Iraqi Journal for Computer Science and Mathematics

Volume 5 | Issue 4 Article 7

2024

Robust-Fragile Watermarking Using Integer Wavelet Transform for Tampered Detection and Copyright Protection

Hendra Budi
Faculty of Computing, Universiti Malaysia Pahang Al-Sultan Abdullah, Pekan Pahang, 26600, Malaysia AND Faculty of Information Technology, Universitas Nusa Mandiri, Pasar Minggu Jakarta Selatan, Jakarta, 12540, Indonesia

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

Agit Amrullah
Faculty of Computing, Universiti Malaysia Pahang Al-Sultan Abdullah, Pekan Pahang, 26600, Malaysia AND Faculty of Computer Science, Universitas AMIKOM Yogyakarta, Ring Road Utara Condong Catur Sleman, Yogyakarta, 55283, Indonesia

Recommended Citation

Budi, Hendra; Ernawan, Ferda; and Amrullah, Agit (2024) "Robust-Fragile Watermarking Using Integer Wavelet Transform for Tampered Detection and Copyright Protection," *Iraqi Journal for Computer Science and Mathematics*: Vol. 5: Iss. 4, Article 7.
DOI: https://doi.org/10.52866/2788-7421.1207
Available at: https://ijcsm.researchcommons.org/ijcsm/vol5/iss4/7

IRAQI JOURNAL FOR COMPUTER SCIENCE AND MATHEMATICS 2024;5:70–81

RESEARCH ARTICLE

Robust-Fragile Watermarking Using Integer Wavelet Transform for Tampered Detection and Copyright Protection

Hendra Budi [a,b], Ferda Ernawan [a,b,*], Agit Amrullah [a,c]

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

ABSTRACT

The use of the internet and advanced technologies enables the distribution of information and data through diverse digital images. Nevertheless, this ease of use comes with the potential risk of data misappropriation, encompassing unauthorized alterations, duplications, and reproductions of digital images. Ongoing research is being conducted in the field of watermarking to enhance the capabilities of protecting digital images. The objective of this work is to enhance the strength of copyright protection and the vulnerability of watermarking for authentication in digital images by utilizing the Integer Wavelet Transform (IWT). The watermarking approach involves embedding a durable watermark in the red layer and a delicate watermark in the blue layer of the host image. The watermark is incorporated into the singular value of the Singular Value Decomposition (SVD). The red layers with watermarks are generated using a Hash function and subsequently integrated into the blue layer using the Least Significant Bit (LSB) method. The experimental findings demonstrate that the proposed strategy effectively enhances both imperceptibility and robustness in comparison to the previous benchmark research. The suggested scheme attained an average PSNR value of 51,935 and an average SSIM value of 0.976. The proposed scheme demonstrated an average improvement of 14.19% in PSNR compared to existing schemes. This study offers efficient and suitable remedies for safeguarding digital images against unauthorised and alteration without consent.

Keywords: Color image, Watermarking, Copyright protection, Integer Wavelet Transform (IWT), Robust-fragile

1. Introduction

In the rapidly evolving digital era, numerous sectors are experiencing digital transformation, including the field of digital image technology. The advancement of technology has made the creation and sharing of colour digital images easier, thanks to devices such as smartphones. The act of exchanging information and data in the type of digital documents, image, audio, and videos has become extremely easy. The accessibility of information has facilitated the alteration, duplication, and manipulation of data through several means [1]. Moreover, the accessibility of software tools for editing has increasingly become more intuitive, facilitating extensive use. It is crucial to secure digital images from potential altering risks to maintain their copyright protection. Watermarking has become an essential component of information security to combat the unauthorised use of images in the digital realm and communication [2].

The method of watermarking involves two essential steps: embedding, which conceals information inside a host image, and extraction, which returns the

Received 17 December 2023; accepted 2 August 2024.
Available online 25 November 2024

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

https://doi.org/10.52866/2788-7421.1207

hidden information [3]. The watermark data that has been extracted can be utilised to ascertain whether an image has undergone any modifications or remains in its original state. Watermarking techniques are commonly used to protect copyrights in numerous areas [4]. Watermarking provides a method to protect image and video content that is connected to human visual perception. The success of watermarking is evaluated based on imperceptibility and robustness, which are crucial metrics.

The points emphasise various reasons that contribute to the identification of the problem: the widespread production and dissemination of digital images, their growing utilisation in various fields, and the resulting requirement for an effective mechanism to safeguard copyright protection. This project seeks to enhance copyright protection for colour digital images by employing the Integer Wavelet Transform (IWT) watermarking approach. This process entails incorporating a resilient-fragile watermark in the R layer and implementing tamper detection in the B layer of the original image.

Shaohua Duan et al. [5] examined DWT in robust-fragile watermarking of colour images. Although it demonstrated satisfactory imperceptibility and resilience, there is still room for improvement in the PSNR value. DWT is generally utilized to reduce the computation complexity [6]. Furthermore, the DWT approach is vulnerable to several attacks such as noise, filtered images, cropping, and histogram equalization. The susceptibility mentioned is due to the sensitivity of DWT to image compression. This sensitivity can cause considerable changes in DWT coefficients when the image is subjected to attacks, which may ultimately result in the loss of the watermark.

This study presents a dual watermarking strategy that utilizes the integer wavelet transform (IWT) for both robust and fragile watermarking. The IWT is an efficient and rapid lifting wavelet transform and its properties are best suited to enhance the robustness and preserve the imperceptibility [7]. The red channel of the image performed an IWT transformation to obtain the LL-sub band. This LL-sub band was subsequently embedded with a watermark logo. Furthermore, a hash was generated for the blue channel of the image. Thus, the hash derived from the created red channel can be effectively utilized to embed information in the blue channel, enhancing its resilience. The tests utilized eight colour images with a resolution of 512 by 512 pixels as hosts, along with two extra host images obtained through a cell phone camera. The watermark logo is a binary image with dimensions of 32×32 pixels.

2. Theoretical framework

2.1. Watermarking

The development of image watermarking can be traced back to its initial application as a method of identification for artwork or papers, primarily used to authenticate and establish ownership. In the digital realm, a watermark refers to hidden data that is embedded within an image to convey ownership or identity details. The process of embedding a watermark requires two inputs: the original host image and the watermark logo. The procedure of removing the watermark allows for the establishment of copyright information [8]. The purpose of watermarking is to verify the genuineness of images and validate rightful ownership, acting as a protective measure against the unauthorised abuse of electronic information and documents [9].

Image watermarking techniques can be classified into two primary categories: spatial domain methods and transform domain approaches. Spatial domain approaches refer to the direct modification of pixel values within the host image in its original spatial representation. This procedure involves altering the levels of pixel brightness in the original image by incorporating the watermark into these pixels. In this scenario, the watermark can be concealed using techniques such as Least Significant Bit (LSB). The primary advantage of spatial domain approaches is their straightforward installation and detection capabilities. Nevertheless, they are simple yet susceptible to assaults such as compression and transformations [10].

In contrast, transform domain approaches modify the watermark by applying mathematical transformations to the host image. The transform domain encompasses techniques such as DWT, DCT, IWT and SVD [10]. In the field of image watermarking, the watermark is inserted into the altered coefficients of the original image. This watermark can be retrieved by using the inverse transformation. Transform domain techniques provide robustness against image manipulations such as compression and filtering [6].

IWT is a mathematical technique that utilises operations using whole numbers [7]. During the process of embedding, the original image and watermark are decomposed using the IWT, which produces wavelet coefficients at different resolution scales. Subsequently, these coefficients are adjusted to incorporate watermark data. During the extraction phase, the changed image is analysed using the IWT to get wavelet coefficients. These coefficients are then utilized to extract the watermark by comparing them with the original watermark. By employing the

inverse IWT approach [11], the restoration of watermarks is accomplished with a high level of precision.

The process of watermarking utilizing the IWT method comprises multiple sequential steps. The first phase involves partitioning, whereby the original signal is divided into two segments: one containing even values and the other containing odd values. The prediction step utilises a designated predictor to forecast odd values based on even values. Subsequently, the update process entails producing novel even values by merging projected odd values with initial even values via an update procedure. The predicted odd values correspond to coefficients with high frequencies, whereas the even values correspond to coefficients with low frequencies. An inversion operation is done to restore the signal to its original condition [12].

Robust-fragile watermarking is a method that combines the qualities of being strong and resilient while still being delicate and responsive to alterations. This approach is specifically developed to provide robust security against unauthorized manipulation and modifications to images, while also facilitating the identification of adjustments. This watermark is highly durable and resistant to a wide range of threats. Any alterations to the image without authorization lead to the destruction or removal of the watermark, therefore indicating that the image has been tampered with [13].

Wavelet types consist of a variety of wavelet functions that possess unique properties. Every form of wavelet has a distinct profile that is well-suited for different image processing applications. A wavelet is a high-frequency oscillating waveform that has a finite duration. Wavelets exist in several forms and types, with the most prevalent ones being Haar, Daubechies, Symlets, and Coifflets [14, 15].

Darwish and Al-Khafaji [16] presented a novel solution for image copyright protection through the combination of segmented and successive watermarking with dual watermarking scheme. It takes a number of standards and criteria to develop an appropriate dual watermark embedding. Consequently, it is not easy to find the best embedding strength and appropriate embedding sites. Recently, experts in this subject have paid close attention to the optimization strategies that may be used with the picture watermarking scheme to increase its efficacy and performance in many contexts. This scheme presents an innovative approach to create an intelligent dual watermarking scheme for color images that ensures the protection of ownership and publication rights and can be effectively utilized in various applications that consider image quality. The scheme was inspired by the difficulties encountered with dual image watermarking and addresses them. In order to achieve resilience and imperceptibility, the watermarking embedding parameters are optimized here using a multi-purpose genetic algorithm. High capacity (Payload) is achieved by the recommended model. Examining the image's capacity can reveal the maximum amount of watermark data that can be encoded while still meeting the requirements for resilience and imperceptibility. The proposed scheme has moderate complexity; the two primary challenges of difficulty are the number of embedders and detectors and the speed of embedding and detection. Benchmark photos have been used to assess the suggested model. The outcomes verified that the suggested scheme is capable of being both imperceptible and resilient. The peak signal to noise ratio is improved by 23% when using the evolutionary algorithm in place of the conventional, non-optimized dual watermarking techniques. The scheme may be improved to take use of additional color spaces like YUV and CMYK, which could boost performance, as a blueprint for future projects. By combining the DWT with other transforms, more characteristics may be looked at to improve the performance of the dual watermarking methods. Additionally, if another suitable optimization technique is preferred over GA, it may be used to fine-tune the parameters of the watermarking embedding. Lastly, connect the suggested paradigm to contemporary e-business tools like Blockchain.

Sing et al. [17] presented a self-recoverable dual watermarking system to ensure integrity of the copyright. This scheme proposed a dual watermarking approach that combines ownership assertion and integrity check functionality. The recovery information of every non-overlapping block measuring 2×2 was reduced to a mere eight bits. These bits were then further encoded to yield a mere four bits, which were then embedded into the mapping block of the cover picture. The resilience element of the method was added by effectively integrating the copyright information using the reduced storage needs for recovery bits. The plan held up well against a wide range of attacks, including filtering, rotation, JPEG compression, histogram equalization, and noise. For each of the three main categories of natural, texture, and satellite photos, the scheme's pixel-level tamper detection could precisely identify the areas that had been manipulated. The random chaotic mapping of blocks enhanced the efficacy of the scheme against tampers even upto 50%. With acceptable PSNR values for both watermarked and recovered photos, evaluation of the derived watermark logo using a range of appropriate error measures further enhanced its benefits.

Shi et al. [18] proposed a semi-fragile technique for dual-watermarking that is region-adaptive. In this scheme, a dual watermarking technique based on bit substitution and status code technologies is semi-fragile and region adaptive. The original image is converted by IWT in the suggested scheme, after which it is split into three regions: one without a watermark, one with a strong watermark, and one with a weak watermark. Then, depending on the technology, the strong and weak watermarks are inserted into various places. The extracted robust watermark can be strengthened further by the extracted fragile watermark, improving its HVS compatibility. The robust and fragile watermarks are unrelated to the embedding order. The experimental findings demonstrate the robustness of the suggested system, which can withstand filter attacks, noise, and JPEG compression, as well as its fragility, which can better accomplish integrity verification and provide dual function capability. Compared to previous designs that have been put forth in the literature, the suggested scheme also boasts a greater capacity, stronger security, and a higher PSNR.

Li et al. [19] introduced a tampering and recovery approach that utilizes a chaotic watermarking system to identify tampered areas and restore image. In this scheme, a various picture self-recovery approach based on watermarking technology is applied to locate the tamper region and validate the integrity of the digital image. Then, the chaotic system creates the mapping link between the subblocks to improve the security purposes. The content of the picture block generates both the recovery information and the authentication. The recovery performance is improved by using the optimization process to locate better recovery information. Unlike the conventional Level-2 recovery system, a weight adaptive approach is presented to assign distinct weights to the original block and the primary recovery block, resulting in improved 3×3 neighbor block recovery. Numerous tests and evaluations were conducted to demonstrate the improved performance of this scheme.

Fang et al. [20] introduced an adaptive watermarking approach to enhance the quality of watermarked images and raise the resilience of watermark extraction. In order to fully utilize the direction feature of the photos, a new digital watermarking approach for active forensics is proposed in this scheme. This scheme is proposed a direction-coefficient mapping that illustrates the relationships between DCT coefficients and direction characteristics. The mapping ensures that when the associated DCT coefficients are changed, the picture blocks maintain the intended directional properties. This is the crucial step in ensuring that the image retains its high visual quality even after the message has been included. Based on the assumption of high visual quality, the studies demonstrate that the suggested method outperforms alternative schemes in many circumstances when it comes to various sorts of distortions. It is important to emphasize that the suggested technique has a limited resistance against attacks using Gaussian noise. Therefore, it will enhance the robustness against noise attacks in our future work.

2.2. Watermark embedding

This research uses the IWT using the Daubechies (DB4) wavelet. The integration of IWT (Integer Wavelet Transform) with DB4 (Daubechies 4) wavelet is intended to enhance the visual quality of images after embedding watermarks, making them imperceptible. The Daubechies wavelet is chosen and employed in the experiment for this investigation. The Daubechies wavelet is selected for its multiresolution features, which allow for the efficient representation of signals with gradual frequency variations. The Daubechies wavelet is characterized by a set of wavelet functions labelled as "dbN," with N indicating the quantity of filter coefficients. Greater values of N indicate a larger number of filter coefficients employed in the Daubechies wavelet. Frequently employed N values consist of 4, 6, 8, and so forth. The Daubechies wavelet is a highly effective multiresolution wavelet transform that can be used to insert logos in digital images [15]. Additionally, it intends to strengthen the resistance of watermarked images against attacks, ensuring their robustness. The method of installing the watermark is visually illustrated in Fig. 1. The red dashed lines represent the procedure of including the durable watermark, while the dashed blue lines indicate the method of incorporating the delicate watermark.

Embedding Robust Watermark Explanation:

Step 1: Apply a single-level shearlet transformation to the R layer to obtain the low-pass sub band LL.
Step 2: Apply the IWT transformation to LL subband.
Step 3: Divide the low-frequency area (LL) into 8×8 blocks and apply the process to each block.
Step 4: Choose the middle frequency from the coefficients within the block, which consists of two matrices M1 and M2.
Step 5: Decompose M1 and M2 to obtain matrices of singular values. The singular value matrices of M1 and M2 are referred to as S1 and S2.

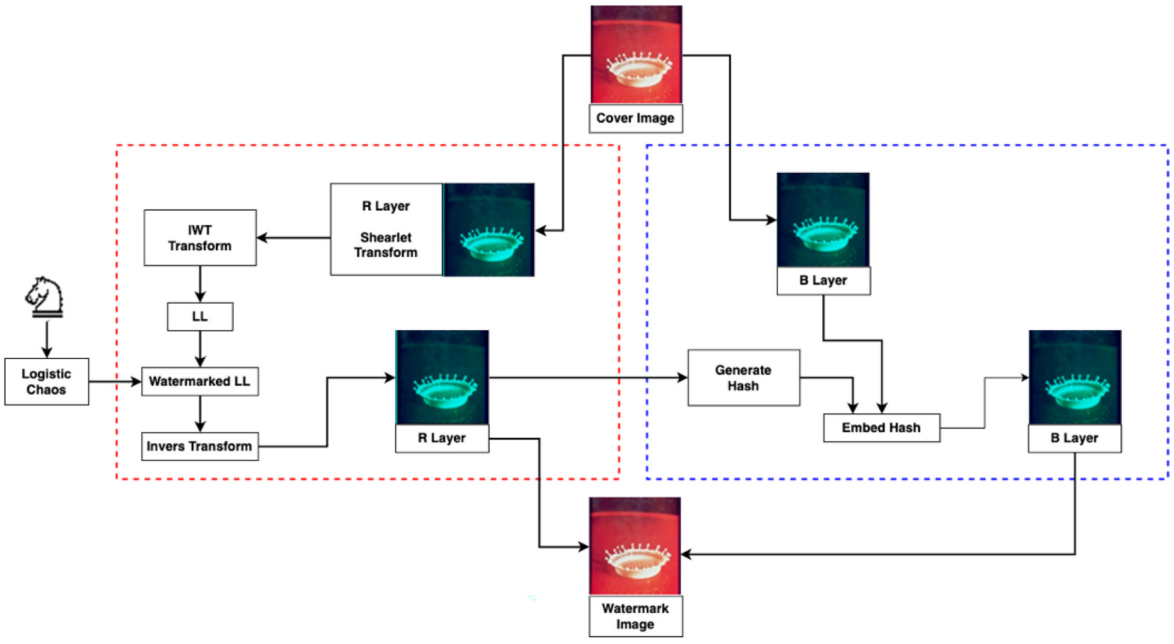

Fig. 1. Proposed watermark embedding procedure.

Step 6: Utilize the following equation (1) to embed the watermark:

$$S_1(1,1) = \begin{cases} E + \lambda, & \text{if } W_e = 1, \\ E - \lambda, & \text{if } W_e = 0 \end{cases} \text{ and}$$

$$S_2(1,1) = \begin{cases} E + \lambda, & \text{if } W_e = 1, \\ E - \lambda, & \text{if } W_e = 0 \end{cases} \quad (1)$$

Step 7: Repeat steps 4–6 and then perform the inverse transform to embed the watermark in the R layer.

Explanation of Embedding Fragile Watermark:

Step 1: Divide the watermarked color image with an embedded watermark into blocks of size 8×8.
Step 2: Generate a hash function based on the watermarked image (Red Layer).
Step 3: Embed the hash function into the B layer using the LSB technique.
Step 4: Repeat steps 2–3 for all blocks until the entire image is processed.

2.3. Watermark extraction

In the watermark extraction process, the embedded watermark logo within the host image will be extracted from the image for subsequent comparison with the original watermark logo. The watermark extraction process is illustrated in Fig. 2.

Explanation of extracting robust watermark:

Step 1: Apply the same transformation (IWT) used during the embedding of the robust watermark to the attacked R layer of the image.
Step 2: Obtain the singular value matrices S1 and S2 through step 1, then use the following equation (2) for watermark extraction:

$$W'_e = \begin{cases} 1, & \text{if } S'_1(1,1) > S'_2(1,1), \\ 0, & \text{if } S'_1(1,1) < S'_2(1,1) \end{cases} \quad (2)$$

Explanation of extracting fragile watermark:

Step 1: Split the targeted image into eight-by-eight pixels.
Step 2: Create a hash sequence using the R layer.
Step 3: Using the LSB technique, extract the stored hash sequence from the B layer and compare it to the hash sequence that was produced in step 2.
Step 4: Repeat steps 2–3 for the entire image. If the comparison results are the same, then extract the watermark. However, if the comparison results are different, mark the area in the image, and subsequently extract the watermark.

3. Evaluation

The PSNR is a quantitative measure used to assess the quality and perceived clarity of a digital image.

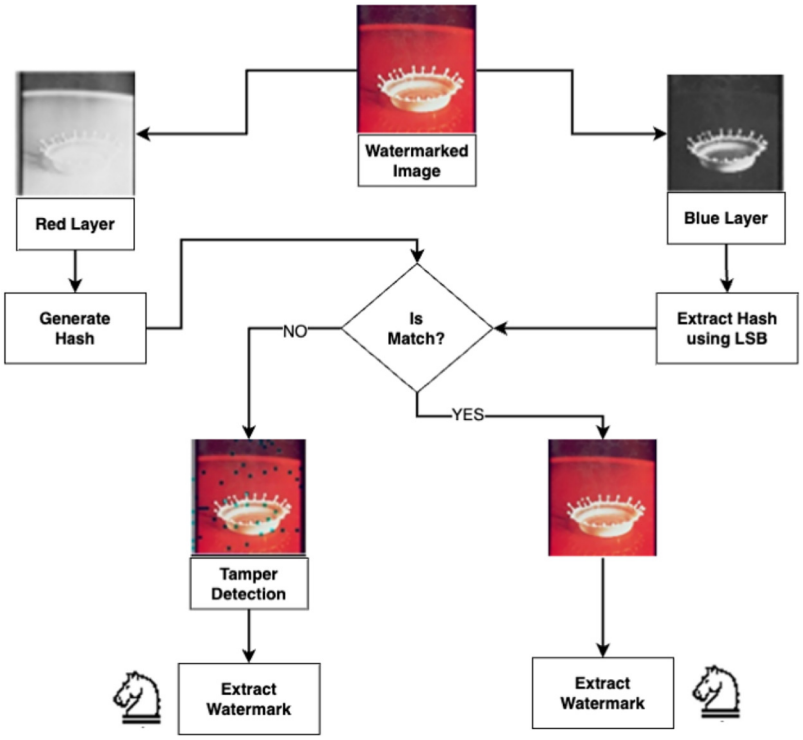

Fig. 2. Proposed watermark extracting procedure.

The PSNR is calculated by taking the logarithm of the MSE present in an image. The PSNR is measured in decibels (dB), and a greater number signifies superior image quality attained. PSNR, a metric used to assess image quality, can be utilised to compare the results of image compression, measure the amount of information lost during processing, and evaluate image quality in different applications like image processing, video processing, or image watermarking. PSNR, a frequently employed technique [21], is determined by comparing the original and processed images. The definition of PSNR is given by [22, 23]:

$$PSNR(o,w) = 10\log_{10}\left(MAX^2/MSE(o,w)\right) \tag{3}$$

$$MSE(o,w) = \frac{1}{WH}\sum_{x=1}^{M}\sum_{y=1}^{N}\left(o_{x,y} - w_{x,y}\right)^2 \tag{4}$$

where x, y are the image's pixel coordinate, $o_{x,y}$ and $w_{x,y}$ are the cover image and watermarked image, respectively. The Structural Similarity Index (SSIM) serves as a quantitative measure for assessing the structural similarity between two images. SSIM provides a more detailed assessment compared to simple measures such as PSNR, as it considers not just variations in pixel brightness but also incorporates spatial arrangement and texture inconsistencies within the image. The SSIM metric measures the similarity in structure between two images by considering three main factors: brightness, contrast, and structure. The SSIM value is a numerical measure that varies from 0 to 1, with a value of 1 indicating complete structural similarity between two images. A higher SSIM score indicates a greater similarity in the structure and texture of the two images [24, 25]. The definition of SSIM is given by:

$$\mathrm{SSIM}(o,w) = l(o,w)c(o,w)s(o,w) \tag{5}$$

$$l(o,w) = \frac{2\mu_o\mu_w + C_1}{\mu_o^2 + \mu_w^2 + C_1} \tag{6}$$

$$c(o,w) = \frac{2\sigma_o\sigma_w + C_2}{\sigma_o^2 + \sigma_w^2 + C_2} \tag{7}$$

$$s(o,w) = \frac{\sigma_{ow} + C_3}{\sigma_o\sigma_w + C_3} \tag{8}$$

Where $l(o,w)$ is the structural component (luminance) that measures the similarity of intensity patterns (mean value), $c(o,w)$ is the contrast component that measures the similarity of contrast between the two images and $s(o,w)$ is the structural component that reflects the similarity in texture distribution between the two images.

Normalized Correlation (NC) is a measurement utilized to gauge the degree of similarity between two images [22]. This metric calculates the correlation

Table 1. Various types of attack.

Attack	Description	Attack	Description
1	*Salt & Pepper density = 0.001*	7	*JPEG Compression 30*
2	*Salt & Pepper density = 0.005*	8	*JPEG Compression 50*
3	*Gaussian Noise 0.0001*	9	*Cropping 15%*
4	*Gaussian Noise 0.0005*	10	*Gaussian Filter* 3×3
5	*Speckle Noise 0.001*	11	*Histogram Equalization*
6	*Speckle Noise 0.005*	12	*No Attack*

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 -1 and 1, with a score of 1 indicating a complete positive correlation between two images, a value of 0 indicating no correlation, and a score of -1 representing negative 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:

$$NC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} W(i,j) \cdot W\cdot(i,j)}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N} W(i,j)^2 \sum_{i=1}^{M}\sum_{j=1}^{N} W\cdot(i,j)^2}} \tag{9}$$

where $W(i, j)$ is the original watermark and $W(i, j)$ is the extracted 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 is calculated by:

$$BER = \sum_{i=1}^{M}\sum_{j=1}^{N} \frac{W(i,j) \times W'(i,j)}{M \times N} \tag{10}$$

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.

3.1. Types of image attacks

An image containing a watermark can be susceptible to various types of assaults, including the insertion of extra noise, lossy compression, geometric distortions, and image filtering. Therefore, to assess the strength of the watermark contained in the image, it is necessary to expose the image to several assault scenarios. These assaults are designed to evaluate the ability of the watermark to withstand modifications within the image. This study encompassed a variety of attack categories, as specified in Table 1.

4. Experimental results

This study experiment utilized a total of eight (8) colour images as hosts, with each image having dimensions of 512 by 512 pixels. In addition, two colour images were taken using a mobile phone camera, each with dimensions of 512×512 pixels. For the watermark logo, a binary image of dimensions 32×32 pixels was used. Imperceptibility plays a vital role during the watermark embedding procedure, aiming to ensure that the image containing the watermark remains visually inconspicuous, thereby safeguarding the embedded information, which is the watermark logo, without introducing any significant alteration to the original image's appearance. Fig. 3 displays the host images and watermark logo used in this study:

The assessment outcomes for imperceptibility by PSNR and SSIM metrics, are presented in the Table 2.

Table 3 presents the results of evaluating PSNR and SSIM values obtained from experiments done on

Table 2. Evaluation of PSNR and SSIM.

	S. Duan [5]		Proposed	
Image	PSNR	SSIM	PSNR	SSIM
Lena	45.46	0.9951	52.0296	0.9976
Baboon	44.44	0.9954	50.5492	0.9981
House	45.05	0.9947	51.3259	0.9978
Peppers	45.73	0.9912	52.2948	0.9968
Sailboat	45.40	0.9930	51.9250	0.9975
Plane	45.29	0.9942	50.8927	0.9969
Splash	46.22	0.9923	53.3329	0.9967
Tiffany	46.27	0.9950	53.1300	0.9977

Fig. 3. Host images and watermark logo.

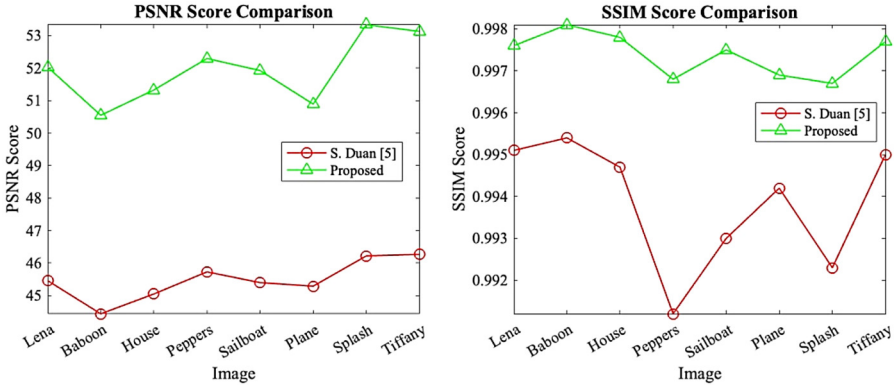

Fig. 4. Comparing of the proposed scheme with the scheme by Duan [5] in terms of PSNR and SSIM values.

images captured by a mobile camera. The PSNR and SSIM values of images captured by the mobile camera exhibit a negligible difference when compared to the PSNR and SSIM values of the remaining eight reference images. This suggests that the proposed technique can efficiently be utilised for images taken by mobile cameras in real-life situations.

From Table 3, it can be observed that the proposed method has demonstrated its capability to enhance imperceptibility in all the utilized host images. This is evident from the PSNR and SSIM values of each host image, which have shown improvements when compared to the PSNR and SSIM values of the S. Duan [5] method. The following visuals illustrate how the PSNR and SSIM values of the proposed method exhibit a better performance compared to the S. Duan [5] method as shown in Fig. 4.

Table 3. Evaluation of PSNR and SSIM for mobile camera images.

	Eval	
Image	PSNR	SSIM
Catze	51.3820	0.9980
Coffee	52.4631	0.9965

Fig. 4 depicts curves comparing image quality metrics PSNR and SSIM values. This visual representation highlights the significance of imperceptibility or the quality of the host image after watermark embedding within the IWT method. It also displays a graph comparing the SSIM values.

4.1. Robustness

By embedding watermarks into each host image and analyzing the outcomes under various attack scenarios, it is critical to determine the robustness of image watermarking techniques. Image watermarking technologies that are effective typically exhibit resilience against several attacks, including noise, filtering, scaling, rotation, and even JPEG compression. The findings of the studies are presented in Table 4, which displays the detection outcomes for the 8 host images after undergoing attacks. The presence of a delicate watermark is clearly able to expose the specific regions that have been altered in images that have undergone attacks.

Fig. 5 presents the experimental results of the extracted logo watermark from each of the 8 host

Table 4. Tamper detection for eight watermarked image.

Image							
Lena	Baboon	House	Peppers	Sailboat	Plane	Splash	Tiffany

Images	Salt & Pepper density=0.001		Gaussian Noise 0.0005		Speckle Noise 0.001		Cropping		*No Attack*	
	Duan [5]	Proposed	Duan [5]	Proposed	Duan [5]	Proposed	Duan [5]	Proposed	Duan [5]	Proposed
Lena	NC=0.9749, BER=0.0390, FPR = 0.11	NC=0.9755, BER=0.0380, FPR = 0.06	NC=0.9329, BER=0.1025, FPR = 0.23	NC=0.9406, BER=0.0908, FPR = 0.16	NC=0.9134, BER=0.1308, FPR = 0.23	NC=0.9767, BER=0.0361, FPR = 0.04	NC=0.8692, BER=0.1923, FPR = 0.11	NC=0.8783, BER=0.1796, FPR = 0.07	NC=0.9981, BER=0.0029, FPR = 0.01	NC=0.9981, BER=0.0029, FPR = 0.01
Baboon	NC=0.9786, BER=0.0332, FPR = 0.06	NC=0.9825, BER=0.0273, FPR = 0.08	NC=0.9525, BER=0.0732, FPR = 0.19	NC=0.9640, BER=0.0556, FPR = 0.15	NC=0.9667, BER=0.0517, FPR = 0.16	NC=0.0.9621, BER=0.0585, FPR = 0.12	NC=0.8712, BER=0.1894, FPR = 0.08	NC=0.8804, BER=0.1767, FPR = 0.06	NC=0.9975, BER=0.0039, FPR = 0.00	NC=0.9993, BER=0.0009, FPR = 0.00
House	NC=0.9710, BER=0.0449, FPR = 0.10	NC=0.9673, BER=0.0.0507, FPR = 0.08	NC=0.9334, BER=0.1015, FPR = 0.16	NC=0.9485, BER=0.0791, FPR = 0.15	NC=0.9427, BER=0.0878, FPR = 0.19	NC=0.9491, BER=0.0781, FPR = 0.14	NC=0.8798, BER=0.1777, FPR = 0.09	NC=0.8798, BER=0.1777, FPR = 0.11	NC=0.9968, BER=0.0048, FPR = 0.01	NC=0.9968, BER=0.0048, FPR = 0.02
Peppers	NC=0.9723, BER=0.0478, FPR = 0.10	NC=0.9780, BER=0.0.341, FPR = 0.05	NC=0.9381, BER=0.09472, FPR = 0.19	NC=0.9486, BER=0.0791, FPR = 0.18	NC=0.9562, BER=0.0673, FPR = 0.09	NC=0.9595, BER=0.0625, FPR = 0.1	NC=0.8777, BER=0.1806, FPR = 0.10	NC=0.8791, BER=0.1787, FPR = 0.10	NC= 0.9987, BER= 0.0019, FPR = 0	NC= 0.9981, BER= 0.0029, FPR = 0.01
Sailboat	NC=0.9793, BER=0.0322, FPR = 0.07	NC=0.9850, BER=0.0234, FPR = 0.06	NC=0.9441, BER=0.0859, FPR = 0.21	NC=0.9590, BER=0.0634, FPR = 0.18	NC=0.9334, BER=0.1015, FPR = 0.18	NC=0.9717, BER=0.0439, FPR = 0.1	NC=0.8776, BER=0.1806, FPR = 0.08	NC=0.8811, BER=0.1757, FPR = 0.07	NC=0.9987, BER=0.0019, FPR = 0.00	NC=0.9981, BER=0.0029, FPR = 0.01

Fig. 5. Extracted watermark under various attacks.

Table 5. The comparison of NC values obtained from the proposed scheme with the existing scheme under various attacks 1–6.

	S. Duan [5]						Proposed					
Image	Attack1	Attack2	Attack3	Attack4	Attack5	Attack6	Attack1	Attack2	Attack3	Attack4	Attack5	Attack6
Lena	0.8376	0.8444	0.8376	0.9039	0.8981	0.7940	0.8942	0.9274	0.8849	0.9124	0.9309	0.8509
Baboon	0.8376	0.8801	0.8376	0.9019	0.9219	0.8162	0.8302	0.8414	0.8315	0.9162	0.9142	0.8742
House	0.8360	0.8454	0.8360	0.9092	0.8987	0.7608	0.8369	0.8883	0.8376	0.9142	0.9068	0.8433
Peppers	0.8446	0.9247	0.8470	0.9076	0.9264	0.8078	0.8338	0.9004	0.8469	0.9077	0.8845	0.8463
Sailboat	0.8523	0.8380	0.8326	0.9047	0.9070	0.8570	0.8771	0.8860	0.8368	0.9072	0.9220	0.9215
Plane	0.8450	0.8594	0.8376	0.8886	0.9006	0.7761	0.8812	0.8786	0.8822	0.8996	0.8937	0.8090
Splash	0.8523	0.8971	0.8376	0.9005	0.8996	0.8540	0.8940	0.8483	0.9114	0.8666	0.8530	0.7882
Tiffany	0.8765	0.9121	0.9122	0.8839	0.8534	0.7169	0.8967	0.8959	0.8730	0.8263	0.8138	0.7577

Table 6. The comparison of NC values obtained from the proposed scheme with the existing scheme under various attacks 7–12.

	S. Duan [5]						Proposed					
Image	Attack 7	Attack 8	Attack 9	Attack 10	Attack 11	Attack 12	Attack 7	Attack 8	Attack 9	Attack 10	Attack 11	Attack 12
Lena	0.7185	0.7901	0.7567	0.7930	0.7330	0.9981	0.8085	0.8006	0.8975	0.8997	0.9094	0.9981
Baboon	0.7181	0.7175	0.8234	0.8144	0.7574	0.9975	0.8247	0.7961	0.9062	0.8450	0.9144	0.9993
House	0.7497	0.7587	0.8452	0.7841	0.7128	0.9968	0.7499	0.7995	0.9134	0.8596	0.8964	0.9968
Peppers	0.7264	0.7513	0.8331	0.8679	0.7433	0.9987	0.7616	0.7908	0.9200	0.8883	0.9065	0.9981
Sailboat	0.7283	0.7520	0.8868	0.8047	0.6780	0.9987	0.7406	0.7963	0.9099	0.8751	0.9144	0.9981
Plane	0.7513	0.7597	0.8423	0.8149	0.7017	0.9975	0.7666	0.8169	0.8760	0.8741	0.8771	0.9975
Splash	0.7116	0.7671	0.7914	0.8638	0.6953	0.9938	0.7824	0.7869	0.9018	0.9184	0.9224	0.9993
Tiffany	0.7329	0.7612	0.8652	0.8364	0.7499	0.9950	0.7659	0.7991	0.8836	0.8606	0.8830	0.9950

images subjected to attacks 1–5 using the method by S. Duan [5].

Referring to Fig. 5, It can be observed that the proposed watermarking achieved better NC and BER values than the schemes by S. Duan [5], except against Salt & Pepper noises with density 0.001. The embedded watermark image through IWT transform obtains high robust of extracted watermark images from various attack. The watermark logo clearly shows alterations during attacks 1–4 and no attack on the 5 host images. The modification is a result of attacks 1–4 altering the composition of the host images, resulting in the extracted watermark logo having a distinct shape compared to the original logo watermark. To make a more comprehensive comparison, an evaluation is performed on each of the extracted watermark logos stated earlier to compare them with the original logo. The comparison of NC values of proposed scheme and scheme by S. Duan [5] can be seen in Table 5 and Table 6.

Based on the information shown in Tables 5 and 6, the watermark logos produced by the suggested approach have superior quality compared to those generated by S. Duan's method [5] when subjected to different attacks. Specifically, even when subjected to attacks 7–12, the suggested method demonstrates a higher level of excellence in extracting watermark logos. It is worth mentioning that in certain cases of assaults 1–6, the S. Duan [5] technique exhibits a relative superiority compared to the suggested method, albeit only inside a small subset of the host images.

The analysis of the NC and BER values for the extracted watermark logos after attacks 1–12, comparing the S. Duan [5] approach and the suggested method, reveals significant discoveries. While assaults 1–6 do not result in higher NC and BER for each host image, it can be concluded that the suggested method can improve NC and BER values for a significant number of the host images used. On the other hand, attacks 7–12 exhibit a clear increase in NC and BER for each attack on the host images. This suggests that the suggested technique outperforms the S. Duan [5] method in these situations. Additionally, the experimental findings for detecting applied attacks on images recorded from the mobile phone are shown in Fig. 6.

Moreover, the following are the outcomes of watermark extraction from two images taken by the mobile phone camera. These images were subjected to watermark embedding and underwent attacks 1–12. As illustrated in Table 7, the retrieved watermark logos from attacks 1–6, and 11 and 12 may still be extracted with results that are visually discernible by humans. However, for attacks 7–10, the logo exhibits significant distortion as a result of those attacks.

This is additionally facilitated by the experimentation conducted on the logo inside the images. The results showed that after being subjected to attacks

Table 7. Extracted watermark after attacks 1–12 on mobile phone camera images.

	Attack								
Image	1	2	3	4	5	6	10	11	12
Catze									
Coffee									

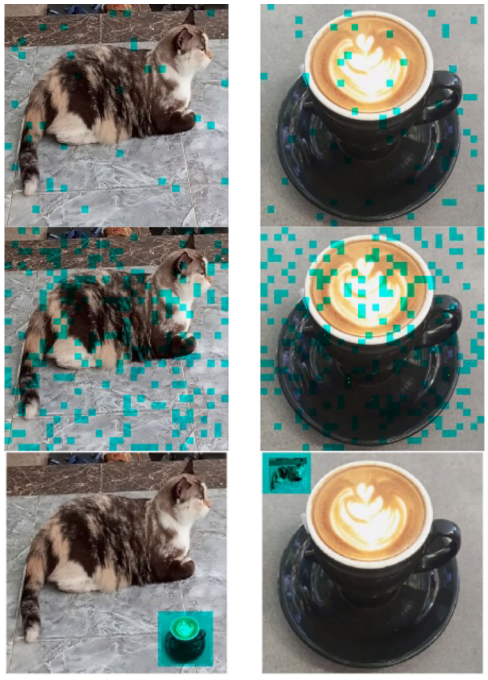

Fig. 6. Tamper detection on mobile phone images.

1–12, the NC and BER values of the images taken with the mobile phone camera were similar to those of the other 8 original images. This illustrates the potential applicability of the proposed technique to images captured by mobile phone cameras often employed in daily activities.

5. Conclusion

This study presents a delicate image watermarking technique that applies the IWT for copyright protection and authentication. The method's imperceptibility and durability were assessed by simulation employing 8 colour images as the host with an embedded watermark logo. The watermarked images exhibited exceptional visual quality, typified by a high average PSNR value of 51.935 dB and SSIM values of 0.976. Moreover, the method's ability to withstand different attacks was proven by the greater NC and BER values achieved when extracting watermarks from host images that had been subjected to various forms of manipulation. An analysis of the empirical results greatly enhances the quality of watermarked image, while also showcasing their robustness against attacks. A comparison study comparing the robustness of the suggested and referred approaches showed that the suggested scheme outperforms the existing scheme. In future research, the technique of watermarking images can be implemented into video data and achieve greater imperceptibility and robustness against various attacks.

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, Malaysia.

Conflicts of interest

The author declares no conflict of interest.

References

1. S. P. Ambadekar, J. Jain, and J. Khanapuri, "Digital image watermarking through encryption and DWT for copyright protection," in *Recent Trends in Signal and Image Processing*, S. Bhattacharyya, A. Mukherjee, H. Bhaumik, S. Das, and K. Yoshida, eds., in Advances in Intelligent Systems and Computing, vol. 727, Singapore: Springer Singapore, pp. 187–195, 2019. doi: 10.1007/978-981-10-8863-6_19.

2. B. B. Haghighi, A. H. Taherinia, and R. Monsefi, "An effective semi-fragile watermarking method for image authentication based on lifting wavelet transform and feed-forward neural network," *Cogn. Comput.*, vol. 12, no. 4, pp. 863–890, 2020. doi: 10.1007/s12559-019-09700-9.
3. O. P. Singh, A. K. Singh, G. Srivastava, and N. Kumar, "Image watermarking using soft computing techniques: A comprehensive survey," *Multimed. Tools Appl.*, vol. 80, no. 20, pp. 30367–30398, 2021. doi: 10.1007/s11042-020-09606-x.
4. J. Liu *et al.*, "An optimized image watermarking method based on HD and SVD in DWT domain," *IEEE Access*, vol. 7, pp. 80849–80860, 2019. doi: 10.1109/ACCESS.2019.2915596.
5. S. Duan, H. Wang, Y. Liu, L. Huang, and X. Zhou, "A novel comprehensive watermarking scheme for color images," *Secur. Commun. Netw.*, vol. 2020, pp. 1–12, 2020. doi: 10.1155/2020/8840779.
6. A. Mehmood, A. Shafique, S. A. Chaudhry, M. Alawida, A. N. Khan, and N. Kumar, "A time-efficient and noise-resistant cryptosystem based on discrete wavelet transform and chaos theory: An application in image encryption," *J. Inf. Secur. Appl.*, vol. 78, p. 103590, 2023. doi: 10.1016/j.jisa.2023.103590.
7. K. Naik, S. Trivedy, and A. K. Pal, "An IWT based blind and robust image watermarking scheme using secret key matrix," *Multimed. Tools Appl.*, vol. 77, no. 11, pp. 13721–13752, 2018. doi: 10.1007/s11042-017-4986-1.
8. P. Kadian, S. M. Arora, and N. Arora, "Robust digital watermarking techniques for copyright protection of digital data: A survey," *Wirel. Pers. Commun.*, vol. 118, no. 4, pp. 3225–3249, 2021. doi: 10.1007/s11277-021-08177-w.
9. L. Rakhmawati, S. Suwadi, W. Wirawan, "Blind robust and self-embedding fragile image watermarking for image authentication and copyright protection with recovery capability," *Int. J. Intell. Eng. Syst.*, vol. 13, no. 5, pp. 197–210, 2020. doi: 10.22266/ijies2020.1031.18.
10. A. Singha and M. A. Ullah, "Transform domain digital watermarking with multiple images as watermarks," 2019. doi: 10.20944/preprints201910.0188.v1.
11. P. K. Muhuri, Z. Ashraf, and S. Goel, "A novel image steganographic method based on integer wavelet transformation and particle swarm optimization," *Appl. Soft Comput.*, vol. 92, p. 106257, 2020. doi: 10.1016/j.asoc.2020.106257.
12. F. Ernawan and D. Ariatmanto, "Image watermarking based on integer wavelet transform-singular value decomposition with variance pixels," *Int. J. Electr. Comput. Eng. IJECE*, vol. 9, no. 3, p. 2185, 2019. doi: 10.11591/ijece.v9i3.pp2185-2195.
13. S. B. B. Ahmadi, G. Zhang, M. Rabbani, L. Boukela, and H. Jelodar, "An intelligent and blind dual color image watermarking for authentication and copyright protection," *Appl. Intell.*, vol. 51, no. 3, pp. 1701–1732, 2021. doi: 10.1007/s10489-020-01903-0.
14. S. H. Farghaly and S. M. Ismail, "Floating-point discrete wavelet transform-based image compression on FPGA," *AEU - Int. J. Electron. Commun.*, vol. 124, p. 153363, 2020. doi: 10.1016/j.aeue.2020.153363.
15. H. A. Salman and A. Kalakech, "Image enhancement using convolution neural networks," *Babylonian Journal of Machine Learning*, pp. 30–47, 2024. 10.58496/BJML/2024/003.
16. S. M. Darwish and L. D. S. Al-Khafaji, "Dual watermarking for color images: A new image copyright protection model based on the fusion of successive and segmented watermarking," *Multimed. Tools Appl.*, vol. 79, no. 9–10, pp. 6503–6530, 2020. doi: 10.1007/s11042-019-08290-w.
17. P. Singh and S. Agarwal, "A self recoverable dual watermarking scheme for copyright protection and integrity verification," *Multimed. Tools Appl.*, vol. 76, no. 5, pp. 6389–6428, 2017. doi: 10.1007/s11042-015-3198-9.
18. H. Shi, M. Li, C. Guo, and R. Tan, "A region-adaptive semi-fragile dual watermarking scheme," *Multimed. Tools Appl.*, vol. 75, no. 1, pp. 465–495, 2016. doi: 10.1007/s11042-014-2301-y.
19. Y. Li, W. Song, X. Zhao, J. Wang and L. Zhao, "A novel image tamper detection and self-recovery algorithm based on watermarking and chaotic system," *Mathematics*, vol. 7, no. 10, p. 955, 2019. doi: 10.3390/math7100955.
20. H. Fang, H. Zhou, Z. Ma, W. Zhang, and N. Yu, "A robust image watermarking scheme in DCT domain based on adaptive texture direction quantization," *Multimed. Tools Appl.*, vol. 78, no. 7, pp. 8075–8089, 2019. doi: 10.1007/s11042-018-6596-y.
21. J. Gao, B. Wang, Z. Wang, Y. Wang, and F. Kong, "A wavelet transform-based image segmentation method," *Optik*, vol. 208, p. 164123, 2020. doi: 10.1016/j.ijleo.2019.164123.
22. H.-J. Ko, C.-T. Huang, G. Horng, and S.-J. Wang, "Robust and blind image watermarking in DCT domain using inter-block coefficient correlation," *Inf. Sci.*, vol. 517, pp. 128–147, 2020. doi: 10.1016/j.ins.2019.11.005.
23. 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.
24. F. Ernawan, N.A. Abu, and N. Suryana, "An adaptive JPEG image compression using psychovisual model," *Advanced Science Letters*, vol. 20, no. 1, pp. 26–31, 2014. doi: 10.1166/asl.2014.5255.
25. J. Ayad and M. A. Jalil, "Robust color image encryption using 3D chaotic maps and S-box algorithms," *Babylonian Journal of Networking*, pp. 148–161, 2024. doi: 10.58496/BJN/2024/015.