International Journal of Safety and Security Engineering
Vol. 14, No. 6, December, 2024, pp. 1921-1931
Journal homepage: http://iieta.org/journals/ijsse

Enhancing Image Watermarking: An Innovative Multi-Objective Genetic Algorithm-Based DWT-SVD Approach for Robustness and Imperceptibility

Hiba Al-Khafaji[1*], Bayadir Al-Himyari[2], Hasanein Alharbi[2]

[1] Department of Software, College of Information Technology, University of Babylon, Babel 51001, Iraq
[2] Department of Information Security, College of Information Technology, University of Babylon, Babel 51001, Iraq

Corresponding Author Email: hibamj.alkhafaji@uobabylon.edu.iq

https://doi.org/10.18280/ijsse.140626

Received: 9 July 2024
Revised: 18 August 2024
Accepted: 17 December 2024
Available online: 31 December 2024

Keywords:
Arnold transforms, Discrete Wavelet Transform (DWT), embedding distortion, image watermarking, multi-objective genetic algorithm (MOGA), robustness, singular value decomposition

ABSTRACT

This paper investigates the enhancement of the image watermarking algorithm through its robustness and imperceptibility. We propose a watermarking method for protecting image data that is established using an optimal Discrete Wavelet Transform and Singular Value Decomposition (DWT-SVD). A multi-objective genetic algorithm (MOGA) with two conflicting objectives (i.e., PSNR and Hamming Distance (HD)) is employed to minimize the embedding distortion and maximize the robustness. These goals are achieved by merging natural selection and GA, producing a powerful tool for coefficients embedding optimization. GA has been used to guide the selection process of DWT coefficients for watermark embedding. We use Arnold transform to scramble the watermark bits to increase the watermark security. Consequently, various evaluation functions such as Peak signal-to-noise and SSIM are calculated to examine the watermarked image quality. Eventually, the selected coefficients represent the optimal choices to minimize the embedding distortion and maximize the robustness against attack. The final results of experiments demonstrate that the presented method is robust to many types of attacks, namely, Salt & Pepper, Gaussian, Speckle, Poisson, Resizing, Rotation, Median filter, cropping, and compression. The findings demonstrate that the suggested method performed better by implying embedding distortion and attack resistance than the current techniques.

1. INTRODUCTION

Digital content has been rapidly growing in the past decades. As a result, an urgent need for content management systems to safeguard digital content is raised. Watermarking techniques arise as a powerful solution for protecting and authenticating digital multimedia. Imperceptibility and robustness are the primary goals of any watermarking approach. However, it is often observed that enhancing robustness can lead to a decrease in imperceptibility. Therefore, a successful watermarking approach must secure a delicate balance between robustness and imperceptibility [1].

Conventional watermarking methods have relied on fixed algorithms and pre-defined parameters, leading to potential performance limitations. These techniques often encounter challenges concerning imperceptibility, robustness against detection and attacks, and the capacity to hide a substantial amount of data. Evolutionary algorithms, such as genetic algorithms (GAs), are employed to optimize watermarking techniques to address these shortcomings. GAs mimics the natural process of selection, reproduction, and mutation. They enhance the effectiveness and robustness and maximize hidden data capacity within watermarking techniques [2, 3].

The basic principle of using genetic algorithms in watermarking techniques is to treat the problem as an optimization task. The optimization task objective is to find an optimum or near-optimum solution. GAs start by developing a potential solutions population. Then, iteratively, refining and choosing individuals depending on their fitness to a predefined objective function. The proposed solution population is explored using various genetic operations such as selection, crossover, and mutation.

Eventually, the algorithm scans the solution space to find the most suitable hiding strategy that meets the desired criteria, such as imperceptibility, robustness, and capacity [3-5].

On the other hand, many researchers [6-9] have proven that the spread spectrum watermarking approach is very powerful in image protection. Its primary benefits stem from developments in signal transformation techniques, including the Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT).

This paper introduces a novel watermarking approach using multi-objective genetic algorithm (MOGA). The main objective is to minimize the embedding distortion and maximize the robustness of the watermarking approach. This is accomplished by inserting watermark bits into precisely chosen image pixels that satisfy a given fitness function's requirements. The primary novelty of our research lies in identifying and utilizing optimal pixels, which effectively reduce the embedding distortion while enhancing robustness

against various attacks. Different types of attacks, Salt & Pepper, Gaussian, Speckle, Poisson, Resizing, Rotation, Median filter, cropping, and compression, are executed to evaluate the presented method. The key contributions of our approach include the following:

1) Proposing a new watermarking approach based on MOGA. This research aims to achieve two conflicting objectives: maximization of PSRN and minimization of Hamming Distance (HD). It is a multi-objective optimization problem that has more than one objective function. The best solution for one goal might not always be the greatest solution for the other objectives in these kinds of challenges. Given that a single solution would not be the best way to achieve every goal, it is necessary to propose various alternatives that make concessions to various goals. To tackle this scenario, a weighted sum MOGA approach is applied. The multi-objective functions are combined into one scalar that consists of a composite objective function with a weighted sum.
2) Proposing a new watermarking approach using an optimal Discrete Wavelet Transform Singular Value Decomposition (DWT-SVD) that decreases the embedding distortion in the watermarked image.
3) Proposing a new approach using an optimal DWT-SVD to make the embedded watermark robust against many attacks.

The paper's subsequent sections are organized as follows: Section 2 introduces a review of the pertinent literature on image watermarking, focusing on genetic algorithms. Section 3 offers preliminaries about Discrete Wavelet Transform and Singular value decomposition, followed by an overview of genetic algorithms. In Section 4, the suggested methodology is introduced. Section 5 delves into a comprehensive discussion of the proposed method's performance, supported by experimental results. Finally, Section 6 introduces the concluding remarks of the study.

2. RELATED WORK

Watermarking approaches are primarily categorized into two groups: spatial and frequency domains. In the spatial domain approaches, the watermark is embedded straight into the image pixels [10-13]. In the frequency domain, the watermark is hidden in the image coefficients [1, 7-9, 14].

This section reviews various spatial and frequency domain techniques. For example, the work presented in Abraham and Paul's study [15] proposes a watermarking embedding technique that utilizes the least significant bits (LSB). Then, the watermark spreads over a region of image pixels. The results indicate that this approach exhibits robustness against attacks while maintaining high image quality.

Su et al. [16] submitted a blind watermarking approach established using Schur decomposition. The suggested approach is implemented for copyright protection. The obtained results demonstrated low computational complexity and robustness. A watermarking approach is established using LSB and Hill Cipher techniques proposed by Kumar and Singh [13]. Watermark is encrypted and embedded in the blocks secured with the highest entropy using the Hill Cipher encryption approach. The evaluation of the robustness of the suggested approach was done using several image processing attacks, including Salt and Pepper, Median filter attacks, and Gaussian filter attacks.

In Ali's study [17], a blind and robust watermarking approach has been presented. Image pixels are directly altered in the spatial domain to embed the watermark based on quantizing the block-wise invariant maximum singular value. To create a new image, the pixels from the cover image are redistributed by a distribution rule. The new image is detached into non-overlapping and square blocks to acquire invariant maximum singular values based on the matrix 2-norm in the spatial domain without needing an SVD transform.

On the other hand, in the frequency domain, the approach presented in Roy and Pal's study [18] shows a hybrid robust watermarking method. DWT and SVD were used in the suggested method. An RGB color image is first transformed to a YCbCr color space, where only the Y achromatic component is taken into account while adding the watermark. The Y component is broken down into non-overlapping blocks in the next phase, and then DWT is implemented for each block. In conclusion, singular values of DWT-transformed host picture blocks conceal non-overlapping decomposed grey watermark image blocks. The proposed approach exhibits robustness against popular geometric transformation attacks such as flip operation, shearing, rotation, scaling, cropping, and column operation or deletion of lines. Additionally, the robustness against compression, popular enhancement technique attacks, and combinational attacks are evaluated.

Another work applied discrete stationary wavelet transforms and SVD is presented in Chellappan et al.'s study [19] to conceal a watermark from view. SVD and three-level wavelet decomposition are used. The watermarked image is subjected to various treatments, including geometric changes, noise attacks, and filtering operations. The suggested work demonstrates strong resilience against these assaults. Furthermore, compared to the existing methods, the obtained result shows a superior performance in terms of normalized cross-correlation coefficient, bit error rate, and peak signal-to-noise ratio.

The approach presented by Elbasi et al. [20] proposed a semi-blind watermarking technique, where images are transformed into discrete Wavelet Transformations (DWTs) by dividing them into 4 X 4 blocks. Following that, each block has a binary picture integrated into it, applying the flexible scaling factor method. The findings indicate that the suggested method outperforms block-based wavelet techniques and standard wavelet transformation regarding similarity ratio (SR) and peak signal-to-noise ratio (PSNR). Furthermore, the optioned findings demonstrate that the suggested hybrid algorithm outperforms block-based DWT and DWT techniques in effectiveness, robustness, resistance, and security.

El Houbyand and Yassin's study [21] suggests a blind watermarking approach using the Hadamard transform and Discrete Wavelet Transform (DWT). A genetic algorithm (GA) is utilized to balance distortion and robustness. Consequently, the obtained results illustrate that the presented approach is robust against multiple attacks, such as compression, cropping, and median filtering.

In Bassel et al.'s study [22], another GA-based watermarking approach is proposed. GA is adopted to hide the watermark in the S component of the SVD. The objective function calculates the PSNR and correlation, as the correlation measures the normalized cross-correlation

between the extracted watermark from each modified image and the original watermark. The experiments illustrate that the watermark can survive after severe attacks. The results demonstrate that the presented approach is outperforming the existing work.

In Mood and Konkula's study [23], GA is integrated with Redundant Wavelet Transform (RWT) and SVD to propose a secure and robust watermarking technique. While SVD and RWT are utilized for feature extraction, GA is utilized for optimization. Furthermore, a signature embedding mechanism has been suggested to secure the watermarked image. The performance of the proposed approach is tested using various performance measures such as Normalized Correlation (NC) and PSNR. Overall, the acquired results demonstrate superior quality compared to the conventional approach. Additionally, the proposed method provides an effective defense against attacks such as scaling, histogram equalization, median filtering, cropping, rotation, contrast enhancement, and Gaussian noise.

In a slightly different manner, Meenakshi et al. [24] presented a hybrid watermarking method that combines SVD and wavelet transform. The GA is executed to enhance the method's robustness and imperceptibility by optimizing the watermarking metrics. In Zhu et al.'s study [25], an optimized image watermarking algorithm has been proposed, where integer wavelet transform (IWT) and SVD are investigated. In the initial stage, the host images are divided into blocks. Next, the low frequency portion of the SVD is performed after the block-based integer wavelet transform has been implemented. Lastly, to strengthen the resilience of digital watermarking, the first unique value is employed. In parallel, GA is used to maximize image watermarking's resilience and imperceptibility. Experimental results illustrate that the suggested method has good NC and PSNR values compared to existing methods. Additionally, it shows good performance against various attacks as: Gaussian noise, low-pass filtering, changing the size, JPEG compression, and gamma correction. In a different study [26], a blind watermarking approach using fractional Fourier transform and GA is implemented on both spatial and frequency domains. By minimizing the root mean square error between the input and the watermarked images, GA is used to identify the ideal fractional domain while the watermark is encoded in the fractional Fourier coefficients. The experimental results demonstrate that the watermarked images exhibit high performance even after subjected to JPEG compression and exposure to Gaussian noise.

Sivananthamaitrey and Kumar [27] presented a watermarking approach for color image. The stationary wavelet transforms and SVD are utilized in this work. Two watermarks were used in the suggested approach to handle copy-right protection and tamper localization problems. A greyscale picture watermark is buried in the green plane of the host image's transform domain for copyright protection. Furthermore, the least significant bit approach is used to insert a watermark in the blue plane's spatial domain of the cover image. After that, GA is applied to optimize the suggested strategy to enhance robustness and perceptual quality. Ultimately, many attacks on the watermarked image have been used to assess the robustness of the suggested technique. Furthermore, the algorithm's embedding capacity and the suggested fitness function's temporal complexity are contrasted with other published researches.

Based on the evidence drawn from the recent works, it can be concluded that the main drawback of traditional watermarking methods is embedding the watermark without considering the optimal positions of pixels or coefficients with regard to imperceptibility and robustness against attack. In contrast, GA offer an advantageous solution by identifying the optimal positions of pixels that minimize distortion and maximize robustness against various attacks. As a result, these are two conflicting objectives, in order to deal with the MOGA was introduced. This is a promising approach to enhance the performance of watermarking methods in terms of resistance to attacks and imperceptibility.

3. PRELIMINARIES

3.1 Discrete Wavelet Transform (DWT)

DWT is a powerful signal processing and analysis tool. It's known for its high performance in the time and frequency domain. A time-scale representation of the signal is generated by DWT through the use of digital filtering techniques. Digital signal under study is subjected to filters with different scales and cutoff frequencies. The four sub-bands that DWT breaks down an image into are LL, HL, LH, and HH. In order to generate the lower resolution approximate sub-band (LL) which roughly describes the image, within both directions the digital signal is passed through a low-low filter. Conversely, the targeted image is passed through a high-pass filter in one direction and a low-pass filter in the other to obtain the LH and HL sub-bands. Finally, a high-pass filter that captures the high frequency component along the diagonals is applied in both directions to get the HH sub-band.

As a result of processing the image signal using DWT, the LL image contains the majority of the information included in the original image. On the other hand, the horizontal edges' corresponding vertical features information is primarily contained in the LH. Similarly, horizontal detail information from the vertical edges is represented by HL. Overall, DWT's exceptional spatial-frequency localization capabilities have demonstrated its value in identifying regions of the source image where a watermark can be subtly added. Thus, watermarking is commonly used. The conflict between robustness and transparency is overcome by implementing a modifications to the HH, LH, and HL sub-bands. Generally speaking, embedding watermark data through modifying the DWT coefficients is done.

DWT is recommended because it offers simultaneous spatial localization and frequency dispersion of the watermark within the cover image. The primary goal of DWT in image processing is to differentiate and break down a picture into sub-images with independent frequencies and distinct spatial domains. As a result, DWT is regarded as an optimal choice in the watermarking field [28, 29].

3.2 Singular Value Decomposition (SVD)

In linear algebra, singular value decomposition (SVD) is considered a significant tool, commonly performed in many research fields such as principal component analysis, data compression and canonical correlation analysis. Let X be a matrix with size M×N. The decomposition for X can be represented by Eq. (1) as follows:

$$X = USV^T \tag{1}$$

where, T stands for the conjugate transpose operation and U, V, and W are the eigen-vectors of matrix X. The terms "left eigenvector" and "right eigenvector" refer to the U and V^T components, respectively. Eq. (2) specifies the orthogonal matrices that form the two components.

$$I_M = U_M^T U^M \\ I_N = V_N^T V^N \tag{2}$$

where, M×M and N×N are the respective sizes of the identity matrices, I_M and I_N. In the singular value domain, component S is a diagonal matrix containing non-negative real values.

$$S_{MN} = \begin{bmatrix} \sigma(1,1) & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \sigma(M,N) \end{bmatrix} \tag{3}$$

where, $(1,1) \geq \sigma(2,2) \geq \cdots \geq \sigma(M, N) \geq 0$.

SVD involves a very important feature related to its singular value of the images which is the stability when inserting a small data to the images and survive the embedding data without a distortion. Therefore, SVD is a common algorithm in the image watermarking [30, 31].

3.3 Genetic algorithm (GA)

GA is classified as heuristic optimization algorithms, drawing inspiration from the concept of species evolution [32]. Their operation revolves around generating a population through random initialization and subsequently selecting the most promising individuals based on fitness functions across generations, while replacing weaker offspring. Unlike methods relying on a single solution, GA initiate with multiple potential solutions. Over numerous generations, applying crossover and mutation eventually leads to the attainment of the optimal solution (optimal offspring) [33, 34]. GA includes the following steps:

1) Evaluation of Individual: Based on a fitness function, GA provides the natural selection in evolution process where each individual in the population is evaluated. The fitness function is used to measure the quality of each individual. The higher individual score is the best individual.
2) Reproduction (Crossover and Mutation): The selected individuals undergo both crossover and mutation processes. Crossover emulates biological reproduction by merging two chosen individuals to create a new offspring with characteristics inherited from both parents. The probability of crossover occurrence, denoted as Pc, ranges from 0 to 1. Crossover takes place if a randomly generated number, Rc, is less than or equal to Pc. Otherwise, the parents produce offspring without undergoing crossover. Following crossover, mutation is applied to introduce random changes to each element of an individual. This mutation process is inspired by the genetic changes observed in an organism's DNA.
3) Replacement: In the evolutionary process, the replacement mechanism holds vital importance. It involves selecting the best individuals based on their fitness scores to become part of the next generation. Following the reproduction operation and after obtaining the fitness function for each offspring, this step is then applied for determining whether they are replaced or retained in the population.
4) Initialization and Stopping Criteria**:** In the evolutionary cycle, both initialization and stopping criteria are essential. Initialization aims to generate a random initial population, setting the foundation for the evolutionary process. On the other hand, stopping criteria are necessary to halt the evolutionary cycle based on specific conditions, such as reaching a maximum number of generations or obtaining the best solution. These criteria determine when the algorithm should cease its search and output the final result.

4. PROPOSED METHOD

This section gives a comprehensive explanation of the proposed method. The chosen method for non-blind watermarking is known as magnitude-based multiplicative watermarking techniques due to its simplicity [35]. The proposed method includes two steps: embedding and extraction processes.

In the first step ,embedding process, the host image (I) is decomposed using DWT (for N1 levels) into 4 sub-bands: LL, HL, HH, and LH. Secondly, the singular values of HL and LH sub-bands are calculated. Then, the watermark (w) is scrambled using Arnold transform. Next, the scrambled watermark is embedded in the singular values of LH and HL bands, to do balance between the impeccability and robustness as follows:

$$S_{HL_w} = S_{HL} + (S_{HL} W_s \alpha) \\ S_{LH_w} = S_{LH} + (S_{LH} W_s \alpha) \tag{4}$$

where,

$\boldsymbol{S_{HL}}$ and $\boldsymbol{S_{LH}}$ are the singular values of LH and HL bands.

α is the watermark strength.

w_s is the scrambled watermark.

After that, we apply inverse SVD to acquire the new LH and HL coefficients. Finally, inverse DWT is applied on the coefficients to acquire the watermarked image (I_w).

In the extraction process, the steps of the embedding process are inversed. In order to extract the watermark, the original host image is required. Firstly, the watermarked image is decomposed into 4 sub-bands: LL, HL, LH, and HH. Then, the singular values of HL and LH bands are calculated. Next, we extract the scramble watermark from singular values of HL and LH bands as follows:

$$w_s{}' = \frac{S_{HL_w} - S_{HL}}{S_{HL}\alpha} \\ w_s{}' = \frac{S_{LH_w} - S_{LH}}{S_{LH}\alpha} \tag{5}$$

Finally, we perform an inverse Arnold transform to obtain the embedded watermark.

While w_0 and w_1 are the selected watermark values for hiding a 0 and 1, a threshold value T is used to identify the extracted watermark bit b.

where,

$$T = \frac{w_0 \quad + w_1}{2} \tag{6}$$

$$b' = \begin{cases} 0 \ , if \ w' < T \\ 1 \ , if \ w' > T \end{cases} \quad (7)$$

4.1 Multi-object genetic algorithm (MOGA)

MOGA is utilized to find the optimal solutions. The length of the constructed MOGA chromosome is equal to the length of the watermark bits. Initially, a random population is generated from the host image. The size of the generated population is equal to the number of chromosomes that represent all possible solutions. Furthermore, a crossover operation is applied to obtain an offspring chromosome. The number of the chromosome genes depends on the number of the watermark bits. The scan for new chromosomes is stopped when the max generations is reached. Finally, the watermark is hidden in the best chromosome, which represents the optimal solution.

The two conflicting goals of this study are to minimize the Hamming Distance (HD) and maximize PSRN. There are multiple objective functions in this multi-objective optimization problem. In these kinds of issues, the best answer for one goal may not always be the best answer for the other objectives. Since there isn't a single optimum approach to accomplish every goal, it's important to offer a range of options that compromise on different objectives. A weighted sum MOGA technique [36, 37] is used to address this situation. One scalar made up of a composite objective function with a weighted sum is created by combining the multiple objective functions.

$$f(x) = g1f1(x) + g2f2(x) + \cdots + gkfk(x) \quad (8)$$

Eq. (8) indicates that that the weighting coefficients (*g1,g2,…gk*) represent the importance of the functions (*f1(x),f2(x),…fk(x)*). The solutions highly depend on the weights which have positive values, as explained in Eq. (9).

$$\sum_{i=1}^{k} gi = 1, \qquad gi \ \varepsilon \ (0,1) \quad (9)$$

This paper focused on two indicators: the invisible indicator, PSNR, and HD as the robustness indicator. Where, the embedding distortion indicator is calculated as follows:

$$F_{distortion} PSNR \ (I, \ I_w) \quad (10)$$

$$PSNR = 10 \times log_{10} \frac{255^2}{MSE} \quad (11)$$

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (I(i,j) - I_w(i,j))^2 \quad (12)$$

where,

- M and N are the width and length of the image.
- I and I_w are the original host image and watermarked image.
- Furthermore, the robustness against R attacks is measured as follows:

$$F_{\text{robustness}} = \frac{1}{R} \sum_{l=1}^{R} HD(w, w'_{\text{R}}) \quad (13)$$

$$H(w, \quad w') = \frac{1}{Q} \sum w \oplus \quad w' \quad (14)$$

where,

- Q represents the watermark length.
- $\oplus$ is the XOR logical operation.

Accordingly, the fitness function of MOGA will be:

$$Fitness = g1 * F_{distortion} + \frac{1}{g2 * F_{robustness}} \quad (15)$$

where, *g1, g2*=0.5. Consequently, the objective function is turned to one maximum objective function.

4.2 Optimal pixels selections

The ultimate goal is to find the optimal coefficients that ensure both: imperceptibility and robustness. This problem has been expressed mathematically by using the suitable indicators. The indicators are used to quantify the robustness and imperceptibility. In this research HD is utilized to represent the robustness indicator, while PSNR is the invisible indicator.

The following algorithm describes the embedding and extraction processes in details.

4.3 Authentication process

Authenticity is performed by applying Hamming Distance (HD), explained in Eq. (14), to compare the extracted watermark bits (w') with the original watermark bits (W).

5. PERFORMANCE EVALUATION

The performance of the proposed model is evaluated using various attacks and embedding distortion. Overall, three criteria are employed to assess the efficiency of the proposed model: embedding distortion, robustness against attacks and comparison to existing works.

5.1 Experimental setup

Kodak [38] dataset and standard test images (Figure 1) are used to evaluate the proposed watermarking method. Additionally, two types of watermark data are used: set of five binary logos (Figure 2) and pseudo-random binary sequences. The testing images are decomposed using two levels of DWT and watermark strength=0.3. MOGA parameters include a maximum of 100 generations, population size equal to chromosome count, chromosome length corresponding to watermark bits, and a 0.9 crossover probability. Tournament selection and one-point crossover are applied for offspring selection.

Algorithm: Embedding and extraction procedures
Inputs: Host Image (I), watermark logo (w).
Outputs: Watermarked Image (I_w) and extracted watermark (w')
Step 1: decompose the host image (I) using DWT into: LL, HL, LH, and HH
Step 2: generate a random initial population of a potential solutions.
Step 3: calculate the values for HL and LH.

Step 4: scramble the watermark logo (Ws) using Arnold transform.
Step 5: Embed the scrambled watermark (Ws) in the singular values of HL and LH using Eq. (4).
Step 6: Apply the inverse SVD to obtain the new HL and LH coefficients.
Step 7: Perform the inverse DWT to obtain the watermarked image (Iw).
Step 8: Calculate the PSNR for I and Iw.
Step 9: Apply the predetermined R types of attacks, one by one, against the watermarked image.

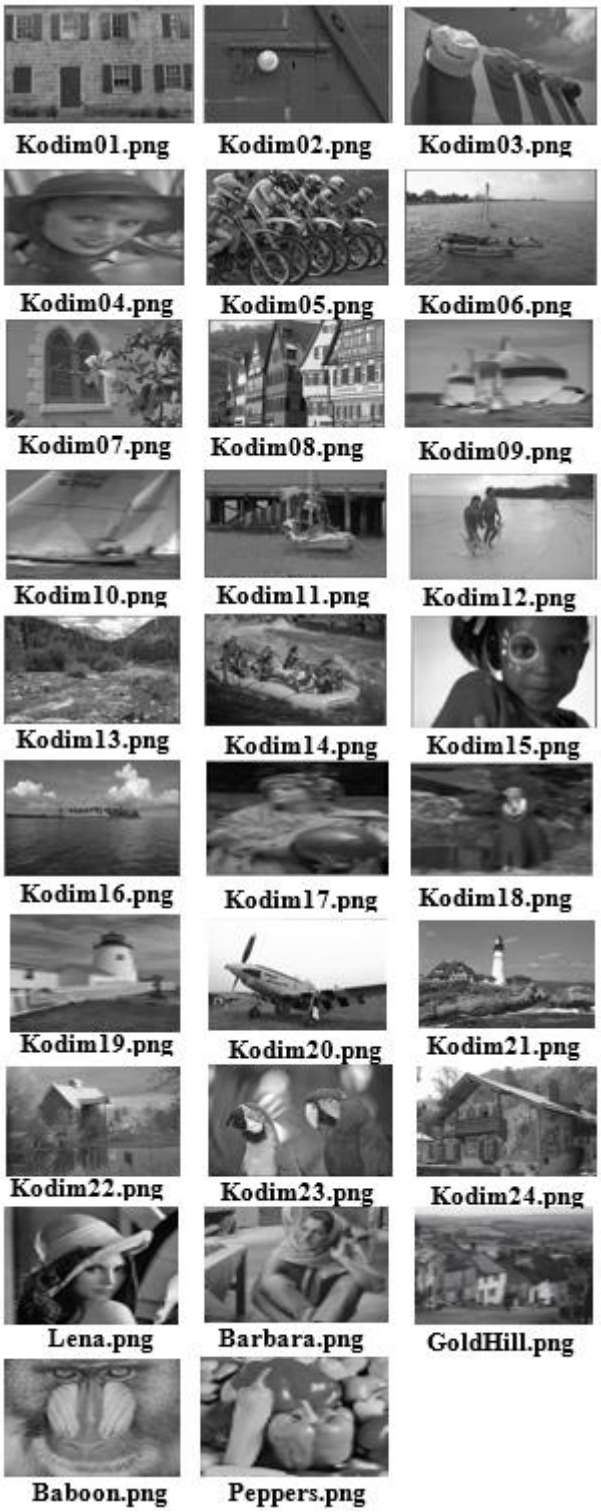


Figure 1. Images dataset

Step 10: Perform the WET upon watermarked image after attacks Iw.
Step 11: Extract the watermarks (Ws) using Eq. (5).
Step 12: Perform the inverse Arnold transform to obtain the extracted watermark (w').
Step 13: Evaluate the objective function to every chromosome of the population.
Step 14: Apply the selection process and crossover operation.
Step 15: Repeat steps 5 to 15 until satisfy the stopping condition.

(a) (b) (c) (d) (e)

Figure 2. Binary watermark logos (a) ieee (b) arrow (c) medicine (d) Sheffield_logo (e) Babylon_logo

5.2 Embedding distortion performance

Peak Signal-to-Noise Ratio (PSNR) metric of the watermarked images is used to assess the embedding distortion performance of the proposed approach. In the initial experiment, we decompose the testing images of size 512×512 pixels for two levels. The watermark logos with a size of 40×40 pixels are embedded in the singular values of DWT coefficients of the second level with watermark strength=0.3. The embedded coefficients are selected according to fitness function. In this experiment, we embed the watermark logos in each band separate in order to show the effect of the embedding distortion in each band. It can be noticed that the highest embedding distortion (lowest PSNR value) is obtained when we embed the watermark logos in the LL band while the lowest embedding distortion (highest PSNR value) is obtained when embedding the watermark in the HH band. On the other hand, embedding the watermark in the LL band provides a high robustness compared to the HH band. Therefore, we have to do a balance between the distortion and robustness. For this reason, we select the LH and HL bands for embedding the watermark because these bands have a low distortion compared to LL band and have a high robustness compared to HH band. Figure 3 illustrates the average value of PSNR of watermarked images after embedding the watermark logos in the selected coefficients of four bands separately using images dataset and watermark strength=(0.3). It can be observed that the HH2 band has the highest PSNR value while the LL2 band has the lowest PSNR value.

Another parameter which has a high effect on the distortion and robustness performance is the watermark strength (α). High watermark strength increases the robustness and the distortion and vice versa. Figure 4 demonstrates the average value of PSNR of the watermarked images (after hiding the watermark in the HL and LH bands) for various watermark strength values (α=0.1, 0.3, 0.5). We can observe that the PSNR value decreases when we increase the watermark strength value. It can be seen that a highest PSNR value of the proposed method is when using the watermark strength value=0.1. To maintain equilibrium between the DWT coefficients' resistance to attack and distortion, the watermark strength (α) can be adjusted in response to the rising frequency.

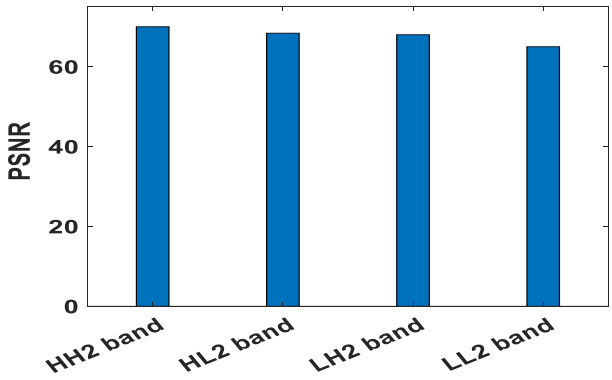


Figure 3. Average PSNR values of the proposed method using four embedding bands

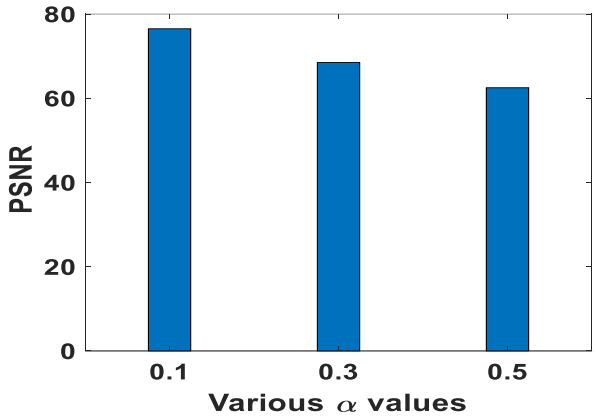


Figure 4. Average PSNR values of the proposed method using various watermark strength values (α)

Our experiments suggest choosing different α values according to the frequency bands: low, mid, and high frequencies. Different α value is used to refer to various frequency group. While αlow<αmid<αhigh refer to low, mid and high frequencies respectively. To assess the embedding distortion, we calculate the PSNR of the watermarked images for the proposed method at various embedding capacities, Pseudo-random binary sequences (b=0.1) are employed as watermark bits to embed in the DWT coefficients of HL and LH bands which are selected according to fitness function.

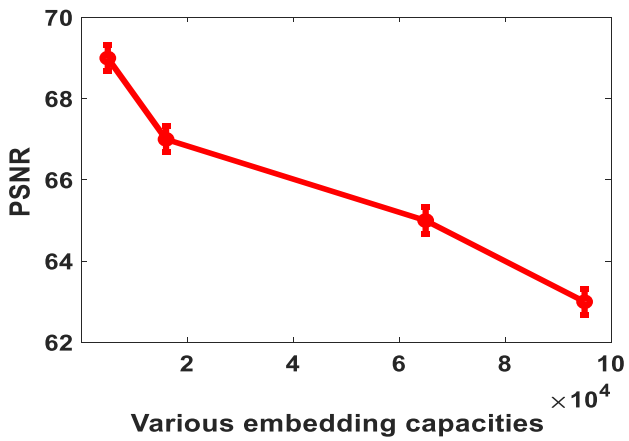


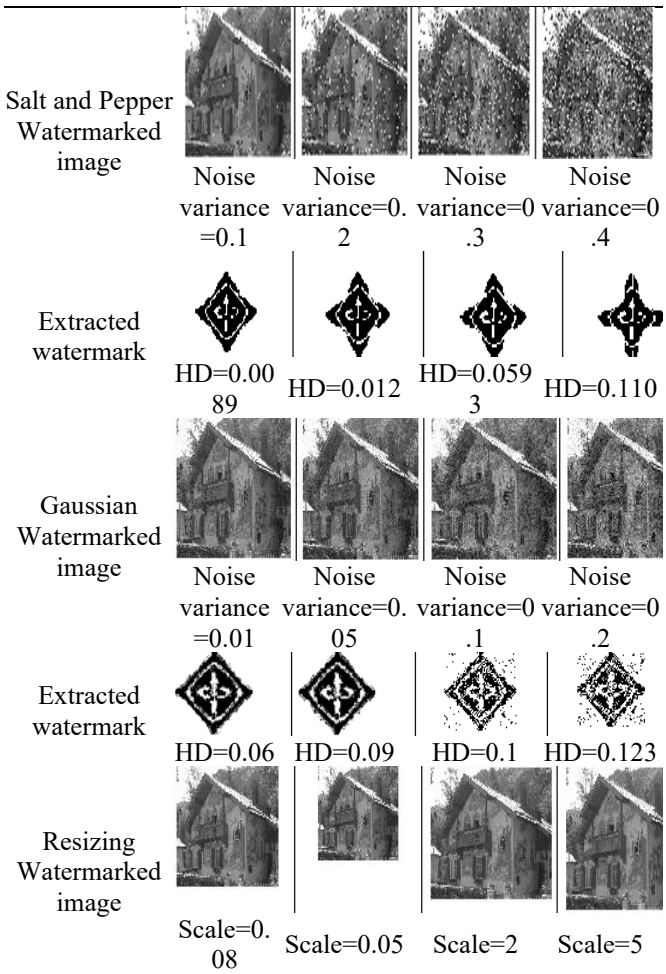
Figure 5. Average PSNR values of the proposed method using various embedding capacities

Figure 5 illustrates the average of PSNR values for the watermarked images of testing dataset and watermark strength α=0.3 across different embedding capacities (5000, 16000, 65000, and 95000). The results show that increasing the embedding capacity leads to an increase in embedding distortion. It is obvious that the highest PSNR value when we embed 5000 bits only.

5.3 Robustness performance

The robustness of the proposed non-blind watermarking methods is assessed against different types of attacks. Specifically, rotation, median filter, cropping, Salt and Pepper, Gaussian, Poisson, Speckle, resizing, and compression. We have calculated the Hamming Distance (HD) of the watermarks for each type of attack for various parameters. During these experiments, the images dataset is decomposed into two levels. Then, the binary logos of size, 40X40, are hiden in the singular values of the HL and LH bands of the second level with watermark strength (α) set to 0.3.

Figure 6 demonstrates the effect of diverse attacks types on watermarked image (kodim24). Additionally, the HD of the extracted watermark (ieee logo) after each attack are calculated. It can be noticed that, the suggested watermarking method is resistant to nine types of attack. As shown in Figure 6 that the watermark can be survived when the values of noice variance is less than 0.2 for Salt and Pepper, Gaussian, Speckle; scale less than 6 for Resizing; angle is less than 60° for Rotation; crop more than 100 pixels for Cropping; more than 50 Quality for Compression. Generally, the watermark can be extracted with a low distortion when the HD is less than 0.2.



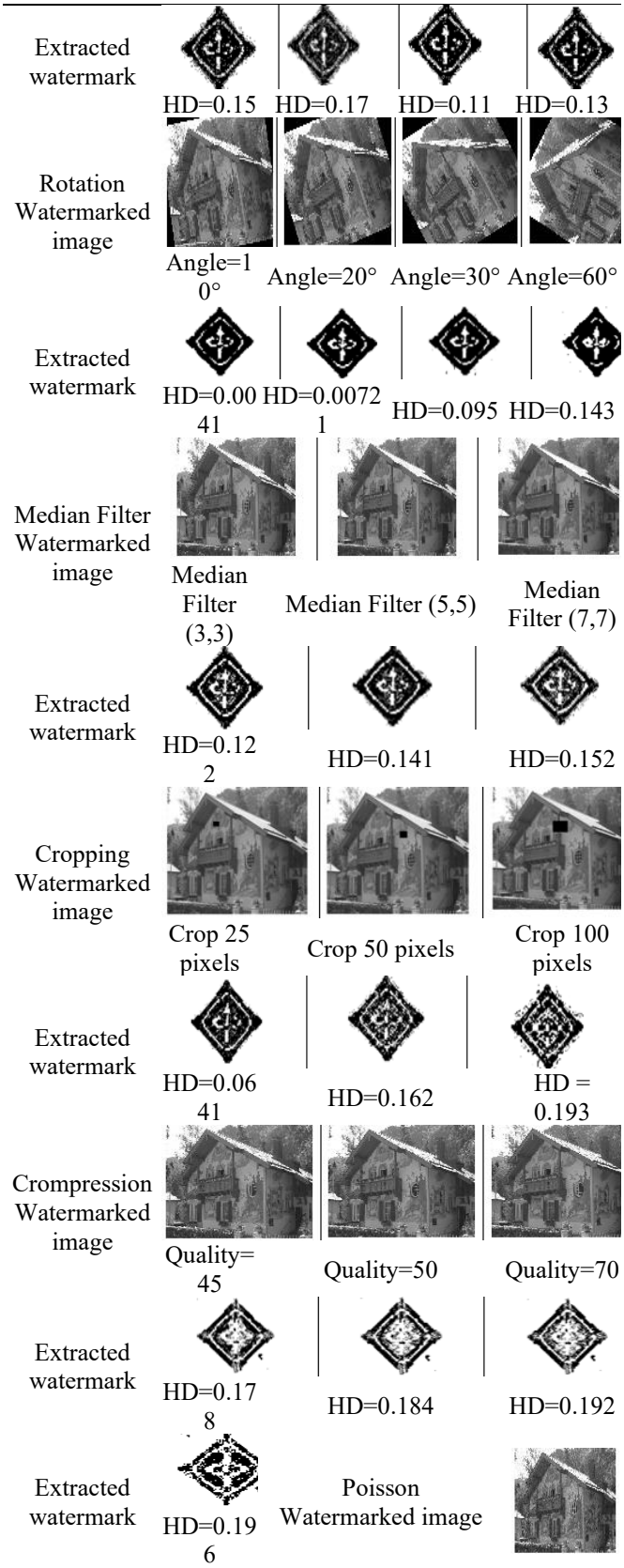


Figure 6. HD of extracted watermark after 9 types of attack

5.4 Comparison with existing methods

In this section, we conduct a comparison between the suggested non-blind watermarking method using MOGA and the existing works: Ali [17] Roy and Pal [18], Chellappan et al. [19], Elbasi et al. [20], and Mood and Konkula [23]. The evaluation is based on embedding distorting and robustness against additive noise. To assess the embedding distortion, we calculate the PSNR of the watermarked images for the suggested approach and the existing works using testing images for the same parameters in the existing methods. We can notice that the proposed method has a low distortion compared to the existing work as shown in Figure 7. This is due to the proposed method taking into consideration two objectives which are related to the distortion and the robustness at the same time.

To compare the suggested approach with the existing works in terms of robustness against 9 types of attack, namely, Salt & Pepper, Gaussian, Speckle, Poisson, Resizing, Rotation, Median filter, cropping and compression using the same parameters. In the first experiment, we have computed the HD of the recovered watermark for the proposed method and Roy and Pal [18] and Chellappan et al. [19] after 4 types of attack, namely, Salt & Pepper, Gaussian, Speckle and Median filter. Figure 8 illustrates that the proposed approach can recover the embedded bits without any distortion in the absence of an attack compared to Roy and Pal [18] and Chellappan et al. [19]. This is due to the proposed extraction process that is a lossless process. This means that we can extract the embedded bits without any distortion in the case of no attack by reversing the embedding process. Additionally, the suggested approach is more robust (less Hamming distance) compared to Roy and Pal [18] and Chellappan et al. [19]. This is mainly due to using a multi objectives instead on one objective.

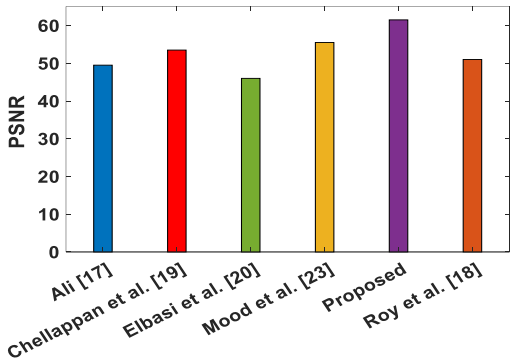


Figure 7. Comparison the suggested approach with the existing works in terms of distortion

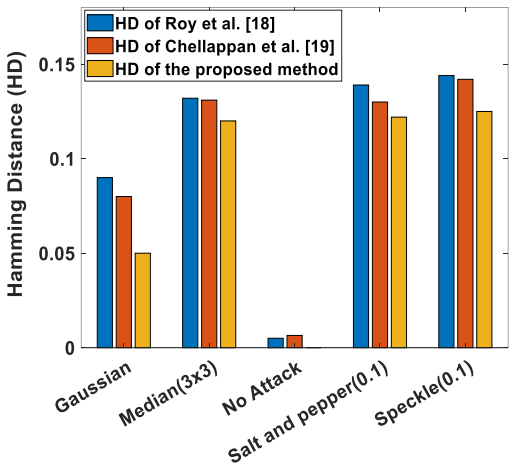


Figure 8. Comparison robustness of the suggested approach with Roy and Pal [18] and Chellappan et al. [19] after 4 types of attack

In the second experiment, the Hamming Distance (HD) of the recovered watermark is calculated for the proposed method and Ali [17] after 7 types of attack, namely, Salt & Pepper, Gaussian, Speckle, Rotation, Median filter, cropping and compression. As illustrated in Figure 9, the suggested approach has less HD value compared to Ali [17], this is mainly due to hiding the bits in the frequency domain.

In the next experiment, we compare the structural similarity index measure (SSIM) of the recovered bits for the proposed method and Mood and Konkula [23] after 5 types of attack, namely, Salt & Pepper, Gaussian, Rotation, Median filter and cropping and compression. Figure 10 illustrates that the proposed approach can recover the embedded bits without any distortion in the absence of an attack compared to Mood and Konkula [23]. This is because the extraction procedure is the reverse of the embbedding procedure. Additionally, the suggested approach is more robust (has high SSIM value) compared to Mood and Konkula [23]. This is mainly due to uing MOGA instead of the traditional GA.

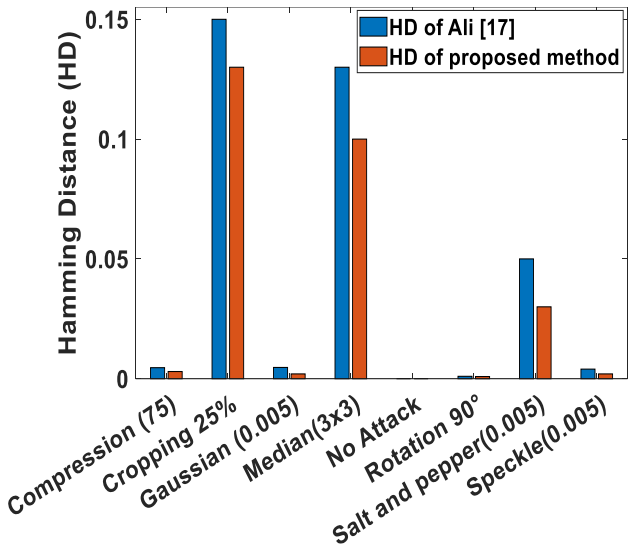


Figure 9. Comparison robustness of the proposed method with Ali [17] after 7 types of attack

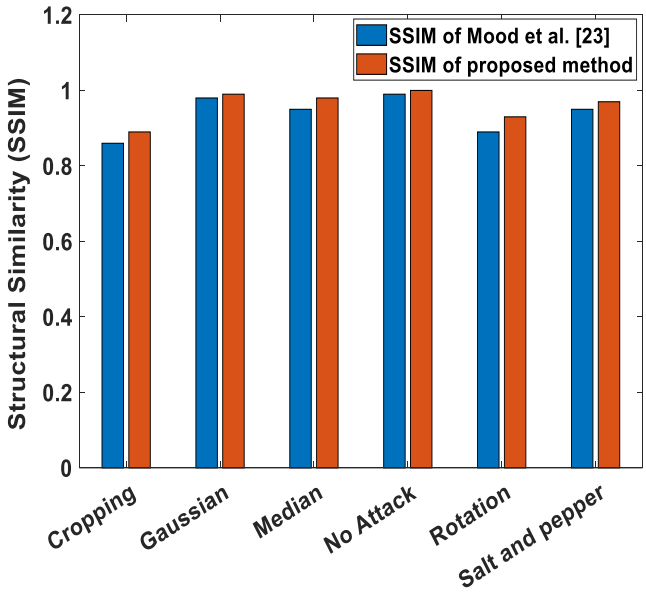


Figure 10. Comparison robustness of the suggested method with Mood and Konkula [23] after 5 types of attack

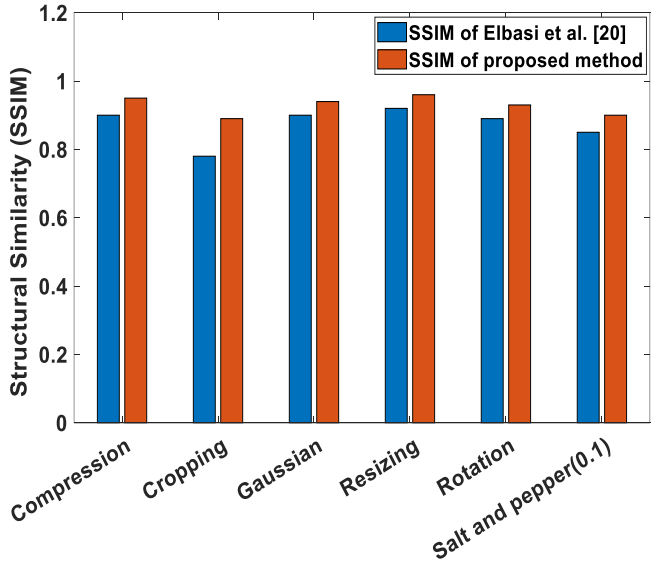


Figure 11. Comparison robustness of the proposed approach with Elbasi et al. [20] after 6 types of attacks

In another experiment, we calculate the SSIM of the recovered watermark for the proposed method and Elbasi et al. [20] after 6 types of attack, namely, Salt & Pepper, Gaussian, Resizing, Rotation, cropping and compression. Figure 11 illustrates that the suggested approach is more resistant to attack compared to Elbasi et al. [20]. This is mainly due to hiding the watermark in the singular values of the DWT coefficients rather than embedding the watermark in the DWT coefficients directly.

6. CONCLUSIONS

This paper introduces a non-blind watermarking approach dealing with the protection of image data. The proposed method employed DWT-SVD and MOGA to identify the optimal coefficients that satisfy the fitness functions conditions. Hamming Distance (HD) and PSNR are utilized as criteria to select the optimal coefficients. The ultimate aim of the proposed method is to minimize error distortion and maximize resistant for different attacks type: Salt & Pepper, Gaussian, Speckle, Poisson, Resizing, Rotation, Median filter, cropping and compression. We evaluate the suggested method in terms of embedding distortion and resistant against several types of attack. Experimental results indicate that the presented approach can be extracted the watermark without any distortion with (HD=0) in the absence of an attack. The embedded bits can be recovered with a low distortion when the HD value is less than 0.2. The proposed method can be improved by using another objectives or adding more objectives. In addition, we can consider another important requirement of the watermarking which is the security of the suggested approach.

REFERENCES

[1] Begum, M., Uddin, M.S. (2020). Digital image watermarking techniques: A review. Information, 11(2): 110. https://doi.org/10.3390/info11020110

[2] Wazirali, R., Alasmary, W., Mahmoud, M.M., Alhindi, A. (2019). An optimized steganography hiding capacity

and imperceptibly using genetic algorithms. IEEE Access, 7: 133496-133508. https://doi.org/10.1109/ACCESS.2019.2941440
[3] Ma, J., Chen, J., Wu, G. (2022). Robust watermarking via multidomain transform over wireless channel: Design and experimental validation. IEEE Access, 10: 92284-92293. https://doi.org/10.1109/ACCESS.2022.3202984
[4] Rajwar, K., Deep, K., Das, S. (2023). An exhaustive review of the metaheuristic algorithms for search and optimization: Taxonomy, applications, and open challenges. Artificial Intelligence Review, 56(11): 13187-13257. https://doi.org/10.1007/s10462-023-10470-y
[5] Melman, A., Evsutin, O. (2023). Image data hiding schemes based on metaheuristic optimization: A review. Artificial Intelligence Review, 56(12): 15375-15447. https://doi.org/10.1007/s10462-023-10537-w
[6] Kushlev, S., Mironov, R.P. (2020). Analysis for watermark in medical image using watermarking with wavelet transform and DCT. In 2020 55th International Scientific Conference on Information, Communication and Energy Systems and Technologies (ICEST), Niš, Serbia, pp. 185-188. https://doi.org/10.1109/ICEST49890.2020.9232700
[7] Mulani, A.O., Shinde, G.N. (2021). An approach for robust digital image watermarking using DWTPCA. Journal of Science & Technology (JST), 6(Special Issue 1), 59-62. https://doi.org/10.46243/jst.2021.v6.i04.pp59-62
[8] Tiwari, A., Srivastava, V.K. (2023). Novel schemes for the improvement of lifting wavelet transform-based image watermarking using Schur decomposition. The Journal of Supercomputing, 79(12): 13142-13179. https://doi.org/10.1007/s11227-023-05167-6
[9] Tavakoli, A., Honjani, Z., Sajedi, H. (2023). Convolutional neural network-based image watermarking using discrete wavelet transform. International Journal of Information Technology, 15(4): 2021-2029. https://doi.org/10.1007/s41870-023-01232-8
[10] Qin, C., Ji, P., Chang, C.C., Dong, J., Sun, X. (2018). Non-uniform watermark sharing based on optimal iterative BTC for image tampering recovery. IEEE MultiMedia, 25(3): 36-48. https://doi.org/10.1109/MMUL.2018.112142509
[11] Wan, W., Zhou, K., Zhang, K., Zhan, Y., Li, J. (2020). JND-guided perceptually color image watermarking in spatial domain. IEEE Access, 8: 164504-164520. https://doi.org/10.1109/ACCESS.2020.3022652
[12] Fotopoulos, V., Skodras, A.N. (2003). Digital image watermarking: An overview. EURASIP Newsletter, 14(4): 10-19.
[13] Kumar, S., Singh, B.K. (2021). Entropy based spatial domain image watermarking and its performance analysis. Multimedia Tools and Applications, 80(6): 9315-9331. https://doi.org/10.1007/s11042-020-09943-x
[14] Devi, H.S., Mohapatra, H. (2023). A novel robust blind medical image watermarking using rank-based DWT. International Journal of Information Technology, 15(4): 1901-1909. https://doi.org/10.1007/s41870-023-01234-6
[15] Abraham, J., Paul, V. (2019). An imperceptible spatial domain color image watermarking scheme. Journal of King Saud University-Computer and Information Sciences, 31(1): 125-133. https://doi.org/10.1016/j.jksuci.2016.12.004
[16] Su, Q., Yuan, Z., Liu, D. (2018). An approximate Schur decomposition-based spatial domain color image watermarking method. IEEE Access, 7: 4358-4370. https://doi.org/10.1109/ACCESS.2018.2888857
[17] Ali, M. (2023). Robust image watermarking in spatial domain utilizing features equivalent to SVD transform. Applied Sciences, 13(10): 6105. https://doi.org/10.3390/app13106105
[18] Roy, S., Pal, A.K. (2019). A hybrid domain color image watermarking based on DWT-SVD. Iranian Journal of Science and Technology, Transactions of Electrical Engineering, 43: 201-217. https://doi.org/10.1007/s40998-018-0109-x
[19] Chellappan, R., Satheeskumaran, S., Venkatesan, C., Saravanan, S. (2021). Discrete stationary wavelet transform and SVD-based digital image watermarking for improved security. International Journal of Computational Science and Engineering, 24(4): 354-362. https://doi.org/10.1504/IJCSE.2021.117016
[20] Elbasi, E., Mostafa, N., Cina, E. (2022). Robust, secure and semi-blind watermarking technique using flexible scaling factor in block-based wavelet algorithm. Electronics, 11(22): 3680. https://doi.org/10.3390/electronics11223680
[21] El Houby, E.M., Yassin, N.I. (2020). Wavelet-Hadamard based blind image watermarking using genetic algorithm and decision tree. Multimedia Tools and Applications, 79(37): 28453-28474. https://doi.org/10.1007/s11042-020-09333-3
[22] Bassel, A., Nordin, M.J., Abdulkareem, M.B. (2017). An improved robust image watermarking scheme based on the singular value decomposition and genetic algorithm. In Advances in Visual Informatics: 5th International Visual Informatics Conference, IVIC 2017, Bangi, Malaysia, Proceedings. Springer International Publishing, 5: 702-713. https://doi.org/10.1007/978-3-319-70010-6_65
[23] Mood, N.N., Konkula, V.S. (2018). A novel image watermarking scheme based on wavelet transform and genetic algorithm. International Journal of Intelligent Engineering and Systems, 11(3): 251-260. https://doi.org/10.22266/ijies2018.0630.27
[24] Meenakshi, K., Vennela, A., Ramya, D., Sameer, S., Sreeja, V., Keerthi, V., (2022). A hybrid watermarking using genetic algorithm. In 2022 2nd Asian Conference on Innovation in Technology (ASIANCON), Ravet, India, pp. 1-5. https://doi.org/10.1109/ASIANCON55314.2022.9909195
[25] Zhu, T., Qu, W., Cao, W. (2022). An optimized image watermarking algorithm based on SVD and IWT. The Journal of Supercomputing, 78(1): 222-237. https://doi.org/10.1007/s11227-021-03886-2
[26] Kumari, R., Mustafi, A. (2022). The spatial frequency domain designated watermarking framework uses linear blind source separation for intelligent visual signal processing. Frontiers in Neurorobotics, 16: 1054481. https://doi.org/10.3389/fnbot.2022.1054481
[27] Sivananthamaitrey, P., Kumar, P.R. (2022). Optimal dual watermarking of color images with SWT and SVD through genetic algorithm. Circuits, Systems, and Signal Processing, 41(1): 224-248. https://doi.org/10.1007/s00034-021-01773-y
[28] Bhowmik, D., Abhayaratne, C. (2019). Embedding

distortion analysis in wavelet-domain watermarking. ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), 15(4): 1-24. https://doi.org/10.1145/3357333

[29] Kumari, R.R., Kumar, V.V., Naidu, K.R. (2021). Optimized dwt based digital image watermarking and extraction using RNN-LSTM. International Journal of Interactive Multimedia & Artificial Intelligence, 7(2): 150-162. https://doi.org/10.9781/ijimai.2021.10.006

[30] Qazzaz, A.A., Kadhim, N. (2023). Watermark based on singular value decomposition. Baghdad Science Journal P-ISSN, 20(5): 2078-8665. https://doi.org/10.21123/bsj.2023.7168

[31] Vaisnavi, K.V., Yaashikaa, P.R. (2023). Discrete wavelet transform based digital image watermarking for satellite image security in comparison with singular value decomposition. AIP Conference Proceedings, 2822(1): 020117. https://doi.org/10.1063/5.0173438

[32] Darwin, C. (2004). On the Origin of Species, 1859. https://lccn.loc.gov/88022464.

[33] Mohammadi, F.G., Amini, M.H., Arabnia, H.R. (2020). Evolutionary computation, optimization, and learning algorithms for data science. In Optimization, Learning, and Control for Interdependent Complex Networks, Springer, Cham, 37-65. https://doi.org/10.1007/978-3-030-34094-0_3

[34] Cicirello, V.A. (2024). Evolutionary computation: Theories, techniques, and applications. Applied Sciences, 14(6): 2542. https://doi.org/10.3390/app14062542

[35] Amini, M., Ahmad, M.O., Swamy, M.N.S. (2016). A robust multibit multiplicative watermark decoder using a vector-based hidden Markov model in wavelet domain. IEEE Transactions on Circuits and Systems for Video Technology, 28(2): 402-413. https://doi.org/10.1109/TCSVT.2016.2607299

[36] Jiao, L., Shang, R., Liu, F., Zhang, W. (2020). Chapter 3-Theoretical basis of natural computation. In Brain and Nature-Inspired Learning Computation and Recognition; Eds, 81-95. https://doi.org/10.1016/B978-0-12-819795-0.00003-7

[37] Yang, X.S. (2020). Nature-inspired optimization algorithms. Academic Press, pp. 197-211. https://dl.acm.org/doi/abs/10.5555/3099753.

[38] Kodak, E. (2013). Kodak lossless true color image suite (PhotoCDPCD0992). https://r0k.us/graphics/kodak/.