{a=1}^{k_1}\sum_{b=1}^{k_2}\left(G(a,b)-G'(a,b)\right)^{2}}{k_1 \times k_2} \quad (18)$$

Where: The maximum value of a pixel in an image is called MAX, and it is usually 255 in 8-bit images. The figure 6 represents the PSNR values obtained from different watermark extraction techniques applied to various images.

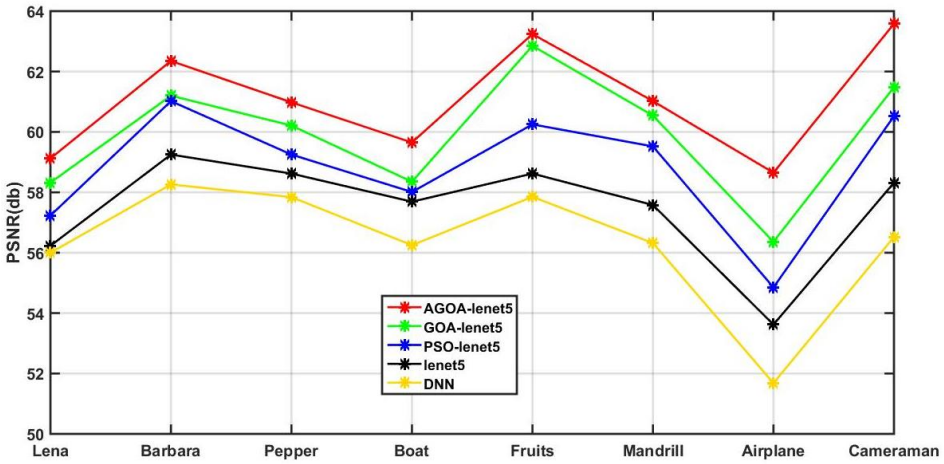

Fig. 6. illustrates the PSNR values obtained from different watermark extraction techniques applied to various images.

4.4. Structural Similarity Index

SSIM is an image quality metric used to assess the performance of watermark extraction techniques, indicating better preservation of structural details and comparison between the original and extracted images. The figure 7 provides the SSIM values for different watermark extraction techniques applied to various images.

$$SSIM(J,K) = P(J,K)Q(J,K)R(J,K) \quad (19)$$

$$P(J,K) = \frac{2\mu_J\mu_K + A_1}{\mu^{2}{}_J + A_1} \quad (20)$$

$$Q(J,K) = \frac{2\sigma_J\sigma_K + A_2}{\sigma^{2}{}_J + \sigma^{2}{}_K + A_2} \quad (21)$$

$$R(J,K) = \frac{\sigma_{JK} + A_3}{\sigma_J\sigma_K + A_3} \quad (22)$$

SSIM is calculated via Equation (19), and the image's brightness is compared using Equation (20). It facilitates the measurement of the proximity between the mean luminance images μJ and μK. If indeed μJ = μK, it suggests that the highest degree of resemblance, which equals one, is present. The contrast is measured using the function found in Equation (21). It gauges how closely the two images' contrasting characteristics are related to one another. For this purpose, standard deviation (σ_J and σ_K) are utilized. When $\sigma_J = \sigma_K$, it denotes that the factor is maximum and equal to 1. When comparing structures, the expression in Equation (22) is utilized to get the coefficient of correlation between the images (J & K). The term σ_{JK} denotes covariance between images J and K. The quantities A_1, A_2 and A_3 are positive constants utilized for avoiding divide-by-zero error.

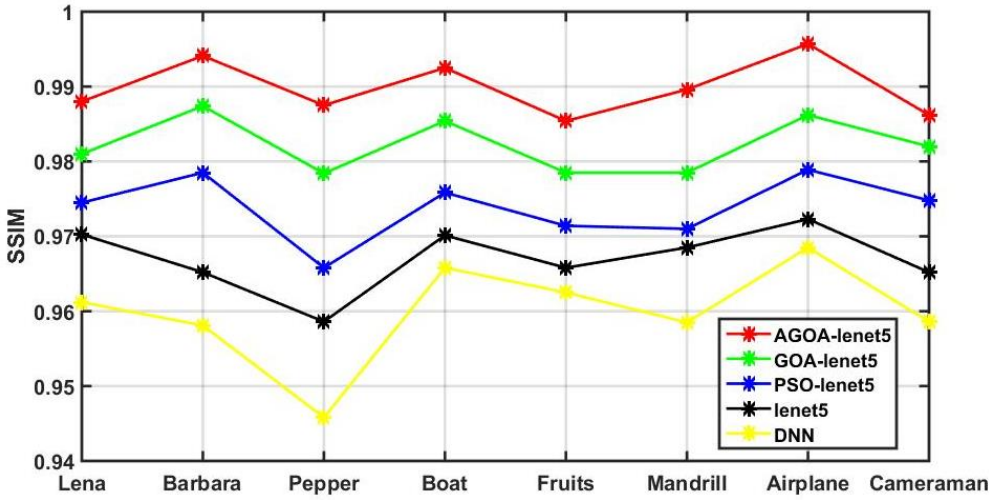

Fig. 7. Illustrates the SSIM values obtained from different watermark extraction techniques applied to various images.

5. Conclusion

In order to provide security and dependability, the proposed approach aims to achieve a balance between robustness and imperceptibility in digital image watermarking. It works to combine AGOA with the LeNet-5 architecture to find the best hyperparameters. The AGOA-lenet5 technique consistently does a better job than other methods. Higher NCC, PSNR, and SSIM values, which indicate accurate watermark extraction and preservation of structural details, are evidence of this. The study affirms the technique's robustness against various common image processing attacks, highlighting its suitability for real-world applications prioritizing image content security. The incorporation of Random Walk as an adaptive strategy enhances the AGOA algorithm's exploration capabilities, making it adept at navigating complex optimization problems. The superior outcomes in terms of robustness and imperceptibility position the AGOA-lenet5 technique as a promising solution for secure digital image watermarking in diverse scenarios. Future research may focus on further optimizing and addressing emerging challenges in the digital content protection domain.

Declaration of Conflicting Interests

The authors have affirmed the absence of any potential conflicts of interest concerning the research, authorship, and/or publication of this article.

Funding

The authors did not receive any financial support for the research, authorship, and/or publication of this article.

References

[1] S. I. Hasan, J. Boaddh, and A. Shrivastava, “A survey on visual properties and techniques of digital image data hiding,” *International Journal of Scientific Research & Engineering Trends.*, no. 5, pp. 54-158, 2019.

[2] O. Hosam, “Attacking image watermarking and steganography-a survey,” *IJCNIS.*, vol. 3, no. 1, pp. 23–37, 2019. DOI:10.5815/ijitcs.2019.03.03

[3] S. I. Batool, T. Shah, and M. Khan, “A color image watermarking scheme based on affine transformation and S4permutation,” *Neural Comput. Appl.*, vol. 25, no. 7–8, pp. 2037–2045, 2014. https://doi.org/10.1007/s00521-014-1691-0

[4] M. W. Hatoum, J. F. Couchot, R. Couturier, and R. Daraz, "Using deep learning for image watermarking attack," *Signal Process. Image Commun.*, vol. 90, pp. 116019, 2021. https://doi.org/10.1016/j.image.2020.116019

[5] N. M. Makbol, and B.E. Khoo, “Robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition,” *AEU-Int J Electron Commun.*, vol. 67, no. 2, pp.102–112, 2013. https://doi.org/10.1016/j.aeue.2012.06.008

[6] J. E. Lee, Y. H. Seo, and D. W. Kim, "Convolutional neural network-based digital image watermarking adaptive to the resolution of image and watermark," *Appl. Sci.*, vol. 10, no. 19, pp.6854, 2020. https://doi.org/10.3390/app10196854

[7] F. Daraee, and S. Mozaffari, “Watermarking in binary document images using fractal codes,” *Pattern Recognit. Lett.*, vol. 35, pp. 120–129, 2014. https://doi.org/10.1016/j.patrec.2013.04.022

[8] W., Zheng, S. Mo, X. Jin, Y. Qu, F. Deng, J. Shuai, Z. Xie, C. Zheng, and S. Long, "Robust and high capacity watermarking for image based on DWT-SVD and CNN". *In 2018 13th IEEE Conference on Industrial Electronics and Applications (ICIEA)*, pp. 1233-1237, IEEE, 2018.DOI: 10.1109/ICIEA.2018.8397898

[9] Y.S. Lee, Y.H. Seo, D.W. Kim, “Blind image watermarking based on adaptive data spreading in n-

level DWT subbands," *Secur. Commun. Netw.*, pp. 357251, 2019. https://doi.org/10.1155/2019/8357251

[10] H. Fırat, M. E. Asker, M. İ. Bayindir, and D. Hanbay, "Spatial-spectral classification of hyperspectral remote sensing images using 3D CNN based LeNet-5 architecture," *Infrared Phys. Technol.*, vol. 127, pp.104470, 2022. https://doi.org/10.1016/j.infrared.2022.104470

[11] A. M. Abdelhakim, and M. Abdelhakim, "A time-efficient optimization for robust image watermarking using machine learning," *Expert Syst Appl.*, 100, pp.197-210, 2018.

[12] A. M. Abdelhakim, H. I. Saleh, and A. M. Nassar, "A quality guaranteed robust image watermarking optimization with Artificial Bee Colony," *Expert Syst Appl.*, vol. 72, pp.317-326, 2017. https://doi.org/10.1016/j.eswa.2016.10.056

[13] Y. Guo, B. Z. Li, and N. Goel, "Optimised blind image watermarking method based on firefly algorithm in DWT-QR transform domain", *IET Image Process.*, vol. 11, no. 6, pp. 406-415, 2017. https://doi.org/10.1049/iet-ipr.2016.0515

[14] M. Moosazadeh, and G. Ekbatanifard, "An improved robust image watermarking method using DCT and YCoCg-R color space," *Optik.*, vol. 140, pp. 975-988, 2017. https://doi.org/10.1016/j.ijleo.2017.05.011

[15] R. Mehta, N. Rajpal, and V. P. Vishwakarma, "LWT-QR decomposition based robust and efficient image watermarking scheme using Lagrangian SVR," *Multimed. Tools Appl.*, vol. 75, pp. 4129-4150, 2016. https://doi.org/10.1007/s11042-015-3084-5

[16] M. Vafaei, H. Mahdavi-Nasab, and H. Pourghassem, "A new robust blind watermarking method based on neural networks in wavelet transform domain," *World Appl. Sci. J.*, vol. 22, no. 11, pp.1572-1580. 2013.

[17] W. Taiyue, and L. Hongwei, "A Novel digital image watermarking algorithm based on curvelet transform," *International Journal of Digital Content Technology and its Applications*, vol. 7, no. 1, pp. 512, 2013. https://doi.org/10.1155/2015/937432

[18] X. Wang, D. Ma, K. Hu, J. Hu, and L. Du, "Mapping based residual convolution neural network for non-embedding and blind image watermarking," *Journal of Information Security and Applications.*, vol. 59, pp. 102820, 2021. https://doi.org/10.1016/j.jisa.2021.102820

[19] H. K. Singh, and A. K. Singh, "Digital image watermarking using deep learning," *Multimed. Tools Appl.*, pp.1-16, 2023. https://doi.org/10.1007/s11042-023-15750-x

[20] S. Mellimi, V. Rajput, I. A. Ansari, and C. W. Ahn, "A fast and efficient image watermarking scheme based on deep neural network," *Pattern Recognit. Lett.*, vol. 151, pp. 222-228, 2021. https://doi.org/10.1016/j.patrec.2021.08.015

[21] M. Begum, and M. S. Uddin, "Towards the development of an effective image watermarking system," *Security and Privacy*, vol. 5, no. 2, pp. e196, 2022. https://doi.org/10.1002/spy2.196

[22] S. S. Sharma, and V. Chandrasekaran, "A robust hybrid digital watermarking technique against a powerful CNN-based adversarial attack," *Multimed. Tools Appl.*, vol. 79, no. 43-44, pp.32769-32790, 2020. https://doi.org/10.1007/s11042-020-09555-5

[23] J. O. Agushaka, A. E. Ezugwu, and L. Abualigah, "Gazelle Optimization Algorithm: A novel nature-inspired metaheuristic optimizer," *Neural Comput. Appl.*, vol. 35, no. 5, pp.099-4131, 2023. https://doi.org/10.1007/s00521-022-07854-6

[24] M. Islam, A. Roy, and R. H. Laskar, "SVM-based robust image watermarking technique in LWT domain using different sub-bands," *Neural Comput. Appl.*, vol. 32, pp.1379-1403, 2020. https://doi.org/10.1007/s00521-018-3647-2