

Article

# Robust Image Watermarking in Spatial Domain Utilizing Features Equivalent to SVD Transform

Musrrat Ali 

Department of Basic Sciences, PYD, King Faisal University, Al Ahsa 31982, Saudi Arabia; mkasim@kfu.edu.sa

**Abstract:** In recent years, digital image watermarking has gained a significant amount of popularity and developed into a crucial and essential tool for copyright protection, security, and the identification of multimedia content. Despite its high computational complexity, singular value decomposition (SVD) is an extensively utilized transformation in digital image watermarking. This research presents a robust and blind image watermarking scheme that directly alters the image pixels in the spatial domain to incorporate the watermark by quantizing the block-wise invariant maximum singular value. Using a distribution rule, pixels from the cover image are redistributed to obtain a new image that is divided into square and non-overlapping blocks to obtain invariant maximum singular values by using the matrix 2-norm in the spatial domain without performing an SVD transform. This modifies the pixels of the cover image such that the outcome is equivalent to the difference between the maximum singular values of the corresponding blocks in covers and watermarked images. The strengths of the proposed approach are highlighted by a comparison of experimental results with the most recent and comparable watermarking approaches.

**Keywords:** singular value decomposition; image watermarking; invariant singular value; quantization; matrix 2-norm



**Citation:** Ali, M. Robust Image Watermarking in Spatial Domain Utilizing Features Equivalent to SVD Transform. *Appl. Sci.* **2023**, *13*, 6105. <https://doi.org/10.3390/app13106105>

Academic Editor: Mostafa Fouda

Received: 4 April 2023

Revised: 10 May 2023

Accepted: 11 May 2023

Published: 16 May 2023



**Copyright:** © 2023 by the author. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

## 1. Introduction

In recent years, digital media has evolved into an essential component of the routine activities of each and every person. Due to recent technical breakthroughs, it is now simpler than ever to manipulate and share digital multimedia files. However, this has raised concerns about the unauthorized copying of copy-protected media, and its protection is a challenging task [1–3]. The digital watermarking scheme was developed to handle such issues [4–8], and since then, it has been developed into a novel area of study and is generating substantial attention among scientists [9,10]. Watermarking is a relatively new field of study that provides effective solutions for a number of security applications, such as authentication and copyright protection [11,12]. Several watermarking methods have been created, which can be classified according to various factors, such as robust or fragile watermarking, visible or invisible watermarking, spatial or frequency domain watermarking, and hybrid domain watermarking. In the following paragraphs, a concise analysis of watermarking schemes that take these factors into consideration is provided. However, interested researchers may refer to [9,10,12–15] to obtain more details about watermarking techniques. There are two main components of any watermarking scheme—embedding and extraction. A general framework for image watermarking is given in Figure 1.

Watermarking schemes that directly modify the image pixels to insert the watermark's information without any transformation are considered spatial domain watermarking schemes [16–18]. The most basic method of watermarking in this category is to introduce the watermark by modifying the least significant bits (LSBs) of the pixels in the cover image [19,20]. These watermarking techniques are simple to implement and require less effort than other schemes, although they generally compromise the quality.

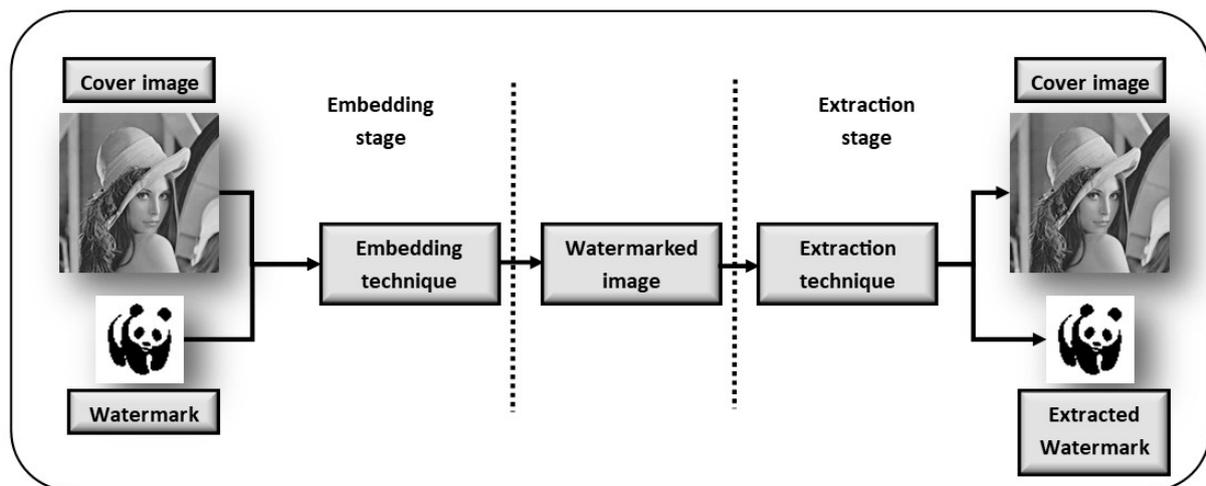


Figure 1. The general framework of an image watermarking scheme.

In contrast, frequency-domain watermarking techniques incorporate watermark information in frequency coefficients by converting spatial representation into the frequency domain. Several transforms have been used in watermarking, including discrete wavelet transform (DWT), discrete cosine transform (DCT), discrete Fourier transform (DFT), discrete fractional Fourier transform (DFrFT), quaternion wavelet transform (QWT), singular value decomposition (SVD), and their combinations [21–26]. Li et al. [27] presented image watermarking based on the redistributed invariant discrete wavelet transform (RIDWT). This scheme is invariant relative to row and column flips as well as ninety-degree rotations. It is accomplished by simply relocating the image's pixels to their new places, applying the wavelet transform, and performing some normalization. Liu et al. [28] suggested a blind color image watermarking approach with variable steps based on the Schur decomposition. Using the Walsh–Hadamard transform (WHT), Prabha et al. [29] presented an effective, resilient, and invisible blind color image watermarking technique. Garg et al. [30] proposed a robust image watermarking strategy that focuses on the protection of biometric images by combining discrete wavelet transform, SVD transform, and chaotic encryption. Using a hybrid transform consisting of discrete wavelet transform and singular value decomposition, Zermi et al. [31] proposed a watermarking scheme to preserve medical images.

The suitable choice of the parameters used in watermarking and location selection to embed the watermark has been a hectic task. Several researchers have used optimization techniques and machine learning for this task, such as fuzzy logic, neural networks, support vector machine, and evolutionary algorithms (EAs) [17,32–41]. From the evolutionary algorithm family, the firefly algorithm (FA) [42], artificial bee colony (ABC) [43], particle swarm optimization (PSO) [44], genetic algorithm (GA) [41], differential evolution (DE) [17], and teaching-learning based optimization (TLBO) [45] have all made significant contributions to watermarking. By viewing watermarking as a multi-objective problem, Hatami et al. [46] proposed an intelligent watermarking scheme that uses PSO to determine the optimal parameters.

In some instances, it is possible to achieve transform domain-equivalent features in the spatial domain, which could be used for watermarking with the same effect as transform domain watermarking. The direct current (DC) value of the DCT of any image is the average of its pixels value. Considering the complexity of DCT, some researchers have proposed watermarking in the spatial domain by directly altering the pixel's value, which has the same effect, as the watermark information is embedded by modifying the direct current (DC) value [17,47–50]. Similarly, watermarking techniques based on SVD transform mostly insert the watermark in the singular values of the host image obtained by the SVD transform [24,51]. The implementation of SVD is a time-consuming process due to the multiplication of matrices [49,52]. In response to this issue, Zhang et al. [49] proposed a

robust watermarking scheme in the spatial domain based on SVD. Using matrix norm, a binary watermark is inserted in the maximum singular value of each image block in the spatial domain.

Although the SVD-based image watermarking schemes, discussed above, have achieved a certain level of success, their resistance to some simple attacks is not yet acceptable. These attacks simply attempt to harm the watermark by relocating pixels without changing their intensity. In order to combat such attacks, this research aims to develop a scheme capable of performing effective image watermarking in the spatial domain. Unlike the existing schemes [49], the proposed approach uses the redistributed invariant discrete wavelet transform (RIDWT) concept proposed by Li et al. [27] before obtaining singular values for watermark embedding. It is invariant to row and column flips as well as ninety-degree rotations. The proposed scheme replicates the concepts in the spatial domain that they have used in the transform domain. This is accomplished by simply relocating the image's pixels to their new locations and performing a normalization process. The singular values of a matrix, as well as its transpose, rotation, and row and column flip matrices, are all the same. The singular values will remain the same regardless of how the values are permuted, so the order of the entries in a matrix is irrelevant. Motivated by the property of a matrix's singular values, this study proposes a novel approach to image watermarking. Initially, the pixels in the cover image are rearranged to ensure that every block of the image has the same pixel values when rotated by  $90^\circ$  degrees, and its row and column are flipped. Blocks of this new image under these attacks will have the same pixel values, and subsequently, the singular values of these blocks are invariant to these attacks. Due to the high complexity of the SVD transform, in the proposed scheme, the matrix 2-norm is utilized to obtain the maximum singular block-wise value. This maximum singular value is modified by a quantization factor, and the difference between the original and modified singular values is calculated. Based on this, a difference block is obtained to directly modify the host image block's pixel value so that the total magnitude of change equals the change in the singular values before and after embedding. Using a set of common image distortion attacks, ten standard test images, and four binary watermarks, we evaluated the efficacy of the proposed watermarking scheme. Using well-known evaluation metrics, such as the structural similarity measure (SSIM), peak signal-to-noise ratio (PSNR), bit error ratio (BER), and normalized correlation coefficient (NCC), the proposed watermarking approach is compared to similar approaches described in the literature. The result's analysis demonstrates the robustness of the proposed watermarking scheme against image distortion attacks and its excellent imperceptibility.

The following is a summary of the key contributions of this work:

1. Replication of the redistributed invariant wavelet transform concept to the spatial domain;
2. Application of the matrix 2-norm instead of SVD to obtain singular values;
3. Development of a new image watermarking scheme in the spatial domain;
4. Evaluation of the performance of the proposed scheme for grayscale images using a number of metrics and attacks.

The article is structured as follows. An overview of the algorithmic concepts is provided in Section 2. The proposed watermarking scheme is described in Section 3. Section 4 compares and analyzes the results. Section 5 contains the concluding observations and suggestions for future research.

## 2. Review of the Algorithmic Concepts

This section briefly describes the concepts related to the proposed watermarking scheme and the maximum singular value with SVD and without SVD by means of the matrix 2-norm. Researchers interested in obtaining more details may refer to [24,40,49,51,52].

### 2.1. Singular Value Decomposition

Singular value decomposition (SVD) [10] based on the linear algebra concept is a diagonalization of a rectangular matrix, and it is a very useful and powerful multimedia

tool, particularly in the contexts of data analysis, satellite data, image dimension reduction, etc. It transforms correlated variables into a collection of uncorrelated variables to reveal the relationships in the original data more clearly. Several SVD-based watermarking schemes have been proposed due to the stability of singular values, which may withstand modest image processing disruptions [10,15]. A rectangular matrix 'A' of order  $m \times m$  can be partitioned into the product of three matrices, namely orthogonal matrix U, diagonal matrix S, and the transpose of orthogonal matrix V, in accordance with the theory. It can be theoretically represented by its component matrices as follows:

$$A = \begin{bmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,m} \\ a_{2,1} & a_{2,2} & \dots & \\ \vdots & & \ddots & \\ a_{m,1} & & & a_{m,m} \end{bmatrix} = U S V^T = \begin{bmatrix} u_{1,1} & u_{1,2} & \dots & u_{1,m} \\ u_{2,1} & u_{2,2} & \dots & \\ \vdots & & \ddots & \\ u_{m,1} & & & u_{m,m} \end{bmatrix} \times \begin{bmatrix} \sigma_1 & 0 & \dots & 0 \\ 0 & \sigma_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \sigma_m \end{bmatrix} \times \begin{bmatrix} v_{1,1} & v_{1,2} & \dots & v_{1,m} \\ v_{2,1} & v_{2,2} & \dots & \\ \vdots & & \ddots & \\ v_{m,1} & & & v_{m,m} \end{bmatrix}^T \quad (1)$$

where  $UU^T = I_m$  and  $VV^T = I_m$ , and  $I_m$  is the identity matrix of order  $m$ . The elements of the diagonal matrix S are in decreasing order, satisfying Relation (2), where  $r$  is the rank of the matrix.

$$\sigma_1 \geq \sigma_2 \geq \dots \geq \sigma_r > \sigma_{r+1} = \sigma_{r+2} \dots = \sigma_m = 0 \quad (2)$$

### 2.2. Matrix Norm

The Frobenius norm of a matrix A, denoted  $\|A\|_F$ , is the square root of the sum of the square of the singular values and is defined as follows [52]:

$$\|A\|_F = \sqrt{\sum_{i=1}^m \sum_{j=1}^m a_{i,j}^2} = \sqrt{\text{trace}(A^T A)} = \sqrt{\sum_{i=1}^{\min\{m,n\}} \sigma_i^2} \quad (3)$$

The matrix 2-norm (or spectral norm) of matrix A is the maximal singular value of A or the square root of the maximum eigenvalue  $\lambda_{max}$  of  $A^T A$ . When  $F = 2$ , the matrix 2-norm is identical to the maximum singular value and is provided by the following formula:

$$\|A\|_2 = \sqrt{\lambda_{max}(A^T A)} = \sigma_{max} \quad (4)$$

To obtain the maximum singular value of an image, SVD is a widely used technique in digital watermarking because the maximum singular value of an image does not change considerably when it is subjected to conventional image processing attacks. However, the matrix product in SVD calculations will enhance its complexity and the cost of computation. On the other hand, the largest singular value of a matrix is equivalent to the matrix 2-norm [49]. Zhao et al. [52] compared the complexity of the SVD transform and matrix 2-norm and found that matrix 2-norm is faster. Due to the relationship between the matrix 2-norm and the maximum singular value, the proposed watermarking scheme uses the matrix 2-norm instead of the singular values from the SVD transform.

### 2.3. SVD-Based Watermarking Scheme

In SVD-based image watermarking [49], watermark W is divided into three components by SVD to embed the principal component into the host image by modifying its singular values.

$$W \Rightarrow U_w S_w V_w^T \quad (5)$$

The host image is transformed into the frequency domain by DWT, and the low-frequency sub-band (LL) is selected to divide it into several non-overlapping blocks. SVD is applied to each block to obtain the largest singular value to embed the principal component of the watermark image. It can be given by the following expression:

$$\sigma'_{max} = \sigma_{max} + \alpha U_w S_w \quad (6)$$

where  $\sigma_{\max}$  and  $\sigma'_{\max}$  are the original and modified largest singular values of the host image block, and  $\alpha$  is the embedding intensity control factor. After the modification of the largest singular value of each block of the host image, the watermarked image is achieved by the reverse process. The principal component of the embedded watermark can be extracted from the watermarked image by the following expression:

$$U_w S_w = \frac{1}{\alpha} (\sigma'_{\max} - \sigma_{\max}) \tag{7}$$

With the help of side information  $V_w$  from the watermark insertion phase and by the principal component obtained in Equation (7), the watermark can be extracted by the following equation:

$$U_w S_w V_w^T \Rightarrow W \tag{8}$$

According to Zheng et al. [49], changes equivalent to the watermarking in the SVD domain explained above can be achieved in the spatial domain as follows:

$$A_w = U(S + \Delta S)V^T = USV^T + U\Delta S V^T = A + \Delta A \tag{9}$$

where  $\Delta A$  is the difference between host image  $A$  and watermarked image  $A_w$ , and  $\Delta S$  represents the watermark information. According to Equation (9), the goal of watermarking schemes in the SVD domain is to distribute the watermark information across all pixels of the cover image. Therefore, SVD-based watermarking is possible by directly altering pixel values in the spatial domain if it is possible to obtain the difference matrix  $\Delta A$ . For example,  $\Delta A$  can be calculated as follows by taking a  $4 \times 4$  image block:

$$\Delta A = U \Delta S V^T = \begin{bmatrix} u_{1,1} & u_{1,2} & u_{1,3} & u_{1,4} \\ u_{2,1} & u_{2,2} & u_{2,3} & u_{2,4} \\ u_{3,1} & u_{3,2} & u_{3,3} & u_{3,4} \\ u_{4,1} & u_{4,2} & u_{4,3} & u_{4,4} \end{bmatrix} \times \Delta S \times \begin{bmatrix} v_{1,1} & v_{1,2} & v_{1,3} & v_{1,4} \\ v_{2,1} & v_{2,2} & v_{2,3} & v_{2,4} \\ v_{3,1} & v_{3,2} & v_{3,3} & v_{3,4} \\ v_{4,1} & v_{4,2} & v_{4,3} & v_{4,4} \end{bmatrix}^T \tag{10}$$

$$\Delta A = U \Delta S V^T = \begin{bmatrix} u_{1,1} & u_{1,2} & u_{1,3} & u_{1,4} \\ u_{2,1} & u_{2,2} & u_{2,3} & u_{2,4} \\ u_{3,1} & u_{3,2} & u_{3,3} & u_{3,4} \\ u_{4,1} & u_{4,2} & u_{4,3} & u_{4,4} \end{bmatrix} \times \begin{bmatrix} w & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \times \begin{bmatrix} v_{1,1} & v_{1,2} & v_{1,3} & v_{1,4} \\ v_{2,1} & v_{2,2} & v_{2,3} & v_{2,4} \\ v_{3,1} & v_{3,2} & v_{3,3} & v_{3,4} \\ v_{4,1} & v_{4,2} & v_{4,3} & v_{4,4} \end{bmatrix}^T \tag{11}$$

$$\Delta A = U \Delta S V^T = w \begin{bmatrix} u_{1,1} \\ u_{2,1} \\ u_{3,1} \\ u_{4,1} \end{bmatrix} \times [v_{1,1} \ v_{2,1} \ v_{3,1} \ v_{4,1}] = w u_1 v_1^T \tag{12}$$

where  $w$  indicates the watermark information, and  $u_1$  and  $v_1$  are column vectors in the matrices  $U$  and  $V$ . It is clear in Equation (12) that difference matrix  $\Delta A$  can be achieved by the multiplication of the watermark's information and eigenvectors  $u_1 v_1^T$ .

Zheng et al. [49] claimed that when the elements of a matrix are similar,  $u_1 v_1^T$  is closely associated with its matrix size. Using this property and taking a special case where all elements of a square matrix  $A$  are the same, it is expressed as follows:

$$A = \begin{bmatrix} a & a & a & a \\ a & a & a & a \\ a & a & a & a \\ a & a & a & a \end{bmatrix} = \begin{bmatrix} u_{1,1} & u_{1,2} & u_{1,3} & u_{1,4} \\ u_{2,1} & u_{2,2} & u_{2,3} & u_{2,4} \\ u_{3,1} & u_{3,2} & u_{3,3} & u_{3,4} \\ u_{4,1} & u_{4,2} & u_{4,3} & u_{4,4} \end{bmatrix} \times S \times \begin{bmatrix} v_{1,1} & v_{1,2} & v_{1,3} & v_{1,4} \\ v_{2,1} & v_{2,2} & v_{2,3} & v_{2,4} \\ v_{3,1} & v_{3,2} & v_{3,3} & v_{3,4} \\ v_{4,1} & v_{4,2} & v_{4,3} & v_{4,4} \end{bmatrix}^T = \sigma u_1 v_1^T \tag{13}$$

where  $\sigma$  is the unique singular value of diagonal matrix  $S$  of an image block of size  $n \times n$  (in this study  $n = 4$ ). In this case, this unique singular value is equal to the multiplication of

block size ‘4’ and matrix element ‘a’. With the help of Equation (13), the  $u_1v_1^T$  matrix can be calculated as follows:

$$u_1v_1^T = \frac{A}{\sigma} = \frac{1}{4a} \begin{bmatrix} a & a & a & a \\ a & a & a & a \\ a & a & a & a \\ a & a & a & a \end{bmatrix} = \frac{1}{4} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \tag{14}$$

Zhang et al. [49] verified the correctness of the above concept via an experimental analysis of a case study and found that if difference matrix  $\Delta A$  is obtained by the above process, watermarking in the spatial domain can be achieved, with the same impact as SVD-based watermarking. Figure 2 illustrates the fundamental similarity between the SVD-based watermarking and the watermarking scheme based on the largest singular value in the spatial domain.

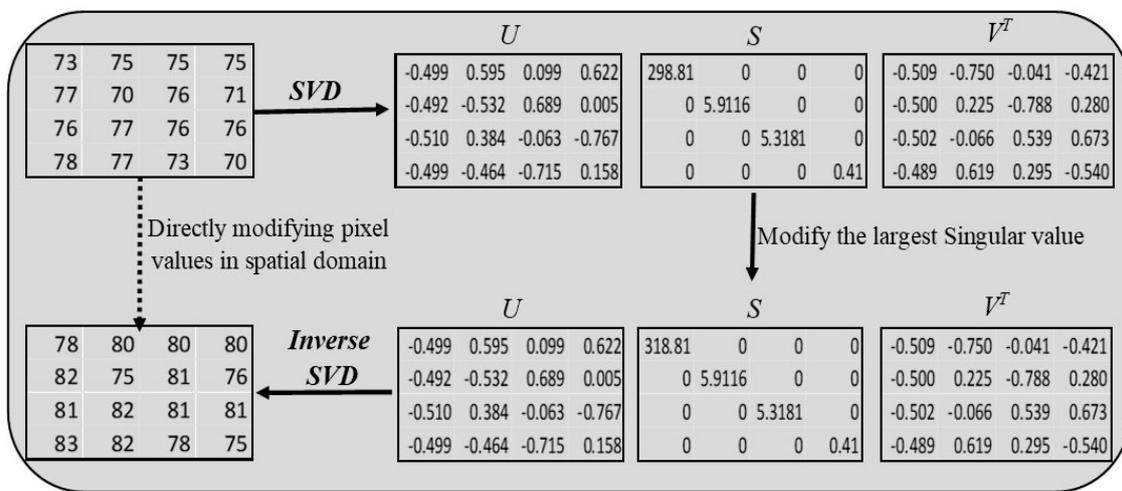


Figure 2. Illustration of SVD-based watermarking and spatial domain watermarking.

### 3. Proposed Watermarking Scheme

This section describes the components of the proposed watermarking scheme components, including the computation of the block-wise invariant maximum singular value, watermark embedding and extraction processes, and watermark preprocessing.

#### 3.1. Block-Wise Invariant Maximum Singular Value in the Spatial Domain

Several image-watermarking schemes by modifying the singular values to embed the watermark are proposed in the literature [10,15]. While these approaches can withstand some typical image distortion attacks, there is still room for improvement in a number of areas, such as image flipping and rotation by multiples of ninety degrees, where these schemes do not produce satisfactory results. To destroy the embedded watermark information, these basic techniques modify the spatial positions of the pixels in a watermarked image without affecting their intensities. The singular value of a matrix only considers the matrix elements irrespective of their locations. Keeping this in mind, the image pixels are redistributed in such a way that in each block, the pixel values remain the same irrespective of their locations to obtain the same singular value after the attacks.

This goal is achieved by utilizing the approach developed by Li et al. [27] and adopted by others [53]. A square image ‘A’ of size  $m \times m$  is divided into four sub-images of equal size, and the mean intensities of each are computed and collected in a matrix as

$\begin{bmatrix} \mu_1 & \mu_2 \\ \mu_3 & \mu_4 \end{bmatrix}, \mu_i \geq 0$ . A normalization matrix (N) is generated as follows using these means:

$$N = \begin{bmatrix} N_1 & N_2 \\ N_3 & N_4 \end{bmatrix} = \begin{bmatrix} \mu_1 + \mu_2 + \mu_3 + \mu_4 & \mu_1 - \mu_2 + \mu_3 - \mu_4 \\ \mu_1 - \mu_2 + \mu_3 - \mu_4 & \mu_1 - \mu_2 + \mu_3 - \mu_4 \end{bmatrix} \tag{15}$$

Using the distribution rule described in Equation (16), the pixels of the given image (A) are relocated to new locations to obtain a new image (B).

$$\begin{cases} B(2i - 1, 2j - 1) = A(i, j), & \text{if } 1 \leq i \leq m/2, 1 \leq j \leq m/2 \\ B(2i - 1, 2j - m) = A(i, 3m/2 - j + 1), & \text{if } 1 \leq i \leq m/2, m/2 \leq j \leq m \\ B(2i - m, 2j - 1) = A(3m/2 - i + 1, j), & \text{if } m/2 \leq i \leq m, 1 \leq j \leq m/2 \\ B(2i - m, 2j - m) = A(3m/2 - i + 1, 3m/2 - j + 1), & \text{if } m/2 \leq i \leq m, m/2 \leq j \leq m \end{cases} \tag{16}$$

If the absolute value of  $N_2$  is more than  $N_3$  in Equation (15), matrix  $B$  is left unchanged; otherwise, the transpose of  $B$  is taken to obtain the normalized image. Image  $B$  is divided into square blocks of size  $2^n$  ( $n = 1, 2, 3 \dots |2^n < m/2$ ) (in this study,  $n = 2$ ), which are represented by  $B_{ij}$  ( $i = 1, 2, \dots, m/4; j = 1, 2, \dots, m/4$ ). The largest singular value  $\sigma_{max}$  of each image block is calculated using the matrix 2-norm given in Equation (4) in the spatial domain instead of utilizing the SVD transform. Figure 3 provides an illustration of the concept described above using the example of a square image with dimensions of 32 by 32 pixels, which has been split into blocks with dimensions of 4 by 4 pixels. It is evident from the figure that the largest singular value of the image blocks remains the same under different attacks.

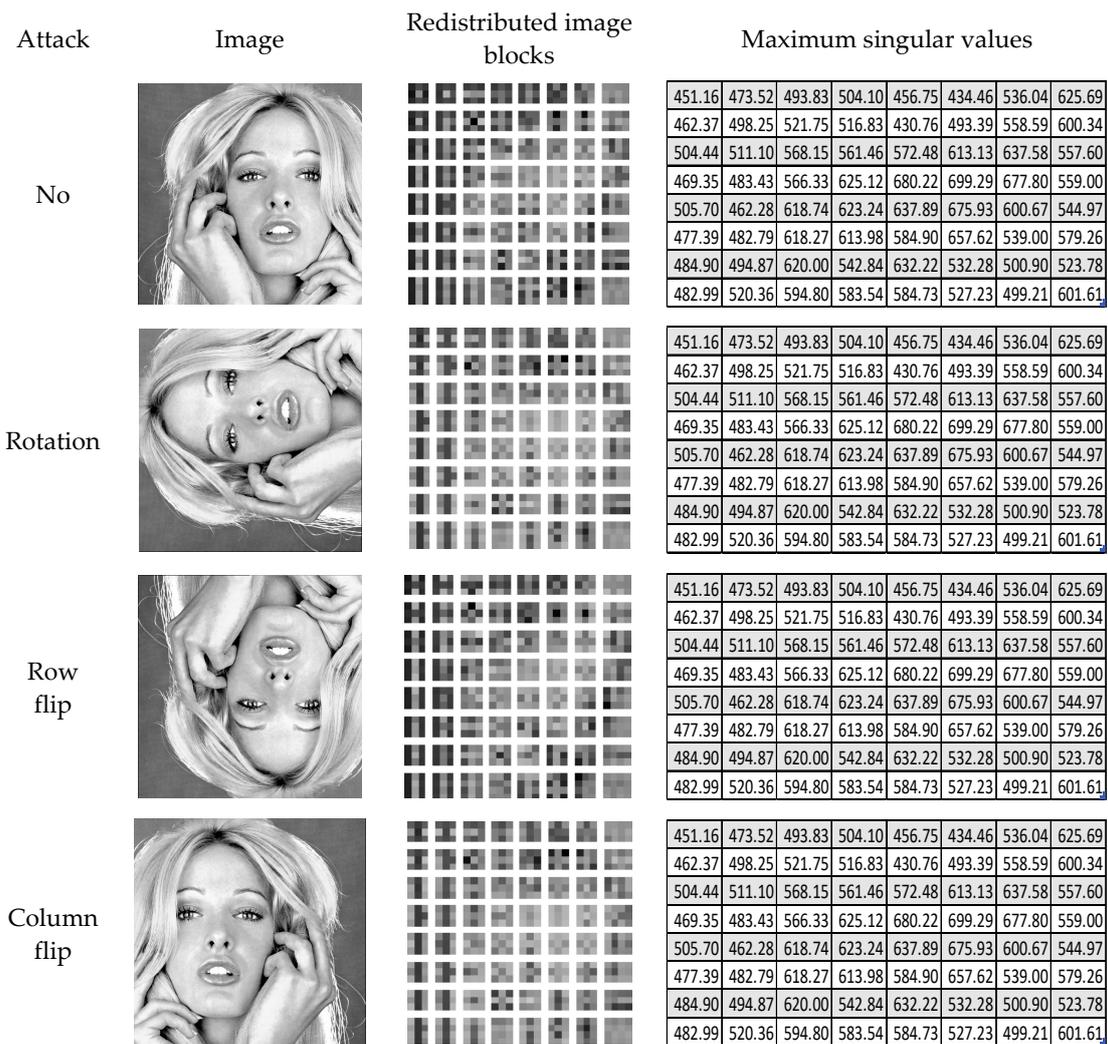


Figure 3. Illustration of block-wise invariant maximum singular values under various attacks.

### 3.2. Watermark Embedding Process

The process of embedding a watermark may be broken down into the following steps for easier understanding:

- Step 1: Encrypt the watermark image  $W$  using the piecewise linear chaotic map (PWLCM) [54] prior to embedding it into the cover image using a secret key ( $k$ ) to increase the security of the watermarking approach by adding an additional layer. This is one of the chaotic maps that has recently gained popularity due to its dynamic nature, simple form, and effective implementation. Without the correct security key, an impostor or unauthorized user cannot detect the watermark in the watermarked image.
- Step 2: Image  $B$  is created by rearranging the pixels of cover image 'A' in order to obtain the invariant features described in Section 3.1, and this image is split into  $4 \times 4$  non-overlapping blocks  $B_{i,j}$  ( $i = 1, 2, \dots, m/4; j = 1, 2, \dots, m/4$ ). Because a watermark is introduced one bit at a time into each block, the number of non-overlapping blocks must be greater than or equal to the number of watermark bits. Using the matrix 2-norm (Equation (4)), the invariant largest singular value  $\sigma_{max}$  of each image block of redistributed image  $B$  is calculated in the spatial domain instead of applying the SVD transform. In the proposed scheme, the number of blocks is more than the watermark's size, so these singular values are arranged in descending order, and the largest of these are selected according to the watermark's capacity. The selection of these singular values is motivated by their good imperceptibility relative to other singular values.
- Step 3: Modification magnitudes  $T_1$  and  $T_2$ , which are decided based on the watermark information, are given by Equation (17):

$$\begin{aligned} T_1 &= 0.5Q, & T_2 &= -1.5Q & \text{if } w &= 1 \\ T_1 &= -0.5Q, & T_2 &= 1.5Q & \text{otherwise} \end{aligned} \tag{17}$$

where 'Q' is the quantization factor, which controls imperceptibility and robustness.

- Step 4: The potential quantization results  $Q_1$  and  $Q_2$ , utilizing these magnitudes  $T_1$  and  $T_2$ , are now calculated as follows:

$$Q_1 = 2kQ + T_1, \quad Q_2 = 2kQ + T_2 \tag{18}$$

where  $k$  is an integer such that  $k = \text{floor}(\text{ceil}(\sigma_{max}/Q)/2)$ ,  $\text{ceil}(*),$  and  $\text{floor}(*)$  represents the smallest integer that is greater than or equal to the given value and the greatest integer that is less than or equal to the given value, respectively.

- Step 5: Based on  $Q_1$  and  $Q_2$ , the modified singular value  $\sigma'_{max}$  corresponding to the singular value  $\sigma_{max}$  is obtained as follows:

$$\sigma'_{max} = \begin{cases} Q_2 & \text{if } (|\sigma_{max} - Q_2| < |\sigma_{max} - Q_1|) \\ Q_1 & \text{else} \end{cases} \tag{19}$$

- Step 6: Singular value difference  $\Delta\sigma$  between modified singular value  $\sigma'_{max}$  and its corresponding singular value,  $\sigma_{max}$ , is calculated using Equation (20).

$$\Delta\sigma = \sigma'_{max} - \sigma_{max} \tag{20}$$

- Step 7: Difference matrix  $\Delta A$  can be achieved with the help of the difference in singular value  $\Delta\sigma$  using Equation (12) as  $\Delta A = \Delta\sigma u_1 v_1^T$ . With the help of this difference matrix and using Equation (9), watermark bits are directly inserted into image block  $B_{i,j}$  by altering the image pixels. The procedure is repeated until all watermark bits are embedded, and then the reverse process is applied to put back the pixels in their original places to create watermarked image  $Aw$ .

### 3.3. Watermark Extraction Process

A watermark,  $W$ , that has been inserted into a watermarked image,  $Aw$ , which subsequently has been subjected to image manipulation attacks, can be extracted by the procedure described here. The extracted watermark ( $W'$ ) may be distorted or of the same quality as when inserted:

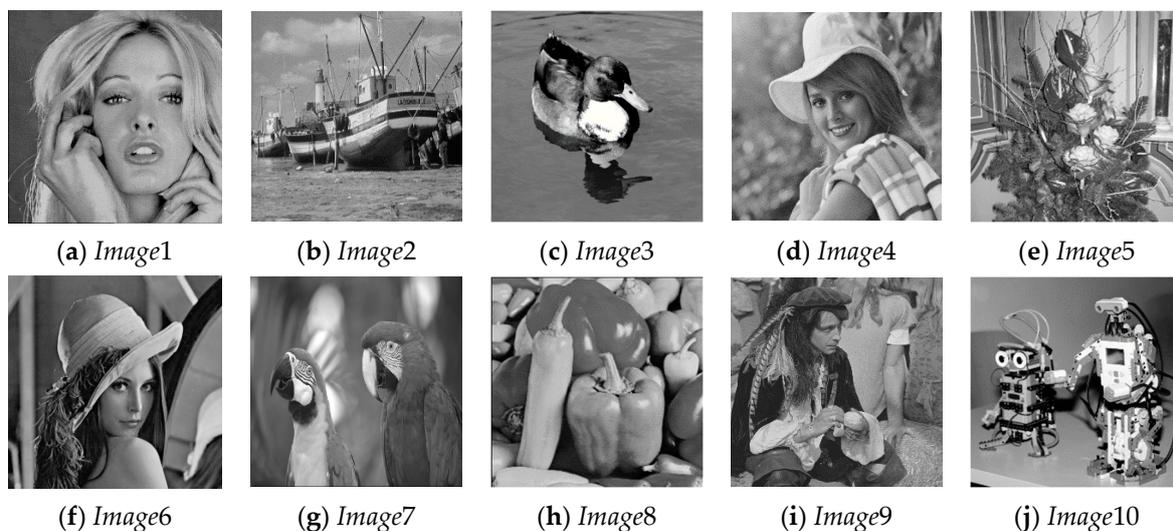
- Step 1: The pixels of the distorted watermarked image ' $Aw$ ' are redistributed, as described in Section 3.1. The image is divided into  $4 \times 4$  blocks, and the blocks with the watermark information are selected to directly compute the invariant maximum singular value in the spatial domain instead of the SVD transform by Equation (4).
- Step 2: With the help of the singular values obtained in Step 1 and quantization parameter ' $Q$ ', the encrypted watermark can be extracted by the following Equation (21).

$$W' = \text{mod} \left( \text{ceil} \left( \frac{\sigma'_{\max}}{Q} \right), 2 \right) \quad (21)$$

- Step 3: The decryption process is applied with the proper key to obtain the embedded watermark  $W'$  that was extracted in Step 2.

## 4. Experimental Results Discussion

In this section, a comparison of the performance of the proposed watermarking scheme with the performance of other relevant watermarking techniques that have been developed by Parah et al. [48], Zhang et al. [49], Zeng et al. [50], Su et al. [47], and Elbasi et al. [26] is carried out. All these schemes have, in some way or another, utilized an idea that is similar to the proposed scheme. Ten grayscale standard test images (*Image1* to *Image10*) with a size of  $512 \times 512$  and four binary watermarks ( $W1$ ,  $W2$ ,  $W3$ , and  $W4$ ) with a size of  $64 \times 64$  were considered for evaluating the performance of the proposed scheme and are given in Figures 4 and 5, respectively. These test images were compiled from a variety of publicly accessible open-source image libraries. To verify the robustness of the proposed approach, the quality of the watermarked image was degraded using a variety of standard image distortion attacks, as shown in Table 1. The proposed scheme was tested on a personal computer (PC) configured with MATLAB, an Intel core i7 processor, NVIDIA GeForce MX450 graphic card, Windows 11, and 16 GB of RAM. The results are given in Table 6 and Figures 12 and 13 for the comparison of algorithms. The best result corresponding to each row is highlighted in bold.



**Figure 4.** Test images: Ten test images labeled from *Image1* to *Image10*.



**Figure 5.** Watermark images: Watermark images labeled from W1 to W4.

**Table 1.** Attacks used to destroy watermarks.

Attack Index	Description
Index0	No change in watermarked image
Index1	Average filter taking a $3 \times 3$ window size
Index2	$90^\circ$ anticlockwise rotation
Index3	25% central region cropping
Index4	Addition of Gaussian noise with mean 0 and variance 0.005.
Index5	JPEG compression taking a quality factor of 75
Index6	Rescaling $512 \rightarrow 256 \rightarrow 512$
Index7	Median filter taking a $3 \times 3$ window size
Index8	Salt and pepper noise addition with density of 0.005
Index9	10 rows and 10 columns from arbitrary locations are deleted
Index10	Low-pass Gaussian filter with a $3 \times 3$ window
Index11	Rows flip
Index12	Columns flip
Index13	Motion blur with a $3 \times 3$ window
Index14	Pixelation with a $2 \times 2$ window
Index15	Speckle noise with mean of zero and variance of 0.005

The peak signal-to-noise ratio (PSNR) is a widely used metric for evaluating the quality of a watermarked image among the different quality metrics reported in the literature [49]. A higher *PSNR* value points toward the higher imperceptibility of the watermarked image. The *PSNR* of 8-bit image  $A$  with a size of  $m \times m$  and its watermarked image  $Aw$  is given by the following equation.

$$PSNR(A, Aw) = 10 \log_{10} \left( \frac{(255)^2}{\frac{1}{m \times m} \sum_{i=1}^m \sum_{j=1}^m (A_{i,j} - Aw_{i,j})^2} \right) (dB) \quad (22)$$

Another metric for the imperceptibility measurement is the structural similarity (*SSIM*) index [49], which measures the similarity between original image  $A$  and watermarked image  $Aw$ . It models any image distortion as a combination of three factors, which are a loss of correlation  $s(A, Aw)$ , contrast distortion  $c(A, Aw)$ , and luminance distortion  $l(A, Aw)$ . The human visual system (HVS) quality perception and structural similarity are correlated. It is defined as the follows:

$$SSIM(A, Aw) = l(A, Aw)c(A, Aw)s(A, Aw) \quad (23)$$

$$l(A, Aw) = \frac{2\mu_A\mu_{Aw} + C_1}{\mu_A^2 + \mu_{Aw}^2 + C_1}, \quad c(A, Aw) = \frac{2\sigma_A\sigma_{Aw} + C_2}{\sigma_A^2 + \sigma_{Aw}^2 + C_2}, \quad s(A, Aw) = \frac{\sigma_{AAw} + C_3}{\sigma_A\sigma_{Aw} + C_3} \quad (24)$$

where  $\mu_A$ ,  $\mu_{Aw}$ ,  $\sigma_A$ ,  $\sigma_{Aw}$ , and  $\sigma_{AAw}$  are the mean, the variance of image  $A$  and its watermarked image  $Aw$ , and the covariance between these images, while constants  $C_1$ ,  $C_2$ , and  $C_3$  are stability constants used to avoid division by zero.

The extracted watermark ( $W'$ ) may not be identical to the embedded watermark ( $W$ ) with a size of  $n \times n$  due to the implementation of the image distortion attacks on the watermarked image. Consequently, a standard is necessary to evaluate the robustness of the watermarking scheme, and often, the normalized correlation coefficient (NCC) and bit

error ratio (BER) are employed for this purpose. These two measures were defined and utilized for the robustness analysis in the current study:

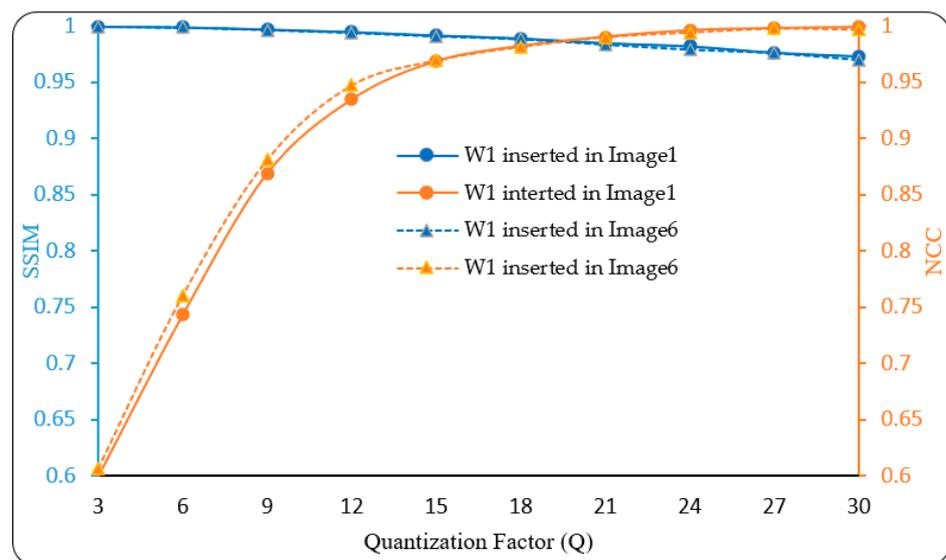
$$BER(W, W') = \frac{\sum_{i=1}^n \sum_{j=1}^n W_{i,j} \oplus W'_{i,j}}{n \times n} \tag{25}$$

$$NCC(W, W') = \frac{\sum_{i=1}^n \sum_{j=1}^n W_{i,j} \times W'_{i,j}}{\sqrt{\sum_{i=1}^n \sum_{j=1}^n W_{i,j}^2} \sqrt{\sum_{i=1}^n \sum_{j=1}^n W'_{i,j}^2}} \tag{26}$$

where subscripts *i* and *j* indicate the pixel’s position in the images, and ‘ $\oplus$ ’ refers to the XOR operation.

#### 4.1. Sensitivity Analysis of Quantization Factor Q

The watermark imperceptibility and robustness are two characteristics of a watermarking algorithm that are mutually exclusive and connected. In the proposed watermarking scheme, these properties are balanced using quantization factor ‘Q’. A smaller value of Q will implant less information into the host image, resulting in a small decrease in the visual quality; however, this information may be easily deleted using basic modification techniques. Although a greater value of Q will implant more information into the host image, resulting in a significant decrease in the visual quality, this information cannot be simply removed using basic modification techniques. Thus, a lower Q favors imperceptibility, and a higher value favors robustness. Finding the appropriate value for this parameter is a very important and challenging task. A sensitivity analysis of Q is performed using several images and watermarks to resolve the trade-off between the robustness and imperceptibility of the proposed watermarking approach. The NCC and SSIM values are computed to represent robustness and imperceptibility, respectively. On the basis of these assessment metrics, the value of Q of the proposed scheme is nearly the same for each image, with minor variations. Some results are given in Figure 6, where a watermark (W1) was embedded into the host *image1* and *image6* by taking different quantization factor ‘Q’, and the associated NCC and SSIM values were calculated. In the graph of these NCC and SSIM values, it can be seen that Q = 20 was a suitable choice, which was considered in further calculations.



**Figure 6.** The NCC and SSIM values obtained by the proposed scheme by taking different values of quantization factor Q.

#### 4.2. Imperceptibility Analysis

Imperceptibility in invisible watermarking is associated with the human visual system. If both the host and watermarked images are identical, it is argued that the watermarking scheme is imperceptible. To investigate the invisibility of the inserted watermark, the structural similarity measure (*SSIM*) and peak signal-to-noise ratio (*PSNR*) explained above are widely applied in evaluation metrics. This study also used these metrics to investigate the watermarked image's imperceptibility. The *PSNR* and *SSIM* values obtained by the proposed watermarking scheme are listed in Table 2, corresponding to each watermark inserted in the given host images. As can be observed in Table 2, the *PSNR* and *SSIM* values for each of the images are close to 49 dB and 1, respectively, for each watermark insertion. This demonstrates that the proposed watermarking scheme has a high level of imperceptibility.

**Table 2.** *PSNR* (dB) and *SSIM* values of watermarked images.

IMAGE	PSNR				SSIM			
	W1	W2	W3	W4	W1	W2	W3	W4
<i>Image1</i>	49.6187	49.1559	49.5421	49.7881	0.9957	0.9952	0.9965	0.9966
<i>Image2</i>	49.2557	49.1345	49.8637	49.7539	0.9950	0.9938	0.9977	0.9969
<i>Image3</i>	49.0906	49.6372	49.5223	49.5529	0.9955	0.9967	0.9958	0.9962
<i>Image4</i>	48.8722	49.1299	49.2188	48.8660	0.9972	0.9963	0.9971	0.9973
<i>Image5</i>	49.0075	48.7838	49.3393	49.2890	0.9964	0.9956	0.9974	0.9965
<i>Image6</i>	48.6690	49.0954	49.2958	48.9566	0.9946	0.9956	0.9949	0.9951
<i>Image7</i>	48.8956	49.2559	48.8997	49.0164	0.9957	0.9973	0.9954	0.9964
<i>Image8</i>	49.2894	49.1746	48.8634	48.8375	0.9841	0.9845	0.9846	0.9857
<i>Image9</i>	48.8736	49.1341	49.2494	48.8962	0.9940	0.9923	0.9942	0.9934
<i>Image10</i>	49.1469	49.0825	49.3130	48.9508	0.9954	0.9949	0.9963	0.9939

#### 4.3. Robustness Analysis against Attacks

This section analyzes the robustness of the proposed watermarking scheme, utilizing image distortion attacks to distort the watermarked image shown in Table 1 and the extraction procedure described in Section 3.3. The normalized correlation coefficient (*NCC*) and bits error ratio (*BER*), which are defined in Equations (25) and (26), were employed for this task. A higher *NCC* value means higher robustness, while a smaller *BER* value means higher robustness. Therefore, *BER* and *NCC* values approaching zero and one, respectively, indicate that the embedded and extracted watermarks are almost the same. The *NCC* and *BER* values of the extracted watermarks corresponding to inserted watermarks *W1* to *W4* are given in Tables 3–5. To investigate the collective robustness of the proposed scheme, the average *NCC* and *SSIM* of all the attacks of the extracted watermarks corresponding to each image are given in Table 3. According to the table, the proposed watermarking scheme was resistant to all distortion attacks with *NCC* values close to 1 and *BER* values close to 0. Figures 7 and 8 demonstrate the same phenomenon, representing the average *NCC* and the average *BER*, respectively. To investigate the robustness of the proposed scheme against each image manipulation attack, the average *NCC* and *BER* values of all extracted watermarks for each image are given in Tables 4 and 5, respectively. The proposed watermarking scheme's ability to retrieve the watermarks exactly as they were inserted is demonstrated by the *NCC* values of 1 and *BER* values of 0 in the cases of 90-degree rotation and row and column flipping (*index2*, *index11*, and *index12*). The outcome of the research comes close to fulfilling the objectives of the study. Due to space constraints, the extracted watermarks only from 'image1' are given in Figure 9. The figure demonstrates that the recovered watermarks by the proposed scheme were almost similar to the embedded watermark in every instance. Except in a few cases, the extracted watermark may be recognized with the naked eye. The extracted watermarks in the cases of attack *indices* 1, 6, 7, 8, 9, and 13 have poor quality in comparison to the other cases. Further improvement of the watermarking scheme is needed considering these cases.

**Table 3.** Average NCC and BER values of all the attacks corresponding to each image.

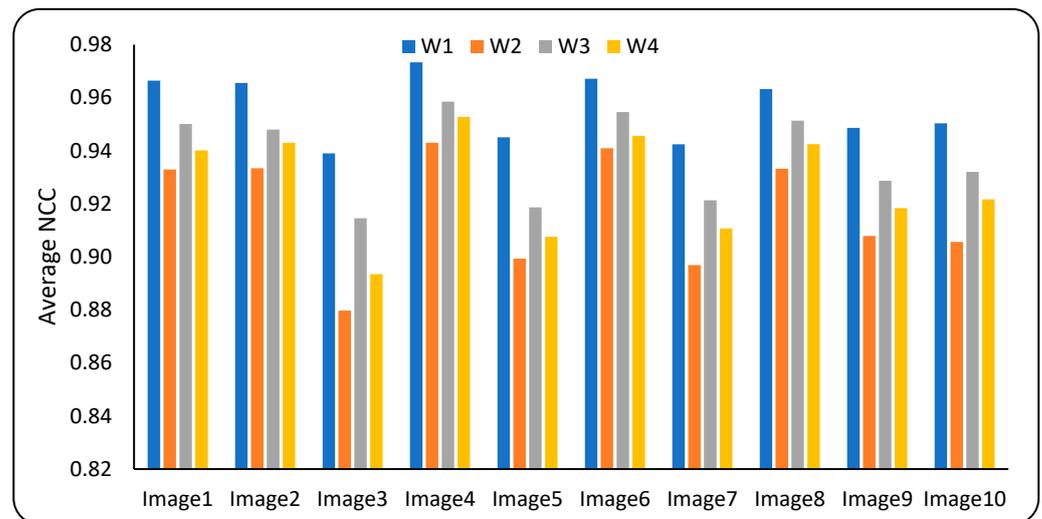
IMAGE	NCC				BER			
	W1	W2	W3	W4	W1	W2	W3	W4
<i>Image1</i>	0.9664	0.9329	0.9501	0.9401	0.0464	0.0376	0.0422	0.0407
<i>Image2</i>	0.9655	0.9334	0.9480	0.9430	0.0478	0.0377	0.0442	0.0390
<i>Image3</i>	0.9390	0.8797	0.9145	0.8935	0.0851	0.0740	0.0767	0.0777
<i>Image4</i>	0.9733	0.9430	0.9585	0.9527	0.0376	0.0321	0.0357	0.0324
<i>Image5</i>	0.9451	0.8993	0.9187	0.9076	0.0747	0.0597	0.0693	0.0641
<i>Image6</i>	0.9672	0.9410	0.9546	0.9456	0.0460	0.0328	0.0387	0.0368
<i>Image7</i>	0.9424	0.8969	0.9213	0.9107	0.0754	0.0581	0.0647	0.0599
<i>Image8</i>	0.9632	0.9332	0.9513	0.9425	0.0505	0.0373	0.0413	0.0389
<i>Image9</i>	0.9486	0.9079	0.9287	0.9184	0.0694	0.0524	0.0598	0.0558
<i>Image10</i>	0.9503	0.9056	0.9320	0.9217	0.0676	0.0546	0.0580	0.0545

**Table 4.** Average NCC values considering all the watermarks corresponding to each attack.

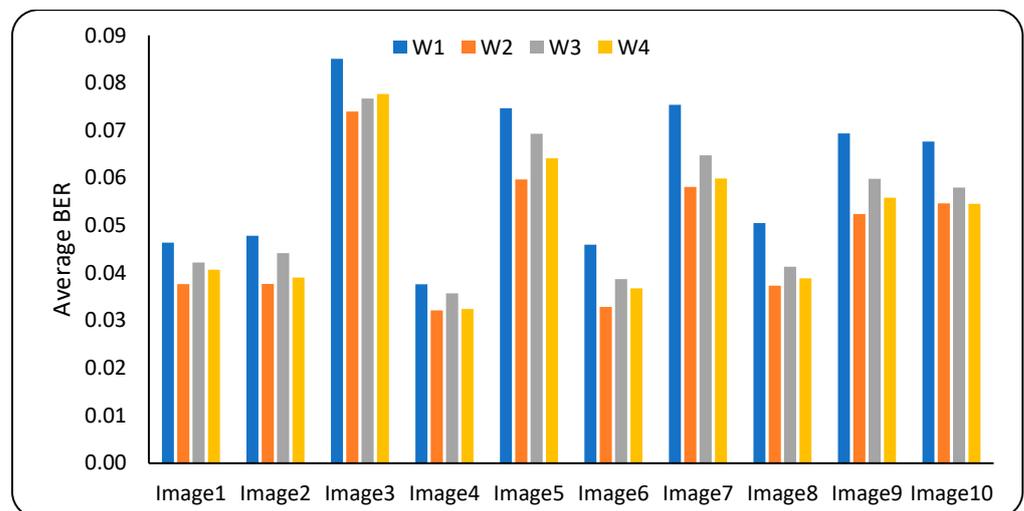
Image/ Attack	<i>Image1</i>	<i>Image2</i>	<i>Image3</i>	<i>Image4</i>	<i>Image5</i>	<i>Image6</i>	<i>Image7</i>	<i>Image8</i>	<i>Image9</i>	<i>Image10</i>
<i>Index0</i>	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
<i>Index1</i>	0.7691	0.7511	0.7390	0.7906	0.6424	0.7861	0.7187	0.7851	0.7024	0.6909
<i>Index2</i>	1.0000	1.0000	0.9714	1.0000	1.0000	1.0000	0.9998	1.0000	1.0000	1.0000
<i>Index3</i>	0.8209	0.9039	0.7628	0.9495	0.8348	0.8619	0.6213	0.7844	0.7515	0.7896
<i>Index4</i>	0.9994	0.9991	0.9528	0.9997	0.9984	0.9996	0.9949	0.9995	1.0000	0.9962
<i>Index5</i>	0.9998	0.9996	0.9553	0.9996	0.9987	0.9992	0.9943	0.9990	0.9997	0.9961
<i>Index6</i>	0.9179	0.8910	0.8473	0.9394	0.8051	0.9301	0.8525	0.9150	0.8620	0.8397
<i>Index7</i>	0.8406	0.8313	0.7901	0.8651	0.7572	0.8686	0.8085	0.8768	0.7925	0.8385
<i>Index8</i>	0.9212	0.9270	0.9057	0.9377	0.9348	0.9345	0.9414	0.9245	0.9208	0.9381
<i>Index9</i>	0.9490	0.9675	0.9045	0.8866	0.9274	0.9139	0.8976	0.9290	0.9061	0.9239
<i>Index10</i>	0.9996	0.9878	0.9372	0.9827	0.9577	0.9971	0.9857	0.9937	0.9832	0.9636
<i>Index11</i>	1.0000	1.0000	0.9714	1.0000	1.0000	1.0000	0.9998	1.0000	1.0000	1.0000
<i>Index12</i>	1.0000	1.0000	0.9714	1.0000	1.0000	1.0000	0.9998	1.0000	1.0000	1.0000
<i>Index13</i>	0.9405	0.9014	0.8771	0.9594	0.8274	0.9421	0.8755	0.9539	0.8961	0.8662
<i>Index14</i>	1.0000	1.0000	0.9685	1.0000	0.9997	1.0000	0.9994	1.0000	1.0000	0.9984
<i>Index15</i>	1.0000	1.0000	0.9522	1.0000	0.9991	1.0000	0.9962	1.0000	1.0000	0.9974

**Table 5.** Average BER values considering all the watermarks corresponding to each attack.

Image/ Attack	<i>Image1</i>	<i>Image2</i>	<i>Image3</i>	<i>Image4</i>	<i>Image5</i>	<i>Image6</i>	<i>Image7</i>	<i>Image8</i>	<i>Image9</i>	<i>Image10</i>
<i>Index0</i>	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
<i>Index1</i>	0.1826	0.1984	0.2444	0.1650	0.2952	0.1710	0.2338	0.1744	0.2432	0.2564
<i>Index2</i>	0.0000	0.0000	0.0231	0.0000	0.0000	0.0000	0.0002	0.0000	0.0000	0.0000
<i>Index3</i>	0.1448	0.0799	0.1848	0.0440	0.1331	0.1130	0.2713	0.1708	0.1915	0.1667
<i>Index4</i>	0.0004	0.0007	0.0378	0.0002	0.0013	0.0003	0.0040	0.0004	0.0001	0.0031
<i>Index5</i>	0.0001	0.0003	0.0356	0.0003	0.0011	0.0005	0.0046	0.0009	0.0003	0.0033
<i>Index6</i>	0.0647	0.0884	0.1284	0.0494	0.1586	0.0574	0.1201	0.0681	0.1120	0.1309
<i>Index7</i>	0.1230	0.1328	0.1866	0.1035	0.1945	0.1028	0.1514	0.0973	0.1655	0.1266
<i>Index8</i>	0.0636	0.0585	0.0754	0.0500	0.0521	0.0524	0.0468	0.0606	0.0636	0.0495
<i>Index9</i>	0.0408	0.0258	0.0770	0.0921	0.0590	0.0696	0.0828	0.0576	0.0763	0.0616
<i>Index10</i>	0.0003	0.0098	0.0502	0.0136	0.0338	0.0022	0.0115	0.0048	0.0132	0.0289
<i>Index11</i>	0.0000	0.0000	0.0231	0.0000	0.0000	0.0000	0.0002	0.0000	0.0000	0.0000
<i>Index12</i>	0.0000	0.0000	0.0231	0.0000	0.0000	0.0000	0.0002	0.0000	0.0000	0.0000
<i>Index13</i>	0.0473	0.0805	0.1004	0.0333	0.1414	0.0477	0.1017	0.0370	0.0840	0.1087
<i>Index14</i>	0.0000	0.0000	0.0255	0.0000	0.0002	0.0000	0.0005	0.0000	0.0000	0.0013
<i>Index15</i>	0.0000	0.0000	0.0383	0.0000	0.0007	0.0000	0.0031	0.0000	0.0000	0.0021



**Figure 7.** Average NCC values corresponding to each image, taking all the attacks.



**Figure 8.** Average BER values corresponding to each image, taking all the attacks.

#### 4.4. Comparison with Similar Schemes

This section compares the proposed watermarking scheme with other related watermarking schemes, as presented by Parah et al. [48], Zhang et al. [49], Zeng et al. [50], Su et al. [47], and Elbasi et al. [26]. The schemes selected for the comparison in this study are denoted by scheme1, scheme2, scheme3, scheme4, and scheme5 respectively in Figures 10–13. The reason behind the selection of the schemes is that all these schemes have, in some way or another, utilized an idea that is similar to the proposed scheme. The imperceptibility of the schemes was compared by calculating the average of the imperceptibility measurements of all watermarks for each host image, and the findings are shown in Figures 10 and 11 with the help of bar charts. From these Figures, it can be observed that the PSNR and SSIM values achieved by the proposed watermarking approach are relatively better than those achieved by the other approaches in most cases. The scheme proposed by Zhang et al. [49] is second best in terms of imperceptibility. The proposed scheme's average PSNR and SSIM are also greater than those of competing schemes.

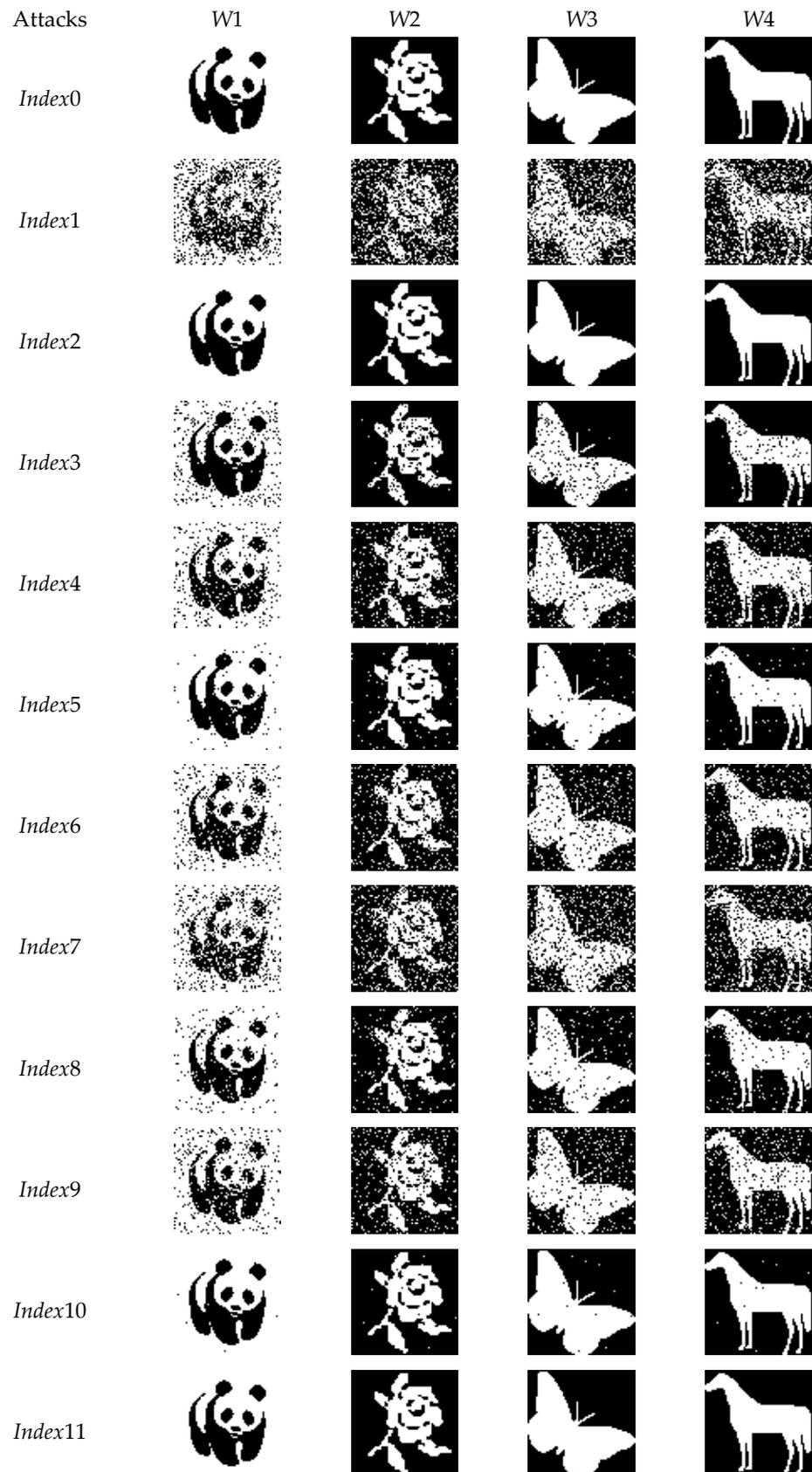


Figure 9. Cont.

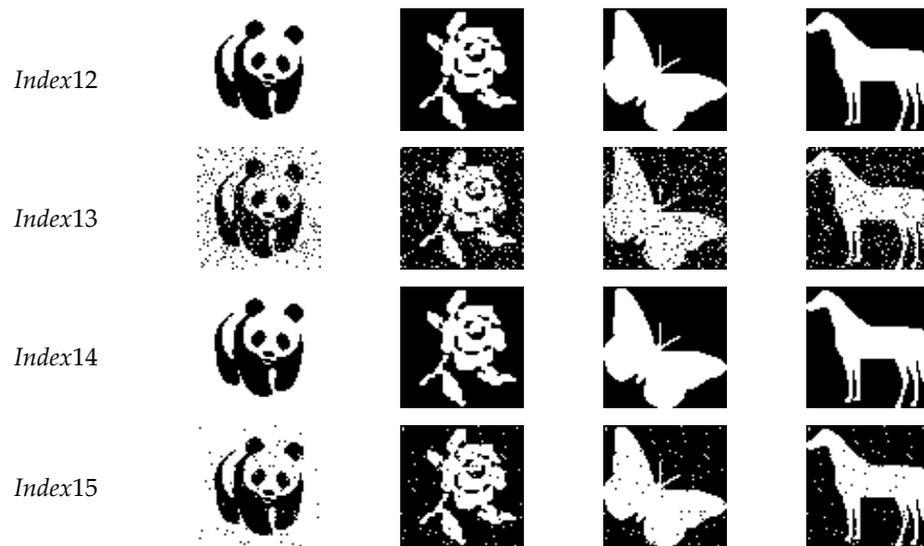


Figure 9. Extracted watermarks from watermarked images corresponding to various distortion attacks.

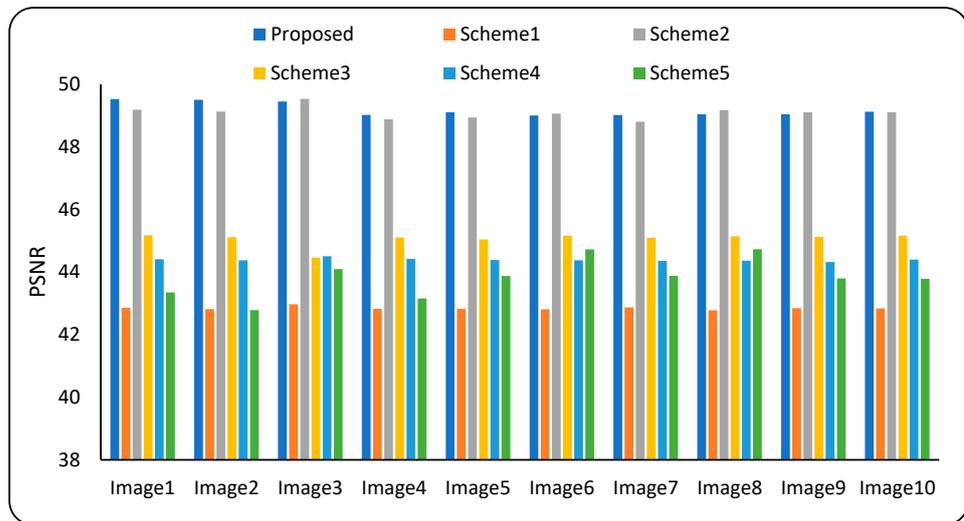


Figure 10. Average PSNR over all the watermarks and all the attacks corresponding to each image.

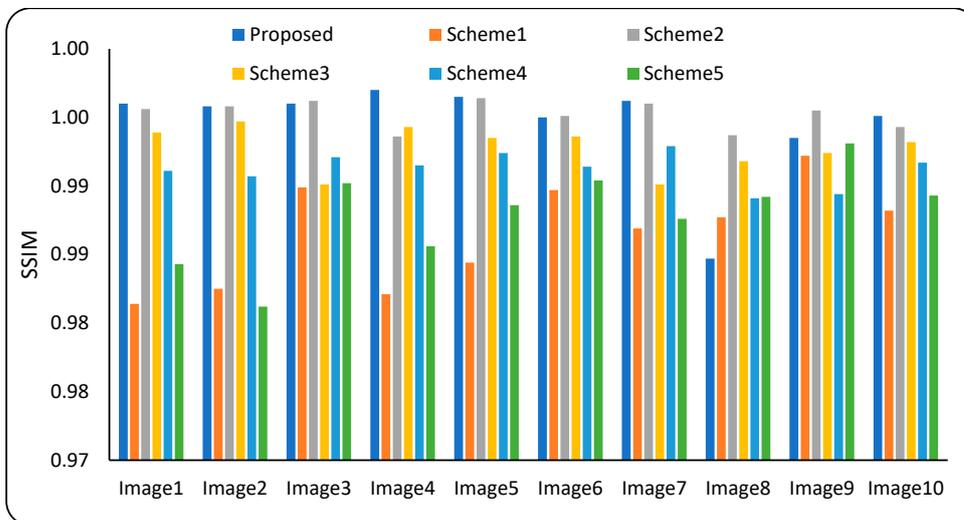


Figure 11. Average SSIM over all the watermarks and all the attacks corresponding to each image.

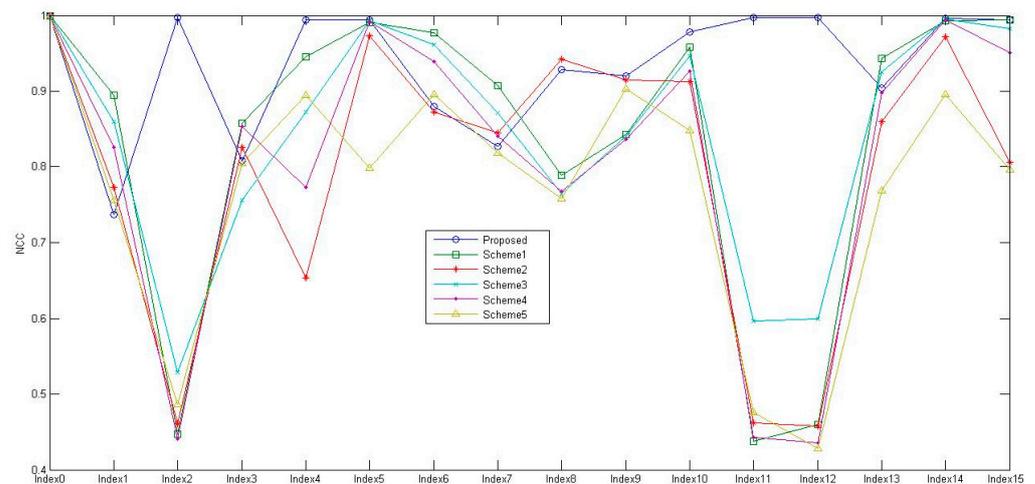


Figure 12. Average NCC over all watermarks and all images corresponding to each attack.

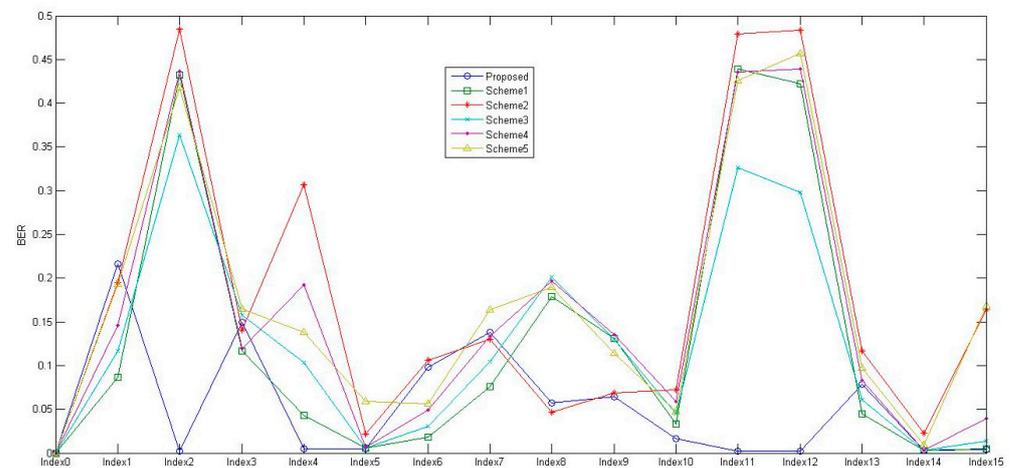


Figure 13. Average BER over all watermarks and all images corresponding to each attack.

To evaluate the robustness of the schemes, the average NCC values for all test images and all watermarks corresponding to each attack were calculated and are reported in Figure 12. The results of using a similar approach to determine the BER are shown in Figure 13. A close examination of these Figures reveals that, for attack *indices 2, 11, and 12*, which are rotation, row flipping, and column flipping, respectively, the performance of the other schemes is noticeably worse than the proposed scheme. The proposed watermarking scheme’s ability to retrieve the watermarks exactly as they were inserted is demonstrated by the NCC values of 1 and BER values of 0 in the cases of 90-degree rotation and row and column flipping (*index2, index11, and index12*). Similarly, in the other instances, the proposed scheme performed reasonably well compared to the alternative schemes. In a few instances, such as *indices 1, 3, and 7*, it did not perform as expected, requiring further investigation into the causes of its failure to meet expectations.

Schemes were also compared based on their computational time in terms of embedding and extraction times, and they are provided in Table 6. The basic purpose of copyright protection watermarking schemes is to demonstrate ownership regardless of time. Therefore, this is not a vital element in these situations; however, it cannot be ignored in broadcast monitoring when embedding and extraction are conducted live. In Table 6, it is evident that the computational complexity of the proposed scheme is greater than the other schemes but comparable to the scheme provided by Zhang et al. [49] and is less than the scheme proposed by Elbasi et al. [26]. This is due to the time required to redistribute the pixels in the image to their new locations in order to obtain singular values that are invariant.

The proposed scheme achieved better imperceptibility and robustness at the cost of high complexity. Hence, reducing the complexity of this approach may be a future study topic.

**Table 6.** Watermark embedding and extraction times of the schemes.

Time	Proposed	Parah et al. [48]	Zhang et al. [49]	Zeng et al. [50]	Su et al. [47]	Elbasi et al. [26]
Embedding time	0.3086	0.0246	0.3041	0.0279	0.0288	1.3742
Extraction time	0.2895	0.0092	0.2837	0.0090	0.0144	0.9874
Total	0.5982	0.0339	0.5878	0.0369	0.0432	2.3616

## 5. Conclusions

This study proposes a robust image watermarking scheme that is based on a block-wise maximum singular value produced by the matrix 2-norm without an SVD transformation. These singular values are insensitive to ninety-degree rotations and row and column flips and are used to modify the pixel values in the spatial domain using a quantization parameter to incorporate the watermark's information. This study presents an alternate method for enhancing image watermarking schemes by using block-wise invariant singular values. The experimental results of the proposed watermarking system were analyzed using ten standard test images, four binary watermarks, and fifteen image distortion attacks. The examination of the numerical data and the quality of the recovered watermark images revealed that the proposed watermarking scheme worked extremely well against the majority of attacks considered in this study. The proposed scheme performed better on average than the other schemes tested in terms of imperceptibility and robustness. However, it did not operate as intended in some situations, indicating that additional research is needed in this domain. The complexity of the proposed scheme is slightly higher than that of the other schemes but comparable, so reducing this scheme's complexity may be the next step in this study. This approach may also be used for color images, medical images, and video and audio watermarking.

**Funding:** This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia [Grant No. 3405].

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** All the relevant data is contained within the article, further inquiries can be directed to the corresponding author.

**Conflicts of Interest:** The author declares no conflict of interest.

## References

- Dhawan, S.; Gupta, R. Analysis of Various Data Security Techniques of Steganography: A Survey. *Inf. Secur. J. A Glob. Perspect.* **2020**, *30*, 63–87. [\[CrossRef\]](#)
- Huh, J.H.; Seo, Y.S. Understanding Edge Computing: Engineering Evolution with Artificial Intelligence. *IEEE Access* **2019**, *7*, 164229–164245. [\[CrossRef\]](#)
- Tran, D.T.; Huh, J.H. Forecast of Seasonal Consumption Behavior of Consumers and Privacy-Preserving Data Mining with New S-Apriori Algorithm. *J. Supercomput.* **2023**, 1–46. [\[CrossRef\]](#)
- Cox, I.; Miller, M.L.; Bloom, J.A. *Digital Watermarking*; Morgan Kaufmann Publishers Inc.: Burlington, MA, USA, 2001; ISBN 1-55860-714-5.
- Gupta, S.; Saluja, K.; Solanki, V.; Kaur, K.; Singla, P.; Shahid, M. Efficient Methods for Digital Image Watermarking and Information Embedding. *Meas. Sens.* **2022**, *24*, 100520. [\[CrossRef\]](#)
- Sanivarapu, P.V.; Rajesh, K.N.V.P.S.; Hosny, K.M.; Fouda, M.M. Digital Watermarking System for Copyright Protection and Authentication of Images Using Cryptographic Techniques. *Appl. Sci.* **2022**, *12*, 8724. [\[CrossRef\]](#)
- El-Kenawy, E.S.M.; Khodadadi, N.; Khoshnaw, A.; Mirjalili, S.; Alhussan, A.A.; Khafaga, D.S.; Ibrahim, A.; Abdelhamid, A.A. Advanced Dipper-Throated Meta-Heuristic Optimization Algorithm for Digital Image Watermarking. *Appl. Sci.* **2022**, *12*, 10642. [\[CrossRef\]](#)
- Wan, W.; Wang, J.; Zhang, Y.; Li, J.; Yu, H.; Sun, J. A Comprehensive Survey on Robust Image Watermarking. *Neurocomputing* **2022**, *488*, 226–247. [\[CrossRef\]](#)

9. Giri, K.J.; Quadri, S.M.K.; Bashir, R.; Bhat, J.I. DWT Based Color Image Watermarking: A Review. *Multimed. Tools Appl.* **2020**, *79*, 32881–32895. [[CrossRef](#)]
10. Alshoura, W.H.; Zainol, Z.; Teh, J.S.; Alawida, M.; Alabdulatif, A. Hybrid SVD-Based Image Watermarking Schemes: A Review. *IEEE Access* **2021**, *9*, 32931–32968. [[CrossRef](#)]
11. Abdulloh, F.F.; Rahardi, M.; Putra, W.S.; Amikom, Y.; Sleman, I. A Blind Robust Image Watermarking on Selected DCT Coefficients for Copyright Protection. *Artic. Int. J. Adv. Comput. Sci. Appl.* **2022**, *13*, 2022. [[CrossRef](#)]
12. Ray, A.; Roy, S. Recent Trends in Image Watermarking Techniques for Copyright Protection: A Survey. *Int. J. Multimed. Inf. Retr.* **2020**, *9*, 249–270. [[CrossRef](#)]
13. Boujerfaoui, S.; Riad, R.; Douzi, H.; Ros, F.; Harba, R. Image Watermarking between Conventional and Learning-Based Techniques: A Literature Review. *Electronics* **2022**, *12*, 74. [[CrossRef](#)]
14. Khan, A.; Siddiqa, A.; Munib, S.; Malik, S.A. A Recent Survey of Reversible Watermarking Techniques. *Inf. Sci.* **2014**, *279*, 251–272. [[CrossRef](#)]
15. Ahmadi, S.B.B.; Zhang, G.; Wei, S. Robust and Hybrid SVD-Based Image Watermarking Schemes: A Survey. *Multimed. Tools Appl.* **2020**, *79*, 1075–1117. [[CrossRef](#)]
16. Mehraj, S.; Mushtaq, S.; Parah, S.A.; Giri, K.J.; Sheikh, J.A.; Gandomi, A.H.; Hijji, M.; Muhammad, K. Spatial Domain-Based Robust Watermarking Framework for Cultural Images. *IEEE Access* **2022**, *10*, 117248–117260. [[CrossRef](#)]
17. Ali, M.; Ahn, C.W.; Pant, M.; Kumar, S.; Singh, M.K.; Saini, D. An Optimized Digital Watermarking Scheme Based on Invariant DC Coefficients in Spatial Domain. *Electronics* **2020**, *9*, 1428. [[CrossRef](#)]
18. Su, Q.; Yuan, Z.; Liu, D. An Approximate Schur Decomposition-Based Spatial Domain Color Image Watermarking Method. *IEEE Access* **2019**, *7*, 4358–4370. [[CrossRef](#)]
19. Bin Faheem, Z.; Ishaq, A.; Rustam, F.; Díez, I.D.L.T.; Gavilanes, D.; Vergara, M.M.; Ashraf, I. Image Watermarking Using Least Significant Bit and Canny Edge Detection. *Sensors* **2023**, *23*, 1210. [[CrossRef](#)]
20. Bin Faheem, Z.; Ali, M.; Raza, M.A.; Arslan, F.; Ali, J.; Masud, M.; Shorfuzzaman, M. Image Watermarking Scheme Using LSB and Image Gradient. *Appl. Sci.* **2022**, *12*, 4202. [[CrossRef](#)]
21. Sakthivel, S.M.; Sankar, A.R. Computation-Efficient Image Watermarking Architecture with Improved Performance. *Comput. Electr. Eng.* **2020**, *84*, 106649. [[CrossRef](#)]
22. Yuan, Z.; Liu, D.; Zhang, X.; Su, Q. New Image Blind Watermarking Method Based on Two-Dimensional Discrete Cosine Transform. *Optik* **2020**, *204*, 164152. [[CrossRef](#)]
23. Ariatmanto, D.; Ernawan, F. Adaptive Scaling Factors Based on the Impact of Selected DCT Coefficients for Image Watermarking. *J. King Saud Univ. Comput. Inf. Sci.* **2022**, *34*, 605–614. [[CrossRef](#)]
24. Pei, L. Research on Digital Image Watermarking Algorithm Based on Scrambling and Singular Value Decomposition. *J. Math.* **2022**, *2022*, 4656010. [[CrossRef](#)]
25. Singh, R.; Izhar, L.I.; Elamvazuthi, I.; Ashok, A.; Aole, S.; Sharma, N. Efficient Watermarking Method Based on Maximum Entropy Blocks Selection in Frequency Domain for Color Images. *IEEE Access* **2022**, *10*, 52712–52723. [[CrossRef](#)]
26. Elbasi, E.; Mostafa, N.; Cina, E. Robust, Secure and Semi-Blind Watermarking Technique Using Flexible Scaling Factor in Block-Based Wavelet Algorithm. *Electronics* **2022**, *11*, 3680. [[CrossRef](#)]
27. Li, L.; Xu, H.H.; Chang, C.C.; Ma, Y.Y. A Novel Image Watermarking in Redistributed Invariant Wavelet Domain. *J. Syst. Softw.* **2011**, *84*, 923–929. [[CrossRef](#)]
28. Liu, D.; Yuan, Z.; Su, Q. A Blind Color Image Watermarking Scheme with Variable Steps Based on Schur Decomposition. *Multimed. Tools Appl.* **2020**, *79*, 7491–7513. [[CrossRef](#)]
29. Prabha, K.; Shatheesh Sam, I. An Effective Robust and Imperceptible Blind Color Image Watermarking Using WHT. *J. King Saud Univ. Comput. Inf. Sci.* **2022**, *34*, 2982–2992. [[CrossRef](#)]
30. Garg, P.; Jain, A. A Robust Technique for Biometric Image Authentication Using Invisible Watermarking. *Multimed. Tools Appl.* **2023**, *82*, 2237–2253. [[CrossRef](#)]
31. Zermi, N.; Khaldi, A.; Kafi, M.R.; Kahlessenane, F.; Euschi, S. Robust SVD-Based Schemes for Medical Image Watermarking. *Microprocess. Microsyst.* **2021**, *84*, 104134. [[CrossRef](#)]
32. Shoron, S.H.; Islam, M.; Uddin, J.; Shon, D.; Im, K.; Park, J.H.; Lim, D.S.; Jang, B.; Kim, J.M. A Watermarking Technique for Biomedical Images Using Smqt, Otsu, and Fuzzy c-Means. *Electronics* **2019**, *8*, 975. [[CrossRef](#)]
33. Maity, S.P.; Maity, S.; Sil, J.; Delpha, C. Collusion Resilient Spread Spectrum Watermarking in M-Band Wavelets Using GA-Fuzzy Hybridization. *J. Syst. Softw.* **2013**, *86*, 47–59. [[CrossRef](#)]
34. Yang, H.-Y.; Wang, X.-Y.; Zhang, Y.; E-nuo, M. Robust Digital Watermarking in PDTDFB Domain Based on Least Squares Support Vector Machine. *Eng. Appl. Artif. Intell.* **2013**, *26*, 2058–2072. [[CrossRef](#)]
35. Takore, T.T.; Rajesh Kumar, P.; Lavanya Devi, G. A New Robust and Imperceptible Image Watermarking Scheme Based on Hybrid Transform and PSO. *Int. J. Intell. Syst. Appl.* **2018**, *10*, 50–63. [[CrossRef](#)]
36. Devi, K.J.; Singh, P.; Dash, J.K.; Thakkar, H.K.; Santamaria, J.; Krishna, M.V.J.; Romero-Manchado, A. A New Robust and Secure 3-Level Digital Image Watermarking Method Based on G-BAT Hybrid Optimization. *Mathematics* **2022**, *10*, 3015. [[CrossRef](#)]
37. Pallaw, V.K.; Singh, K.U.; Kumar, A.; Singh, T.; Swarup, C.; Goswami, A. A Robust Medical Image Watermarking Scheme Based on Nature-Inspired Optimization for Telemedicine Applications. *Electronics* **2023**, *12*, 334. [[CrossRef](#)]

38. Garg, P.; Kishore, R.R. An Efficient and Secured Blind Image Watermarking Using ABC Optimization in DWT and DCT Domain. *Multimed. Tools Appl.* **2022**, *81*, 36947–36964. [[CrossRef](#)]
39. Wang, L.; Ji, H.A.; Wang, L.; Ji, H. A Watermarking Optimization Method Based on Matrix Decomposition and DWT for Multi-Size Images. *Electronics* **2022**, *11*, 2027. [[CrossRef](#)]
40. Ali, M.; Ahn, C.W.; Pant, M.; Siarry, P. An Image Watermarking Scheme in Wavelet Domain with Optimized Compensation of Singular Value Decomposition via Artificial Bee Colony. *Inf. Sci.* **2015**, *301*, 44–60. [[CrossRef](#)]
41. Maity, S.P.; Maity, S.; Sil, J.; Delpha, C. Perceptually Adaptive MC-SS Image Watermarking Using GA-NN Hybridization in Fading Gain. *Eng. Appl. Artif. Intell.* **2014**, *31*, 3–14. [[CrossRef](#)]
42. Goyal, A.; Malik, M.; Sharma, S.; Choudhary, S.; Sharma, V.K.; Goyal, A. Image Watermarking in Frequency Domain Using Hu's Invariant Moments and Firefly Algorithm. *Int. J. Image Graph. Signal Process.* **2022**, *2*, 1–15. [[CrossRef](#)]
43. Yazdan Bakhsh, F.; Moghaddam, M.E. A Robust HDR Images Watermarking Method Using Artificial Bee Colony Algorithm. *J. Inf. Secur. Appl.* **2018**, *41*, 12–27. [[CrossRef](#)]
44. Cedillo-Hernandez, M.; Cedillo-Hernandez, A.; Garcia-Ugalde, F.J. Improving DFT-Based Image Watermarking Using Particle Swarm Optimization Algorithm. *Mathematics* **2021**, *9*, 1795. [[CrossRef](#)]
45. Moosazadeh, M.; Ekbatanifard, G. A New DCT-Based Robust Image Watermarking Method Using Teaching-Learning-Based Optimization. *J. Inf. Secur. Appl.* **2019**, *47*, 28–38. [[CrossRef](#)]
46. Hatami, E.; Rashidy Kanan, H.; Layeghi, K.; Harounabadi, A. An Optimized Robust and Invisible Digital Image Watermarking Scheme in Contourlet Domain for Protecting Rightful Ownership. *Multimed. Tools Appl.* **2023**, *82*, 2021–2051. [[CrossRef](#)]
47. Su, Q.; Niu, Y.; Wang, Q.; Sheng, G. A Blind Color Image Watermarking Based on DC Component in Thespatial Domain. *Optik* **2013**, *124*, 6255–6260. [[CrossRef](#)]
48. Parah, S.A.; Loan, N.A.; Shah, A.A.; Sheikh, J.A.; Bhat, G.M. A New Secure and Robust Watermarking Technique Based on Logistic Map and Modification of DC Coefficient. *Nonlinear Dyn.* **2018**, *93*, 1933–1951. [[CrossRef](#)]
49. Zhang, H.; Wang, C.; Zhou, X. A Robust Image Watermarking Scheme Based on SVD in the Spatial Domain. *Future Internet* **2017**, *9*, 45. [[CrossRef](#)]
50. Zeng, G.; Qiu, Z. Image Watermarking Based on DC Component in DCT. In Proceedings of the 2nd 2008 International Symposium on Intelligent Information Technology Application Workshop, IITA 2008 Workshop, Shanghai, China, 21–22 December 2008; pp. 573–576. [[CrossRef](#)]
51. Zhang, M.; Ding, W.; Li, Y.; Sun, J.; Liu, Z. Color Image Watermarking Based on a Fast Structure-Preserving Algorithm of Quaternion Singular Value Decomposition. *Signal Process.* **2023**, *208*, 108971. [[CrossRef](#)]
52. Zhao, J.; Xu, W.; Zhang, S.; Fan, S.; Zhang, W. A Strong Robust Zero-Watermarking Scheme Based on Shearlets' High Ability for Capturing Directional Features. *Math. Probl. Eng.* **2016**, *2016*, 2643263. [[CrossRef](#)]
53. Ali, M.; Ahn, C.W.; Pant, M.; Siarry, P. A Reliable Image Watermarking Scheme Based on Redistributed Image Normalization and SVD. *Discret. Dyn. Nat. Soc.* **2016**, *2016*, 3263587. [[CrossRef](#)]
54. Bakhshandeh, A.; Eslami, Z. An Authenticated Image Encryption Scheme Based on Chaotic Maps and Memory Cellular Automata. *Opt. Lasers Eng.* **2013**, *51*, 665–673. [[CrossRef](#)]

**Disclaimer/Publisher's Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.