Iraqi Journal for Computer Science and Mathematics

Volume 5 | Issue 4 Article 4

2024

Image Watermarking using Firefly Algorithm–IWT-SVD for Copyright Protection

Anjahul Khuluq
Faculty of Information Technology, Universitas Nusa Mandiri, Pasar Minggu Jakarta Selatan, Jakarta, 12540, Indonesia

Ferda Ernawan
Faculty of Information Technology, Universitas Nusa Mandiri, Pasar Minggu Jakarta Selatan, Jakarta, 12540, Indonesia AND Faculty of Computing, Universiti Malaysia Pahang Al-Sultan Abdullah Pekan Pahang, 26600, Malaysia, ferda1902@gmail.com

Agit Amrullah
Faculty of Computer Science, Universitas AMIKOM Yogyakarta, Ring Road Utara Condong Catur Sleman, Yogyakarta, 55283, Indonesia

Mohd Arfian Ismail
Faculty of Computing, Universiti Malaysia Pahang Al-Sultan Abdullah Pekan Pahang, 26600, Malaysia

Recommended Citation

Khuluq, Anjahul; Ernawan, Ferda; Amrullah, Agit; and Ismail, Mohd Arfian (2024) "Image Watermarking using Firefly Algorithm–IWT-SVD for Copyright Protection," *Iraqi Journal for Computer Science and Mathematics*: Vol. 5: Iss. 4, Article 4.
DOI: https://doi.org/10.52866/2788-7421.1202
Available at: https://ijcsm.researchcommons.org/ijcsm/vol5/iss4/4

IRAQI JOURNAL FOR COMPUTER SCIENCE AND MATHEMATICS 2024;5:36–46

RESEARCH ARTICLE

Image Watermarking using Firefly Algorithm–IWT-SVD for Copyright Protection

Anjahul Khuluq [a], **Ferda Ernawan** [a,b,*], **Agit Amrullah** [c], **Mohd Arfian Ismail** [b]

[a] Faculty of Information Technology, Universitas Nusa Mandiri, Pasar Minggu Jakarta Selatan, Jakarta, 12540, Indonesia
[b] Faculty of Computing, Universiti Malaysia Pahang Al-Sultan Abdullah Pekan Pahang, 26600, Malaysia
[c] Faculty of Computer Science, Universitas AMIKOM Yogyakarta, Ring Road Utara Condong Catur Sleman, Yogyakarta, 55283, Indonesia

ABSTRACT

Image watermarking is a technique used to ensure the legitimacy of ownership by safeguarding images. This research presented the Firefly algorithm–IWT-SVD to enhance resistance and robustness performance against different type of attacks. The cover image is split into blocks of 4×4 pixels, and each block is then computed by IWT-SVD. The Firefly algorithm is used to determine the appropriate scaling factor to incorporate the watermark using a predefined set of principles. The watermarked images have been evaluated under various attacks such as noise addition, filtered image, compressed image and scaled image. The experimental results demonstrate exceptional imperceptibility, with an average PSNR value of 39.8489 dB and a SSIM value of 0.9993. The proposed scheme achieved a strong robustness performance, with an average NC value of 0.92.

Keywords: Watermarking, Copyright protection, Firefly Optimization, Integer Wavelet Transform, Singular Value Decomposition

1. Introduction

In this ever-complex digital era, the distribution and usage of images through digital platforms has become highly commonplace. Nevertheless, this phenomenon also gives rise to innovative challenges, such as copyright violation and unapproved alteration of digital images. Consequently, watermarking techniques have been devised as a remedy to safeguard copyright and preserve the authenticity of digital images [1]. This approach for adding watermarks to images can be performed in both the spatial domain and the frequency domain.

Watermarking is a security measure commonly employed on digital data, such as images, video, music, to identify and safeguard the original information from unauthorized utilization [2]. Utilizing digital watermarking can establish unequivocal verification of an image's validity and legally substantiate ownership of the image. Image watermarking methods can be categorized into two distinct groups: spatial domain methods and transformation domain approaches.

Watermarks are embedded directly into the pixels of an image in the spatial domain. Using this method has the advantage of being computationally efficient and straightforward to execute [3]. This method can achieve a high level of imperceptibility, but it is vulnerable to JPEG compression and noise attacks [4]. Domain transformation-based image watermarking exhibits robustness against several types of attacks and widely employed in image watermarking systems include DWT [5, 6], DCT [7, 8], and IWT [9, 10]. Transformation domain methods offer several advantages, such as the ability to withstand compression and reinsertion attacks. This is achieved by distributing the watermark over the image using transformation coefficients. Nevertheless,

Received 17 December 2023; accepted 25 March 2024.
Available online 25 November 2024

* Corresponding author.
E-mail address: ferda@umpsa.edu.my, ferda1902@gmail.com (F. Ernawan).

https://doi.org/10.52866/2788-7421.1202

the implementation of these approaches can be more intricate and necessitate greater computational processing in contrast to spatial domain methods [11].

The IWT conduct employs integer operations, rendering it particularly well-suited for hardware implementations that prioritise computational efficiency. DWT, in addition, partitions the signal into low and high frequency constituents by the utilisation of low-pass and high-pass filters, commonly employed in image processing and data compression. Meanwhile, Discrete Cosine Transform (DCT), which employs the cosine transformation to convert data into the frequency domain, is the primary method used for data compression, particularly in formats like JPEG for images. The three components play a vital role in data processing, although IWT outperforms the others in systems with limited hardware resources and a need for efficient arithmetic operations [10].

The importance of robustness in watermarking systems for digital images relies on its ability to withstand numerous challenges and threats that can potentially compromise the effectiveness of watermarking in safeguarding copyright and image integrity. Watermarked images in intricate and ever-changing digital settings are frequently susceptible to alterations and assaults, including compression, filtration, cropping, or other forms of modification. Consequently, possessing a high level of robustness entails the ability to precisely identify and restore the watermark, even in the face of alterations or attacks. A reliable watermarking technique will ensure the protection of image copyright and concealed information [12], thereby minimizing the probability of copyright violation and verifying the truthfulness of images in a time when image distribution and reproduction are becoming more effortless and commonplace.

The watermarking approach employed is a composite of multiple methods in order to enhance resilience against attacks. The integration of the watermarking technique with SVD and the application of the firefly algorithm yielded favorable outcomes in terms of imperceptibility and resilience [9]. This study aimed to enhance the resilience against sophisticated cyber-attacks through the development of advanced techniques.

This study proposes an image watermarking technique that utilises the IWT and enhances amount of embedding by applying the Firefly algorithm. The purpose of this approach is to improve the resistance and robustness of the watermark against various kinds of attacks. The proposed method involves embedding a watermark in 4×4 pixel blocks using a watermarking methodology. The optimum scaling factor for including the watermark is determined using the Firefly algorithm method, which follows a specified set of principles. This approach results in a watermarked image that is more robust against various forms of attacks.

2. Existing watermarking schemes

Mishra et al [13] devised a gray-scale image watermarking method that utilises the Firefly algorithm to ascertain the optimal scale factor for embedding the watermark image. The trials employed six images containing a watermark measuring 32×32 pixels. The technique employed Discrete Wavelet Transform-Singular Value Decomposition (DWT-SVD), and the outcomes demonstrate a commendable level of imperceptibility and robustness. This research exhibits some limitations, including the aspect of durability, which can yet be enhanced. The absence of robustness in the DWT approach renders it vulnerable to several forms of attacks. Hence, it is imperative to conduct additional research including diverse forms of attacks to enhance the resilience against a wide range of attacks on images that have been embedded with watermarks.

Guo et al. [9] devised a blind image watermarking scheme through the implementation of the Firefly algorithm, DWT, and QR decomposition to ascertain the optimal scale factor for each watermark image. The experimental outcomes demonstrate that the scheme not only satisfies the requirement for invisibility but also exhibits significantly superior resistance compared to watermarking methods evaluated in other investigations [14–16]. The study done by Guo et al [9] specifically examined the degree to which implanted images may be detected by the human eye. Nevertheless, the research's robustness can be enhanced by improving the computations generated by DWT. Hence, additional investigation is required to enhance the resilience of images including watermarks against diverse forms of attacks.

Luo et al. [12] presented a watermarking based on IWT-SVD, operating on a dual scale. This approach utilises the IWT to partition the image into sub-blocks of varying resolutions. It then employs the SVD to derive a matrix of singular values from these sub-blocks. By integrating these two methodologies, this approach is capable of securely embedding and identifying watermarks. The performance evaluation demonstrates that this approach exhibits excellent imperceptibility, meaning that the watermark is undetectable to the human eye, as well as great resilience against attacks such as image compression and cropping. Therefore, this technology has extensive potential for use in ensuring and safeguarding the genuineness of images in digital contexts.

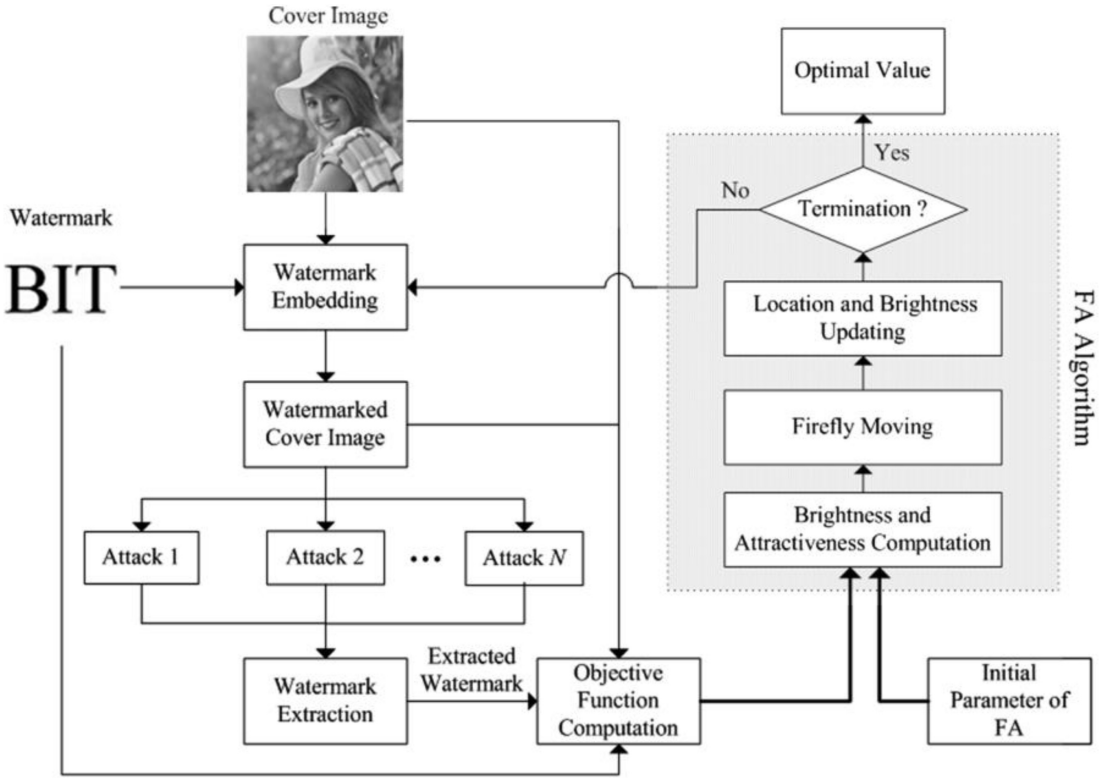

Fig. 1. Flow chat of FA-based watermarking method in DWT-QR transform domain [9].

An efficient method for preserving image integrity and authenticity was developed by Ernawan & Ariatmanto [4] by combining IWT-based watermarking techniques with SVD with pixel variance. This technique employs the capacity of integer waveform transformation to acquire a frequency domain depiction of the image, enabling the incorporation of a watermark that possesses robustness and resilience against attacks. Moreover, employing SVD in conjunction with variance pixels enables accurate identification and elimination of watermarks, all the while preserving the visual integrity of the resultant image. When used together, these strategies provide an efficient solution for guaranteeing genuineness and safeguarding visual material against unauthorized alteration.

2.1. Singular value decomposition

The singular value decomposition calculates each block matrix of IWT transform. The SVD can be defined by [17]:

$$\mathrm{SVD(H)} = U_h S_h V_h \tag{1}$$

The rectangular matrix A with $n_1 \times m_1$ dimension obtains output the transpose matrices of the diagonal symmetric matrices U, S, and V. U represents the right orthogonal matrix of size $n_1 \times m_1$. While S represents a non-negative real integer in size $n_1 \times m_1$, and V represents a matrix in size $n_1 \times m_1$ as a left orthogonal matrix. In this study, the embedding procedure is conducted by investigating S values.

2.2. Firefly algorithm

The detailed procedure of FA-based watermarking method in IWT-QR transform domain are shown in Fig. 1:

Step 1: Initialise the basic parameters of FA and generate randomly the locations $\lambda i (i = 1, 2, \ldots, n)$ of fireflies $i = 1, 2, \ldots, n$.

Step 2: The following processes are carried out for each firefly i's position λi:

i. The watermarked cover image Xw can be obtained using the cover image X and watermark embedding strength λi, in accordance with the watermarking embedding technique depicted in Fig. 2.

ii. Use N distinct attacks on the watermarked cover image, in that order.

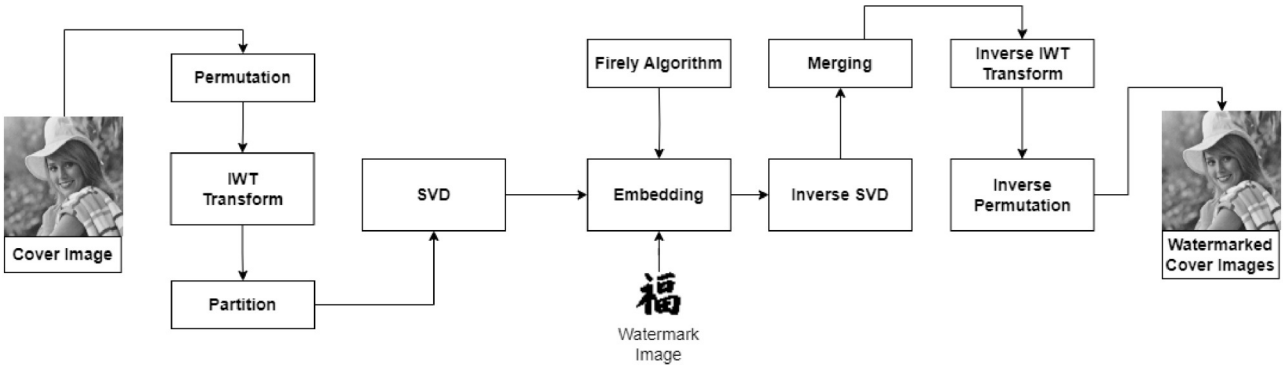

Fig. 2. Proposed embedding watermark.

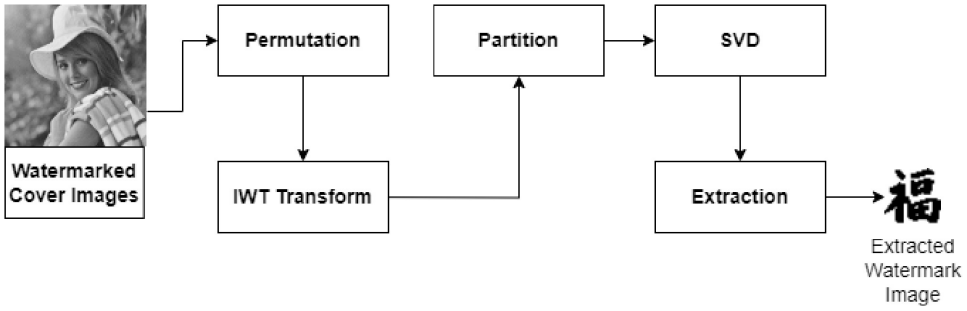

Fig. 3. Proposed extracting watermark.

Using the watermark extraction process depicted in Fig. 3.

iii. Calculate BER(w,wi') and SSIM(X,Xw) using the information from steps i and ii. Using the following formula, get each λi's objective function value:

iv. Using the following formula, get each λi's objective function value:

$$f(\lambda i) = [1 - \mathrm{SSIM}(X, Xw)] + 30 \times 1N\Sigma i = 1N\mathrm{BER}(w, wi') \quad (2)$$

Step 3: Update the location of each firefly according to (3).

Step 4: Repeat steps 2 and 3 until the maximum iteration T is reached.

2.3. Permutation

In the permutation stage, Arnold cat map is used to scramble the cover image. After that, the image is encrypted from bottom to top and left to right. Nevertheless, the encryption algorithms are ineffective if these images have different sizes. The method suggested in [18] splits each image into eight bitplanes and then applies bit-level permutation operations to each bitplane, changing both the position and the values of pixels simultaneously. However, it takes a long time to generate permutation coordinates for every bitplane. The Arnold transform is defined by:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} mod\ N \quad (3)$$

where x', y' represent the vector position after shifting, x, y are the original vector position. The permutation is performed with a secret key to encrypt the cover image. Without the secret key, the unauthorized persons are not able to extract the embedded watermark.

3. Watermarking scheme

3.1. Proposed embedding

This research uses IWT with Daubechies (DB4) wavelet. The incorporation of IWT with DB4 wavelet aims to amplify image quality post watermark embedding for imperceptibility and fortify the resilience for robustness against attacks on watermarked images. The watermark embedding process is visually depicted in Fig. 2.

The embedding watermark is given by:

Step 1: The process begins by computing a cover image by using permutation with a secret key.
Step 2: Perform IWT to the permutation results and decompose it into non overlapping blocks.
Step 3: Divide the sub bands of the IWT on the LL sub-band into non-overlapping blocks. Each block has a dimension of 4 × 4 pixels.
Step 4: Apply Singular Value Decomposition (SVD) to divide into the matrix through three distinct matrices: the left singular matrix (U), the value singular matrix (S), and the right singular matrix (V).
Step 5: The embedding watermark can be performed by the subsequent formula:

$$SS(i,i) = S(i,i) + \text{lambda}^{*}Sw(i,i);$$

where lambda is embedding strength obtained from Firefly algorithm.
Step 6: Compute inverse SVD.
Step 7: Merge all these watermarked blocks together, then computed by inverse IWT.
Step 8: Compute inverse permutation to obtain the watermarked image with a secret key.

The firefly algorithm is used to prescribe the amount of embedded watermarks. To find the ideal amount of embedding watermark, the Firefly Algorithm (FA) is employed in the watermarking system. The watermark is encoded into binary values using this approach. A fitness function that assesses the watermarked image's quality is defined. A random generator creates a population of fireflies, each of which represents a possible solution with a particular degree of embedding. Local and global exploration of the watermarked area is made possible by these fireflies. The technique iteratively optimizes until it finds a solution that maximizes fitness, suggesting the ideal watermark embedding quantity to achieve a compromise between resilience and imperceptibility. This method allows for dynamic embedding amounts, allowing the performance of the watermark to be customized to match unique needs.

The Firefly algorithm optimizes the trade-off between resilience and imperceptibility to find the scaling factor for watermark embedding. The objective function assesses the watermarked image's quality by taking into account its resistance to attacks and other criteria. Within the search space, fireflies are randomly initialized, each of them indicating a potential scaling factor. The method moves across the solution space iteratively, both locally and globally. Finally, the scaling factor corresponding to the firefly with the highest fitness value is extracted, offering the best compromise between the robustness and watermark imperceptibility.

3.2. Proposed extracting

The watermark extraction technique involves extracting the embedded watermark logo from the host image in order to compare it with the original watermark logo. The procedure of extracting the watermark is depicted in Fig. 3.

The extracting watermark is defined by:

Step 1: The watermarked image is computed by permutation with a secret key.
Step 2: Apply one level of IWT to a random image to obtain four sub-bands.
Step 3: Choose LL sub-band to be divided into 4 × 4 pixels.
Step 4: Perform SVD to the LL sub-band.
Step 5: Use the singular value to extract the watermark with the equation as follows:

$$w(i,i) = \left(Sb(i,i) - S(i,i)\right)/\text{lambda}$$

where lambda is embedding strength obtained from Firefly algorithm.
Step 6: Generate the extracted watermark.

3.3. Imperceptibility and robustness evaluation

The PSNR is a metric that is used to assess the quality and perceived clarity of a digital image [19]. A higher PSNR value indicates superior image quality. PSNR is a metric used to assess image quality, can be utilized to compare the results of image compression, measure the loss of information during processing, and evaluate the quality of images in different applications like image processing, video processing, or image watermarking. PSNR, a regularly employed technique [20], is determined by comparing the original and processed images. The formula for calculating PSNR is given by:

$$PSNR = 10\,log_{10}\frac{S^2}{\frac{1}{M-N}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}(cv(x,y) - wr(x,y))} \quad (4)$$

where S represents the maximum intensity value of 255 on an 8-bit image, cv is the cover image, and wr is the watermarked or recovered image. The SSIM functions as a metric for measuring the structural similarity between two images. SSIM offers a more intricate measurement than basic metrics like PSNR,

as it not only considers differences in pixel intensity but also factors in spatial structure and texture discrepancies within the image. SSIM quantifies the structural likeness between two images by accounting for three primary components: luminance, contrast, and structure [21]. The SSIM value ranges between 0 and 1, where a value of 1 indicates perfect structural similarity between two images. A higher SSIM value signifies a closer match in the structure and texture of the two images. The general formula for calculating SSIM is given by:

$$SSIM(p,q) = \frac{2\mu_p\mu_q + C_1}{\mu_p^2 + \mu_q^2 + C_1} \cdot \frac{2\sigma_p\sigma_q + C_2}{\sigma_p^2 + \sigma_q^2 + C_2} \cdot \frac{\sigma_{pq} + C_3}{\sigma_p\sigma_q + C_3} \tag{5}$$

where the division of a weak denominator is stabilized by the numerical constants C_1, C_2, and C_3. SSIM examines the local image structure of two images in tiny windows. An overall SSIM score is calculated by summing the parameters of brightness, contrast, and window structure similarity between the two images. NC is a measurement utilized to gauge the degree of similarity between two images [22]. This metric calculates the correlation between two-pixel vectors, represented as feature vectors from the two images being compared. During the NC calculation, both the reference image's feature vector and the tested image's feature vector are normalized beforehand. This normalization step accounts for variations in brightness and contrast between the two images. The NC value varies between 0 to 1, with a score of 1 indicating a complete positive correlation between two images, a value of 0 indicating no correlation. NC is frequently utilized in image processing to evaluate the likeness between a reference image and a tested image [22]. The NC calculation is defined by:

$$NC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} W(i,j) \cdot W \cdot (i,j)}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N} W(i,j)^2 \sum_{i=1}^{}\sum_{j=1}^{} W \cdot (i,j)^2}} \tag{6}$$

where $W \cdot (i,j)$ is the extracted watermark and $W(i,j)$ is the original watermark. BER is a measurement utilized to assess the level of bit inaccuracies within an image or digital signal [22]. This metric computes the proportion between the count of incorrect bits and the total count of bits present in the image. Every bit in the image is scrutinized to ascertain whether its value matches the corresponding bit in the reference image. Any disparity between the scrutinized bit and the reference bit is classified as an error. This methodology is considered resilient against attacks when the BER value equals 0, thus indicating that a lower BER value corresponds to enhanced performance [22]. The BER calculation is defined by:

$$BER = \sum_{i=1}^{M}\sum_{j=1}^{N} \frac{W(i,j) \times W'(i,j)}{M \times N} \tag{7}$$

where $W(i,j)$ represents the extracted watermark and $W(i,j)$ denotes the original watermark. M and N denote the row and column size.

4. Experimental results

This study experiment utilized eight grayscale images as hosts images, each having dimensions of 512×512 pixels. A binary image with the size of 32×32 pixel was utilized for the watermark logo. Fig. 4 displays the images of the host and the watermark logo that were used in the present study.

Imperceptibility is one of the parameters to measure the invisibility performance of the embedding watermark into host image. An image that has been watermarked and resembles the original host image more closely is said to have increased imperceptibility. The invisibility of the watermarked image is quantified by PSNR and SSIM evaluation. The results of the imperceptibility performance experiment are provided in Table 1.

According to Table 1, The "House" image achieved the greatest PSNR value of 39.8837, based on the analysis of many images using the PSNR measurement. Conversely, the "Cameraman" image has the lowest PSNR value of 39.7781. Although its PSNR score is still very high, compared with other image shows that "Cameraman" suffers from slightly greater distortion than other images in the dataset. A lower PSNR value may suggest a greater disparity between the processed image and the source image. Nevertheless, the PSNR values for all images remain

Table 1. Evaluation of PSNR and SSIM.

Image	PSNR	SSIM
Lena	39.8614	0.9993
Elaine	39.8568	0.9993
Cameraman	39.7781	0.9991
Barbara	39.8557	0.9994
House	39.8837	0.9992
Peppers	39.8381	0.9993
Airplane	39.8802	0.9993
Mandril	39.8375	0.9994
Average	39.8489	0.9993

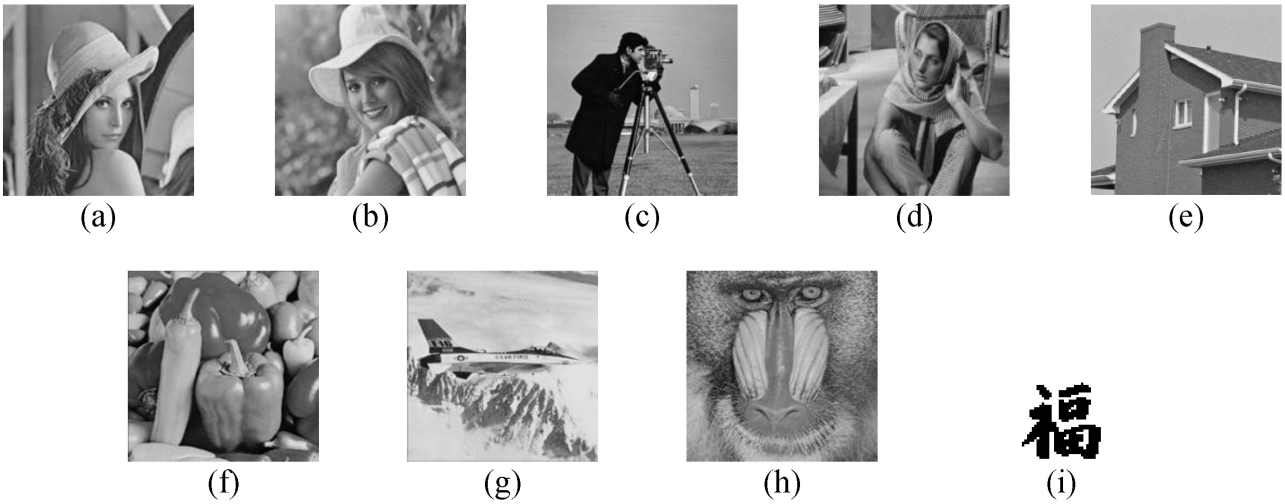

Fig. 4. Host images: (a) Lena, (b) Elaine, (c) Cameraman, (d) Barbara, (e) House, (f) Peppers, (g) Airline, (h) Mandrill, (i) Watermark.

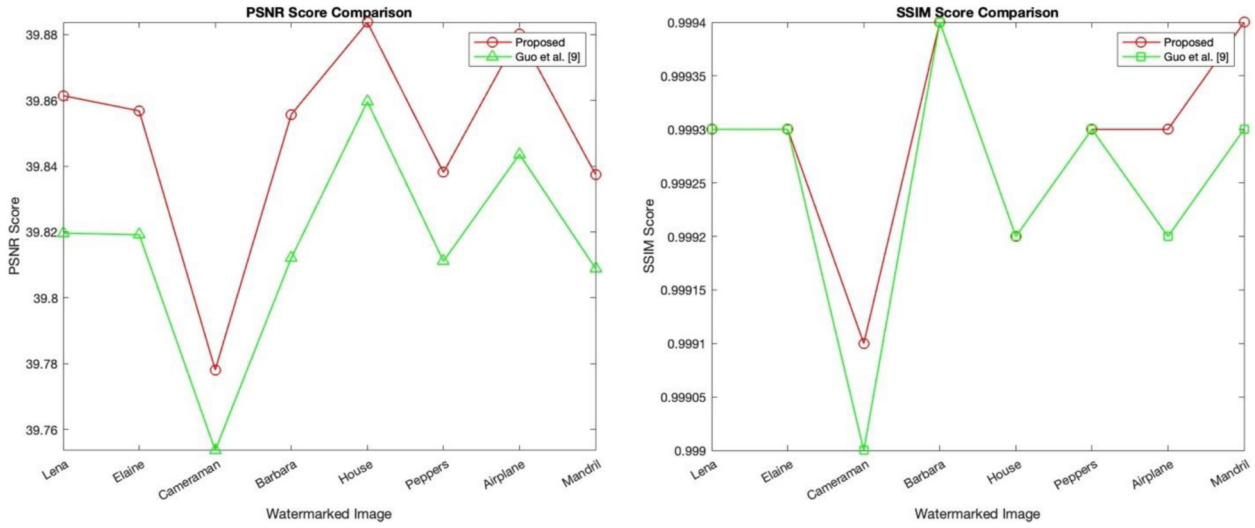

Fig. 5. Comparison of PSNR and SSIM values with the existing benchmark.

exceedingly high, signifying excellent image quality and minimal overall distortion in our examination.

Fig. 5 illustrates curves that compare PSNR and SSIM values for different images. This graphic representation emphasized the importance of imperceptibility, which refers to the quality of the host image after inserting a watermark using the IWT approach. Additionally, it presents a graphical representation that compares the SSIM outcomes. Assessing the resilience of image watermarking technologies is crucial. This involves embedding watermarks into each host image and evaluating the outcomes under various assault scenarios. The findings of the studies are displayed in Table 1, which showcases various instances of detection outcomes on the 8 host images after undergoing attacks. The presence of a delicate watermark is clearly capable of exposing the specific regions that have been altered in images that suffered attacks.

The approach preserves confidential data or watermarks on images that suffered several forms of attacks. The findings of the watermark extraction analysis will offer an in-depth knowledge of the effectiveness and superiority of the suggested approach in preserving the true origin and integrity of images. Additionally, it will reveal the method's behavior in different image attack scenarios. Hence, the outcomes of watermark extraction hold significance in assessing and contrasting the effectiveness of the suggested approach within the domain of image processing and the implementation of watermarking techniques.

The extracted watermark under various attacks has been shown in Table 2. The proposed scheme still can achieve high visual quality of the extracted

Table 2. The visual attacked image and extracted watermark image.

	JPG with quality factor 20		Poison		median filter with window size 4 × 4		speckle noise with variance 0.001		Gaussian noise with mean zero and standard deviation 0.02		scaling 0.5	
	Attacked images	Watermark image	Attacked images	Watermark image	Attacked images	Watermark image	Attacked images	Watermark image	Attacked images	Watermark image	Attacked images	Watermark image
Lena												
Elaine												
Cameraman												
Barbara												
House												
Peppers												
Airplane												
Mandril												

Table 3. Evaluation of Normalized Correlation (NC) Lena, Elaine, Cameraman, dan Barbara.

	House		Peppers		Airplane		Mandril	
Attack index	[9]	Proposed	[9]	Proposed	[9]	Proposed	[9]	Proposed
Scaling 0.5	0.9802	0.9974	0.9710	0.9981	0.9139	0.9840	0.8796	0.9914
Gaussian noise with mean zero and Standard deviation 0.02	0.6640	0.8608	0.6172	0.7777	0.5953	0.6525	0.6573	0.7945
Salt and pepper noise with noise density 0.05	0.5723	0.6952	0.5341	0.6378	0.5574	0.6083	0.6095	0.6744
Speckle noise with variance 0.001	1.0000	1.0000	1.0000	1.0000	0.9999	0.9999	1.0000	1.0000
Median filter with window size 4 × 4	0.9260	0.9596	0.9364	0.9782	0.8312	0.9199	0.8024	0.9385
Poison	0.9342	0.9962	0.9198	0.9934	0.9564	0.9957	0.9730	0.9967
JPG with quality factor 20	0.9960	0.9965	0.9976	0.9961	0.9973	0.9972	0.9982	0.9967
Average	0.8645	0.9126	0.8527	0.8977	0.8420	0.8762	0.8483	0.9009

Table 4. Evaluation of Normalized Correlation (NC) House, Peppers, Airplane dan Mandril.

	House		Peppers		Airplane		Mandril	
Attack index	[9]	Proposed	[9]	Proposed	[9]	Proposed	[9]	Proposed
Scaling 0.5	0.9772	0.9963	0.9630	0.9970	0.9421	0.9917	0.8748	0.9791
Gaussian noise with mean zero and Standard deviation 0.02	0.6193	0.8002	0.6396	0.7933	0.5703	0.7040	0.7393	0.9244
Salt and pepper noise with noise density 0.05	0.5476	0.6044	0.5620	0.6190	0.3907	0.2478	0.6652	0.8086
Speckle noise with variance 0.001	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
Median filter with window size 4 × 4	0.9378	0.9723	0.9379	0.9769	0.9099	0.9657	0.7558	0.8831
Poison	0.8859	0.9901	0.9472	0.9955	0.9276	0.9936	0.9839	0.9975
JPG with quality factor 20	0.9984	0.9915	0.9982	0.9958	0.9975	0.9933	0.9967	0.9976
Average	0.8527	0.8959	0.8619	0.8986	0.8225	0.8404	0.8592	0.9233

watermark. The extracted watermark has small distortion especially under JPEF with quality factor of 20. In the experiments, the proposed scheme also was tested under Gaussian noise with density of 0.02, the watermarked image was destroyed with a huge addition noise, while it still can visually recognize the extracted watermark.

The results of the Normalized Correlation (NC) evaluation on the eight images can be found in Table 3 and Table 4, while the Bit Error Rate (BER) evaluation results are in Table 5 and Table 6.

IWT-SVD allows for more efficient computation and storage. For large-scale optimization problems, this can result in reduced computation and faster evaluation. The Firefly algorithm has the potential to yield better robustness performance by more accurately selecting the ideal scaling factor. The study's findings show that the suggested approach performs better than the alternative techniques for almost all attack kinds and image combinations. It is evident from the average NC value of each image that the proposed method has a greater value compared to the method described in reference [9]. The research findings consistently provide superior BER values than the alternative method. Among the ten types of attacks that were examined, the proposed technique exhibited a lower BER value in comparison to the method described in reference [9]. This suggests a higher degree of accuracy. The decrease in the BER value, indicating a lower value, demonstrates the enhanced efficiency of the suggested strategy in preserving image integrity, even in the presence of

Table 5. Evaluation of Bit Error Rate (BER) Lena, Elaine, Cameraman, dan Barbara.

	House		Peppers		Airplane		Mandril	
Attack index	[9]	Proposed	[9]	Proposed	[9]	Proposed	[9]	Proposed
Scaling 0.5	0.2094	0.1584	0.2104	0.2005	0.2495	0.2068	0.2569	0.1981
Gaussian noise with mean zero and Standard deviation 0.02	0.3891	0.3005	0.4160	0.3235	0.4585	0.4337	0.4019	0.3612
Salt and pepper noise with noise density 0.05	0.4584	0.4175	0.4782	0.4286	0.4704	0.4544	0.4433	0.4283
Speckle noise with variance 0.001	0.1582	0.1792	0.1296	0.1030	0.2905	0.2860	0.1553	0.1587
Median filter with window size 4 × 4	0.2412	0.2239	0.2358	0.2131	0.2675	0.2081	0.2862	0.2029
Poison	0.2352	0.2059	0.2470	0.2091	0.2331	0.2709	0.2160	0.1858
JPG with quality factor 20	0.1935	0.1191	0.1752	0.1143	0.2292	0.0991	0.2036	0.0928
Average	0.2693	0.2406	0.2680	0.2319	0.3168	0.2893	0.2768	0.2398

Table 6. Evaluation of Bit Error Rate (BER) House, Peppers, Airplane dan Mandril.

	House		Peppers		Airplane		Mandril	
Attack index	[9]	Proposed	[9]	Proposed	[9]	Proposed	[9]	Proposed
Scaling 0.5	0.2070	0.1579	0.2168	0.1777	0.2328	0.2123	0.2586	0.2051
Gaussian noise with mean zero and Standard deviation 0.02	0.4173	0.3012	0.4143	0.3627	0.4372	0.3376	0.3382	0.2622
Salt and pepper noise with noise density 0.05	0.4667	0.4318	0.4734	0.4513	0.5538	0.6341	0.3915	0.3610
Speckle noise with variance 0.001	0.1159	0.1205	0.2119	0.1778	0.0599	0.0754	0.0843	0.1023
Median filter with window size 4×4	0.2136	0.1779	0.2197	0.1813	0.2344	0.1852	0.3015	0.2093
Poison	0.2578	0.2137	0.2328	0.2066	0.2381	0.1884	0.1996	0.1991
JPG with quality factor 20	0.1258	0.0803	0.2335	0.1095	0.1635	0.1432	0.2220	0.1909
Average	0.2556	0.2206	0.2882	0.2471	0.2671	0.2526	0.2502	0.2224

attacks on diverse images. This demonstrates that the suggested approach exhibits superior resilience against many forms of attacks and is dependable in the realm of image processing for preserving optimal image quality.

5. Conclusion

In this study, a new optimized image watermarking method based on Firefly algorithm in the IWT-SVD domain has been proposed. The firefly algorithm has been used to prescribe the amount of embedding watermark. The method's imperceptibility and robustness were assessed by a simulated experiment including eight images measuring 512×512 pixels, each containing a watermark measuring 32×32 pixels. Subsequently, eight different types of assaults were conducted on each image with the inserted watermark. The results indicate that the PSNR achieves a high value for every cover image, with an average PSNR of 39.8489. The proposed method has successfully attained an exceptionally high SSIM value of around 0.9993. This value signifies that the watermarked images exhibit virtually imperceptible disparities to the human eye when compared to the original image. The research findings consistently provide superior BER values for the proposed method compared to the existing method. Among the 10 types of assaults that were examined, the suggested technique had a lower BER value compared to the existing schemes. The proposed method exhibits enhanced resilience against several forms of attacks and demonstrates a high level of dependability in image processing, hence ensuring superior image quality preservation.

Acknowledgement

This work was supported by the Ministry of Higher Education for providing financial support under Fundamental Research Grant Scheme (FRGS), No. FRGS/1/2022/ICT04/UMP/02/2 (University reference RDU220133).

Funding

Ministry of Higher Education.

Conflicts of interest

The author declares no conflict of interest.

References

1. F. Ernawan and D. Ariatmanto, "A recent survey on image watermarking using scaling factor techniques for copyright protection," *Multimed Tools Appl.*, vol. 82, pp. 27123–27163, 2023. doi: 10.1007/s11042-023-14447-5.
2. F. Ernawan, "Tchebichef image watermarking along the edge using YCoCg-R color space for copyright protection," *International Journal of Electrical and Computer Engineering*, vol. 9, no. 3, pp. 1850–1860, 2019.
3. M. Khalili, "DCT-Arnold chaotic based watermarking using JPEG-YCbCr," *Optik (Stuttg)*, vol. 126, no. 23, pp. 4367–4371, 2015. doi: 10.1016/j.ijleo.2015.08.042.
4. F. Ernawan and D. Ariatmanto, "Image watermarking based on integer wavelet transform-singular value decomposition with variance pixels," *International Journal of Electrical and Computer Engineering*, vol. 9, no. 3, pp. 2185–2195, 2019. doi: 10.11591/ijece.v9i3.pp2185-2195.
5. P. Khare and V. K. Srivastava, "A novel dual image watermarking technique using homomorphic transform and DWT," *Journal of Intelligent Systems*, vol. 30, no. 1, 2021. doi: 10.1515/jisys-2019-0046.
6. A. Alzahrani, "Enhanced invisibility and robustness of digital image watermarking based on DWT-SVD," *Appl Bionics Biomech*, vol. 2022, 2022. doi: 10.1155/2022/5271600.
7. N. B. Zhu and J. G. Li, "A DCT-based robust watermarking using genetic algorithms," *Journal of Hunan University Natural Sciences*, vol. 38, no. 4, 2011.
8. S. P. Singh and G. Bhatnagar, "A new robust watermarking system in integer DCT domain," *J Vis Commun Image Represent*, vol. 53, 2018. doi: 10.1016/j.jvcir.2018.03.006.
9. 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, 2017. doi: 10.1049/iet-ipr.2016.0515.
10. K. R. Chetan and S. Nirmala, "An efficient and secure robust watermarking scheme for document images using Integer wavelets and block coding of binary watermarks," *Journal of Information Security and Applications*, vol. 24–25, 2015. doi: 10.1016/j.jisa.2015.07.002.
11. R. Ismail and S. M. Ali, "Design of quality improvement technique through ridgelet transform on watermarked video", *Iraqi Journal for Computer Science and Mathematics*, vol. 4, no. 1, pp. 204–210, 2023.
12. H. A. Salman and A. Kalakech, "Image enhancement using convolution neural networks," *Babylonian Journal of Machine Learning*, 30–47, 2024. doi: 10.58496/BJML/2024/003.
13. A. Mishra, C. Agarwal, A. Sharma and P. Bedi, "Optimized gray-scale image watermarking using DWT-SVD and Firefly Algorithm," *Expert Syst Appl*, vol. 41, no. 17, pp. 7858–7867, 2014. doi: 10.1016/j.eswa.2014.06.011.
14. M. Ali and C. W. Ahn, "Comments on 'optimized gray-scale image watermarking using DWT-SVD and Firefly Algorithm," *Expert Syst Appl*, vol. 42, no. 5, 2015. doi: 10.1016/j.eswa.2014.10.045.
15. M. Ali, C. W. Ahn, M. Pant and P. Siarry, "An image watermarking scheme in wavelet domain with optimized compensation of singular value decomposition via artificial bee colony," *Information Science*, vol. 301, 2015. doi: 10.1016/j.ins.2014.12.042.
16. M. Ali, C. W. Ahn and P. Siarry, "Differential evolution algorithm for the selection of optimal scaling factors in image watermarking," *Eng Appl Artif Intell*, vol. 31, 2014. doi: 10.1016/j.engappai.2013.07.009.
17. F. Ernawan and M. N. Kabir, "A block-based RDWT-SVD image watermarking method using human visual system characteristics," *The Visual Computer*, vol. 36, pp. 19–37, 2020.
18. S. A.. Sahy and Y. Niu, "Image fragment reconstruction and restoration method based on genetic algorithm", *KHWARIZMIA*, vol. 2023, pp. 1–9, 2023. doi: 10.70470/KHWARIZMIA/2023/001
19. Y. Naderahmadian and S. Hosseini-Khayat, "Fast and robust watermarking in still images based on QR decomposition," *Multimed Tools Appl*, vol. 72, no. 3, 2014. doi: 10.1007/s11042-013-1559-9.
20. L. Zhang and D. Wei, "Image watermarking based on matrix decomposition and gyrator transform in invariant integer wavelet domain," *Signal Processing*, vol. 169, 2020. doi: 10.1016/j.sigpro.2019.107421.
21. L. Y. Hsu and H. T. Hu, "Robust blind image watermarking using crisscross inter-block prediction in the DCT domain," *J Vis Commun Image Represent*, vol. 46, 2017. doi: 10.1016/j.jvcir.2017.03.009.
22. Ayad, J. and M. A. Jalil, "Robust color image encryption using 3D chaotic maps and S-Box algorithms," *Babylonian Journal of Networking*, 148–161, 2024. https://doi.org/10.58496/BJN/2024/015.