Hindawi
Applied Bionics and Biomechanics
Volume 2022, Article ID 5271600, 13 pages
https://doi.org/10.1155/2022/5271600

Research Article

Enhanced Invisibility and Robustness of Digital Image Watermarking Based on DWT-SVD

Ali Alzahrani

Department of Computer Engineering, King Faisal University, Al-Ahsa, Saudi Arabia

Correspondence should be addressed to Ali Alzahrani; aalzahrani@kfu.edu.sa

Received 27 November 2021; Revised 18 December 2021; Accepted 27 December 2021; Published 28 January 2022

Academic Editor: Fahd Abd Algalil

The propagation of digital media over the Internet has helped improve digitization, which has given an excessive lead to copyright issues. Digital watermarking techniques have been applied to address copyright issues. In research, a system is being developed to handle veracious types of watermarked attacks, for obtaining extreme security and an adequate level of visibility and robustness. The discrete wave transform (DWT) and singular value decomposition (SVD) approaches were applied to analyze veracious types of attacks. The DWT method was used to embed the host image in four levels; this level was processed using the SVD method. The peak signal-to-noise ratio (PSNR) and structural similarity index measure (SSIM) were applied to measure the invisibility, and the normalization correlation (NC) was used to examine the robustness of watermarked images. The empirical results showed that the proposed DWT-SVD achieved superior accuracy in identifying the various attacks. The proposed DWT-SVD performance was confirmed during the training process, and the proposed system was shown to have high invisibility and robustness against various types of attacks on watermarked images. Finally, the results of the proposed system were compared to existing systems, and it was shown that DWT-SVD achieved better performance in terms of pixel-value modification attacks.

1. Introduction

Electronic document safeguarding was and remains one of the most critical problems in scientific investigation. With the development of Internet technologies, intruders are illegally duplicating, authenticating, and distributing digital materials. Watermarking technologies have thus been investigated for a variety of purposes, including broadcasting, tracking, intellectual property protection, document verification, and copying restriction [1]. With the extensive posting and distribution of electronic information on the Internet, breaches of copyrights, unauthorized usage, reproduction, and online content theft have become more common. Digital images represent high-value-added resources, which involve the protection of their intellectual property copyrights. However, digital watermarking [2] is considered a current and useful technology for protection of such images. Watermarking technique (WM) can be employed to encode the owner's data, which is then preserved or circulated on the Internet. This technique is used to assert proprietorship through retrieving the encoded watermark data when needed, as per the current technologies, applications fields, and other online platform-based systems. Limited studies have been investigated for digital watermarking images. Recently, different approaches have been be implemented to perform watermark embedding, and extracting the WM from the digital image algorithmically or changing it has been introduced [3–9]. Generally, watermarking may be subjected to a harmful attack aimed at destroying or removing the encoded WM data, as well as a nonmalicious attack through procedures that must be used to preserve or circulate the content. As a result, WM embedding could be accomplished in either an algorithmic or a mechanistic manner. WM extraction, on the other hand, has a different scenarios. The WM-incorporated host information may be destroyed as a result of malicious or nonmalicious cyberattacks, and the embedded WM data might be lost. As a result, extracting the WM programmatically or sequentially may well not be effective, and a statistical technique may provide better performance.

One or two merged watermark images can be formed through a sort of semisequence received from such a

pseudorandom cryptographic security. A monochrome or unicolor image can be used as a watermark. Scattered spectral (SS) [10–12] and quantization index manipulation (QIM) [13] are two content protection systems for watermarking schemes, which are commonly characterized as cumulative and alternative, respectively. STDM (spread transform dither modulation) [14] is a type of QIM that is particularly resistant to requantization and external disturbance intrusions. STDM unites the reliability of SS with the efficiency of QIM. The payload, reliability, and authenticity of watermarking techniques are all important aspects. As a result, transformation domains, including singular value segmentation (SVD), discrete cosine transform (DCT), and discrete wave transform (DWT), are frequently employed. The spatial domain is less reliable than that of the DCT type, particularly versus processes like brightening, softening, and noise reduction filtering [15]. In addition, DWT is growing in popularity given its ability to facilitate transformation, which greatly strengthens the security of watermarked digital images. The DWT domain divides the image into several resolution levels and a starting set of processes ranging from highest to lowest resolution [16]. The measure of durability is thus increased by masking watermarks using greater intensity during digital images. Currently, SVD is broadly applied to the watermarking of digital images. SVD maintains the covered image's visualization, as well as its sturdiness against numerous forms of attack [17, 18]. As computer systems and servers continue to come closer to utilizing human-level skills, the fields of machine learning (ML) and learning techniques have also developed in recent years. Today, companies have already begun seeking opportunities to leverage their enormous datasets, such as a test platform for developing algorithms that can engage with the environment in much more practical ways and retrieve heretofore undiscovered insights. Numerous difficulties in speech signal analysis, image processing, computational linguistics, and natural language processing (NLP) can be solved with deep learning- (DL-) based neural network (NN) methods [19–22].

In addition, the convolutional neural network (CNN), a form of deep neural network, has already been utilized, largely for image recognition, fragmentation, categorization, and certain other autocorrelated data analysis [23]. Noise removal from and enhanced clarity of images are two digital image processing techniques of considerable significance that can increase image quality. Neural networks have recently been used to enhance deblurring effectiveness and accuracy by establishing mappings among clear and distorted images [24–27]. CNN can obtain successful results for image denoising, achieving promising outcomes that can be attributed to its massive modeling capability and significant breakthroughs in the training process in the network and design. CNN, using a deep structure model, improves the training phase and noise removal by increasing the capability to leverage image features. Batch normalization and the rectified linear unit (RLU) represent two learning strategies for developing and training CNN, which have made significant progress. Given that an embedded watermark is essentially a chain of noise implanted in an image, this form of noise removal could likely damage the image.

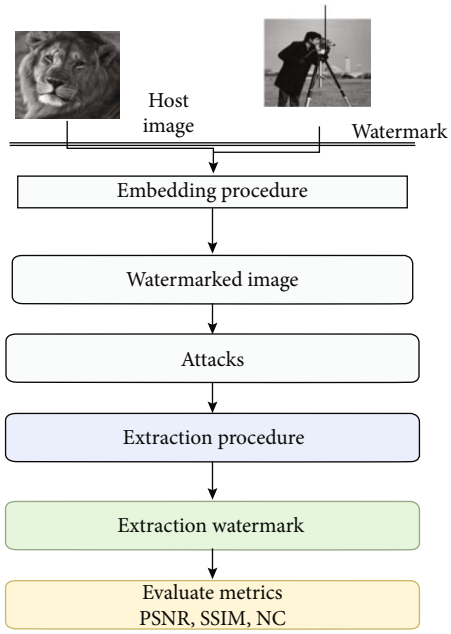

Figure 1: Proposed system.

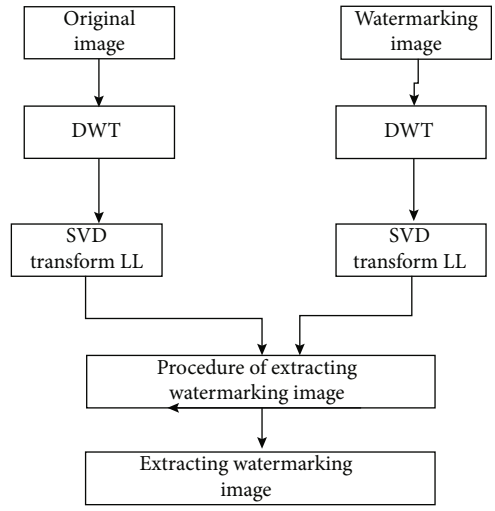

Figure 2: The watermark embedding procedure.

Because it extracts the initial value for every pixel contained in a given image, image enhancement and noise removal present serious opportunities for attacks on digitized embedded watermark images [28–30]. The effectiveness of a fully convolutional neural network (FCNN) over watermarked images was investigated in the present study. We sought to determine whether the normalization of denoising could be utilized as a unique sort of attack through the computerized digital watermarking of images by comparing it to the SS and STDM watermarking approaches.

The digital watermarking images have various forms of attacks, including loss compression, additive noise, geometric deformation, and background subtraction attacks, which may potentially influence watermarked digital images [31, 32]. Salt-and-pepper noise and multiplicative Gaussian noise

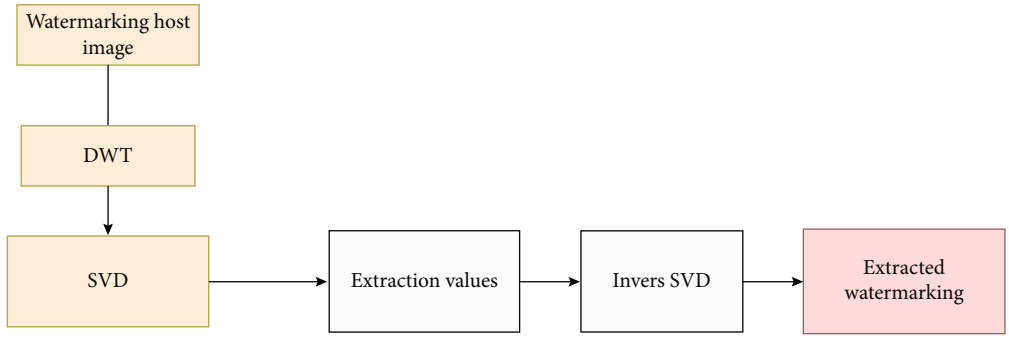

Figure 3: Feature extracting procedure.

Table 1: System requirements.

Hardware	Software
RAM 8 GB	MATLAB R2020a
CPU I7	Windows 10

attacks are the most popular noises that threaten digital watermarking images. For a simple 8-bit grayscale image, salt-and-pepper noises modify the value of each pixel into 0 or 255 (white and white), while cumulative Gaussian noises lower the quality of an image's visual appearance. Image-filtering attacks using averaging, Wiener, median, and Gaussian filtration can effectively erase a watermark that was embedded in a digital image. The median filter is defined as a nonlinear adaptive filtering approach that maintains an image's boundaries while eliminating noise. The Wiener filter is widely used to remove blur from images. The averaging filter lowers brightness variance among pixels by substituting every pixel's value well with the weighted mean of its own neighbors and itself. The Gaussian filter is commonly adopted to blur images while reducing intensity and distortion. Geometric attacks can cause image distortions generated through processes including scaling, rotating, clipping, and translating [33, 34]. Geometric attacks are divided into two categories: local and global. Local geometric threats, namely, chopping attacks, influence parts of the image, whereas global geometric attacks, like rotational and scale attacks, disrupt every pixel in an image. To enhance the durability of different types of geometric attacks, numerous methods have been proposed.

Li et al. [35] proposed a wavelet tree quantization-based blind image using a stenographic approach to improve resistance against geometric distortions, including rotating, resizing, and cutting. Focusing mostly on SVD and the distribution of DWT, Liu et al. [36] proposed scalable multiscale full-band-based image watermarking. Cropping and rotating attacks are not a problem for this approach. Li [37] developed a computer-created hologram-based image watermarking system that is resistant to cryptographic attacks such as translating, rotating, chopping, tilting, and resizing. He et al. [38] suggested a geometrically robust image watermarking technique depending on histogram manipulation, encompassing rotating, cropping, and resizing as well as translation bouts. Regarding the mitigation of geometrical attack, Fazli and Moeini [39] have provided a durable-image watermarking system. There are a number of methods used to embed a host image, such as DWT and SVD methods, as well as DCT [40–45]. Furthermore, some authors have used discrete Fourier transform (DFT) [12–14] to embed host images, proposed DWT [46–48], and presented singular value SVD [49–51]. This technique improves the durability of resizing, translating, and rotating attacks. Two additional types of attacks—JPEG image compression and constant gain attack (CGA)—can damage a watermarked image's watermark information. A CGA attack was used to obtain factors to modify the luminance and blackness of watermarked digital images. Li et al. [52] used a perception-based model to increase the STDM watermarking system's resistance to JPEG compression. In another study presented by Lin et al. [53], the authors enhanced a type of JPEG compression that has been adopted in image watermarking systems. Recently, the CNN technique has been used to develop image priors for removing noise. For image denoising, Zhang et al. [54] developed a deep network CNN (DnCNN) framework that is able to contain convolutional kernels of the size $3 * 3$ for image watermark attack detection. Such a deep network is made up of various layers with distinct convolutional structures. Convolution+Relu are used in the initial layer (first layer), convolution+BatchNorm+Relu are adopted in the hidden layer, and simply the Pooling layer is used in the final layer, whereby the downsampling task is performed. The networks of 17–20 layers learned for blinded denoising with specified levels of noise using cumulative Gaussian denoising surpassed the WNNM [55] and BM3D [56] noise filtering algorithms. Using such algorithms could significantly improve the detection of watermarked image attacks. Zhang et al. [57] presented a new technology called FFDNet, which can address a broad range of excessive levels of noise. FFDNet uses a CNN model similar to that of DnCNN for quick and appropriate denoising; however, this method does not allow for the precise identification of noises. In this design, a bidirectional downsampling operator and adjustable noise-level mapping transfer the image as input into four images to be used in the CNN layers. One of biggest challenges to analyzing watermarked images is invisibility and robustness. A number of studies have sought to find a tradeoff or balance between invisibility and robustness [58], including proposing an artificial bee colony (ABC) [59–61], employing a firefly

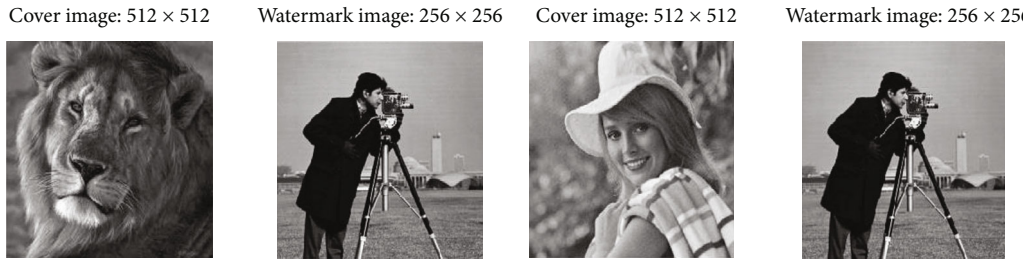

Figure 4: Emended watermark images: (a) own image and (b) standard image.

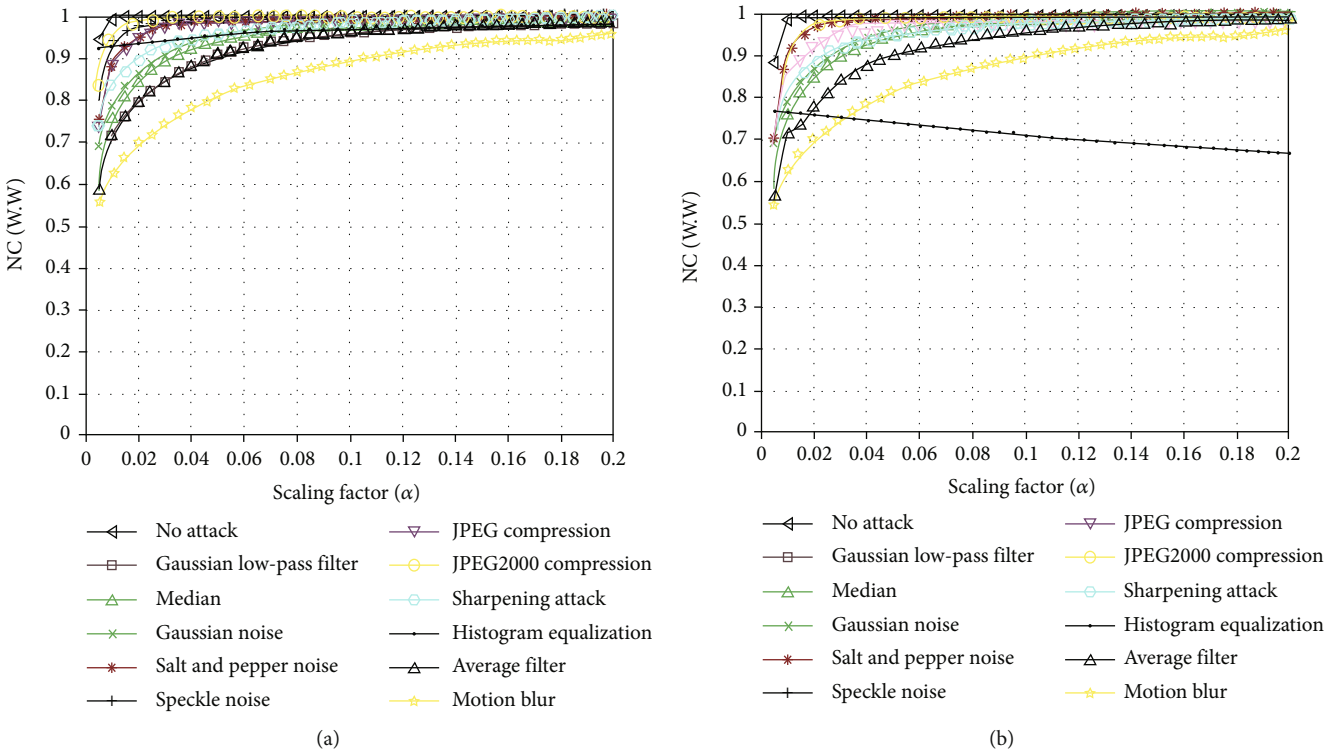

Figure 5: Scaling factors of various parameters by using NC: (a) lion image and (b) Elaine image.

algorithm [62], and using particle swarm optimization (PSO) [63, 64]. The main contributions of the present study are as follows:

(1) We have developed a hybrid model to detect various types of attacks for enhancing watermarked images

(2) In the proposed system, we have used our own watermarked images to verify the ability of the proposed system

(3) The proposed system was evaluated and tested with different types of evaluation metrics

(4) We have applied a scaling factor to measure invisibility–robustness that is used to balance the relationship between these two characteristics, which can help end users control the watermarked images

2. Materials and Methods

Numerous noise sources continue to impact the visibility of digital images. White noise and additive white Gaussian noise (AWGN) represent two types of noise that can be handled by the proposed system. Figure 1 displays the framework of the proposed system to enhance invisibility and robustness on watermarked images to detect various types of attacks.

2.1. Embedding Watermark Images. Figure 2 shows the steps necessary to embed a host image to create watermarked images. The procedure to embed watermark images is as follows:

(1) Select the hosting watermark images

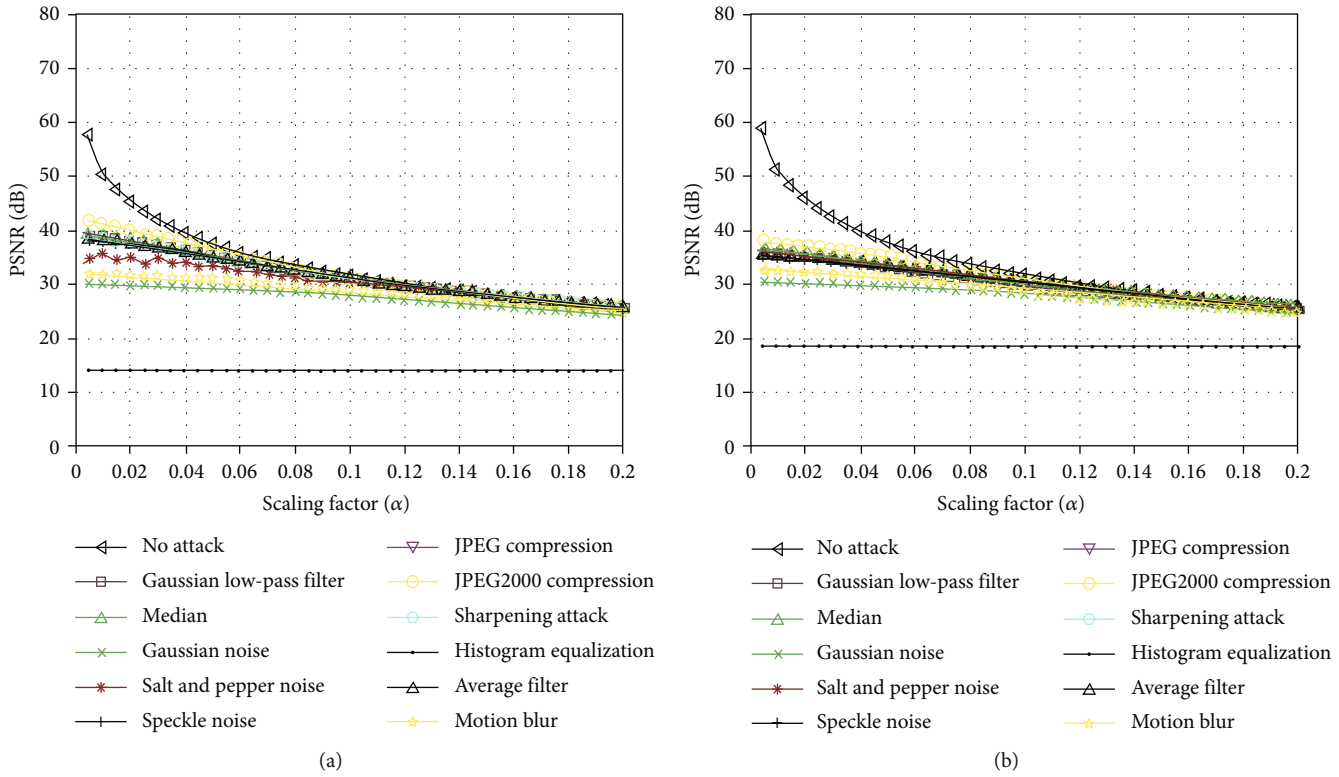

Figure 6: PSNR scaling factors: (a) lion image and (b) Elaine image.

(2) Apply the DWT method to the original image

(3) Apply the SVD method to LL_m of original and watermark images

(4) Use the singular value to compute with single factor α

(5) Use the SVD to generate the watermark LL_m

2.2. Discrete Wavelet Transformation (DWT) Method. DWT is a well-known statistical transformation with a wide range of application-based systems that can be implemented in engineering and science [35]. It delivers energy-efficient input image representation and also has a significant impact and durability on various image recognition attacks in watermark images [17]. DWT divides the original digital image into four spectral bands: low-high (LH), low-low, high-low (HL), and high-high (HH). After the first phase of DWT, the majority of the data details in the input images are focused within the low-low subband. The wave theory allows for even further subdivision until the width of the bands meets the watermark image specifications. In particular, when compared to other subbands, LL appears to perform better against attacks such as filtering and compressing [28, 30]. Because of this performance, the LL subband can be an attractive option for powerful watermarking [37].

2.3. Singular Value Decomposition (SVD) Method. In this method, singular values are differentiated throughout the structure of the symmetric matrix when SVD disintegrates the homogeneous matrix, thus generating three specific matrices [46]. Underneath the matrix decomposition, the three deconstructed matrices include the left single matrix U, single matrix S, and right single matrix V. Assuming Y represents a symmetric matrix, the SVD is calculated in the following equation:

$$USV^T = \mathrm{SVD}(Y), \tag{1}$$

where $VV^T = I_n$ and $UU^T = I_n$. The column elements of U are represented by the orthonormal eigenvectors of YY^T. These orthonormal eigenvectors are also denoted by columns V in the Y^TY matrix, and S is indicated as a diagonal matrix, which encompasses the square roots of the eigenvalues determined from U or V in the descendant direction. If $r(r \le n)$ refers to the standing of matrix Y, then the factors of the diagonal matrix S can be represented as a relative association in equation (2), and matrix Y is expressed in equation (3):

$$\sigma_1 \ge \sigma_2 \ge \cdots \ge \sigma_r \ge \sigma_{r+1} = \sigma_{r+2} = \cdots = \sigma_n = 0, \tag{2}$$

$$Y = \sum_{i=1}^{r} \sigma_i \mu_i v_i, \tag{3}$$

where v_i, μ_i, and i_{th} represent the eigenvector of V and U and σ_i indicates the i_{th} singular value. Throughout this work, the singular value of the watermark is integrated through the host image by such an appropriate

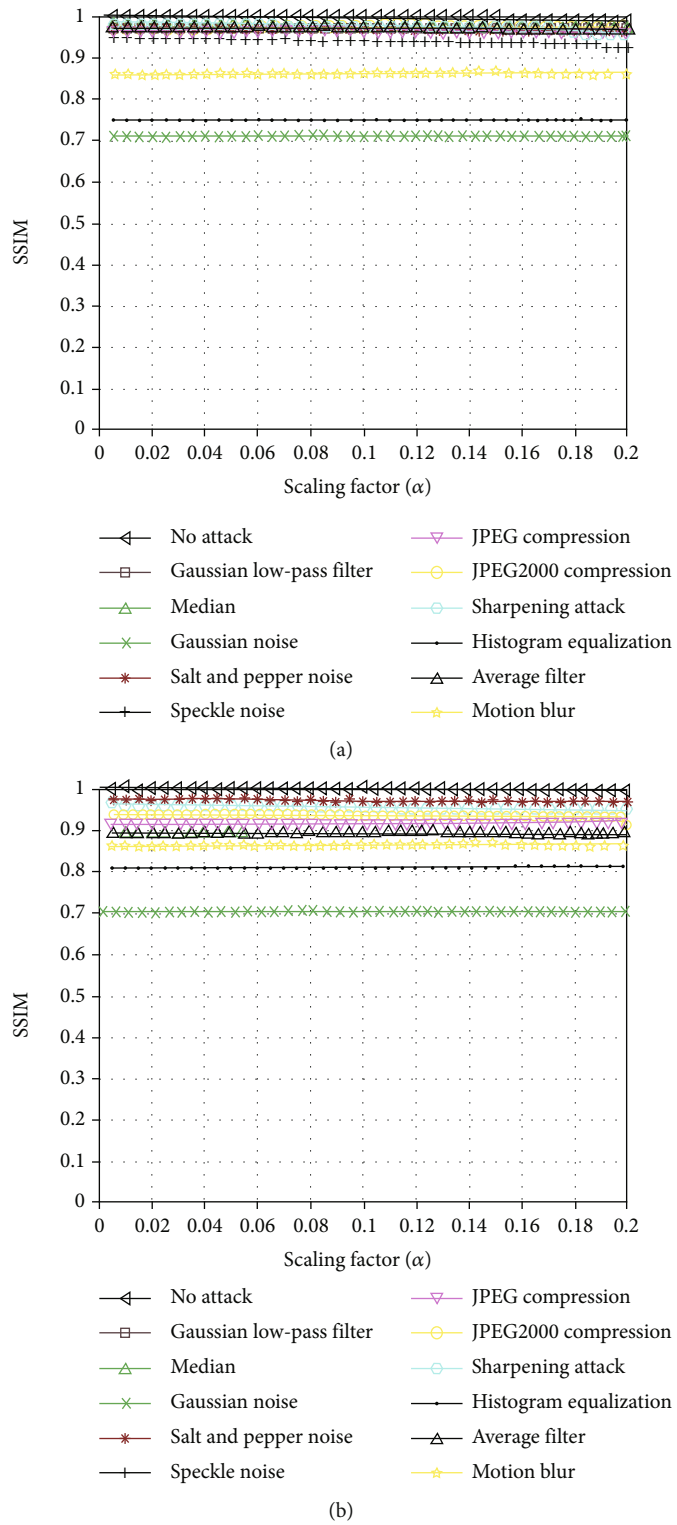

Figure 7: SSIM scaling factors: (a) lion image and b) Elaine image.

magnification factor, and the singular value of the watermark is incorporated further into the host image by using sufficient scaling factor. The invisibility and resilience of the watermarking process are two important aspects of this process. Because the scaling factor remains insufficient, the accurate effectiveness of the suggested method must be optimized. As a result, an optimized algorithm is needed to achieve the maximum relationship between invisibility and resilience of a watermark image.

2.4. Feature Extraction of Watermark Images. Feature extraction is crucial for identifying significant features in

Table 2: Performance of the DWT-SVD method to identify robustness and quality of watermarked images.

	Lion image	Lena image
Attacks	NC	0.9975
No attack	0.9874	0.8243
Gaussian low-pass filter	0.9028	0.9246
Median	0.958	0.9755
Gaussian noise	0.9599	0.9937
Salt-and-pepper noise	0.9824	0.9919
Speckle noise	0.9831	0.9942
Compression	0.96255	99.664
Sharpening	0.9334	0.9024
Histogram equalization	93.14	0.9341
Average filter	0.90063	0.822
Motion blur	0.70774	0.6648

the watermark image. The image mage I and the output of the image are referred to as the watermarking image m^*. Procedure steps to extract the features from inputted watermark images are presented in Figure 3. The procedure steps of the proposed system to extract significant features are as follows:

(1) Setup image I

(2) Use DWT to decompose image into four levels: LL_m, HH_m,LH_m, and HL_m

(3) Apply SVD to HH_m

$$HU^* \, HSb_m^* HV_m^* = \mathrm{SVD}(HH_m), \tag{4}$$

$$S_m^* = \frac{HSb_m^* - HS_m^*}{\alpha}. \tag{5}$$

S_m^* is used to extract the singular value; we have used the inverse SVD method to reconstruct the watermarking image M^*.

2.5. Measurement Performance. Three evaluation metrics, namely, peak signal-to-noise ratio (PSNR) and structural similarity index measure (SSIM), were employed to determine invisibility. To evaluate robustness, the normalization correlation (NC) was applied:

$$\mathrm{PSNR}(C, C^*) = 101g\frac{C_{\max}^2}{\mathrm{MSE}}, \tag{6}$$

$$\mathrm{MSE} = \frac{1}{M^2}\sum_{i=1}^{M}\sum_{j=1}^{M}(C_i j - C_i^*, j)^2, \tag{7}$$

$$\mathrm{SSIM}(C, C^*) = \frac{\mu c \mu c^* + d_1}{\mu^2 c + \mu^2 c + d_1} \cdot \frac{\sigma cc^* + d_2}{\sigma^2 c + \sigma^2 c* + d_2}, \tag{8}$$

$$NC = \frac{\sum_{I=1}^{N}\sum_{J=1}^{N} W_{i,j} w_{i,j}^*}{\sqrt{\sum_{i=1}^{N}\sum_{j=1}^{N} w_{i,j}^2}\sqrt{\sum_{i=1}^{N}\sum_{j=1}^{N} w_{i,j}^2}}, \tag{9}$$

wherein C is the host image, MSE is the mean square error, M is the output watermark, C_i is the host image, C_j is the watermark image, μc is the average values of the host image, and σ^2 is the variance.

3. Experimental Results

In this section, the results of the watermark algorithm are presented, and the invisibility and robustness of watermark images are analyzed using the DWT and SVD algorithms. The results of the proposed system were used to determine the scaling factor of watermarks of different sizes by employing PSNR, SSIM, and NC.

3.1. Environment of the Proposed System. Table 1 shows the proposed system requirements in terms of hardware and software.

3.2. Dataset. In this experiment, two images were used, one of a lion and one of a cameraman, to test the proposed system, and the grayscales of the images were 512×512 and 256×256, respectively. Figure 4 shows the two images used to examine the proposed system.

The performance of the proposed system was evaluated by various attacks, such as filter, cropping, rescaling, histogram equalization, sharpening, noise, compression, motion blur, and rotation attacks. The table summarizes the various attacks.

3.3. Results

3.3.1. Scaling Factor of Watermarks. The scaling factor is calculated by using multiple sizes to require being taken back to OEF. In the proposed system, the host image lion (512×512) and the watermark cameraman image (256×256) are applied to determine optimal scaling by observing the relationship between the scaling factor and significant parameter values, controlling the invisibility and robustness of watermarked images for identifying various types of attacks. The scaling factors of various parameters for detecting attacks are presented by using the NC metric (Figure 5). The scaling factors of attack values [0.02-0.2] are noted, whereas the y-axis NC (W, $W*$) presents watermark images and x-axis scaling factors α.

Figure 6 shows the scaling factors of the various attacks using the PSNR metric. The y-axis represents the values of PSNR, and it was observed that the values of motion blur and average filter were very low. The x-axis shows the scaling factors of all attacks.

The scaling factors of the SSIM metrics are presented in Figure 7. Regarding the scaling factor values of all attacks (y -axis) ranging between 0 and 0.9, it was observed that the Gaussian noise resulted in less scaling compared to various types of attacks.

3.3.2. Results and Discussion. We examined the target watermark images to identify various attack types, including

Figure 8: Watermarked images after applying different attack types: (a) lion image and b) Elaine image.

Table 3: Performance of the DWT-SVD method to find invisibility and quality of watermarked images.

Attacks	Lion image		Lena image	
	PSNR	SSIM	PSNR	SSIM
No attack	52.70	0.99989	47.93	0.9998
Gaussian low-pass filter	38.25	096.774	33.74	0.9148
Median	38.8989	0.9719	35.23	0.9227
Gaussian noise	29.956	0.7053	29.92	0.694
Salt-and-pepper noise	35.4581	0.9739	35.317	0.9736
Speckle noise	37.85	0.9450	35.336	0.8756
Compression	38.85	0.9645	35.52	0.9184
Sharpening	38.88	0.9813	37.86	0.9359
Histogram equalization	14.04	0.7492	34.966	0.96405
Average filter	38.12	96.68	19.117	0.8528
Motion blur	31.75	0.85.622	33.62	0.8528

Gaussian low-pass filter, median, Gaussian noise, salt-and-pepper noise, speckle noise compression, sharpening, histogram equalization, average filter, and motion blur attacks, as well as no attack. The evaluation metrics were applied to measure the parameter values, such as SSIM and PSNR used to analyze the watermarked images after the injection of attacks; moreover, NC was employed to test the robustness between the hosting image and watermark image after being subjected to various attacks.

Table 2 shows the results of the proposed system by employing the NC metric to determine the level of robustness of the parameter values of the attacked watermark images. The proposed system achieved good robustness for enhancing the quality of embedded images: no attacks (98.74%), salt-and-pepper noise (98.24%), and speckle noise (98.31%), whereas NC decreased values with motion blur (70.77%). Overall, the system was shown to improve watermarked images in terms of filtering all types of attacks. Figure 8 displays the results of the DWT-SVD algorithm to extract significant values from watermarked images after applying attacks. It was observed that the values of NC were superior for most attacks.

Table 3 shows the results of the proposed system in terms of the relationship between the level of invisibility of

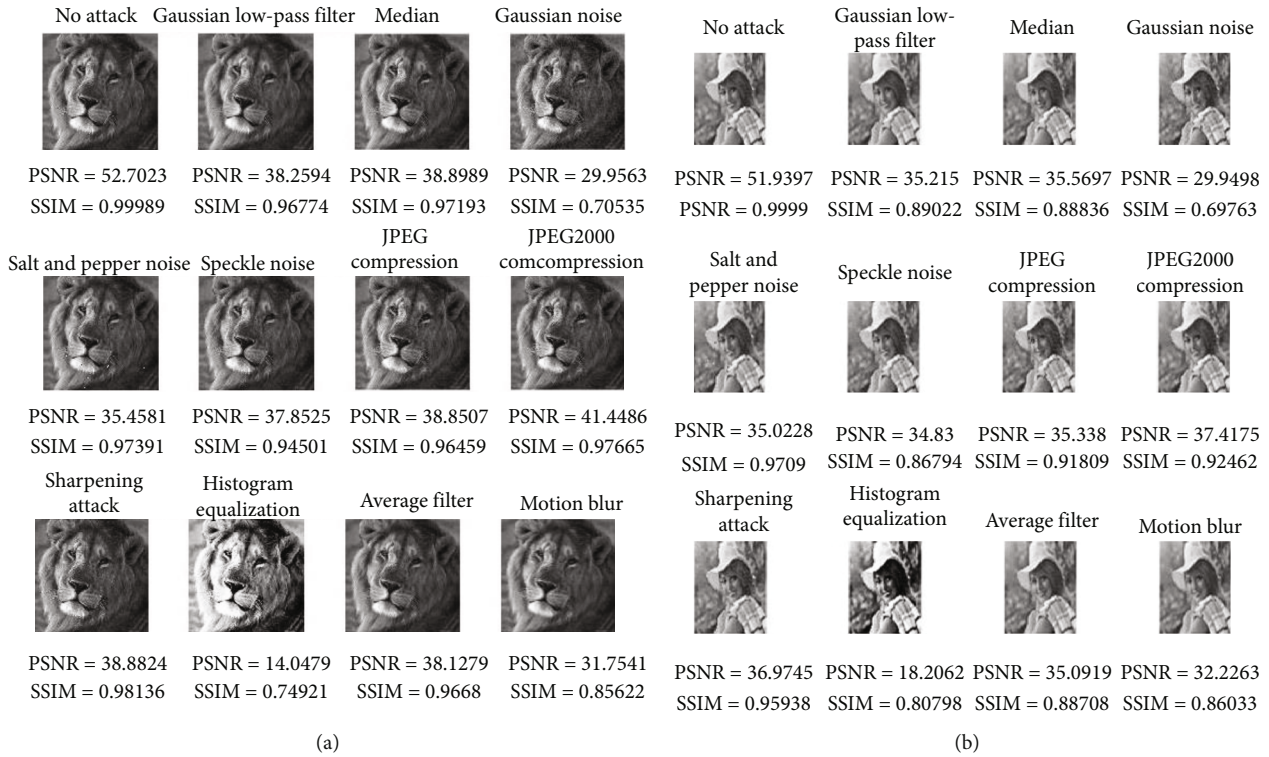

Figure 9: Performance of proposed system to extract attacks from watermarked images with respect to invisibility: (a) lion image and (b) Elaine image.

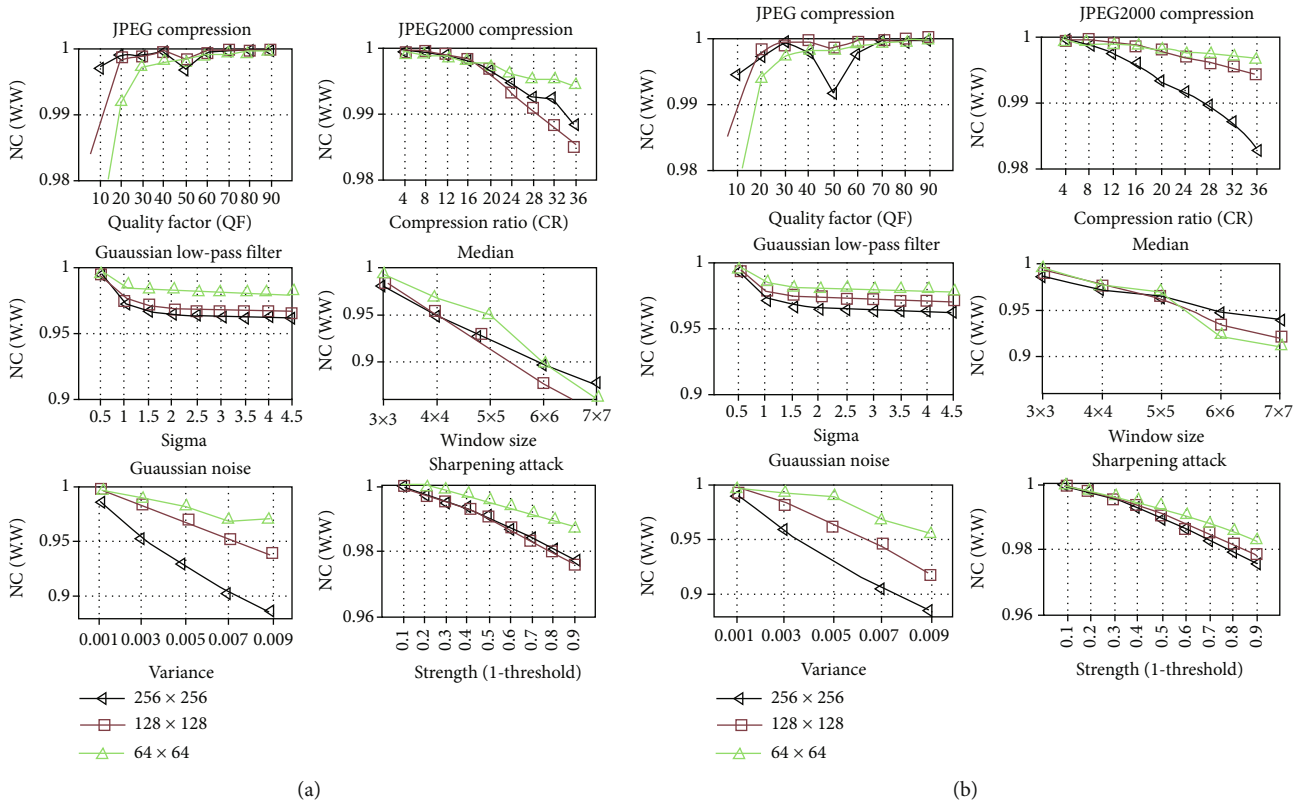

Figure 10: Parameters with different types of attacks with respect to NC values: (a) lion image and (b) Elaine image.

Table 4: Comparison results of the proposed system against an existing study [50].

Proposed system Attacks	NC	SSIM	Existing system NC	SIMM
Median	0.958	0.9719	0.966	0.878
Salt-and-pepper noise	0.9824	0.9739	0.890	0.612
Average filter	0.90063	96.68	0.820	0.418

Table 5: Comparison results of the proposed system against an existing study [65].

	Proposed system	Existing system
Attacks	NC	NC
Histogram equalization	0.958	0.5765
Salt-and-pepper noise	0.9824	0.5775
Sharpening	0.90063	0.52
Gaussian noise	0.9028	0.5512

Table 6: Comparison results of the proposed system against an existing study [66].

	Proposed system	Existing system
Attacks	NC	NC
Histogram equalization	0.958	0.820
Salt-and-pepper noise	0.9824	0.82
Sharpening	0.90063	0.791
Gaussian noise	0.9028	0.831

the embedded image and determining the likelihood of watermark attacks. The proposed system achieved optimal quality of grayscale watermarked image attack on no attack (PSNR = 52.70, SSIM = 99.99%). The system achieved lower quality invisibility in terms of watermarked image histogram equalization (PSNR = 14.04) and Gaussian noise (SSIM = 70.53%). Figure 9 shows the invisibility performance of extracting attacks from watermarked images using PSNR and SSIM metrics. It was noted that watermarked images have good invisibility.

When invisibility is found, robustness must be analyzed and evaluated; therefore, it is crucial to confirm the robustness of embedded images to identify various types of attacks and thus enhance the watermarked images in response. The proposed system was used to measure the invisibility and robustness for obtaining good results in managing all types of watermarked attacks.

3.3.3. Comparison Results. All parameters were evaluated to examine the attacks static, and we applied the proposed system dynamic to test the efficiency and effectiveness of the proposed system. Figure 10 shows the testing phase of the proposed system to check the level of robustness in the quality of the watermarked images. We selected parameters with different sizes of images to examine our proposed system. Furthermore, when the proposed system of DWT-SVD was compared to other systems, it was observed that the results from the proposed system achieved high accuracy in detecting various watermarked attacks. In the present research, various attacks were imposed on the host image to obtain optimal performance.

The research article (Makram et al., 2021) applied a deep learning model to measure the level of robustness of watermarked images after applying attacks, with the authors using six attacks, namely, salt-and-pepper, Gaussian filtering, median filtering, average filtering, and FCNNDA. However, in the proposed research, 11 attacks were considered to enhance the watered images. We compared the results of the proposed system to the existing system in the case of some attacks. The comparison results of Makram et al. (2021) against the proposed research are presented in Table 4. It was observed that the results of the proposed system were superior.

Table 5 shows results of the proposed system against the existing system; in (Arora et al., 2018), the researchers have used the DWT method. The existing system used histogram equalization, salt-and-pepper noise, sharpening, and Gaussian noise attacks to examine their system. It is observed that the proposed system has achieved better than their DWT method.

Furthermore, the results of our proposed system was compared with SVD, which is the existing mode of Joseph et al. (2013); four attacks, namely, histogram equalization, salt-and-pepper noise, sharpening, and Gaussian noise attacks, are presented in Table 6. It is noted that the proposed system is superior.

4. Conclusion

At present, information can be duplicated easily due to the interactive nature of the digital communication of multimedia data. In this paper, we developed a digital watermark method using DWT-SVD that analyzes various types of watermark attacks. This approach was designed to determine the relationship between invisibility and robustness using scaling factors. The focus of this research was the ability to embed and extract various attacks on watermarked images without restrictions on the host or the watermarked images and, furthermore, to enhance this ability by sufficiently monitoring the invisibility and robustness. Some important aspects of the present study are as follows:

(i) DWT was used to embed the host image into watermarked images to test the proposed system

(ii) DWT-SVD was applied to extract various types of significant features to identify all watermark attacks

(iii) We used three evaluation metrics, namely, SSIM, PSNR, and NC, to examine the obtained results from the proposed system. The SSIM and PSNR metrics were applied to evaluate the invisibility of the watermarked images, and NC was used to measure the robustness of watermarked images in terms of analyzing the attacks

(iv) The empirical results showed the excellent performance of the proposed system in measuring all types of attacks employed in the study

(v) The results of the proposed system were compared with state-of-the art works, and it was observed that the proposed system showed better performance

Consequently, we believe the proposed system would be helpful to the field of watermarking for managing digital images, as it permits the embedding and extraction of watermarked images without limitations on the host image and WM information. The proposed system can help to enhance and control invisibility and robustness to achieve optimal performance in response to a variety of attacks.

Data Availability

The standard images are from MATLAB https://www.mathworks.com/matlabcentral/answers/263183-where-to-download-the-example-image.

Conflicts of Interest

The author declares no conflict of interest.

Acknowledgments

The author extends their appreciation to the Deanship of Scientific Research, King Faisal University for funding this research work through the project number no. NA00051.

References

[1] M. Cox, J. Miller, J. Bloom, T. Fridrich, and Kalker, *Digital Watermarking and Steganography*, Morgan Kaufmann, 2007.

[2] I. J. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, *Digital Watermarking Steganigraphy*, Morgan Kaufmann Publisher, Burlington, MA, USA, 2007.

[3] Xiangui Kang, Jiwu Huang, Y. Q. Shi, and Yan Lin, "A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 776–786, 2003.

[4] J. George, S. Varma, and M. Chatterjee, "Color image watermarking using DWT-SVD and Arnold transform," in *Proceedings of the 2014 Annual IEEE India Conference (INDICON)*, pp. 1–6, Pune, India, December 2014.

[5] Y. S. Lee, Y. H. Seo, and D. W. Kim, "Blind image watermarking based on adaptive data spreading in n-level DWT subbands," *Security and Communication Networks*, vol. 2019, Article ID 8357251, 11 pages, 2019.

[6] C. Li, Z. Zhang, Y. Wang, B. Ma, and D. Huang, "Dither modulation of significant amplitude difference for wavelet based robust watermarking," *Neurocomputing*, vol. 166, pp. 404–415, 2015.

[7] J. Ouyang, G. Coatrieux, B. Chen, and H. Shu, "Color image watermarking based on quaternion Fourier transform and improved uniform log-polar mapping," *Computers and Electrical Engineering*, vol. 46, pp. 419–432, 2015.

[8] R. Mehta, V. P. Vishwakarma, and N. Rajpal, "Lagrangian support vector regression based image watermarking in wavelet domain," in *Proceedings of the 2015 2nd International Conference on SPIN*, pp. 854–859, Noida, India, February 2015.

[9] H. Hu, Y. Chang, and S. Chen, "A progressive QIM to cope with SVD-based blind image watermarking in DWT domain," in *Proceedings of the 2014 IEEE China Summit & International Conference on Signal and Information Processing*, pp. 421–425, Xi'an, China, July 2014.

[10] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for images, audio and video," in *Proceedings of 3rd IEEE International Conference on Image Processing*, pp. 243–246, Lausanne, Switzerland, 1996.

[11] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673–1687, 1997.

[12] H. S. Malvar and D. A. F. Florencio, "Improved spread spectrum: a new modulation technique for robust watermarking," *IEEE Transactions on Signal Processing*, vol. 51, no. 4, pp. 898–905, 2003.

[13] B. Chen and G. W. Wornell, "Quantization index modulation: a class of provably good methods for digital watermarking and information embedding," *IEEE Transactions on Information Theory*, vol. 47, no. 4, pp. 1423–1443, 2001.

[14] B. Chen and G. W. Wornell, "Quantization index modulation methods for digital watermarking and information embedding of multimedia," *Journal of VLSI Signal Processing Systems for Signal, Image and Video Technology*, vol. 27, no. 1/2, pp. 7–33, 2001.

[15] V. Potdar, S. Han, and E. Chang, "A survey of digital image watermarking techniques," in *INDIN'05.2005 3rd IEEE International Conference on Industrial Informatics, 2005*, pp. 709–716, Perth, WA, Australia, 2005.

[16] G. C. Langelaar, I. Setyawan, and R. L. Lagendijk, "Watermarking digital image and video data. A state-of-the-art overview," *IEEE Signal Processing Magazine*, vol. 17, no. 5, pp. 20–46, 2000.

[17] Q. Li, C. Yuan, and Y. Zhong, "Adaptive DWT-SVD domain image watermarking using human visual model," in *The 9th International Conference on Advanced Communication Technology*, pp. 1947–1951, Gangwon, Republic of Korea, 2007.

[18] A. K. Singh, M. Dave, and A. Mohan, "Hybrid technique for robust and imperceptible image watermarking in DWT–DCT–SVD domain," *National Academy Science Letters*, vol. 37, no. 4, pp. 351–358, 2014.

[19] A. Graves, A. Mohamed, and G. Hinton, "Speech recognition with deep recurrent neural networks," in *2013 IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 6645–6649, United States, 2013.

[20] L. A. Gatys, A. S. Ecker, and M. Bethge, "Image style transfer using convolutional neural networks," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 2414–2423, San Francisco, CA, USA, 2016.

[21] A. Karpathy, G. Toderici, S. Shetty, T. Leung, R. Sukthankar, and L. Fei-Fei, "Largescale video classification with convolutional neural networks," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 1725–1732, San Francisco, CA, USA, 2014.

[22] Y. Goldberg, "Neural network methods for natural language processing," *Synthesis Lectures on Human Language Technologies*, vol. 10, no. 1, pp. 1–309, 2017.

[23] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet classification with deep convolutional neural networks," in *Advances in Neural Information Processing Systems 25*, F. Pereira, C. Burges, L. Bottou, and K. Weinberger, Eds., pp. 1097–1105, Curran Associates, Inc., 2012.

[24] M. Rastegari, V. Ordonez, J. Redmon, and A. Farhadi, "XNOR-Net: ImageNet classification using binary convolutional neural networks," in *Computer Vision–ECCV 2016*, B. Leibe, J. Matas, N. Sebe, and M. Welling, Eds., pp. 525–542, Springer International Publishing, Cham, Switzerland, 2016.

[25] F. Milletari, N. Navab, and S. Ahmadi, "V-net: fully convolutional neural networks for volumetric medical image segmentation," in *2016 Fourth International Conference on 3D Vision (3DV)*, pp. 565–571, Stanford, CA, USA, 2016.

[26] J. Long, E. Shelhamer, and T. Darrell, "Fully convolutional networks for semantic segmentation," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 3431–3440, San Francisco, CA, USA, 2015.

[27] R. Couturier, G. Perrot, and M. Salomon, "Image denoising using a deep encoder-decoder network with skip connections," in *Neural Information Processing*, L. Cheng, A. C. S. Leung, and S. Ozawa, Eds., pp. 554–565, Springer International Publishing, Cham, Switzerland, 2018.

[28] J. E. Lee, J. W. Kang, W. S. Kim, J. K. Kim, Y. H. Seo, and D. W. Kim, "igital Image Watermarking Processor Based on Deep Learning," *Electronics*, vol. 10, no. 10, p. 1183, 2021.

[29] K. Zhang, W. Zuo, and L. Zhang, "FFDNet: toward a fast and flexible solution for CNN based image denoising," *IEEE Transactions on Image Processing*, vol. 27, no. 9, pp. 4608–4622, 2018.

[30] K. Zhang, W. Zuo, S. Gu, and L. Zhang, "Learning deep CNN denoiser prior for image restoration," in *The IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 3929–3938, San Francisco, CA, USA, 2017.

[31] C. Song, S. Sudirman, M. Merabti, and D. Llewellyn-Jones, "Analysis of digital image watermark attacks," in *2010 7th IEEE Consumer Communications and Networking Conference*, pp. 1–5, Las Vegas, NV, USA, 2010.

[32] H. Tao, L. Chongmin, J. M. Zain, and A. N. Abdalla, "Robust image watermarking theories and techniques: a review," *Journal of Applied Research and Technology*, vol. 12, no. 1, pp. 122–138, 2014.

[33] F. Y. Shih, *Digital Watermarking and Steganography: Fundamentals and Techniques*, CRC press, 2017.

[34] V. Licks and R. Jordan, "Geometric attacks on image watermarking systems," *IEEE Multimedia*, vol. 12, no. 3, pp. 68–78, 2005.

[35] E. Li, H. Liang, and X. Niu, "Blind image watermarking scheme based on wavelet tree quantization robust to geometric attacks," in *2006 6th World Congress on Intelligent Control and Automation*, pp. 10256–10260, Dalian, China, 2006.

[36] J.-C. Liu, C.-H. Lin, L.-C. Kuo, and J.-C. Chang, "Robust multi-scale full-band image watermarking for copyright protection," in *New Trends in Applied Artificial Intelligence*, H. G. Okuno and M. Ali, Eds., pp. 176–184, Springer, Berlin, Heidelberg, 2007.

[37] J. Li, "Robust image watermarking scheme against geometric attacks using a computer-generated hologram," *Applied Optics*, vol. 49, no. 32, pp. 6302–6312, 2010.

[38] X. He, T. Zhu, and G. Yang, "A geometrical attack resistant image watermarking algorithm based on histogram modification," *Multidimensional Systems and Signal Processing*, vol. 26, no. 1, pp. 291–306, 2015.

[39] S. Fazli and M. Moeini, "A robust image watermarking method based on DWT, DCT, and SVD using a new technique for correction of main geometric attacks," *Optik*, vol. 127, no. 2, pp. 964–972, 2016.

[40] S. D. Lin and C.-F. Chen, "A robust DCT-based watermarking for copyright protection," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 3, pp. 415–421, 2000.

[41] M. Barni, F. Bartolini, V. Cappellini, and A. Piva, "A DCT-domain system for robust image watermarking," *Signal Processing*, vol. 66, no. 3, pp. 357–372, 1998.

[42] J. C. Patra, J. E. Phua, and C. Bornand, "A novel DCT domain CRT-based watermarking scheme for image authentication surviving JPEG compression," *Digital Signal Processing*, vol. 20, no. 6, pp. 1597–1611, 2010.

[43] A. K. Singh, B. Kumar, S. K. Singh, S. P. Ghrera, and A. Mohan, "Multiple watermarking technique for securing online social network contents using back propagation neural network," *Future Generation Computer Systems*, vol. 86, no. 1, pp. 926–939, 2018.

[44] A. K. Singh, "Improved hybrid algorithm for robust and imperceptible multiple watermarking using digital images," *Multimedia Tools and Applications*, vol. 76, no. 6, pp. 8881–8900, 2017.

[45] T. K. Tsui, X. Zhang, and D. Androutsos, "Color image watermarking using multidimensional Fourier transforms," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 16–28, 2008.

[46] V. Solachidis and I. Pitas, "Circularly symmetric watermark embedding in 2-D DFT domain," *IEEE Transactions on Image Processing*, vol. 10, no. 11, pp. 1741–1753, 2001.

[47] P. Tao and A. M. Eskicioglu, "An adaptive method for image recovery in the DFT domain," *Journal of Multimedia*, vol. 1, no. 6, pp. 36–45, 2006.

[48] Y. Wang, J. F. Doherty, and R. E. Van Dyck, "A wavelet-based watermarking algorithm for ownership verification of digital images," *IEEE Transactions on Image Processing*, vol. 11, no. 2, pp. 77–88, 2002.

[49] M.-S. Hsieh, D.-C. Tseng, and Y.-H. Huang, "Hiding digital watermarks using multiresolution wavelet transform," *IEEE Transactions on Industrial Electronics*, vol. 48, no. 5, pp. 875–882, 2001.

[50] Z. H. Wei, P. Qin, and Y. Q. Fu, "Perceptual digital watermark of images using wavelet transform," *IEEE Transactions on Consumer Electronics*, vol. 44, no. 4, pp. 1267–1272, 1998.

[51] Q. Su, Y. Niu, Y. Zhao, S. Pang, and X. Liu, "A dual color images watermarking scheme based on the optimized compensation of singular value decomposition," *AEU-International Journal of Electronics and Communications*, vol. 67, no. 8, pp. 652–664, 2013.

[52] Q. Li, G. Doerr, and I. Cox, "Spread transform dither modulation using a perceptual model," in *2006 IEEE Workshop on Multimedia Signal Processing*, pp. 98–102, Victoria, BC, Canada, 2006.

[53] S. D. Lin, S.-C. Shie, and J. Guo, "Improving the robustness of DCT-based image watermarking against JPEG compression," *Comput. Stand. Interfaces*, vol. 32, no. 1-2, pp. 54–60, 2010.

[54] K. Zhang, W. Zuo, Y. Chen, D. Meng, and L. Zhang, "Beyond a Gaussian denoiser: residual learning of deep CNN for image denoising," *IEEE Transactions on Image Processing*, vol. 26, no. 7, pp. 3142–3155, 2017.

[55] S. Gu, L. Zhang, W. Zuo, and X. Feng, "Weighted nuclear norm minimization with application to image denoising," in *The IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 2862–2869, San Francisco, CA, USA, 2014.

[56] K. Dabov, A. Foi, V. Katkovnik, and K. Egiazarian, "Image denoising by sparse 3-d transform-domain collaborative filtering," *IEEE Transactions on Image Processing*, vol. 16, no. 8, pp. 2080–2095, 2007.

[57] K. Zhang, W. Zuo, and L. Zhang, "FFDNet: toward a fast and flexible solution for CNN-based image denoising," *IEEE Transactions on Image Processing*, vol. 27, no. 9, pp. 4608–4622, 2018.

[58] Y. Luo, M. Du, and J. Liu, "A symmetrical image encryption scheme in wavelet and time domain," *Communications in Nonlinear Science and Numerical Simulation*, vol. 20, no. 2, pp. 447–460, 2015.

[59] Q. Su and B. Chen, "A novel blind color image watermarking using upper Hessenberg matrix," *AEU-International Journal of Electronics and Communications*, vol. 78, no. 6, pp. 64–71, 2017.

[60] Q. Su, "Novel blind colour image watermarking technique using Hessenberg decomposition," *IET Image Processing*, vol. 10, no. 11, pp. 817–829, 2016.

[61] J. M. Guo, G. H. Lai, K. Wong, and L. C. Chang, "Progressive halftone watermarking using multilayer table lookup strategy," *IEEE Transactions on Image Processing*, vol. 24, no. 7, pp. 2009–2024, 2015.

[62] M. Ali, C. W. Ahn, and P. Siarry, "Differential evolution algorithm for the selection of optimal scaling factors in image watermarking," *Engineering Applications of Artificial Intelligence*, vol. 31, no. 31, pp. 15–26, 2014.

[63] I. A. Ansari, M. Pant, and C. W. Ahn, "Robust and false positive free watermarking in IWT domain using SVD and ABC," *Engineering Applications of Artificial Intelligence*, vol. 49, pp. 114–125, 2016.

[64] M. W. Hatoum, J.-F. Couchot, R. Couturier, and R. Darazi, "Using deep learning for image watermarking attack," *Signal Processing: Image Communication*, vol. 90, article 116019, 2021.

[65] S. M. Arora, "A DWT-SVD based robust digital watermarking for digital images," *Procedia Computer Science*, vol. 132, pp. 1441–1448, 2018.

[66] A. Joseph and K. Anusudha, "Robust watermarking based on DWT SVD," *International Journal on Signal & Image Security*, vol. 1, pp. 147–164, 2013.