

Robust Image Watermarking Based on Lifting Wavelet Transform-Hessenberg Decomposition for Copyright Protection

Agung Sudrajat¹, Ferda Ernawan^{1,2}^{*}, Agit Amrullah³

¹Faculty of Information Technology, Universitas Nusa Mandiri,
Pasar Minggu Jakarta Selatan, Jakarta, 12540, INDONESIA

²Faculty of Computing, Universiti Malaysia Pahang Al-Sultan Abdullah
Pekan Pahang, 26600, MALAYSIA

³Faculty of Computer Science, Universitas AMIKOM,
Ring Road Utara Condong Catur Sleman, Yogyakarta, 55283, INDONESIA

*Corresponding Author: Ferda Ernawan

DOI: <https://doi.org/10.52866/ijcsm.2024.05.03.043>

Received April 2024; Accepted June 2024; Available online August 2024

ABSTRACT: The modern internet technology enables unauthorized individuals to alter the content of digital images. This work introduces a method for enhancing the robustness of an embedded watermark in images using Lifting Wavelet Transform (LWT) and Hessenberg Decomposition. This study utilizes Hessenberg Decomposition (HD) to insert a watermark image into the LL-sub band of the LWT transform. Singular Value Decomposition (SVD) is employed to convert the H value of HD. Subsequently, the watermark image is put into the singular value. The suggested system underwent testing against a range of image processing assaults, including compression, filters, and noise additions. The testing was conducted using multiple watermark sizes, specifically 256×256, 128×128, and 64×64 pixels. The experimental results demonstrate exceptional imperceptibility, with an average PSNR value of 39.5640 dB and a SSIM value of 0.9993. The results demonstrate a high level of resilience, as indicated by the NC value of 0.96390.

Keywords: watermark, copyright protection, image watermarking, hessenberg decomposition, lifting wavelet transform

1. INTRODUCTION

The dissemination of digital content is expanding at an accelerated rate due to developments in Internet technology. Software for image processing and digital image processing techniques can be used to edit and process digital images, allowing for the distribution of false images [1]. Misinformation can be readily manipulated and disseminated to the public by unauthorized users. Image watermarking is a method for protecting privacy while preserving image quality. For copyright protection, concealed confidential information is embedded within a watermark image [2]. Watermarks serve to authenticate, monitor, and safeguard digital content. They may manifest as logos, digital signatures, or concealed messages. Transformations, pixel value adjustments, and integration with other image components are some of the methods used in the watermarking process for digital images. Furthermore, this suggests a higher chance of copyright violations and forgeries [3]. Therefore, it is also essential to protect the authenticity and integrity of digital content. Digital content can be authenticated by image watermarking as well [4] and may gain benefit from image watermarking by being authentic, trackable, and protected from illegal alteration or reproduction [5] [6].

The utilization of Lifting Wavelet Transform (LWT) in image watermarking provides benefits the terms of signal image compression and efficient watermark embedding [7]. Nevertheless, there are still certain obstacles that must be confronted, such as ensuring the watermark's durability against compression and manipulation attacks [8]. When an image with a watermark is subjected to such attacks, the watermark may experience deformation or possibly be completely lost. Thus, it is necessary to employ methods that can sustain the integrity and visibility of the watermark in such circumstances [9]. In addition, it is necessary to consider the visual fidelity of the image [10]. Thus, researchers propose the use of a hybrid transform to enhance both the visual quality and robustness performance.

Liu et al. [11] introduced an enhanced technique for embedding watermarks into images using HD-SVD transformations in the DWT domain. The research shown notable progress in attaining a favorable balance between the resilience of the watermark and its imperceptibility through the utilization of the image watermarking technique that relies on DWT-HD-SVD. Nevertheless, the effectiveness of this DWT-based approach can be enhanced by integrating the Integer Wavelet Transform (IWT) to bolster its resilience.

Zhang et al. [12] introduced an algorithm that effectively resists rotation and other forms of assaults, while still meeting the usual criterion of invisibility for watermarking techniques. The algorithm has strong security performance. Moreover, Alotaibi and Elrefaei [13] suggest that their suggested technique has exceptional imperceptibility, especially when implemented on Arabic text-images. Their approach not only achieves a high level of invisibility but also exhibits resilience, especially when faced with compression and noise, hence enhancing its efficacy in many situations.

According to a study by Durafe and Patidar [14], even in cases when the size of the secret image is greater than double that of the cover fractal image, there is very little visual degradation (less than 0.6%) in their suggested technique. This solution not only minimizes the usage of network resources and memory space but also successfully guarantees durability in digital watermarking applications. Hu et al. [15] conducted a research investigation that demonstrated the impressive ability of their suggested watermarking method to withstand various image processing attacks and maintain its accuracy even when no attacks are present. Their approach surpasses current SVD-based methods in terms of clarity and resilience of the data, allowing for a payload capacity of 1/16-bit per pixel. Alshoura et al. [16] conducted a study where they introduced a new method for image watermarking. This method combines SVD-IWT and takes advantage of the chaotic features throughout the process of embedding the watermark. This technology is specifically devised to bolster the security and resilience of watermarks against many forms of attacks, such as compression, geometric processing, and others. By utilizing chaos-based algorithms, this approach effectively incorporates watermarks into images, resulting in watermarked images that demonstrate resistance to different types of attacks, hence enhancing the integrity of the watermark.

Zermi et al. [17] conducted a study that showcased the excellent invisibility and durability of watermarked images, which are highly resistant to several types of common attacks. Araghi and Manaf [18] presented a technique that combines the benefits of DWT-SVD to improve both the security and quality of watermarked images. The research affirms that employing a hybrid strategy that combines DWT-SVD can augment the security and integrity of both medical and non-medical images. Sharma et al. [19] demonstrated that the utilization of RDWT-SVD in combination with optimization based on ABC (Artificial Bee Colony) can dynamically improve the efficiency and safety of color image watermarking.

Meng et al. [20] utilized an adaptive approach to modify watermark embedding parameters according on image attributes and application specifications. The adaptive methodology employed in this technology enables efficient embedding of watermarks without compromising the visual image quality. Najafi and Loukhaoukha [21] established that the integration of SVD with local sharp frequency contourlet transform yields an effective and resilient image watermarking technique. Arunkumar et al. [22] demonstrated that employing a fusion of SVD, RIWT and DCT in a steganography method can bolster the security of transmitting medical images, guaranteeing both the integrity and confidentiality of the data. Hu and Lee [23] conducted research that confirmed the effectiveness of a frame-synchronized sound watermarking technique using adaptive modulation and perceptual-based modulation in the DWT domain. This method provides strong security and confidentiality for audio transmissions. In their study, Liya Zhu et al. [24] showed that the combination of block compressive sensing with SVD embedding can result in a secure and significant image encryption method.

This research proposed a watermarking strategy based on Lifting Wavelet Transform and Hessenberg Decomposition to enhance robustness performance. The watermark is incorporated into the single value of LWT-HD-SVD. The proposed scheme examines Lifting Wavelet Transform for embedding watermarks. The proposed scheme can achieve superior visual quality of the watermarked image and strong resilience against different types of attacks. The scheme will be assessed through a range of attacks, including image processing attacks, compression, filters, and noise enhancements. The experiments also investigate the performance of embedding watermarks with various sizes. The performance of imperceptibility and robustness has potential to be improved compared to the existing watermarking scheme. The proposed scheme is expected to achieve high NC value under various attacks. The research is organized into five sections. The following part delves into the theoretical background and the current methodologies. Section 3 examines the suggested process of incorporating and extracting a watermark. Section 4 provides an exposition of the experimental findings and subsequent discussions. Section 5 ultimately concludes a substantial investigation of this subject.

2. THEORETICAL FRAMEWORK

2.1 Lifting Wavelet Transform (LWT)

The lifting scheme has the capability to generate an impeccably reconstructed watermarking image [27]. The lifting wavelet transformation can be performed through three sequential stages: splitting, prediction, and updating. FIGURE 1 illustrates the lifting and inverse lifting operations.

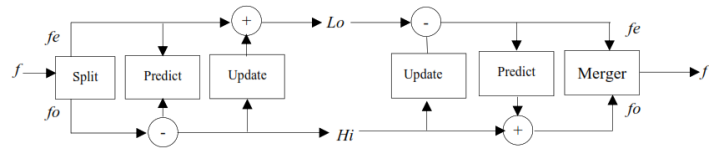


FIGURE 1. Lifting Wavelet Transform Operations

2.2 Hessenberg Decomposition (HD)

Hessenberg Decomposition HD is the procedure by which a square matrix is decomposed into the Hessenberg form, a unique and specific form. The Hessenberg form of a matrix is obtained by transforming all elements below the second diagonal to zero [28]. HD, or matrix reduction, is employed to convert a matrix into a more streamlined format, facilitating mathematical operations such as matrix multiplication and solving systems of linear equations. In addition, HD is useful for calculating the eigenvalues of a matrix. Through the utilization of high-definition (HD) technology, mathematical computations can be executed with greater efficiency and precision.

$$A = Q \cdot H \cdot QT \tag{1}$$

In the given context, Q represents an orthogonal matrix, while H denotes a Hessenberg matrix characterized by zero elements below the second sub diagonal. The HD method commences with a $n \times n$ square matrix. Throughout the process of decomposition, the elements that are not part of the Hessenberg form undergo a slow transformation into zeros. This procedure entails a sequence of matrix transformation operations aimed at streamlining the matrix's structure and removing superfluous members.

2.3 Singular Value Decomposition (SVD)

SVD is a technique in linear algebra used to break down a matrix into three primary components: the singular matrix, left singular vector, and right singular vector [29]. SVD finds application in diverse fields like data compression, factor analysis, and eigenvalue computations [30]. Within the realm of image processing, the single values of an image demonstrate robust stability, as they remain mostly unchanged even in the presence of slight disruptions to the image. SVD possesses the capability to unveil the underlying structure of a matrix and offer more profound understanding of data manipulation. The utilization of SVD involves the application of very efficient numerical techniques. Utilizing SVD provides advantages in revealing the underlying structure of data and enhancing comprehension in the field of data analysis. SVD is a frequently employed mathematical transformation in the field of numerical analysis. In a matrix A of size $M \times N$, with $M \geq N$, the matrix SVD equation is shown below as in equation (2).

$$A = USV^T \tag{2}$$

U represents an orthogonal matrix, S is a diagonal matrix with non-negative elements organised in decreasing order from top left to bottom right, and V is the transpose of another orthogonal matrix V. The benefit of utilizing SVD lies in the stability exhibited by the singular values. Having stable singular values implies that even with a minor disruption in the image, the values of the image will remain mostly unchanged. Hence, this technique is efficient for integrating concise data into an image.

2.4 Imperceptibility Evaluation

The important image quality evaluation metrics in this research are PSNR and SSIM. The measures are utilized to quantify the proximity between the watermarked image and the original image, as well as the visibility of the watermark [31]. The fundamental principles and application of these evaluation measures will be elucidated. PSNR is a quantitative measure utilized to assess the disparity between the intensity of the initial signal and the intensity of noise inside an image [31]. A greater PSNR value signifies reduced distortion between the original image and the watermarked image. PSNR is computed by comparing the pixel intensities of the original image with the watermarked image, considering the image's dynamic range.

The SSIM is a quantitative measure employed to assess the degree of structural similarity between the watermarked image and the source image [27]. SSIM incorporates structural elements such as texture, curves, and variations in pixel intensity. The SSIM values range from 0 to 1, with a value of 1 indicating complete resemblance between the original image and the watermarked image. Imperceptibility refers to the capacity of a methodology or procedure to preserve the visual quality and original attributes of a signal or image following the watermarking process. In the context of watermarking, imperceptibility refers to the quality of a watermark being added without causing substantial or discernible alterations that may be detected by the human eye. PSNR is a quantitative measure that

assesses the visual fidelity of an image by quantifying the discrepancy between the original, and the watermarked image.

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

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

The variables $o(x,y)$ and $w(x,y)$ represent the cover image and watermarked image, respectively. The variables x and y denote the pixel coordinates of the image. PSNR is determined by dividing the greatest signal energy by the noise energy, which is the squared difference between two images. PSNR values are quantified in decibels (dB), with higher values indicating superior visual quality of the image. PSNR is commonly employed as a metric for quantifying the level of distortion or errors present in processed images.

2.5 Structural Similarity Index Metric (SSIM)

The SSIM is a measurement of quantity that assesses the degree of structural similarity between two images [20]. SSIM compares the structural similarity of pixels and image statistics, including luminance, contrast, and spatial structure. SSIM values range from -1 to 1, with a value of 1 indicating perfect similarity between two images. A higher SSIM value indicates a greater similarity in the structure and information between the compared images. SSIM is a valuable tool for quantifying visual quality and assessing the level of resemblance between the original and processed images [20]. The formula for calculating SSIM is as follows:

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

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

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

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

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.

2.6 Robustness Evaluation

The robustness of watermark recovery is evaluated using NC, a metric that quantifies the correlation between the extracted watermark pixels and the original watermark pixels. Robustness, in the context of watermarking, pertains to the capacity of the watermark to endure or remain perceptible despite unauthorised attacks or alterations inflicted upon the signal or image. The objective of robustness is to guarantee the detectability of the watermark and the ability to extract it with a high level of accuracy, even in the presence of undesired modifications or attacks on the signal or image.

For evaluating the robustness of a watermarking technique, it can be tested against a range of typical attack or transformations [27]. Metrics such as NC, BER, or SSIM can quantify the degree of robustness and the capacity to retrieve watermarks from altered or compromised signals or images.

The evaluation of robustness can be conducted by assessing the BER and NC. NC and BER values are obtained by evaluating the watermarked image against different sorts of attacks. The NC is a quantitative measure that assesses the degree of connection between two images. NC is commonly employed to evaluate the accuracy of watermark retrieval or extraction from an image. The range of NC values is from -1 to 1. A value of 1 signifies a perfect correlation between the two images, a value of 0 suggests random correlation, and a value of -1 indicates inverse correlation. A greater NC value corresponds to a superior capacity to retrieve watermarks.

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

where $W(i,j)$ is the extracted watermark and $W'(i,j)$ is the original watermark. The NC value is a number between 0 and 1, where 0 denotes no correlation and 1 denotes a perfect match between the two watermarks. The robustness of the suggested watermarking system may be estimated and the degree to which two images match up can be ascertained by computing the NC between them. The research contribution is described as follows:

1. The proposed scheme enhances the robustness performance in terms of NC value compared to the existing benchmarks for various watermark sizes.
2. The proposed Lifting Wavelet Transform in image watermarking has improved the visual quality of the extracted watermark.

3. PROPOSED WATERMARKING SCHEME

The studies were performed using MATLAB R2022a on an Intel Core i7 equipped with 16 GB of RAM. The experiment uses eight Host images, each with dimensions of 512×512 pixels, as seen in FIGURE 2. The eight host images are Lena, Peppers, Barbara, Cameramen, Elaine, Mailight, Greenpeace, and Sailboat. The experiment employs watermark images of varying sizes, specifically 256×256 , 128×128 , and 64×64 pixels, as depicted in FIGURE 3.

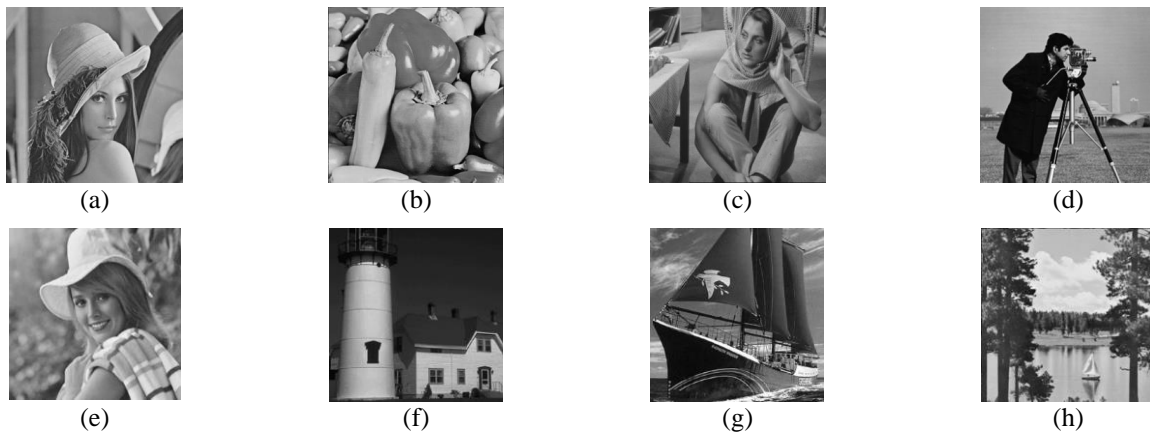


FIGURE 2. Host Images: (a) Lena, (b) Pepper, (c) Barbara, (d) Cameramen, (e) Elaine, (f) Malight, (g) Greenpeace, (h) Sailboat.

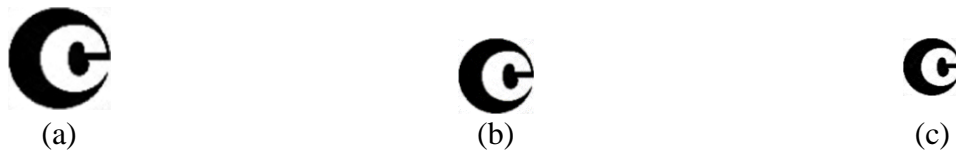


FIGURE 3. Watermark image with size of (a) 256×256 , (b) 128×128 , (c) 64×64

3.1 Watermark Extraction Procedure

The process of embedding a watermark is an essential step in safeguarding the copyright of digital work by injecting a distinct mark into it. Figure 4 displays the block diagram illustrating the process of embedding a watermark. As depicted in FIGURE 4, the process of embedding a watermark is delineated as follows:

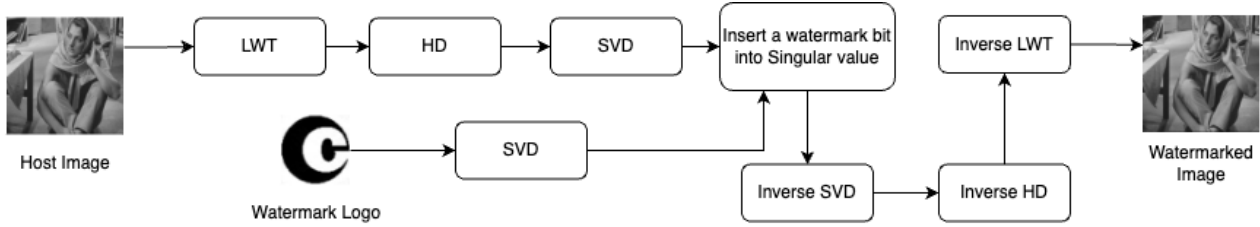


FIGURE 4. Proposed Watermark Embedding Procedure

Watermark embedding procedure:

Step 1: An image is computed by R-level Haar wavelet and decompose image as follows:

$$[LL, HL, LH, HH] = dwt2(coverImage, 'haar') \tag{10}$$

Step 2: The LL sub-band is then performed by Hessenberg Decomposition (HD) to obtain P and H. The LL subband tends to exhibit more predictable and stable statistical characteristics compared to other subbands as follow:

$$[P, H] = hess(LL) \tag{11}$$

Step 3: Select H coefficients of HD to be computed by using SVD to generate sub-bands HUw, HSw, and HVw as follow:

$$[HUw, HSw, HVw] = svd(H) \tag{12}$$

Step 4: Watermark logo is transformed by using SVD to generate sub-bands Uw, Sw, and Vw as follow:

$$[Uw, Sw, Vw] = svd(watermarkLogo) \tag{13}$$

Step 5: Embed a watermark into singular value of sub-band HSw and Sw with a scaling factor α .

$$HSW = HSw + \alpha Sw \tag{14}$$

Step 6: Perform inverse SVD to obtain watermarked H.

$$WH = HUw \times HSW \times HVw \tag{15}$$

Step 7: Compute inverse Hessenberg Decomposition to obtain watermarked LL.

$$LLW = P \times WH \tag{16}$$

Step 8: Reconstructed LL band based on inverse R-level Haar wavelet to obtain watermarked image as follow:

$$watermarkedImages = idwt(LLW, HL, LH, HH) \tag{17}$$

3.2 Watermark Extraction Procedure

The watermark extraction procedure is shown in FIGURE 5. The step-by-step of extracting watermark is defined by:

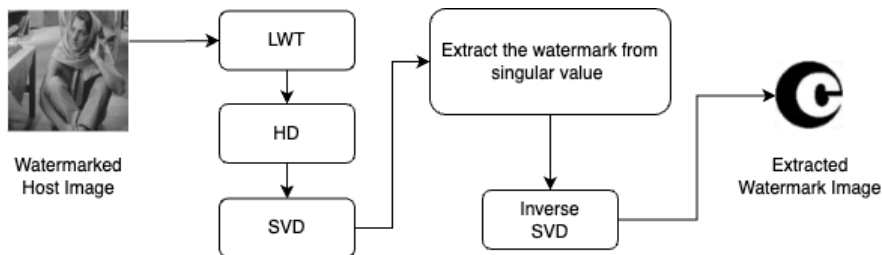


FIGURE 5. Proposed Watermark Extraction Procedure

Watermark extraction procedure:

Step 1: Watermarked image is computed by R-level Haar wavelet as follows:

$$[LL, HL, LH, HH] = dwt2(watermarkedimage, 'haar') \tag{18}$$

Step 2: The LL sub-band is computed Hessenberg Decomposition (HD) to obtain H.

$$[P, H] = hess(LL) \tag{19}$$

Step 3: H coefficient of HD is then transformed by using SVD to generate sub-bands HU, HS, and HV.

$$[HU, HS, HV] = svd(H) \tag{20}$$

Step 4: Extract the watermark singular value as defined by:

$$HSw = \frac{HS - HS_w}{\alpha} \tag{21}$$

Step 5: Extract watermark image by computing the inverse of SVD as defined by:

$$extractedWatermark = uint8(HU \times HSw \times HV) \tag{22}$$

After conducting a comparison between the unaltered images and the images that have been marked with a watermark, it may be deduced that the watermark has been effectively rendered imperceptible. There are little discernible variations between the original image and the watermarked images in the eight examined test images. Hence, the technique of embedding watermarks successfully maintains the visual integrity of the images, ensuring the security of the embedded information without altering the original visual look.

The experimental findings display the values of the Structural Similarity Index (SSIM) based on the eight images that were evaluated. The SSIM metric is employed to quantify the degree to which the visual fidelity of watermarked images may be maintained in comparison to the original images. Below are the findings of the comparison for the eight assessed images.

Table 1. Comparison of SSIM value for different watermark sizes

Host Image	Watermark Size					
	256×256		128×128		64×64	
	Liu et al. [11]	Proposed	Liu et al. [11]	Proposed	Liu et al. [11]	Proposed
Lena	0.99975	0.99935	0.99986	0.99937	0.99994	0.99934
Pepper	0.99970	0.99927	0.99994	0.99927	0.99990	0.99924
Barbara	0.99973	0.99934	0.99990	0.99936	0.99993	0.99931
Cameramen	0.99949	0.99869	0.99993	0.99874	0.99995	0.99879
Elaine	0.99978	0.99949	0.99990	0.99948	0.99993	0.99946
Malight	0.99957	0.99922	0.99996	0.99929	0.99996	0.99926
Greenpeace	0.99987	0.99952	0.99995	0.99954	0.99999	0.99952
Sailboat	0.99969	0.99932	0.99995	0.99936	0.99991	0.99934

While the SSIM values in these results are lower compared to previous studies, it is essential to emphasize that this process exhibits a higher level of robustness. Although the visual differences between the original and processed images might be more noticeable, the reliability in preserving the embedded information under various attacks is higher. This indicates that, despite the lower SSIM values, this process may be more suitable for situations where reliability and resistance to attacks are the primary priorities.

Table 1 displays the host images with embedded watermarks without any attacks, along with the extracted watermarks with sizes of 256×256, 128×128, and 64×64 pixels. The PSNR, SSIM, and NC values are recorded in Table 1. In general, if PSNR>39dB, the host image with the embedded watermark is acceptable, indicating that the watermark is not visible to the human visual system. Furthermore, if SSIM>0.93, the host image with the embedded watermark has a minimal difference from the original host image.

Table 2. The quality of the watermarked images for different watermark sizes of 64×64, 128×128, 256×256 pixels

Host Images	PSNR			SSIM		
	64×64	128×128	256×256	64×64	128×128	256×256
Lena	39.5529	39.5473	39.5467	0.99934	0.99937	0.99935
Pepper	39.5535	39.5248	39.5242	0.99924	0.99927	0.99927
Barbara	39.5731	39.5632	39.5508	0.99931	0.99936	0.99934
Cameramen	39.6483	39.6097	39.6013	0.99879	0.99874	0.99869
Elaine	39.5997	39.5831	39.5774	0.99946	0.99948	0.99949
Malight	39.5323	39.5217	39.5278	0.99926	0.99929	0.99922
Greenpeace	39.6164	39.582	39.597	0.99952	0.99954	0.99952
Sailboat	39.5463	39.532	39.5235	0.99934	0.99936	0.99932

Based on the examination of the findings presented in Table 2, it can be obtained that a PSNR value above 39 dB. It indicates that the watermarked host image has satisfactory quality and is not visually detectable by humans. This indicates that the intended level of imperceptibility has been successfully achieved in the host images that were tested.

3.3 Robustness

Robustness in the context of watermarking or image processing refers to the ability to maintain the integrity and recognizability of embedded or processed information, even under adverse conditions or in the face of deliberate attempts to interfere with or corrupt it. Robustness is the ability to withstand and overcome challenges or attacks that




















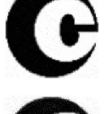










may occur, such image compression, format alterations, cropping, noise introduction, and various forms of manipulation or other attacks.

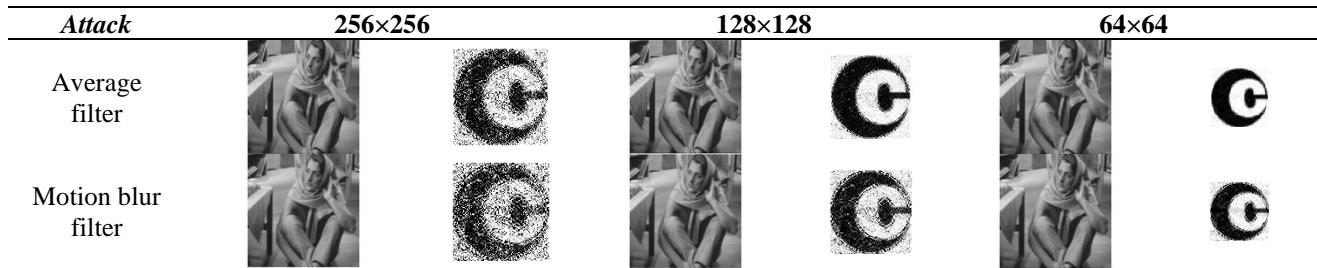
Robustness, in essence, pertains to the capacity of a system or method to uphold the integrity and validity of the embedded or processed information, even in adverse circumstances or in the presence of undesired alterations. The objective is to guarantee that the outcomes of the process or embedding remain identifiable and valuable without compromising their excellence or credibility, delivering consistent and dependable results across different environmental circumstances and application scenarios.

In the testing phase as shown in Table 3, the "Barbara" image, which has been subjected to various attacks, will be evaluated using sizes of 256×256, 128×128, and 64×64 pixels. The purpose of this testing is to assess the level of success and robustness of the method or system in retaining the embedded information in the image, irrespective of any attacks that may compromise or disrupt the image's quality.

This testing will encompass various attacks that may include changes in image quality, compression, noise addition, and other forms of attacks. The test findings will be utilized to evaluate the method or system's ability to withstand and manage these attacks, as well as the watermarked image's capacity to retain the integrity and imperceptibility of the watermark in the presence of diverse challenges.

Table 3. Extracting the watermark from the Barbara images that have been attacked with various watermarks sizes.

<i>Attack</i>	256×256	128×128	64×64
Wiener filter			
Gaussian low-pass filter			
Median filter			
Gaussian noise filter			
Salt and Pepper noise			
Speckle noise			
JPEG compression filter			
JPEG2000 compression filter			
Sharpening attack filter			
Histogram equalization filter			



Robustness needs to be further evaluated once imperceptibility is achieved. The capacity of a system to maintain stability despite modifications to its initial configuration is denoted by its robustness. Robustness in image watermarking systems refers to the capacity to successfully retrieve the watermark from the watermarked host image despite encountering different types of attacks. Hence, it is crucial to authenticate the resilience of an image watermarking technique. In order to assess the resilience of the suggested approach, the fidelity of the extracted watermark is examined under several forms of image tampering applied to the watermarked image. Furthermore, a thorough assessment of the extracted watermark is also performed.

The test results demonstrated a fascinating comparison between the "Barbara" images that have been attacked using watermarks with various sizes, namely 256×256, 128×128, and 64×64 pixels as shown in Table 4. Confronted with various attacks such as alterations in image quality, compression, noise introduction, and other forms of attacks, the approach or system has exhibited a notable degree of resilience. Therefore, these test findings offer compelling proof that the method or system demonstrates a significant degree of resilience in handling typical image attacks while maintaining the integrity and genuineness of the embedded information in the images.

Table 4. The NC comparison results between the proposed method and other methods.

Attack	256×256		128×128		64×64	
	Liu et al. [11]	Proposed	Liu et al. [11]	Proposed	Liu et al. [11]	Proposed
Wiener filter	0.90273	0.96537	0.95130	0.99606	0.85977	0.99853
Gaussian low-pass filter	0.70132	0.81108	0.78039	0.95897	0.77528	0.99367
Median filter	0.84847	0.93006	0.92294	0.99224	0.88678	0.99787
Gaussian noise filter	0.91344	0.97078	0.96264	0.99585	0.93127	0.99913
Salt and Pepper noise	0.98603	0.99528	0.99281	0.99932	0.96371	0.99960
Speckle noise	0.90383	0.96554	0.95005	0.99588	0.94027	0.99876
JPEG compression filter	0.99897	0.99973	0.99692	0.99977	0.96200	0.99966
JPEG2000 compression filter	0.99854	0.99702	0.97590	0.99830	0.96325	0.99930
Sharpening attack filter	0.92938	0.97683	0.97552	0.99730	0.96077	0.99939
Histogram equalization filter	0.93671	0.95319	0.93865	0.96832	0.93606	0.96594
Average filter	0.69954	0.80943	0.77772	0.95804	0.77266	0.99346
Motion blur filter	0.61909	0.72646	0.59487	0.85384	0.50640	0.94035

This research involved the examination of various attack or filters that were implemented on images with dimensions of 256×256, 128×128, and 64×64 pixels. The Normalised Correlation (NC) metric was utilised to quantify the extent of information loss or distortion in the images. A greater numerical coefficient (NC) value signifies superior preservation of image quality following the application of an attack or filter. The experiments conducted on multiple prevalent image processing attacks or filters, yielding insights into the impact of these attacks or filters on image quality across different dimensions. Regardless of the image dimensions, each form of attack generated results with high NC values. This indicates that these attacks or filters effectively maintain image quality while minimizing distortion or loss of information.

The findings of this experiment provide useful insights into the effects of attack or filters on image quality as measured by the NC metric. This knowledge can aid in choosing the suitable attacks or filters to fulfil the requirements of an application or accomplish certain objectives, such as safeguarding image integrity or minimising distortion during image processing. The visualise NC value under various attacks for watermark size of 256×256, 128×128, and 64×64 pixels is shown in FIGURE 6.

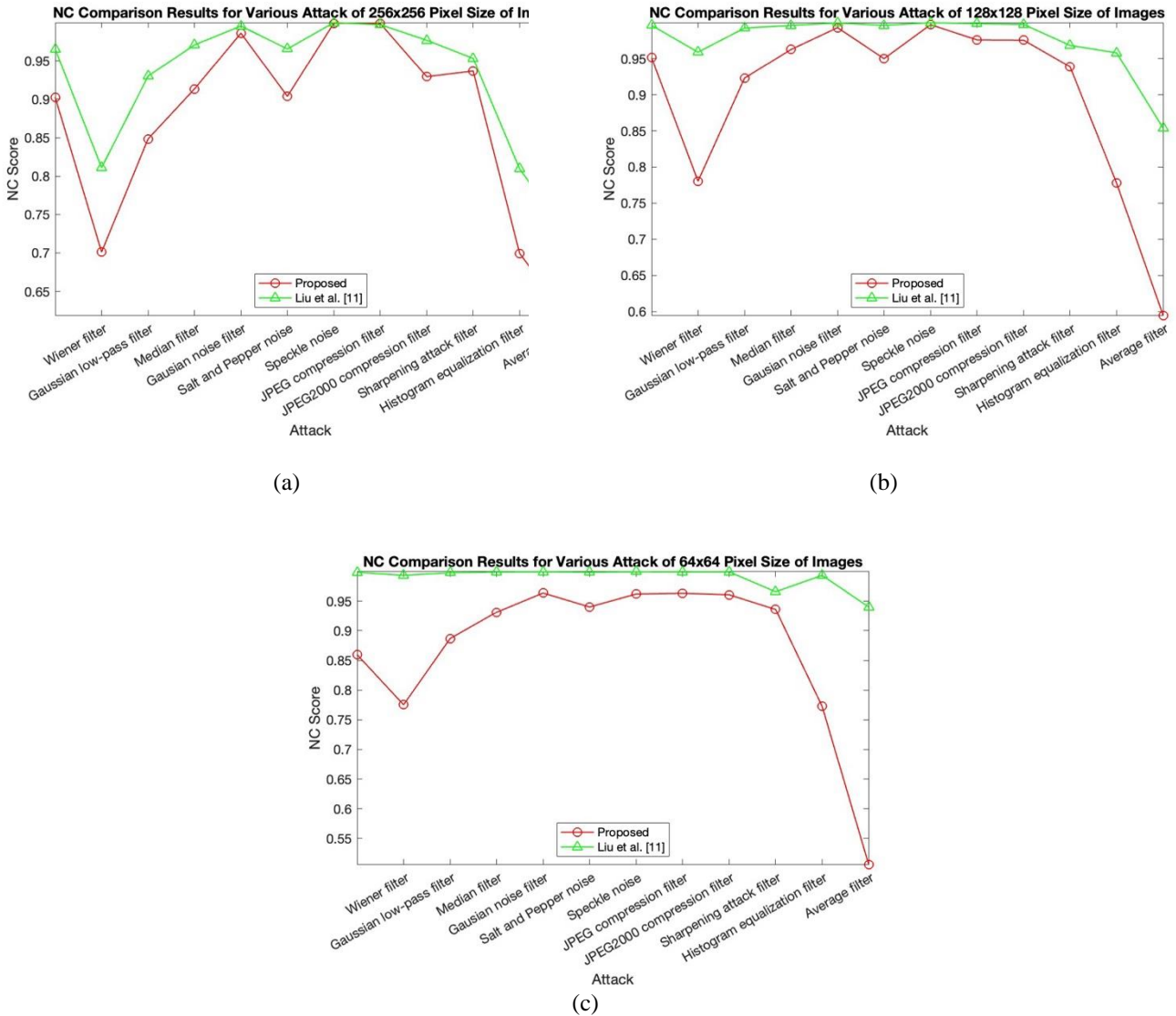


FIGURE 6. Comparison results of NC score against various attacks for different watermark sizes

4. CONCLUSION

This paper has presented embedding watermark based on LWT-HD. The testing results demonstrate that the suggested approach offers superior imperceptibility. The outcomes involve the preservation of image quality following the application of assaults or filters. Utilising techniques such as the filtered image, noise addition and compression result in increased NC values when applying IWT to images. This indicates a reduced level of distortion or loss of information. The results demonstrate that IWT tends to generate images that retain a relatively high level of visual quality even after being subjected to attacks or filters. The IWT transformation preserves image features and sharpness, yielding images of relatively high quality. LWT enables dynamic modifications to the scale throughout the process of embedding or extracting watermarks. By choosing the suitable scale factors, one can attain a compromise between the resilience of the watermark and the best possible visual quality.

Funding

None

ACKNOWLEDGEMENT

This work was supported by the Ministry of Higher Education for providing financial support under Fundamental Research Grant Scheme (FRGS), No FRGS/1/2023/ICT04/UMP/02/1 (University reference RDU230121).

CONFLICTS OF INTEREST

The author declares no conflict of interest.

REFERENCES

- [1] S. Sharma, J. J. Zou, and G. Fang, "A Novel Multipurpose Watermarking Scheme Capable of Protecting and Authenticating Images with Tamper Detection and Localisation Abilities," *IEEE Access*, vol. 10, pp. 85677–85700, 2022, doi: 10.1109/ACCESS.2022.3198963.
- [2] W. Lu, L. Li, Y. He, J. Wei, and N. N. Xiong, "RFPS: A Robust Feature Points Detection of Audio Watermarking for against Desynchronization Attacks in Cyber Security," *IEEE Access*, vol. 8, pp. 63643–63653, 2020, doi: 10.1109/ACCESS.2020.2984283.
- [3] R. Wang, C. Lin, Q. Zhao, and F. Zhu, "Watermark Faker: Towards Forgery Of Digital Image Watermarking," in *Proceedings - IEEE International Conference on Multimedia and Expo*, IEEE Computer Society, 2021. doi: 10.1109/ICME51207.2021.9428410.
- [4] S. Gupta, K. Saluja, V. Solanki, K. Kaur, P. Singla, and M. Shahid, "Efficient methods for digital image watermarking and information embedding," *Measurement: Sensors*, vol. 24, Dec. 2022, doi: 10.1016/j.measen.2022.100520.
- [5] G. Dhevanandhini and G. Yamuna, "An effective and secure video watermarking using hybrid technique," *Multimed Syst*, vol. 27, no. 5, pp. 953–967, Oct. 2021, doi: 10.1007/s00530-021-00765-x.
- [6] H. Rhayma, A. Makhloufi, H. Hamam, and A. Ben Hamida, "Semi-fragile watermarking scheme based on perceptual hash function (PHF) for image tampering detection," *Multimed Tools Appl*, vol. 80, no. 17, pp. 26813–26832, Jul. 2021, doi: 10.1007/s11042-021-10886-0.
- [7] P. Kadian, S. M. Arora, and N. Arora, "Robust Digital Watermarking Techniques for Copyright Protection of Digital Data: A Survey," *Wireless Personal Communications*, vol. 118, no. 4. Springer, pp. 3225–3249, Jun. 01, 2021. doi: 10.1007/s11277-021-08177-w.
- [8] R. Hu and S. Xiang, "Cover-lossless robust image watermarking against geometric deformations," *IEEE Transactions on Image Processing*, vol. 30, pp. 318–331, 2021, doi: 10.1109/TIP.2020.3036727.
- [9] W. Sun, J. Zhou, Y. Li, M. Cheung, and J. She, "Robust High-Capacity Watermarking over Online Social Network Shared Images," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 31, no. 3, pp. 1208–1221, Mar. 2021, doi: 10.1109/TCSVT.2020.2998476.
- [10] T. Zhu, W. Qu, and W. Cao, "An optimized image watermarking algorithm based on SVD and IWT," *Journal of Supercomputing*, vol. 78, no. 1, pp. 222–237, Jan. 2022, doi: 10.1007/s11227-021-03886-2.
- [11] J. Liu, J. Huang, Y. Luo, L. Cao, S. Yang, D. Wei, and R. Zhou, "An optimized image watermarking method based on HD and SVD in DWT domain," *IEEE Access*, vol. 7, pp. 80849–80860, 2019.
- [12] Z. Li, H. Zhang, X. Liu, C. Wang, and X. Wang, "Blind and safety-enhanced dual watermarking algorithm with chaotic system encryption based on RHF and DWT-DCT," *Digital Signal Processing: A Review Journal*, vol. 115, Aug. 2021, doi: 10.1016/j.dsp.2021.103062.
- [13] R. A. Alotaibi and L. A. Elrefaie, "Text-image watermarking based on integer wavelet transform (IWT) and discrete cosine transform (DCT)," *Applied Computing and Informatics*, vol. 15, no. 2, pp. 191–202, Jul. 2019, doi: 10.1016/j.aci.2018.06.003.
- [14] A. Durafe and V. Patidar, "Development and analysis of IWT-SVD and DWT-SVD steganography using fractal cover," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 7, pp. 4483–4498, Jul. 2022, doi: 10.1016/j.jksuci.2020.10.008.
- [15] H. T. Hu, L. Y. Hsu, and H. H. Chou, "An improved SVD-based blind color image watermarking algorithm with mixed modulation incorporated," *Inf Sci (N Y)*, vol. 519, pp. 161–182, May 2020, doi: 10.1016/j.ins.2020.01.019.
- [16] W. H. Alshoura, Z. Zainol, J. Sen Teh, and M. Alawida, "A New Chaotic Image Watermarking Scheme Based on SVD and IWT," *IEEE Access*, vol. 8, pp. 43391–43406, 2020, doi: 10.1109/ACCESS.2020.2978186.
- [17] N. Zermi, A. Khaldi, R. Kafi, F. Kahlessenane, and S. Euschi, "A DWT-SVD based robust digital watermarking for medical image security," *Forensic Sci Int*, vol. 320, Mar. 2021, doi: 10.1016/j.forsciint.2021.110691.
- [18] T. K. Araghi and A. A. Manaf, "An enhanced hybrid image watermarking scheme for security of medical and non-medical images based on DWT and 2-D SVD," *Future Generation Computer Systems*, vol. 101, pp. 1223–1246, Dec. 2019, doi: 10.1016/j.future.2019.07.064.
- [19] S. Sharma, H. Sharma, and J. B. Sharma, "An adaptive color image watermarking using RDWT-SVD and artificial bee colony based quality metric strength factor optimization," *Applied Soft Computing Journal*, vol. 84, Nov. 2019, doi: 10.1016/j.asoc.2019.105696.
- [20] L. Meng, L. Liu, G. Tian, and X. Wang, "An adaptive reversible watermarking in IWT domain," *Multimed Tools Appl*, vol. 80, no. 1, pp. 711–735, Jan. 2021, doi: 10.1007/s11042-020-09686-9.
- [21] E. Najafi and K. Loukhaoukha, "Hybrid secure and robust image watermarking scheme based on SVD and sharp frequency localized contourlet transform," *Journal of Information Security and Applications*, vol. 44, pp. 144–156, Feb. 2019, doi: 10.1016/j.jisa.2018.12.002.

- [22] S. Arunkumar, V. Subramaniaswamy, V. Vijayakumar, N. Chilamkurti, and R. Logesh, "SVD-based robust image steganographic scheme using RIWT and DCT for secure transmission of medical images," *Measurement (Lond)*, vol. 139, pp. 426–437, Jun. 2019, doi: 10.1016/j.measurement.2019.02.069.
- [23] H. T. Hu and T. T. Lee, "Frame-synchronized blind speech watermarking via improved adaptive mean modulation and perceptual-based additive modulation in DWT domain," *Digital Signal Processing: A Review Journal*, vol. 87, pp. 75–85, Apr. 2019, doi: 10.1016/j.dsp.2019.01.006.
- [24] L. Zhu, H. Song, X. Zhang, M. Yan, T. Zhang, X. Wang, and J. Xu, "A robust meaningful image encryption scheme based on block compressive sensing and SVD embedding," *Signal Processing*, vol. 175, pp. 107629, 2020.
- [25] D. G. Savakar and A. Ghuli, "Robust Invisible Digital Image Watermarking Using Hybrid Scheme," *Arab J Sci Eng*, vol. 44, no. 4, pp. 3995–4008, Apr. 2019, doi: 10.1007/s13369-019-03751-8.
- [26] O. Evsutin, A. Melman, and R. Meshcheryakov, "Digital steganography and watermarking for digital images: A review of current research directions," *IEEE Access*, vol. 8, pp. 166589–166611, 2020, doi: 10.1109/ACCESS.2020.3022779.
- [27] 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, Jun. 2019, doi: 10.11591/ijece.v9i3.pp2185-2195.
- [28] O. P. Singh and A. K. Singh, "A robust information hiding algorithm based on lossless encryption and NSCT-HD-SVD," *Mach Vis Appl*, vol. 32, no. 4, Jul. 2021, doi: 10.1007/s00138-021-01227-0.
- [29] Y. Luo *et al.*, "A multi-scale image watermarking based on integer wavelet transform and singular value decomposition," *Expert Syst Appl*, vol. 168, Apr. 2021, doi: 10.1016/j.eswa.2020.114272.
- [30] M. Begum, J. Ferdush, and M. S. Uddin, "A Hybrid robust watermarking system based on discrete cosine transform, discrete wavelet transform, and singular value decomposition," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 8, pp. 5856–5867, Sep. 2022, doi: 10.1016/j.jksuci.2021.07.012.
- [31] F. Ernawan and M. N. Kabir, "A block-based RDWT-SVD image watermarking method using human visual system characteristics," *Visual Computer*, vol. 36, no. 1, pp. 19–37, Jan. 2020, doi: 10.1007/s00371-018-1567-x.