electronics

MDPI

Article

A Robust Zero-Watermarking Scheme in Spatial Domain by Achieving Features Similar to Frequency Domain

Musrrat Ali [1,*] and Sanoj Kumar [2]

[1] Department of Basic Sciences, PYD, King Faisal University, Al Ahsa 31982, Saudi Arabia
[2] Department of Computer Science, UPES, Dehradun 248007, India
* Correspondence: mkasim@kfu.edu.sa

Abstract: In recent years, there has been a substantial surge in the application of image watermarking, which has evolved into an essential tool for identifying multimedia material, ensuring security, and protecting copyright. Singular value decomposition (SVD) and discrete cosine transform (DCT) are widely utilized in digital image watermarking despite the considerable computational burden they involve. By combining block-based direct current (DC) values with matrix norm, this research article presents a novel, robust zero-watermarking approach. It generates a zero-watermark without attempting to modify the contents of the image. The image is partitioned into non-overlapping blocks, and DC values are computed without applying DCT. This sub-image is further partitioned into non-overlapping blocks, and the maximum singular value of each block is calculated by matrix norm instead of SVD to obtain the binary feature matrix. A piecewise linear chaotic map encryption technique is utilized to improve the security of the watermark image. After that, the feature image is created via XOR procedure between the encrypted watermark image and the binary feature matrix. The proposed scheme is tested using a variety of distortion attacks including noise, filter, geometric, and compression attacks. It is also compared with the other relevant image watermarking methods and outperformed them in most cases.

Keywords: singular value decomposition; discrete cosine transform; matrix norm; zero-watermarking; spatial domain; frequency domain

Citation: Ali, M.; Kumar, S. A Robust Zero-Watermarking Scheme in Spatial Domain by Achieving Features Similar to Frequency Domain. *Electronics* **2024**, *13*, 435. https://doi.org/10.3390/electronics13020435

Academic Editor: Frederic Ros

Received: 26 December 2023
Revised: 16 January 2024
Accepted: 18 January 2024
Published: 20 January 2024

1. Introduction

Digital content has become an essential element of the daily routines of every individual in recent times. Recent technological advancements have made the manipulation and sharing of digital multimedia files easier than ever before. While enjoying the benefits of digital media technology, consumers are vulnerable to the threats of copying and modification without proper authorization while transmitting over public networks. Therefore, it is necessary to defend digital media copyrights. To address such concerns, digital watermarking technology was developed [1–4], and it has since evolved into a distinct area of study that is receiving considerable attention from scholars [5–7]. By incorporating watermark information into digital content, digital watermarking ensures its copyright protection. However, this embedded information would make some dents in the original image quality that can be measured in terms of imperceptibility. Any robust image watermarking technique must possess two primary qualities: imperceptibility and robustness. Robustness is defined as the capacity to withstand and recover from a wide range of threats. Imperceptibility refers to the impact that watermark embedding, or attack, has on the aesthetic value of an image. Both attributes are in direct opposition to one another, and achieving a balance between them is perpetually a difficult problem for image watermarking schemes. Hence, it is essential to develop a lossless copyright protection system, and zero-watermarking schemes were invented to achieve it. Zero-watermarking strategies that employ the zero-embedding technique preserve the integrity of the original image and

can be used to safeguard copyright [8]. This ensures that the quality of the image remains unaltered. In contrast to traditional watermarking, zero-watermarking has emerged as a key topic of research in digital watermarking technology due to its ability to retain the high quality of the original image.

Initially, a zero-watermarking technique was introduced by Wen et al. [8]. By employing high-order cumulants for the extraction of image features, this methodology demonstrated remarkable resistance against common image processing attacks. Since then, several research initiatives have been invested in the development of strong zero-watermarking technologies. Rawat et al. [9] devised a zero image watermarking system using ownership sharing and visual secret sharing with the help of fractional Fourier transform and visual cryptography. Their approach demonstrated promising outcomes against some attacks. By utilizing quaternion exponent moments (QEMs), Wang et al. [10] developed a robust image zero-watermarking technique that effectively resisted image manipulation attacks. Shao et al. [11] developed a double zero watermarking scheme that was both robust and effective in protecting the copyright of two images simultaneously. To generate verification images, they implemented scrambled watermarks, and feature images were generated by utilizing the invariants of orthogonal Fourier–Mellin moments (OFMMs). Based on SVD and contourlet transform-SVD (CTSVD), Kavitha et al. [12] suggested two zero-watermarking techniques for image authentication. Considering their remarkable security and robustness, both the schemes are promising options for protecting image copyright. Wu et al. [13] suggested a zero-watermarking technique based on DCT and contourlet transform to guarantee the security of the watermark information in a chaotic environment. The approach used contourlet transform to fetch the texture information and DCT to retrieve the characteristic sequence in the low frequency direction of the sub-band, and logistic map encryption to encrypt the watermark. Liu et al. [14] developed a zero image watermarking technique that incorporates the dual-tree complex wavelet transform with the discrete cosine transform (DTCWT-DCT). They improved this method by creating a more robust zero-watermarking scheme utilizing the Henon map and DTCWT-DCT [15]. This algorithm effectively preserved the original images' integrity while attaining an obvious degree of robustness. Kang et al. [16] developed an innovative zero-watermarking technique for color images by integrating polar harmonic transformations and a 2D logistic-adjusted sine map (2D-LASM). This approach shows commendable robustness and distinguishability. Kang et al. [17] introduced a zero-watermarking system established on the majority voting idea, discrete wavelet transform (DWT), and SVD. Huang et al. [18] developed a resilient zero-watermarking method by utilizing the double-tree complex wavelet transform, multi-level discrete cosine transform (MDCT), and Hessenberg decomposition. By relying on the consistency of the relationships between moment magnitudes that occur in the same order and moment magnitudes that occur with the same repetition, Wang et al. [19] suggested a zero-watermarking approach utilizing the polar complex exponential transform (PCET). The aim of the scheme was to enhance its capability under geometric attacks. Xia et al. [20] introduced the decimal-order polar harmonic transforms moment (DPHTM) in zero image watermarking to achieve high robustness. Tsai et al. [21] employed discrete Fourier transform (DFT) in conjunction with log-polar mapping to ascertain the translation, scaling, and rotation invariants during zero-watermark production. While extracting the zero-watermark, the estimation of the zero-watermark signal is accomplished by employing a trained SVM as the mapping and particle swarm optimization (PSO) to determine the optimal SVM parameters. Utilizing QR decomposition with 1D-DCT, Thanh et al. [22] developed a zero-watermarking approach. In order to scramble the image, the system employs permuted visual map feature (PVMF) and visual map feature (VMF). Ali et al. [23] introduced a zero-watermarking technique as a means of safeguarding the confidentiality of telemedicine patients. To embed an individual's identity in medical speech signals without introducing distortion, the method determines the best regions within the signal for identity insertion by calculating the zero-crossing and Hurst exponent. A lossless robust image watermarking technique was proposed by Ali et al. [24]. This method incor-

porates visual cryptography, singular value decomposition, discrete wavelet transform, and discrete Fourier transform. A distinct zero-watermarking technique that combines similarity-based retrieval and copyright protection for fundus images was developed in [25]. For the protection of copyright, [26] suggests a color image zero-watermarking approach. This approach makes use of quaternion singular value decomposition and demonstrates substantial resistance to geometric attacks like rotation and scaling, in addition to typical signal processing attacks. Based on a combination of SVD and DWT, Singh et al. [27] developed a zero-watermarking technique that generates watermarks using singular value coefficients in the wavelet domain. A robust zero watermarking algorithm is reported in [28] using a NasNet-Mobile convolutional neural network and DCT. To strengthen the security of the data, the chaos mapping technique is used to scramble the watermark data prior to watermark embedding. Following this, the zero watermarking approach is implemented so that it may extract and insert the watermark from the medical image without altering its information.

Overall, the zero-watermarking strategies stated above support the improvement of digital image zero-watermarking schemes. Zero-watermarking in the spatial domain is a straightforward method for embedding watermarks that uses feature extraction algorithms. These techniques, however, have a rather poor resistance to attacks. However, frequency domain-based zero-watermarking offers a wider range of approaches for feature extraction by flexibly processing images using frequency domain transformation tools. Moreover, the characteristics that are retrieved in the frequency domain exhibit relatively better robustness than the spatial domain against various forms of attack. Furthermore, the computational complexity of frequency domain watermarking schemes is high in comparison to spatial domain schemes [29]. Keeping all the above-mentioned issues in mind, the objective of this article is to develop a robust zero-watermarking scheme in the spatial domain, obtaining features like the frequency domain.

This study introduces an innovative, robust zero-watermarking method through the integration of block-based DC values with matrix norm. Without attempting to modify the integrity of the host image, it generates a zero-watermark by fetching image invariant features. Without using DCT, DC values are computed in spatial domain upon partitioning the host image into blocks. The binary feature matrix is obtained by further dividing this sub-image into blocks and computing the maximum singular value using matrix norm rather than SVD. A piecewise linear chaotic map encryption strategy is employed to prop up the security of the watermark image. The feature image is then formed by carrying out an XOR procedure on the binary feature matrix and the encrypted watermark image. Several distortion attacks, including noise, filter, geometric, and compression attacks, were employed to evaluate the proposed method. Furthermore, when compared to other relevant image watermarking schemes, it demonstrated superior performance in the majority of instances.

The objective and motivation behind this research are to investigate a robust and efficient zero-watermarking technique for digital images that meets high robustness standards. An overview of the major contributions of this research is provided below:

1. Developing a novel zero-watermarking approach for the spatial domain that exhibits characteristics comparable to those of the frequency domain.
2. Assessment of the suggested concept's efficacy for grayscale images by use of several evaluation measures and attacks.
3. Comparison of the execution times of the proposed technique with its variant, which uses DCT and SVD.

The article is organized as follows: In Section 2, preliminary materials are presented. In Section 3, the proposed zero-watermarking technique is explained. Section 4 presents a comparison and analysis of the results. Section 5 offers the final remarks and research ideas.

2. Preliminaries

This segment provides a concise overview of the principles associated with the proposed watermarking scheme. For additional information, researchers may consult the accompanying references [3,12,13,30].

2.1. DC Coefficient Computation in Spatial Domain

Among the various mathematical transforms, the discrete cosine transform (DCT) has a broad range of applications in watermarking and image processing [5]. This technique is utilized in the reconstruction of original data from frequency data and helps the transfer of signals from the spatial domain to the frequency domain. The converted signal comprises a single component of direct current (DC), which is the average value of the provided data, along with several components of alternating current (AC). DCT may be used to transform a digital image 'A' of size m × m from the spatial domain to the frequency domain image 'B' of the same size. Subsequently, inverse DCT can be employed to rebuild the original image A from its corresponding frequency data. The following mathematical equations describe DCT and inverse DCT:

$$B(u,v) = \alpha_u \alpha_v \sum_{x=0}^{m-1} \sum_{y=0}^{m-1} A(x,y) \times \cos\left[\frac{(2x+1)u\pi}{2m}\right] \times \cos\left[\frac{(2y+1)v\pi}{2m}\right], \quad (1)$$

$$A(x,y) = \sum_{u=0}^{m-1} \sum_{v=0}^{m-1} \alpha_u \alpha_v \, B(u,v) \times \cos\left[\frac{(2x+1)u\pi}{2m}\right] \times \cos\left[\frac{(2y+1)v\pi}{2m}\right], \quad (2)$$

where

$$\alpha_u = \begin{cases} \sqrt{1/m} & if\ u = 0 \\ \sqrt{2/m} & else \end{cases}, \ \alpha_v = \begin{cases} \sqrt{1/m} & if\ v = 0 \\ \sqrt{2/m} & else \end{cases}. \quad (3)$$

where $x = 0, 1, 2, \ldots, m-1$; $y = 0, 1, 2, \ldots, m-1$ are the pixel's location in the image.

Putting $u = v = 0$ into Equation (1) yields the DC coefficient of the image 'A', which represents the average pixel intensity of the image.

$$DC = B(0,0) = \frac{1}{m} \sum_{x=0}^{m-1} \sum_{y=0}^{m-1} A(x,y) \quad (4)$$

Equation (4) illustrates that the *DC* coefficient may be directly calculated in the spatial domain, bypassing the DCT transform. DCT-based watermarking techniques are typically executed by employing spatially local transformations (block-based DCT). It involves the division of the input image into non-overlapping blocks. The block of dimensions 8 × 8 is a frequently employed block size in DCT watermarking and is also standardized in the JPEG compression standard.

2.2. Singular Value Decomposition (SVD)

Singular value decomposition (SVD) [3] is a powerful tool that is utilized to decompose a rectangular matrix into three matrices: two orthogonal vector matrices and one singular value matrix. There are several applications for it, including data analysis, image processing, and satellite data. By converting correlated variables into an uncorrelated set, it facilitates a clearer understanding of the relationships present in the original data. Numerous watermarking systems have been suggested that make use of singular value decompositions (SVDs) due to their inherent stability, which allows them to endure even the tiniest interruptions in image processing [1,12,17]. A square image 'I' of order m × m may be decomposed into the products of three matrices: a diagonal matrix S, and two orthogonal matrices U and V^T.

$$I = USV^T \quad (5)$$

The arrangement of the elements in the diagonal matrix S is in a decreasing order, as specified in relation (6), where r represents the rank of the matrix.

$$\sigma_1 \geq \sigma_2 \geq \ldots \geq \sigma_r > \sigma_{r+1} = \sigma_{r+2} \ldots = \sigma_m = 0 \tag{6}$$

2.3. Relationship between Maximum Singular Value and Matrix Norm

The Frobenius norm of a matrix A, denoted by $\|A\|_F$, is obtained by taking the square root of the sum of the squares of the singular values. The mathematical equation of this relationship is given here [30]:

$$\|A\|_F = \sqrt{\sum_{i=1}^{m}\sum_{j=1}^{m} a_{i,j}^2} = \sqrt{trace(A^T A)} = \sqrt{\sum_{i=1}^{m} \sigma_i^2}. \tag{7}$$

The maximal singular value of matrix A or the square root of the largest eigenvalue (λ_{max}) of $A^T A$ constitutes the spectral norm. Putting $F = 2$ in Equation (7), we provide the relationship between matrix 2-norm and maximal singular value as follows:

$$\|A\|_2 = \sqrt{\lambda_{\max}(\mathrm{A^T A})} = \sigma_{\max}. \tag{8}$$

Since the maximum singular value of an image remains relatively constant despite standard image processing operations, SVD is a commonly employed approach in digital image watermarking for obtaining the maximum singular value. However, the cost and complexity of SVD computations would be increased due to the matrix product. An alternative expression states that the matrix 2-norm corresponds to the greatest singular value of the matrix. Zhao et al. [30], comparing these two, determined that matrix norm computation is more rapid than SVD. Due to its rapid processing and similar output, the proposed zero-watermarking technique prefers the matrix norm over the SVD to obtain the maximum singular value.

2.4. Piecewise Linear Chaotic Map

To strengthen the security of the watermarking system, a watermark must be scrambled before it is embedded in the cover image. The piecewise linear chaotic map (PWLCM) [31] is one of numerous chaotic maps that may be employed for encryption. It has recently gained attention for its straightforward form, streamlined implementation, and favorable dynamical characteristics. A wide range of applications, including data hiding and encryption, have made extensive use of chaotic signals, which are usually resistant to disturbances because of the poor correlation between starting parameters. In mathematical terms, the PWLCM is denoted by Equation (9):

$$x_{i+1} = f_p(x_i) = \begin{cases} x_i / p & if\ x_i \in [0,\ p) \\ (x_i - p)/(0.5 - p) & if\ x_i \in [p,\ 0.5) \\ f_p(1 - x_i) & if\ x_i \in [0.5,\ 1) \end{cases}. \tag{9}$$

The control parameter, denoted as $p \in (0,\ 0.5)$, and the initial value $x_i \in (0,\ 1)$, are both regarded as the secret key. Extreme sensitivity to beginning circumstances and orbital expansion throughout the entire space are the most appealing characteristics of PWLCM. It transforms the unit interval onto itself in a non-invertible manner.

3. Proposed Zero-Watermarking

This section explains the proposed watermarking technique's aspects, such as zero-watermark generation and watermark recovery from distorted images. In the embedding phase, the zero-watermarking approach does not use inverse operations to obtain the watermarked image. It is the motivation behind the proposed scheme's use of a block-based DC coefficient in a spatial domain and matrix norm to obtain the largest singular

value. A detailed, step-by-step explanation of the scheme is provided here, and a graphical illustration is given in Figure 1.

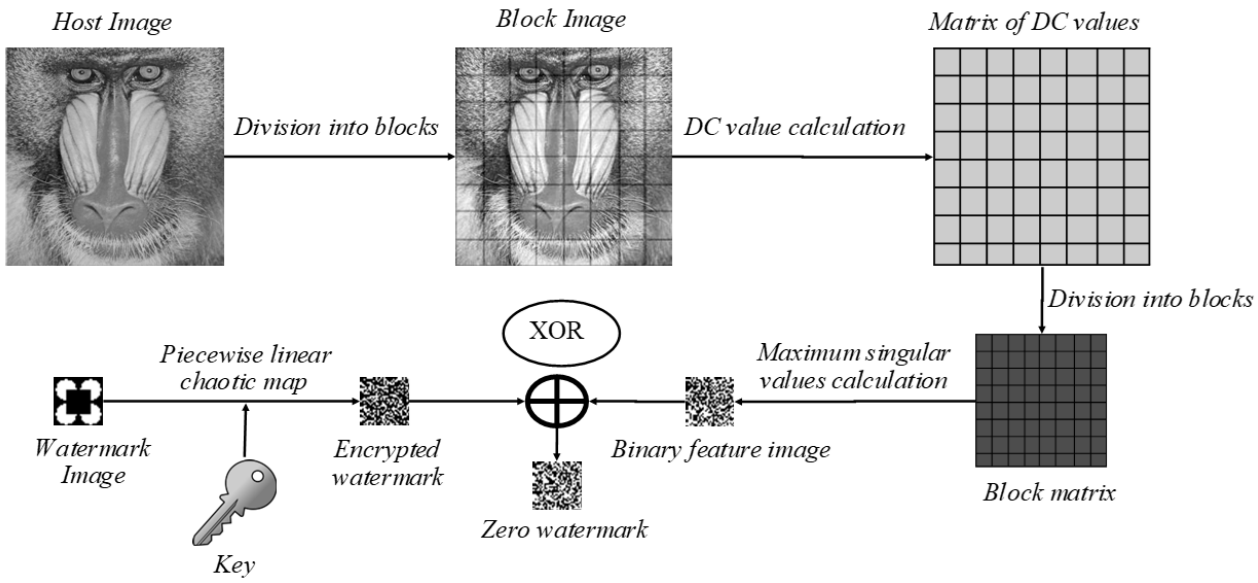

Figure 1. Illustration of zero-watermark generation process.

3.1. Watermark Generation

For the sake of clarity, the process of zero-watermark generation can be divided into the following stages:

- Step 1: Host image 'A' is partitioned into 8×8 non-overlapping blocks $B_{i,j}$ ($i = 1, 2, \ldots, m/8$; $j = 1, 2, \ldots, m/8$), and the DC coefficient of each block is directly calculated with the help of Equation (4) without applying DCT. We adjust the image's dimensions accordingly if their value does not occur as a multiple of eight.
- Step 2: The matrix acquired by the compilation of DC values in step 1 is further partitioned into non-overlapping blocks, and the matrix 2-norm is utilized in place of SVD to determine the block's maximum singular value. This matrix must be divided in such a way that the number of non-overlapping blocks must correspond to the number of watermark bits.
- Step 3: The following rule is applied to the matrix produced by accumulating the maximum singular values acquired in step 2 in order to construct a binary feature (BF) matrix:

$$BF(i,\ j) = \begin{cases} 1 & if\ s_{i,j} \geq s_{avg} \\ 0 & if\ s_{i,j} < s_{avg} \end{cases}, \tag{10}$$

  where $s_{i,j}$ is the maximum singular value of the image block at the location (i, j) and s_{avg} is the average of these singular values.
- Step 4: Apply PWLCM to the watermark image W to obtain its encrypted version to provide an extra security layer.
- Step 5: Zero-watermarking (ZW) is achieved by XOR function between the binary feature (BF) matrix and scrambled watermark image W, as follows:

$$ZW = BF \oplus W. \tag{11}$$

3.2. Watermark Retrieval Process

Watermark W' can be retrieved from the attacked image A' corresponding to the watermark W with the help of zero-watermark ZW generated in the previous section. Here, you may find a comprehensive, precise, and systematic description of the approach. Its graphical illustration is provided in Figure 2.

- Step 1: Apply steps 1 to 3 to the attacked image A' as explained in Section 3.1 to obtain the attacked binary feature matrix BF'.
- Step 2: Apply XOR operation between the attacked binary feature matrix BF' and the zero-watermark ZW to retrieve the W' as follows:

$$W' = BF' \oplus ZW. \tag{12}$$

- Step 3: Using the appropriate secret keys, apply the piecewise linear chaotic map to the encrypted retrieved watermark obtained in step 2 to obtain the decrypted watermark.

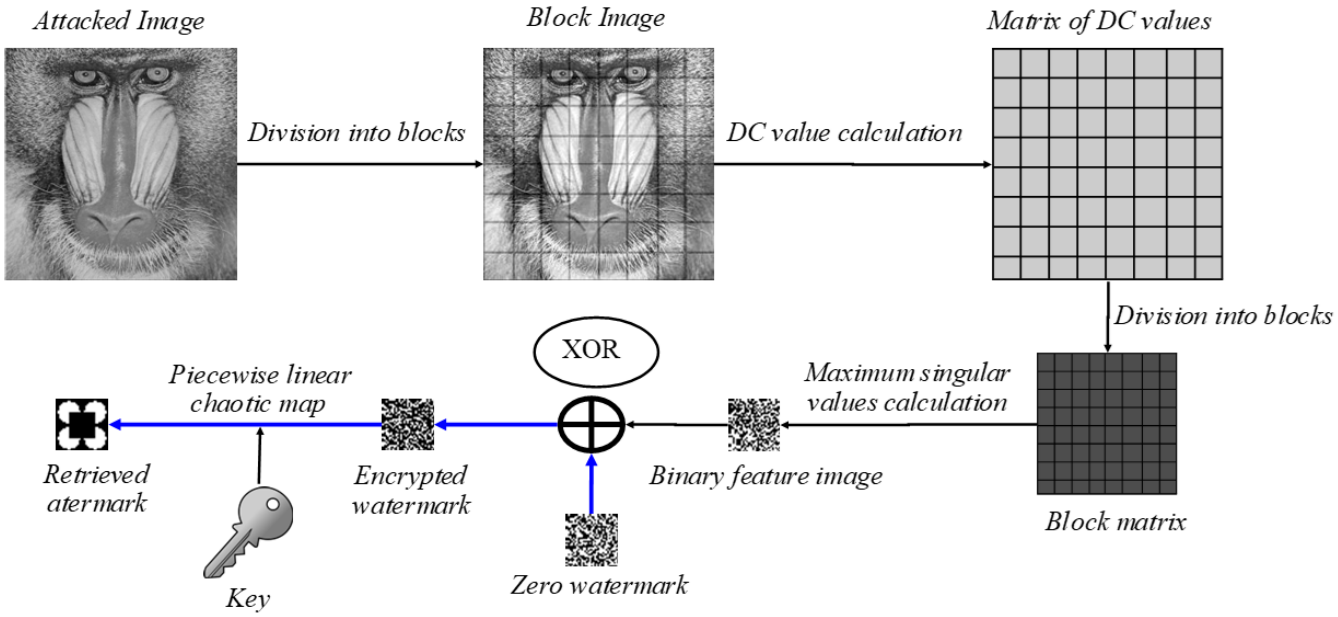

Figure 2. Illustration of watermark retrieval process.

4. Analysis and Discussion of Results

This section provides a detailed analysis and discussion of the results that the proposed scheme achieved. Additionally, a comparison is made between the performance of the proposed watermarking method and that of other related watermarking methods developed by Huang et al. [18], Kang et al. [16,17], Wang et al. [19], and Xia et al. [20]. Each of these schemes has employed a concept that is comparable to the proposed scheme, but in a different manner. To evaluate the effectiveness of the suggested approach, a set of twenty grayscale standard test images (I1 to I20) with dimensions of 512 × 512 and ten binary watermarks (W1 to W10) with dimensions of 32 × 32 were utilized. Figures 3 and 4 represent these images, which were obtained from a variety of freely accessible image resources [32]. The quality of the watermarked image was reduced by the implementation of several typical image manipulation attacks, as illustrated in Table 1, to assess the robustness of the suggested approach. A desktop computer running Windows 11 with 16 GB of RAM, an Intel Core i7 CPU, MATLAB 2014b, and an NVIDIA GeForce MX450 graphics card were used to evaluate the proposed scheme. A comparative analysis of the algorithms is conducted using tables and graphs. Several evaluation measures, which are described below, are used to track the performance of the algorithms. The proposed technique is computationally compared with its variant using DCT and SVD.

(**a**) I1 (**b**) I2 (**c**) I3 (**d**) I4 (**e**) I5

(**f**) I6 (**g**) I7 (**h**) I8 (**i**) I9 (**j**) I10

(**k**) I11 (**l**) I12 (**m**) I13 (**n**) I14 (**o**) I15

(**p**) I16 (**q**) I17 (**r**) I18 (**s**) I19 (**t**) I20

Figure 3. Test images labeled from I1 to I20 (**a**–**t**).

(**a**) W1 (**b**) W2 (**c**) W3 (**d**) W4 (**e**) W5 (**f**) W6 (**g**) W7 (**h**) W8 (**i**) W9 (**j**) W10

Figure 4. Watermark images labeled from W1 to W10 (**a**–**j**).

Table 1. Distortion attacks were applied to destroy the watermark information.

Attack Code	Attack's Description
A0	No distortion attack applied
A1	Gaussian noise addition of mean zero and variance 0.03
A2	Gaussian noise addition of mean zero and variance 0.05
A3	Salt and pepper noise addition of density 0.03
A4	Salt and pepper noise addition of density 0.05
A5	Speckle noise addition of mean zero and variance of 0.03
A6	Speckle noise addition of mean zero and variance of 0.05
A7	Average filter of size 3×3
A8	Average filter of size 5×5
A9	Median filter of size 3×3
A10	Median filter of size 5×5
A11	Gaussian lowpass filter of size 3×3 with *sigma* 0.5
A12	Gaussian lowpass filter of size 5×5 with *sigma* 0.5
A13	Motion blur with 3 pixels and 3-degree angle
A14	Motion blur with 5 pixels and 5-degree angle
A15	Anticlockwise rotation by 5°
A16	Anticlockwise rotation by 10°
A17	Horizontal cropping (1/16)
A18	Vertical cropping (1/16)
A19	Image scaling to half and then to its original size
A20	Image scaling to quarter and then to its original size
A21	Image translation by $[-5, 0]$ pixels
A22	Image translation by $[-5, 5]$ pixels
A23	JPEG compression with quality factor 20
A24	JPEG compression with quality factor 45

4.1. Evaluation Metrics

The peak signal-to-noise ratio (*PSNR*), one of numerous quality metrics published in the literature, is a commonly used metric for measuring the quality of a watermarked image [4]. A higher *PSNR* score signifies a greater degree of similarity between the watermarked and original images. In this article, *PSNR* is used to check the quality of the image after applying distortion attacks. The *PSNR* of 8-bit image 'A' of size $m \times m$ and its modified version 'B' of the same size is provided by the equation below.

$$PSNR(A,B) = 10\log_{10}\left(\frac{(255)^2}{\frac{1}{m\times m}\sum_{i=1}^{m}\sum_{j=1}^{m}\left(A_{i,j}-B_{i.j}\right)^2}\right)(dB) \tag{13}$$

The extracted watermark (W') may differ from the embedded watermark (W) in quality due to the change in watermarked image quality caused by the implementation of image manipulation attacks. As a result, a metric is required to assess the strength of the watermarking system; the bit error ratio (*BER*) and normalized cross-correlation (*NC*) are typically used for this purpose. Consistent with the previously described trend, we implemented these two metrics as well. The normalized cross-correlation (*NC*) and bit error ratio (*BER*) of an embedded watermark (W) and extracted watermark (W') of size $n \times n$ are defined in Equations (14) and (15), respectively.

$$NC(W,W') = \frac{\sum_{i=1}^{n}\sum_{j=1}^{n} W_{i,j} \times W'_{i,j}}{\sqrt{\sum_{i=1}^{n}\sum_{j=1}^{n} W_{i,j}^2}\sqrt{\sum_{i=1}^{n}\sum_{j=1}^{n} W_{i,j}'^2}} \tag{14}$$

$$BER(W,W') = \frac{\sum_{i=1}^{n}\sum_{j=1}^{n} W_{i,j} \oplus W'_{i,j}}{n \times n} \tag{15}$$

where i and j denote pixel positions in the images and '$\oplus$' denotes the XOR operation.

4.2. Imperceptibility Analysis

The visual system of humans is linked to the imperceptibility of invisible watermarking. It is believed that the watermarking approach is imperceptible when the original image is identical to the watermarked image. The methodology under consideration is a zero-watermarking method that preserves the integrity of the image by cognitively associating a watermark sequence with the original image rather than physically embedding it. It obtained perfect imperceptibility, as it does not introduce any distortion in the underlying host image.

4.3. Robustness Evaluation under Distortion Attacks

This section evaluates the suggested watermarking system's resilience via the execution of the extraction technique described in Section 3.2 and the application of the image manipulation attacks to the watermarked image as shown in Table 1. For this purpose, Equations (14) and (15), which describe the normalized cross-correlation (NC) and bits error ratio (BER), were utilized. Superior robustness favors a higher NC value in comparison to a smaller BER value. Table 1 presents an inventory of image distortion attacks, which may be classified into four main categories: noise attacks, filter attacks, geometric attacks, and compression attacks. Detailed explanations of each of them are provided in subsequent subsections using the image 'I11'. Table 2 provides an overall summary of the effects that these attacks have had on the watermarks that were retrieved. The results for each assessment metric are calculated as the mean across all images and watermarks. Although all the images in Figure 3 are utilized throughout the experiment, only the 'house' image is utilized to depict the test results of the proposed method for the sake of presentation. To validate the proposed scheme that the retrieved watermark is the same or not as embedded, in the absence of any distortion attack, results are provided in Table 3. From the table, it is clear that the retrieved watermarks are the same as the original. This observation is further supported by the NC value, which is exactly one in each case.

Table 2. Average PSNR of attacked images and average NC and BER of retrieved watermarks.

Attack	PSNR	NC	BER	Attack	PSNR	NC	BER	Attack	PSNR	NC	BER
A1	15.4858	0.9878	0.0118	A9	22.7604	0.9952	0.0038	A17	16.7772	0.9107	0.0709
A2	13.5660	0.9682	0.0254	A10	20.7534	0.9907	0.0074	A18	18.1181	0.9159	0.0707
A3	20.8375	0.9924	0.0062	A11	30.9804	0.9991	0.0009	A19	23.0755	0.9986	0.0011
A4	18.5498	0.9841	0.0127	A12	30.9804	0.9981	0.0015	A20	20.6715	0.9991	0.0009
A5	20.6590	0.9889	0.0088	A13	26.2167	0.9968	0.0025	A21	15.8300	0.9545	0.0612
A6	18.4881	0.9836	0.0130	A14	23.3126	0.9939	0.0048	A22	15.3420	0.9451	0.0688
A7	22.4658	0.9950	0.0040	A15	14.0738	0.9004	0.0867	A23	24.8804	0.9939	0.0048
A8	20.5790	0.9877	0.0098	A16	13.2172	0.8734	0.0971	A24	27.1407	0.9975	0.0020

Table 3. Extracted watermarks from the watermarked image without any distortion attack and their respective NC values.

Attack and NC	Extracted Watermark									
	W1	W2	W3	W4	W5	W6	W7	W8	W9	W10
A0										
NC	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000

4.3.1. Robustness against Noise Attacks

Signal interference during the transmission of digital images via networks or storage devices can introduce noise, potentially leading to image degradation. Hence, it is essential to investigate the robustness of the proposed scheme against noise-induced damage.

Different types of noises are added to the watermarked image by utilizing the attacks 'A1' to 'A6' defined in Table 1. Extracted watermarks from the distorted image and their NC values with their respective embedded watermarks are given in Table 4. To measure the quality of noisy images, PSNR is utilized and given in the Table. From the table, it can be seen that the image is seriously damaged, but the extracted watermarks are still identified with good NC values in all the cases. The technique is more vulnerable to Gaussian noise in comparison to salt and pepper noise, while speckle noise has no effect. Embedded and retrieved watermarks are identical in the case of speckle noise, while Gaussian noise and salt and pepper noise have little effect on the retrieved watermark images, which exhibit few speckles. The results of the experiment demonstrate that our approach is resistant to noise attacks.

Table 4. PSNR of noise-attacked image and NC values of retrieved watermarks.

PSNR of Attacked Image	Attack and NC	Extracted Watermark									
		W1	**W2**	**W3**	**W4**	**W5**	**W6**	**W7**	**W8**	**W9**	**W10**
16.0386	A1										
	NC	0.9929	0.9933	0.9951	0.9942	0.9942	0.9937	0.9926	0.9938	0.9955	0.9933
20.0388	A3										
	NC	0.9986	0.9987	0.9990	0.9988	0.9988	0.9987	0.9985	0.9988	0.9991	0.9986
20.4005	A5										
	NC	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000

4.3.2. Robustness against Filter Attacks

To lessen the impact of noise on image perception, image filtering is a frequent preprocessing step in the area of image analysis. A robust watermarking scheme must be resistant to filtering attacks. Different types of filter attacks, from A7 to A14 in Table 1, are applied to the cover image. Extracted watermarks from the distorted image and their NC values are given in Table 5. Despite the severe degradation to the image, as shown in the table in terms of PSNR, the extracted watermarks are detected with high NC values. This finding illustrates the algorithm's resilience against filtering attacks.

Table 5. PSNR of distorted image by filter attacks and NC values of retrieved watermarks.

PSNR of Attacked Image	Attack and NC	Extracted Watermark									
		W1	**W2**	**W3**	**W4**	**W5**	**W6**	**W7**	**W8**	**W9**	**W10**
26.8943	A7										
	NC	0.9986	0.9987	0.9990	0.9988	0.9988	0.9987	0.9985	0.9988	0.9991	0.9986
27.9352	A9										
	NC	0.9986	0.9987	0.9990	0.9988	0.9988	0.9987	0.9985	0.9988	0.9991	0.9987
35.7418	A11										
	NC	0.9986	0.9987	0.9990	0.9988	0.9988	0.9987	0.9985	0.9988	0.9991	0.9986
30.2164	A13										
	NC	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000

4.3.3. Robustness against Geometric Attacks

Various common geometric attacks, including scaling, cropping, translation, and rotation, are utilized to destroy the embedded watermark information. These attacks are defined in Table 1 from A15 to A22. Table 6 summarizes the PSNR of the image that has been subjected to various attacks, as well as the retrieved watermarks and their corresponding NC values. Although the retrieved watermark images may have speckles due to operations such as rotation, cropping, and translation, it is still possible to identify the extracted watermarks with good NC values. The performance of the scheme is below expectation for the rotation attacks, while it perfectly withstands the scaling attacks, attaining NC value 1. The findings of this study demonstrate that the proposed technique demonstrates considerable resilience against these types of attacks.

Table 6. PSNR of image distorted by geometric attacks and NC values of retrieved watermarks.

PSNR of Attacked Image	Attack and NC	Extracted Watermark									
		W1	**W2**	**W3**	**W4**	**W5**	**W6**	**W7**	**W8**	**W9**	**W10**
14.1576	A15										
	NC	0.8939	0.8934	0.9034	0.8879	0.8872	0.8987	0.8895	0.8813	0.9100	0.8731
15.9648	A17										
	NC	0.9094	0.9168	0.9373	0.9261	0.9266	0.9199	0.9069	0.9208	0.9417	0.9158
27.5643	A19										
	NC	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
17.3447	A21										
		0.9663	0.9684	0.9765	0.9724	0.9726	0.9695	0.9648	0.9704	0.9784	0.9677

4.3.4. Robustness against Compression Attacks

In order to enhance transfer speed and minimize storage space during the transmission and preservation of images over the network, data compression is an essential process. JPEG compression, which is a common lossy compression approach, is utilized to accomplish this. The test image undergoes JPEG compression attacks utilizing different compression-quality variables. The outcomes of these attacks are presented in Table 7. The PSNR value of the compressed image with quality factor 20, extracted watermarks, and corresponding NC values are given in the table. From the table, it can be seen that the extracted watermarks are identical to the embedded ones, with NC values more than 0.99 in all cases. This technique is robust to attacks induced by JPEG compression, as demonstrated by the experimental outcomes.

Table 7. PSNR of image distorted by compression attacks and NC values of retrieved watermarks.

PSNR of Attacked Image	Attack and NC	Extracted Watermark									
		W1	**W2**	**W3**	**W4**	**W5**	**W6**	**W7**	**W8**	**W9**	**W10**
28.8996	A23										
	NC	0.9986	0.9987	0.9990	0.9988	0.9988	0.9987	0.9985	0.9988	0.9991	0.9987

4.4. Execution Time Analysis

Table 8 displays the results of analyzing the proposed technique based on the computation time of the embedding and extraction procedures. Execution time plays a very important role in real-time watermarking. The proposed watermarking technique is compared with its variant, which used DCT and SVD. The table clearly illustrates the significant variation in execution time. The reason for this is that unlike its variation, the suggested technique employs a simple operation rather than any transformation. As a result, there is a significant variation in execution durations between these two strategies to attain the same robustness. The proposed scheme is almost three times faster than its variant.

Table 8. Computational times of the proposed scheme and its variant.

Time	Proposed	Proposed Scheme with DCT and SVD	% Improvement
Embedding time	0.1428	0.5605	292.51%
Extraction time	0.1420	0.5502	287.46%
Total	0.2848	1.1107	289.99%

4.5. Security Analysis

An encryption method, piecewise linear chaotic map (PWLCM), is utilized by the proposed scheme to safeguard the copyright image. Before embedding, PWLCM is applied to each watermark, with specific values for the starting point and control parameter. These two parameters are used as secret keys. It is possible to achieve successful decryption of an encrypted image by employing the identical values of the parameters utilized during encryption. Any modification, no matter how little, to either of these critical parameters will result in an incorrect decryption of the image. Table 9 displays the results obtained from the implementation of a piecewise linear chaotic map (PWLCM) of decryption and encryption for watermark images. It shows encrypted and decrypted images with different combinations of keys. From the table, it can be seen that the encrypted image can be decrypted correctly with the use of right keys only. Hence, an unauthorized user or forger cannot detect the watermark present in a watermarked image in the absence of the appropriate security key.

Table 9. Encryption and decryption with different combinations of keys.

Image	Encryption Parameters		Encrypted Image	Decryption Parameters		Key Status	Decrypted Image
	Initial Value	Control Parameter		Initial Value	Control Parameter		
	0.9	0.45		0.8	0.45	One wrong	
	0.9	0.45		0.9	0.46	One wrong	
	0.9	0.45		0.7	0.44	Both wrong	
	0.9	0.45		0.9	0.45	Both right	

4.6. Comparison with Relevant Techniques

In this part, a comparative analysis is conducted between the proposed watermarking technique and other relevant watermarking techniques, including those proposed by Huang et al. [18], Kang et al. [16,17], Wang et al. [19], and Xia et al. [20]. In Figures 5–8, the techniques that were chosen for comparison in this research are labeled technique1,

technique2, technique3, technique4, and technique5, respectively. The schemes were chosen on the basis that each of them has, in some fashion, implemented a concept that is comparable to the proposed scheme. To fully assess how well the proposed scheme performed, average NC values are compared. Multiple image distortion attacks are used to remove the embedded data, and then the watermark is extracted and NC values are calculated. The average of these NC values corresponding to each attack is plotted in Figures 5–8. The excellent performance of the proposed scheme against noise attacks in comparison to other schemes can be seen in Figure 5. Results corresponding to the filter attacks are provided in Figure 6. The proposed scheme outperformed the other schemes in both cases. In the case of geometric attacks, which is provided in Figure 7, our scheme performed better than the other scheme in scaling attacks, but in other cases, it performed better than the three schemes and inferior to the remaining two schemes. Figure 8 illustrates that the NC values of the proposed scheme exhibit a marginal increase in comparison to the other schemes when subjected to compression attacks.

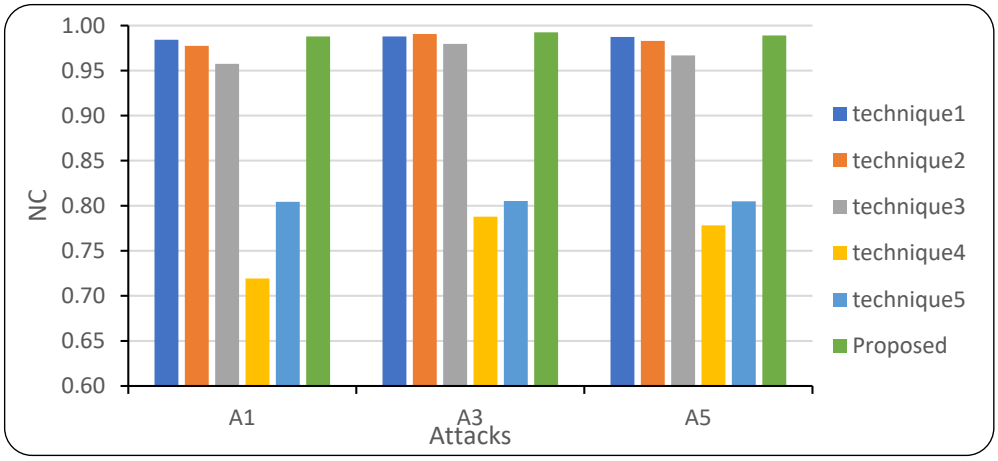

Figure 5. Average NC value comparative analysis of the proposed technique with other zero-watermarking techniques corresponding to noise attacks.

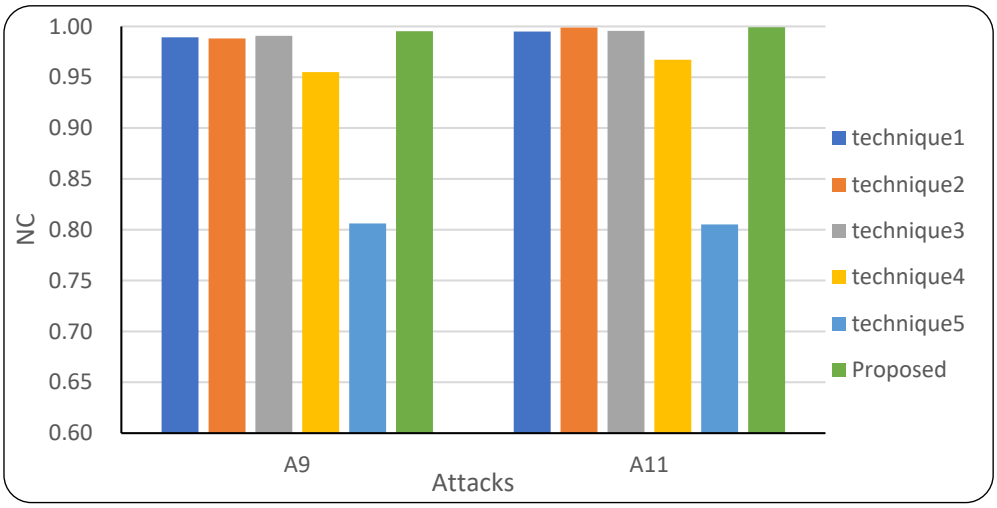

Figure 6. Average NC value comparative analysis of the proposed technique with other zero-watermarking techniques corresponding to filter attacks.

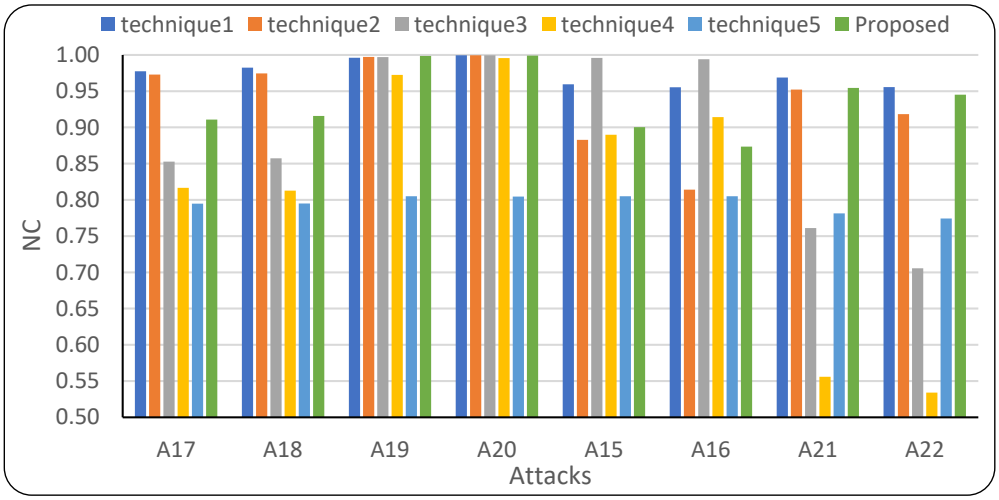

Figure 7. Average NC value comparative analysis of the proposed technique with other zero-watermarking techniques corresponding to geometric attacks.

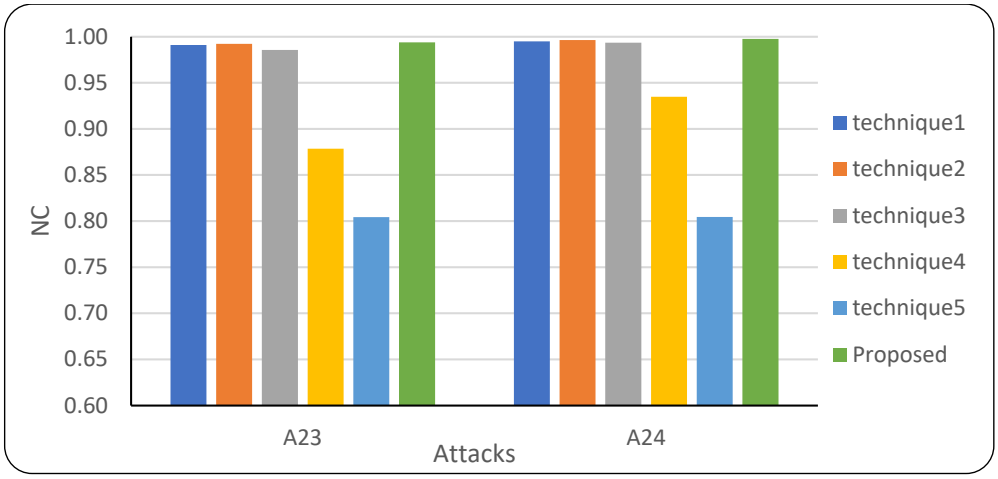

Figure 8. Average NC value comparative analysis of the proposed technique with other zero-watermarking techniques corresponding to compression attacks.

Overall, the proposed scheme outperformed the comparison methods in the case of noise and filter attacks, but in the case of geometric attacks, its performance is comparable. In the geometric attacks category, it performed well for scaling, but for other cases, it did not perform according to our expectations. Hence, it may be a further research direction to investigate the causes of its low performance. It is worth noting here that the scheme for the comparison implements computationally expensive transforms, whereas the proposed scheme uses simple operations instead of complicated transforms. Summarizing the above experimental results, our proposed scheme demonstrated good resistance against a variety of attacks with ease of implementation.

5. Conclusions

A new robust zero image watermarking technique is introduced in this research by the integration of block-based DC values with matrix norm. By avoiding any content alteration of the host image, which is an essential part of any zero-watermarking scheme, a binary feature matrix is obtained. The host image is partitioned into non-overlapping blocks, and DC values are computed without applying DCT. This sub-image is further divided into non-overlapping blocks, and the maximum singular value of each block is computed by matrix norm instead of SVD to obtain the binary feature matrix. An encryption technique

known as piecewise linear chaotic map is applied to the watermark image to enhance its security. After that, the feature image is created by XOR operation between the binary feature matrix and the encrypted watermark image.

The proposed technique was tested using a variety of distortion attacks, including noise, filter, geometric, and compression attacks. The performance of the scheme in terms of robustness was satisfactory, but it did not perform according to our expectations against geometric attacks. It is almost three times faster than its variant when execution times are compared. It is also compared with the other relevant image watermarking schemes. The proposed scheme outperformed the other schemes in cases of noise, filter, and compression attacks. Under the geometric attacks category, the proposed scheme outperformed the other schemes against scaling attacks, but it underperformed in other cases. Under geometric attacks, it performed better than the three schemes and was poorer than the remaining two.

Hence, further research is required in this direction to enhance its robustness against such modifications. We will continue to refine and enhance this technique in the future to deal with emerging security risks and attacks. We will also have to deal with the problem of incorporating this scheme into applications such as e-healthcare and telemedicine. Deep learning that works well on feature extraction has been adopted in a variety of areas, including image-based applications such as face recognition, and has been widely used for access control; its application in mining features for the construction of a robust zero watermark may be another future research possibility.

Author Contributions: Conceptualization, M.A. and S.K.; methodology, M.A. and S.K.; software, M.A.; validation, M.A. and S.K.; formal analysis, M.A. and S.K.; investigation, M.A. and S.K.; resources, M.A..; data curation, M.A.; writing—original draft preparation, M.A.; writing—review and editing, M.A. and S.K.; visualization, M.A. and S.K.; supervision, M.A.; project administration, M.A. and S.K.; funding acquisition, M.A. All authors have read and agreed to the published version of the manuscript.

Funding: The authors extend their appreciation to the Deputyship for Research and Innovation, Ministry of Education in Saudi Arabia, for funding this research work through the project number INST131.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Cox, I.; Miller, M.L.; Bloom, J.A. *Digital Watermarking*; Morgan Kaufmann Publishers Inc.: Cambridge, MA, USA, 2001; ISBN 1-55860-714-5.
2. 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]
3. Ali, M. Robust Image Watermarking in Spatial Domain Utilizing Features Equivalent to SVD Transform. *Appl. Sci.* **2023**, *13*, 6105. [CrossRef]
4. Wu, D.; Li, L.; Wang, J.; Ma, P.; Wang, Z.; Wu, H. Robust Zero-Watermarking Scheme Using DT CWT and Improved Differential Entropy for Color Medical Images. *J. King Saud. Univ. Comput. Inf. Sci.* **2023**, *35*, 101708. [CrossRef]
5. 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]
6. 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]
7. 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]
8. Wen, Q.; Sun, T.; Wang, S. Concept and Application of Zero-Watermark. *Acta Electron. Sin.* **2003**, *31*, 214–216.
9. Rawat, S.; Raman, B. A Blind Watermarking Algorithm Based on Fractional Fourier Transform and Visual Cryptography. *Signal Process.* **2012**, *92*, 1480–1491. [CrossRef]
10. Wang, C.P.; Wang, X.Y.; Xia, Z.Q.; Zhang, C.; Chen, X.J. Geometrically Resilient Color Image Zero-Watermarking Algorithm Based on Quaternion Exponent Moments. *J. Vis. Commun. Image Represent.* **2016**, *41*, 247–259. [CrossRef]
11. Shao, Z.; Shang, Y.; Zhang, Y.; Liu, X.; Guo, G. Robust Watermarking Using Orthogonal Fourier–Mellin Moments and Chaotic Map for Double Images. *Signal Process.* **2016**, *120*, 522–531. [CrossRef]
12. Kavitha, C.; Sakthivel, S. An Effective Mechanism for Medical Images Authentication Using Quick Response Code. *Clust. Comput.* **2019**, *22*, 4375–4382. [CrossRef]

13. Wu, X.; Li, J.; Tu, R.; Cheng, J.; Bhatti, U.A.; Ma, J. Contourlet-DCT Based Multiple Robust Watermarkings for Medical Images. *Multimed. Tools Appl.* **2019**, *78*, 8463–8480. [CrossRef]
14. Liu, J.; Li, J.; Zhang, K.; Bhatti, U.A.; Ai, Y. Zero-Watermarking Algorithm for Medical Images Based on Dual-Tree Complex Wavelet Transform and Discrete Cosine Transform. *J. Med. Imaging Health Inf.* **2019**, *9*, 188–194. [CrossRef]
15. Liu, J.; Li, J.; Ma, J.; Sadiq, N.; Bhatti, U.A.; Ai, Y. A Robust Multi-Watermarking Algorithm for Medical Images Based on DTCWT-DCT and Henon Map. *Appl. Sci.* **2019**, *9*, 700. [CrossRef]
16. Kang, X.; Zhao, F.; Chen, Y.; Lin, G.; Jing, C. Combining Polar Harmonic Transforms and 2D Compound Chaotic Map for Distinguishable and Robust Color Image Zero-Watermarking Algorithm. *J. Vis. Commun. Image Represent.* **2020**, *70*, 102804. [CrossRef]
17. Kang, X.B.; Lin, G.F.; Chen, Y.J.; Zhao, F.; Zhang, E.H.; Jing, C.N. Robust and Secure Zero-Watermarking Algorithm for Color Images Based on Majority Voting Pattern and Hyper-Chaotic Encryption. *Multimed. Tools Appl.* **2020**, *79*, 1169–1202. [CrossRef]
18. Huang, T.; Xu, J.; Yang, Y.; Han, B. Robust Zero-Watermarking Algorithm for Medical Images Using Double-Tree Complex Wavelet Transform and Hessenberg Decomposition. *Mathematics* **2022**, *10*, 1154. [CrossRef]
19. Wang, W.; Li, Y.; Liu, S. A Polar Complex Exponential Transform-Based Zero-Watermarking for Multiple Medical Images with High Discrimination. *Secur. Commun. Netw.* **2021**, *2021*, 6615678. [CrossRef]
20. Xia, Z.; Wang, X.; Han, B.; Li, Q.; Wang, X.; Wang, C.; Zhao, T. Color Image Triple Zero-Watermarking Using Decimal-Order Polar Harmonic Transforms and Chaotic System. *Signal Process.* **2021**, *180*, 107864. [CrossRef]
21. Tsai, H.H.; Lai, Y.S.; Lo, S.C. A Zero-Watermark Scheme with Geometrical Invariants Using SVM and PSO against Geometrical Attacks for Image Protection. *J. Syst. Softw.* **2013**, *86*, 335–348. [CrossRef]
22. Thanh, T.M.; Tanaka, K. An Image Zero-Watermarking Algorithm Based on the Encryption of Visual Map Feature with Watermark Information. *Multimed. Tools Appl.* **2017**, *76*, 13455–13471. [CrossRef]
23. Ali, Z.; Shamim Hossain, M.; Muhammad, G.; Aslam, M. New Zero-Watermarking Algorithm Using Hurst Exponent for Protection of Privacy in Telemedicine. *IEEE Access* **2018**, *6*, 7930–7940. [CrossRef]
24. Ali, M.; Ahn, C.W.; Pant, M. An Efficient Lossless Robust Watermarking Scheme by Integrating Redistributed Invariant Wavelet and Fractional Fourier Transforms. *Multimed. Tools Appl.* **2018**, *77*, 11751–11773. [CrossRef]
25. Zou, B.; Du, J.; Liu, X.; Wang, Y. Distinguishable Zero-Watermarking Scheme with Similarity-Based Retrieval for Digital Rights Management of Fundus Image. *Multimed. Tools Appl.* **2018**, *77*, 28685–28708. [CrossRef]
26. Liu, F.; Ma, L.-H.; Liu, C.; Lu, Z.-M. Zero Watermarking Scheme Based on U and V Matrices of Quaternion Singular Value Decomposition for Color Images. *J. Inf. Hiding Multimed. Signal Process. C* **2018**, *9*, 629–640.
27. Singh, A.; Dutta, M.K. A Robust Zero-Watermarking Scheme for Tele-Ophthalmological Applications. *J. King Saud Univ. Comput. Inf. Sci.* **2020**, *32*, 895–908. [CrossRef]
28. Dong, F.; Li, J.; Bhatti, U.A.; Liu, J.; Chen, Y.W.; Li, D. Robust Zero Watermarking Algorithm for Medical Images Based on Improved NasNet-Mobile and DCT. *Electronics* **2023**, *12*, 3444. [CrossRef]
29. Cao, H.; Hu, F.; Sun, Y.; Chen, S.; Su, Q. Robust and Reversible Color Image Watermarking Based on DFT in the Spatial Domain. *Optik* **2022**, *262*, 169319. [CrossRef]
30. 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]
31. 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]
32. SIPI Image Database. Available online: https://sipi.usc.edu/database/database.php (accessed on 10 November 2023).