mathematics

MDPI

Article

An Adaptive Embedding Strength Watermarking Algorithm Based on Shearlets' Capture Directional Features

Qiumei Zheng, Nan Liu * and Fenghua Wang

College of Computer Science and Technology, China University of Petroleum, Qingdao 266580, China; zhengqm@upc.edu.cn (Q.Z.); fenghuawang@upc.edu.cn (F.W.)

* Correspondence: s18070006@s.upc.edu.cn

Received: 4 August 2020; Accepted: 13 August 2020; Published: 17 August 2020

Abstract: The discrete wavelet transform (DWT) is unable to represent the directional features of an image. Similarly, a fixed embedding strength is not able to establish an ideal balance between imperceptibility and robustness of a watermarked image. In this work, we propose an adaptive embedding strength watermarking algorithm based on shearlets' capture directional features (S-AES). We improve the watermarking algorithm in the domain of DWT using non-subsampled shearlet transform (NSST). The improvement is made in terms of coping with anti-geometric attacks. The embedding strength is optimized by artificial bee colony (ABC) to achieve higher robustness under the premise of satisfying imperceptibility. The principle components (PC) of the watermark are embedded into the host image to overcome the false positive problem. The simulation results show that the proposed algorithm has better imperceptibility and strong robustness against multi-attacks, especially those of high intensity.

Keywords: non-subsampled shearlet transform; artificial bee colony; principle components; false positive problem

1. Introduction

With the development of the Internet, the amount of image data being transmitted has significantly increased. These images are easily copied, modified, subsequently infringing the copyright of the author. Digital image watermarking [1,2] is a technique to protect images' ownership. Watermarking with strong robustness is embedded into the image to protect the ownership of the image. The research on robust watermarking has achieved good research results. Most algorithms presented in the literature have the ability to resist common attacks effectively. In addition, these algorithms also have resistance against geometric attacks, such as rotation and translation attacks. However, the extracted watermarking becomes worse with the increase in the attacks' intensity in many existing algorithms. Therefore, making significant improvements in the resistance provided by robust watermarking against high intensity attacks is an important research problem.

The embedding strength of the digital watermarking algorithm is closely related to robustness and imperceptibility. The larger the value of embedding strength, the better the robustness and the worse the imperceptibility. On the other hand, a smaller value of embedding strength leads to better imperceptibility and worsens robustness [3,4]. Therefore, the appropriate embedding strength must be selected appropriately to maximize the robustness of the algorithm to enable resistance against high intensity attacks. In recent years, researchers optimized embedding strength on the basis of the genetic algorithm (GA) [5], particle swarm optimization (PSO) [6], and artificial bee colony (ABC) [7].

Cui [8] uses the differential evolution algorithm to optimize the embedding strength, which involves normalized correlation (NC) of the watermarked image and the extracted watermark for improving the robustness. Ansari [9] uses artificial bee colony (ABC) to optimize the embedding strength. The proposed methods use peak signal-to-noise ratio (PSNR) of the watermarked image and the average NC value of the extracted watermarking after different types of attacks. The algorithm fully considers the impact of embedding strength on imperceptibility and robustness.

Existing watermarking algorithms are generally divided into two groups, namely, spatial domain algorithms and transform domain algorithms. The spatial domain algorithms realize the embedding of watermarking by modifying the pixel values of the image. On the other hand, the transform domain algorithms consider the embedding position of watermarking by performing DCT (discrete cosine transform) [10], DFT (discrete Fourier transform) [11], and DWT (discrete wavelet transform) [12,13] of the original image. The transform domain algorithms have stronger robustness than the spatial domain algorithms [14]. Currently, the research on robust watermarking mainly focuses on the transform domain. The research community has made efforts to improve the robustness of the watermarking algorithm by selecting the appropriate embedding positions. Sharma in [15] adopts the redundant wavelet transform (RDWT) with translation invariance to select the embedding position for improving the robustness of the algorithm. The watermarking algorithm performs 2-level DWT of the original image proposed by Ansari [9]. The proposed method performs resistance against compression and noise attacks. However, the DWT does not have the ability to represent the multidirectional features of the image effectively, due to the limitation of the types of directional filtering. This limits the resistance ability of the watermarking algorithm based on DWT to geometric attacks. The shearlet transform proposed by Gao [16] has multiscale and multidirectional characteristics, and has the ability to capture the directional features of the image effectively. Similarly, Mardanpour [17] proposed a watermarking algorithm based on shearlet transform to achieve stronger robustness against geometric attacks.

The singular values of matrix have good stability and are beneficial in enhancing the robustness of the watermarking algorithms. Therefore, the singular value decomposition (SVD) and the frequency domain transformations are usually combined in watermarking algorithms [18]. The process of embedding the singular values of the watermark into the host image improves the algorithms' robustness [19,20]. However, the singular value matrix is unable to represent the unique features of the image, thus leading to the false positive problem. The false positive problem is the extraction of a wrong watermark, which was never embedded into the host image, from the watermarked image. Vali [21] embeds a digital signature which is calculated by the watermark's edge information of the watermarked image. This algorithm solves the false positive problem, however, it adds verification steps. Makbol [22], Ali [23] and Lakrissi [24] solve the false positive problem by embedding the principle components or the entire watermark into the image. The principal components can be obtained by SVD. The principal components can represent the unique features of the watermark to make the algorithms free from the false positive problem. Ansari [9] embeds the watermark's principal components into the singular value matrix of the host image to solve the false positive problem. In this algorithm, the image matrix is reconstructed directly after the watermark is embedded.

As presented in the literature, the multiscale and multidirectional characteristics of shearlet transform makes up for the deficiency posed by DWT transform, and the embedding strength is accomplished by using a suitable optimization algorithm to achieve robustness. Therefore, in this work, an adaptive embedding strength watermarking algorithm based on shearlets' capture directional features (S-AES) is proposed. The multi-resolution characteristics of DWT and multi-directional characteristics of shearlet transform increases the resistance ability against common attacks and geometric attacks and optimize the embedding strength by ABC. As compared to other algorithms presented in [8,9,17], S-AES makes up for the lack of resistance ability of DWT against geometric attacks, and also overcomes the problem of shearlet transform to filter attacks. Moreover, S-AES fully considers the watermarking characteristics of imperceptibility and robustness, and uses an optimized algorithm to search for the embedding strength that meets the requirements of the

watermarking algorithm. Therefore, S-AES achieves maximum robustness against various attacks under the premise of satisfying the imperceptibility. S-AES also has the ability to resist many kinds of attacks, especially strong intensity attacks. The main contributions of this work are as follows:

1. The watermarking algorithm in the domain of DWT is improved by using shearlet transform. The embedding position is selected on the basis of DWT and NSST to improve the robustness.
2. The ABC algorithm and the improved optimized function is used to optimize the embedding strength to achieve higher robustness.
3. The principle components of the watermark are embedded into the host image to solve the false positive problem of singular value decomposition.

The rest of this paper is organized as follows:

In Section 2, we present the preliminaries of this work. In Section 3, we present the proposed watermark embedding and extracting algorithm. In Section 4, we present the experimental results and analysis. Finally, in Section 5, we conclude our work.

2. Preliminaries

2.1. Discrete Wavelet Transform (DWT)

DWT is a multiresolution analysis tool [25,26]. DWT decomposes an image into three high frequency sub-bands which are low-high (HL), high-low (LH) and high-high (HH) and one low frequency sub-band low-low (LL). Among these bands, LL contains most of the information presented by the original image. The other three sub-bands, i.e., HL, LH, HH, represent the texture features and the edge information of the image. Figure 1 presents the two-level DWT decomposition of "Lena" [27].

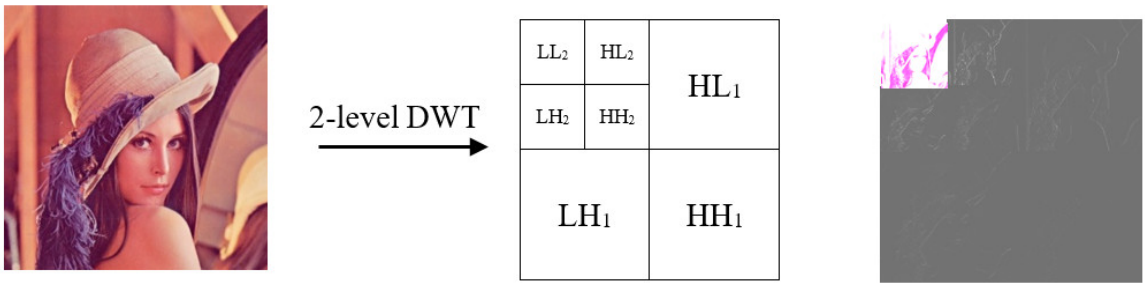


Figure 1. Schematic pictures of two-level discrete wavelet decomposition (DWT).

The low frequency sub-band has good stability to resist different types of attacks because it contains most of the information of the image. S-AES selects low frequency sub-band of two-level DWT decomposition as the embedding position of the watermark.

2.2. Non-Subsampled Shearlet Transform (NSST)

Shearlet transform is a multiscale analysis technique [28]. It has better multiresolution capabilities and stronger directional characteristics as compared to wavelet transform to represent the features of images or high-dimensional signals effectively. The non-subsampled shearlet transform is a discretization of shearlet transform. First, the image is multiscale decomposed by non-subsampled pyramid filter (NSPF). Then, each scale sub-band image is multidirectional decomposed by shear filter (SF) [29]. Figure 2 presents the implementation of non-subsampled shearlet transform.

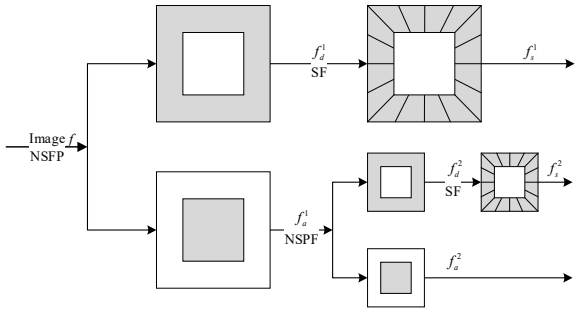


Figure 2. Schematic pictures of non-subsampled shearlet transform (NSST).

Here, f represents the original image. f_d^1 and f_a^1 are the high frequency and low frequency images after the first decomposition, respectively. Similarly, f_d^2 and f_a^2 represent the high frequency and the low frequency images after the second decomposition of the low frequency image, respectively. f_s^2 is detail sub-band by directional decomposition of f_d^2. NSST decomposes an image into different directional sub-bands. Figure 3 presents the NSST decomposition of a zone plate.

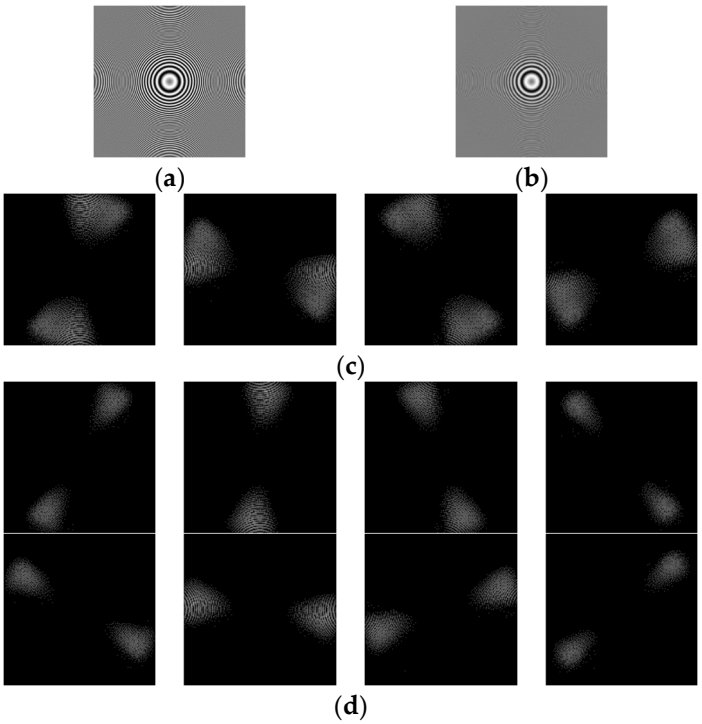


Figure 3. Schematic pictures of NSST decomposition. (**a**) Zone plate. (**b**) Low frequency sub-band. (**c**) Four different directional sub-bands. (**d**) Eight different directional sub-bands.

DWT does not possess the capability to represent the directional features of an image effectively. Contrarily, NSST is able to effectively capture the multidirectional features. Therefore, S-AES performs DWT and NSST on the image, and then selects the sub-band with the richest directional features as the embedding position to improve robustness.

2.3. Singular Value Decomposition (SVD)

Singular value decomposition is one of the useful numerical analysis tools in linear algebra, which can decompose an image into three matrices. For matrix A of size $M \times M$, singular value decomposition is defined as Equation (1):

$$A = USV^T \quad (1)$$

where U, V, and S are the real matrix of size $N \times N$, represent the left singular matrix, the right singular matrix, and the singular matrix, respectively. S is a diagonal matrix, and the diagonal elements of S represent the image luminance. Matrix U and V represent the horizontal and vertical details of the image.

The singular values of the watermark are embedded into the host image to improve the resistance against various attacks because of its good stability. However, the matrices U and V contain the images' important information that the singular values are unable to represent. The watermarking algorithm using singular values will have the false position problem [30]. The principle components (PC) of the watermark are defined as Equation (2) [15]:

$$PC = U \times S \tag{2}$$

The principal components represent the unique features of the image. Therefore, the principle components of the watermark are embedded into the host image to solve the false positive problem and improve the security in S-AES.

2.4. Artificial Bee Colony (ABC)

Artificial bee colony [15] is a global optimization algorithm proposed by Karaboga in 2005. This algorithm estimates the optimal value by maximizing or minimizing the objective function. ABC is widely used for its various advantages, such as fast convergence speed, less control parameters, and easy implementation. S-AES designs a reasonable objective function and uses ABC to find out the embedding strength.

3. The Proposed Scheme

In order to achieve higher robustness under the premise of meeting imperceptibility, an adaptive embedding strength watermarking algorithm based on shearlets' capture directional features (S-AES) is proposed. DWT and NSST are adopted to select the embedding position. ABC is used to optimize the embedding strength. Embedding the principle components of the watermark into the host image solves the false positive problem caused by SVD.

3.1. The Watermark Embedding Scheme

The watermark embedding process is presented in Figure 4. This process comprises seven steps, which are presented below.

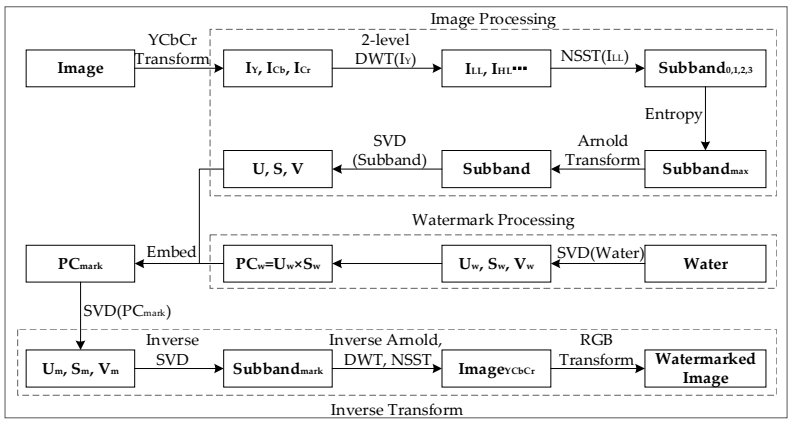


Figure 4. Schematic pictures of the watermark embedding scheme.

Step 1 The color image of size $N \times N$ is transformed from RGB color space to YCbCr color space, which extracts I_Y, I_{Cb}, I_{Cr} of the image, as demonstrated in Equation (3) [31]:

$$\begin{bmatrix} Y \\ Cb \\ Cr \end{bmatrix} = \begin{bmatrix} 0.29890 & 0.58660 & 0.11450 \\ -0.16874 & -0.33126 & 0.50000 \\ 0.50000 & -0.41869 & -0.81310 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix} + \begin{bmatrix} 0 \\ 0.5 \\ 0.5 \end{bmatrix} \quad (3)$$

According to human visual system, the human eyes are not sensitive to luminance components [32]. In order to guarantee better imperceptibility, S-AES embeds the watermark to luminance component I_Y.

Step 2 Apply two-level DWT on I_Y to obtain low frequency sub-band I_{LL} as the embedding position. The low frequency sub-band contains most of the information to resist against different types of attacks to guarantee robustness.

Step 3 Apply NSST on low frequency sub-band I_{LL} to obtain four different directional sub-bands. Calculate the entropy of these sub-bands, which is referred to as Equation (4):

$$H(X) = E\left[log\frac{1}{p(a_i)}\right] = -\sum_{i=1}^{n} p(a_i)\, log\, p(a_i) \quad (4)$$

where n represents the number of gray levels and $p(a_i)$ represents the probability of gray level a_i of the image. The larger the values of entropy, the richer the directional features of the sub-band. The sub-band $Subband_{max}$ with the maximum entropy is selected to embed the watermark to ensure better imperceptibility against attacks.

Step 4 Apply k times Arnold transform on directional sub-band $Subband_{max}$ to obtain $Subband$, which is referred to as Equation (5):

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (mod\ x), x, y \epsilon (0,1, \dots, M-1) \quad (5)$$

where, (x, y) represents the original coordinates of the pixel and (x', y') represents the new coordinates of the transformed pixel. The size of directional sub-band is $M \times M$. Arnold transformation breaks the spatial continuity between image pixels, which is conducive to the security of the algorithm.

Step 5 Apply SVD on scrambled directional sub-band $Subband$ referred to as Equation (6):

$$SVD(Subband) = USV^T \quad (6)$$

Apply SVD on watermark image $Water$, and extract principle components of the watermark PC_{water}, as demonstrated in Equations (7) and (8):

$$SVD(Water) = U_{water} S_{water} V_{water}^T \quad (7)$$

$$PC_{water} = U_{water} \times S_{water} \quad (8)$$

The principle components, which represent the unique features of the image, are embedded into the host image to avoid the false positive problem in the S-AES algorithm.

Step 6 Embed the PC of the watermark into the singular matrix of the host image, as demonstrated in Equation (9):

$$PC_{mark} = S + \alpha PC_{water} \quad (9)$$

where α is embedding strength which is optimized by ABC. Please note that it is necessary to apply SVD on PC_{mark} to maintain good stability of the singular matrix because PC_{mark} is no longer a diagonal matrix.

$$SVD(PC_{mark}) = U_{mark} S_{mark} V_{mark}^T \quad (10)$$

In [3], the authors perform inverse SVD using the singular matrix embedded with PC (e.g., sPC_{mark}), which leads to the worse ability of anti-geometric attacks, such as rotation.

Step 7 Apply inverse SVD to obtain the directional sub-band $Subband_{mark}$ containing the watermark, as demonstrated in Equation (11):

$$Subband_{mark} = U \times S_{mark} \times V^T \quad (11)$$

Apply k times inverse Arnold transform, inverse NSST and inverse DWT on $Subband_{mark}$ to obtain I_{Ymark}. Merge I_{Ymark} with I_{Cb}, I_{Cr}, then transform YCbCr to RGB to obtain the watermarked color image, i.e., $WatermarkedImage$, as demonstrated in Equation (12) [31]:

$$\begin{bmatrix} R \\ G \\ B \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0.14020 \\ 1 & -0.34414 & -0.71414 \\ 1 & 1.77200 & 0 \end{bmatrix} \begin{bmatrix} Y \\ Cb \\ Cr \end{bmatrix} - \begin{bmatrix} 0 \\ 0.5 \\ 0.5 \end{bmatrix} \quad (12)$$

3.2. The Watermark Extracting Scheme

The watermark extracting process is presented in Figure 5. It contains three steps.

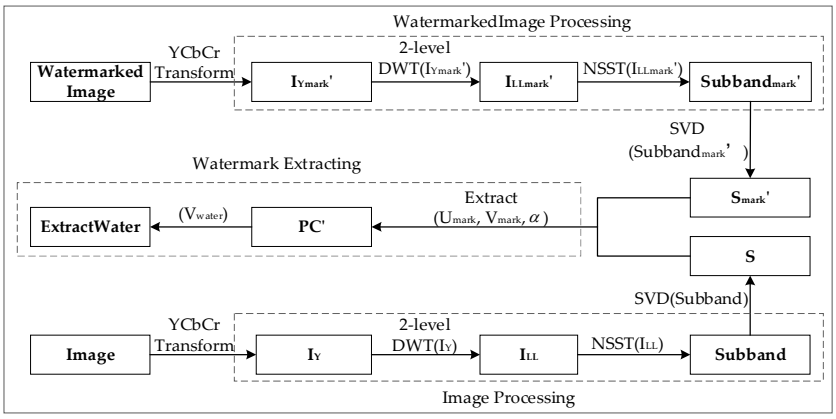


Figure 5. Schematic pictures of the watermark extracting scheme.

Step 1 The watermarked image $WatermarkedImage$ is transformed RGB to YCbCr color space to extract luminance component $I_{Ymark}{}'$. Apply DWT and NSST on $I_{Ymark}{}'$ to obtain the directional sub-band containing the watermark denoted as $Subband_{mark}{}'$. Perform the same transformations on the original image to obtain the directional sub-band $Subband$.

Step 2 Apply k times Arnold transform on directional sub-bands $Subband_{mark}{}'$ and $Subband$, and then apply SVD on $Subband_{mark}{}'$ and $Subband$ to obtain the singular matrices $S_{mark}{}'$ and S. Extract the embedding information as in Equation (13):

$$Embed = U_{mark} \times S_{mark} \times V_{mark}^{T} \quad (13)$$

Step 3 Extract the principle components of the watermark as in Equation (14):

$$PC' = (Embed - S)/\alpha \quad (14)$$

Then extract the watermark using the side information using the following Equation (15):

$$ExtractWater = PC' \times V_{water}^{T} \quad (15)$$

3.3. Optimization of Embedding Strength

Most of the algorithms presented in the literature consider the fixed value of embedding strength. However, different images have different characteristics in terms of color, texture, and some other characteristics. The fixed embedding strength is unable to realize the good imperceptibility and robustness on various kinds of images. S-AES considers the characteristics of the host image and the watermark to optimize the embedding strength using ABC.

Normalized correlation (NC) is used to evaluate the robustness, and peak signal-to-noise ratio (PSNR) is used to evaluate imperceptibility, as demonstrated in Equations (16) and (17) [33]:

$$NC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{M} W(i,j) \times W'(i,j)}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{M} W(i,j)}\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{M} W'(i,j)}} \tag{16}$$

$$PSNR(I,I') = 10\,log_{10}\frac{255^2}{\frac{1}{N\times N}\sum_{i=1}^{N}\sum_{j=1}^{N}[I(i,j)-I'(i,j)]^2}(dB) \tag{17}$$

where W and W' represent the original watermark and the extracted watermark, respectively. I and I' represent the host image and the watermarked image, respectively.

It makes sense to satisfy imperceptibility for the watermarking algorithms. The main idea of S-AES is to achieve higher robustness for multiple attacks under the premise of satisfying imperceptibility. N times different types and intensity attacks are applied to the watermarked image when the PSNR is above the threshold. The robustness of S-AES is maximized by maximizing the proposed objective function presented in Equation (18), where W is the original watermark, and W′ represents the extracted watermark.

$$\begin{cases} PSNR > Threshold \\ fun = \sum_{i=1}^{N} NC(W, W_i')/N \end{cases} \tag{18}$$

The embedding strength optimization process is presented in Figure 6. The values of parameters are presented in Table 1.

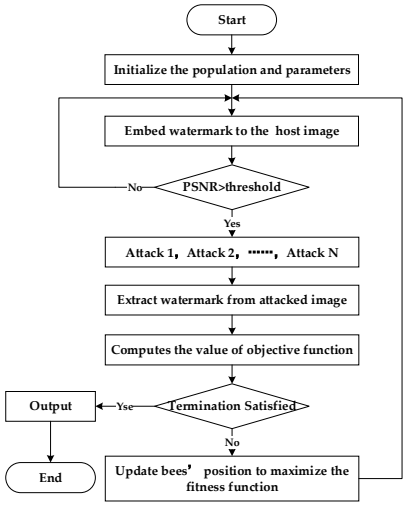


Figure 6. Schematic pictures of embedding strength optimization.

Table 1. Parameters values of embedding strength optimization.

Parameters	Values
Size of swarm	20
Maximum iterations	20
Limit	10
Initialization range	[0.005, 0.1]
Employed bees	50% of size of swarm
Onlooker bees	50% of size of swarm
Scout bees	Variable
Attacks	Crop, filter, noise, compression, rotation, sharpen and translation.

4. Results and Analysis

The experiments of S-AES are performed in MATLABR2017b, and they involve 10 host images and 2 watermark images that were selected from the standard image data-base. The size of each host image is 512 × 512, while that of the watermarked images is 128 × 128, as presented in Figure 7. The threshold value is 38 dB in this experiment. Figure 8 illustrates the convergence graph for the 10 host images embedding with the "UPC" watermark in Figure 7.

Figure 7. The host images and watermark images. (**a**) Lena. (**b**) Pepper. (**c**) Airplane. (**d**) Tiffany. (**e**) Baboon. (**f**) Sailboat. (**g**) Flower. (**h**) Goldhill. (**i**) Soccer. (**j**) Girl. (**k**) UPC. (**l**) Logo.

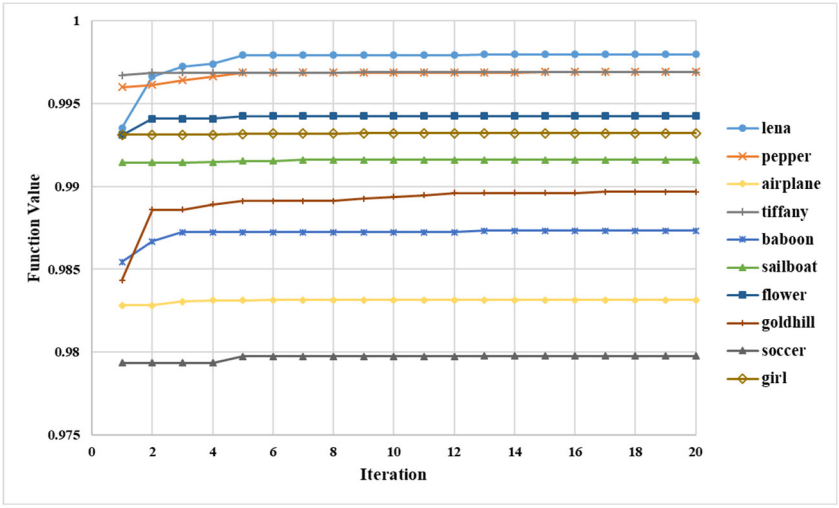


Figure 8. Convergence graph for the 10 host images embedding with the "UPC" watermark.

It is evident from Figure 8 that all 10 host images converge after 16 executed iterations.

4.1. Imperceptibility Analysis

The imperceptibility results are presented in Table 2.

Table 2. Peak signal-to-noise ratio (PSNR) values of S-AES.

PSNR (dB)	Lena	Pepper	Airplane	Tiffany	Baboon	Sailboat	Flower	Goldhill	Soccer	Girl
UPC	38.0088	38.0307	38.0023	38.0001	38.0073	38.0021	38.0073	38.0187	38.0001	38.0190
Logo	38.0135	38.0041	38.0031	38.0048	38.000	38.0117	38.0003	38.0015	38.0087	38.0091

According to the human visual system [34], the watermark has good imperceptibility when PSNR > 35 dB. As presented in Table 2, the PSNR values are about 38 dB, indicating that S-AES has good imperceptibility.

4.2. Robustness Analysis

NC and the bit error ratio (*BER*) are used to evaluate the robustness of the proposed algorithm. The larger value of NC results in better robustness. The BER is an indicator to measure the difference between the extracted watermark and the original watermark. Its mathematical definition is presented in Equation (19) [35].

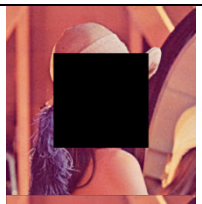
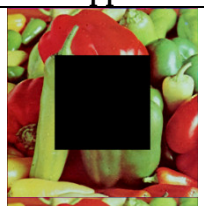
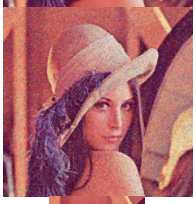
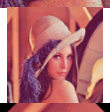
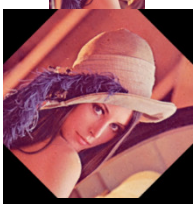
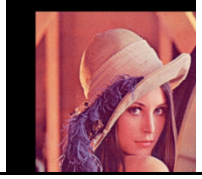
$$BER = \frac{B}{P \times Q} \tag{19}$$

where B is the number of erroneous bits in the extracted watermark, and P×Q represents the total number of bits in the extracted watermark. The lower value of the BER shows greater robustness of the proposed algorithm.

4.2.1. Robustness Results

The extracted "UPC" and "Logo" watermarks from the host images '"Lena" and "Pepper" under crop, filer, and rotation attacks are presented in Table 3.

Table 3. Extracted "UPC" and "Logo" watermarks from "Lena" and "Pepper" under different attacks.

Attacks	Lena	Logo	Pepper	UPC
Centre crop 256 × 256				**UPC** **UPC**
Average filter (3,3)				**UPC** **UPC**
Pepper and salt noise 0.1				**UPC** **UPC**
Rescale 0.25				**UPC** **UPC**
Rotation 45°				**UPC** **UPC**
Translation 80				**UPC** **UPC**

In Table 3, we can see that the extracted watermarks are slightly different from the original watermarks, and can represent the copyright information clearly. This indicates that S-AES has strong robustness under different attacks.

To illustrate the robustness of the algorithm accurately, the NC values are shown in Table 4.

Table 4. The normalized correlation (NC) values of the extracted watermarks under different types and parameters attacks.

Attacks	Parameters	Lena		Pepper	
		UPC	Logo	UPC	Logo
Contrast adjustment	20%	0.9971	0.9989	0.9964	0.9960
Crop	128 × 128	0.9990	0.9972	0.9986	0.9967
	256 × 256	0.9987	0.9976	0.9978	0.9925
	384 × 384	0.9982	0.9970	0.9620	0.9562
Centre crop	128 × 128	0.9992	0.9973	0.9986	0.9969
	256 × 256	0.9987	0.9990	0.9986	0.9961
	384 × 384	0.9782	0.9978	0.9981	0.9939
Gaussian filter	(2,2)	0.9986	0.9970	0.9985	0.9939
	(3,3)	0.9986	0.9971	0.9986	0.9957
	(5,5)	0.9986	0.9971	0.9986	0.9957
Gaussian noise	0.01	0.9987	0.9971	0.9986	0.9969
	0.1	0.9868	0.9990	0.9960	0.9971
	0.3	0.9607	0.9972	0.9729	0.9952
JPEG 2000 compression	5:1	0.9986	0.9971	0.9986	0.9968
	10:1	0.9986	0.9971	0.9986	0.9968
	20:1	0.9986	0.9971	0.9986	0.9969
JPEG compression	20%	0.9986	0.9971	0.9986	0.9968
	40%	0.9986	0.9971	0.9986	0.9968
	60%	0.9986	0.9971	0.9986	0.9968
	80%	0.9986	0.9971	0.9986	0.9968
	100%	0.9986	0.9971	0.9985	0.9967
Average filter	(2,2)	0.9986	0.9970	0.9985	0.9939
	(3,3)	0.9985	0.9946	0.9963	0.9871
	(5,5)	0.9740	0.9680	0.9537	0.9430
Median filter	(2,2)	0.9986	0.9971	0.9986	0.9947
	(3,3)	0.9986	0.9970	0.9985	0.9943
	(5,5)	0.9884	0.9832	0.9880	0.9791
Motion blur	θ = 4, l = 7	0.9986	0.9954	0.9950	0.9862
Pepper and salt noise	0.01	0.9986	0.9971	0.9986	0.9969
	0.1	0.9990	0.9976	0.9985	0.9970
	0.3	0.9797	0.9986	0.9848	0.9969
Rescale	256 × 256	0.9986	0.9971	0.9985	0.9947
	128 × 128	0.9752	0.9695	0.9712	0.9591
	1024 × 1024	0.9986	0.9971	0.9986	0.9968
	2048 × 2048	0.9986	0.9971	0.9986	0.9968
Rotation	5°	0.9976	0.9972	0.9974	0.9959
	−5°	0.9987	0.9971	0.9944	0.9936
	45°	0.9964	0.9970	0.9950	0.9970
	90°	0.9700	0.9990	0.9875	0.9769
	180°	0.9986	0.9971	0.9985	0.9968
	270°	0.9678	0.9990	0.9875	0.9767
Sharpen	0.8	0.9900	0.9923	0.9900	0.9845
Speckle noise	0.01	0.9986	0.9971	0.9986	0.9969
	0.1	0.9992	0.9976	0.9985	0.9970

	0.3	0.9905	0.9990	0.9936	0.9971
Translation	20	0.9772	0.9979	0.9986	0.9960
	40	0.9787	0.9983	0.9985	0.9934
	80	0.9820	0.9990	0.9960	0.9868
	160	0.9935	0.9976	0.9848	0.9744
Weiner filter	(2,2)	0.9986	0.9971	0.9986	0.9964
	(3,3)	0.9986	0.9971	0.9986	0.9952
	(5,5)	0.9979	0.9942	0.9971	0.9896
Histogram equalization		0.9994	0.9987	0.9979	0.9965

The BERs of the extracted watermark under different types and parameter attacks are shown in Table 5.

Table 5. The bit error ratio **(**BER) of the extracted watermarks under different types and parameters attacks.

Attacks	**Parameters**	**Lena**		**Pepper**	
		UPC	**Logo**	**UPC**	**Logo**
Contrast adjustment	20%	0.0043	0.0012	0.0052	0.0046
Crop	128 × 128	0.0015	0.0031	0.0020	0.0038
	256 × 256	0.0020	0.0027	0.0032	0.0085
	384 × 384	0.0027	0.0034	0.0544	0.0504
Centre crop	128 × 128	0.0012	0.0031	0.0020	0.0034
	256 × 256	0.0214	0.0012	0.0020	0.0044
	384 × 384	0.0313	0.0025	0.0027	0.0070
Gaussian filter	(2,2)	0.0020	0.0034	0.0023	0.0069
	(3,3)	0.0020	0.0033	0.0020	0.0048
	(5,5)	0.0020	0.0033	0.0020	0.0049
Gaussian noise	0.01	0.0020	0.0033	0.0021	0.0037
	0.1	0.0190	0.0011	0.0095	0.0033
	0.3	0.0570	0.0029	0.0346	0.0041
JPEG 2000 compression	5:1	0.0020	0.0033	0.0021	0.0037
	12:1	0.0020	0.0033	0.0020	0.0036
	20:1	0.0020	0.0033	0.0020	0.0035
JPEG compression	20%	0.0020	0.0033	0.0020	0.0037
	40%	0.0020	0.0033	0.0020	0.0037
	60%	0.0020	0.0033	0.0020	0.0037
	80%	0.0020	0.0033	0.0021	0.0037
	100%	0.0020	0.0033	0.0021	0.0037
Average filter	(2,2)	0.0020	0.0034	0.0023	0.0069
	(3,3)	0.0021	0.0062	0.0054	0.0147
	(5,5)	0.0375	0.0367	0.0663	0.0657
Median filter	(2,2)	0.0020	0.0033	0.0021	0.0060
	(3,3)	0.0020	0.0034	0.0022	0.0065
	(5,5)	0.0167	0.0191	0.0173	0.0239
Motion blur	θ = 4,l = 7	0.0021	0.0052	0.0073	0.0157
Pepper and salt noise	0.01	0.0020	0.0033	0.0021	0.0035
	0.1	0.0017	0.0027	0.0023	0.0033
	0.3	0.0295	0.0013	0.0204	0.0034
Rescale	256 × 256	0.0020	0.0033	0.0021	0.0060
	128 × 128	0.0358	0.0350	0.0416	0.0472

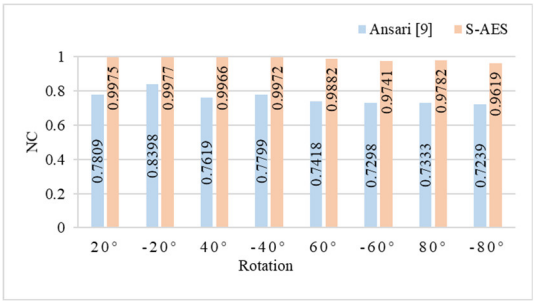
	1024 × 1024	0.0020	0.0033	0.0020	0.0037
	2048 × 2048	0.0020	0.0033	0.0020	0.0037
Rotation	5°	0.0035	0.0032	0.0037	0.0046
	−5°	0.0020	0.0033	0.0082	0.0072
	45°	0.0052	0.0034	0.0073	0.0034
	90°	0.0430	0.0011	0.0181	0.0262
	180°	0.0020	0.0033	0.0023	0.0036
	270°	0.0433	0.0012	0.0181	0.0265
Sharpen	0.8	0.0146	0.0087	0.0146	0.0178
Speckle noise	0.01	0.0020	0.0033	0.0021	0.0037
	0.1	0.0011	0.0030	0.0020	0.0034
	0.3	0.0133	0.0010	0.0095	0.0033
Translation	20	0.0327	0.0024	0.0020	0.0045
	40	0.0307	0.0020	0.0022	0.0075
	80	0.0245	0.0011	0.0058	0.0151
	160	0.0095	0.0027	0.0220	0.0295
Weiner filter	(2,2)	0.0020	0.0033	0.0020	0.0041
	(3,3)	0.0020	0.0033	0.0020	0.0055
	(5,5)	0.0030	0.0066	0.0043	0.0118
Histogram equalization	−	0.0009	0.0015	0.0031	0.0040

According to the information presented in Tables 4 and 5, the NC value of the extracted watermark decreases and the BER increases with the increase in the intensity of the attack. The robustness of "Lena" is stronger than "Pepper" in most cases under the same attack. The NC values of the watermarks are mostly around 0.99 and the BERs are mostly around 0.01. The NC value is above 0.95 and the BER is below 0.05 even under high intensity attacks. The NC values of S-AES are always above 0.99 under crop, Gaussian filter, compression, and speckle noise attacks. However, they drop to 0.95 under an average filter attack with the parameter of (5,5). This is because S-AES uses NSST to capture the texture and directional features of the image. However, the watermark can be extracted successfully, indicating that S-AES has the capability to resist average filter attacks.

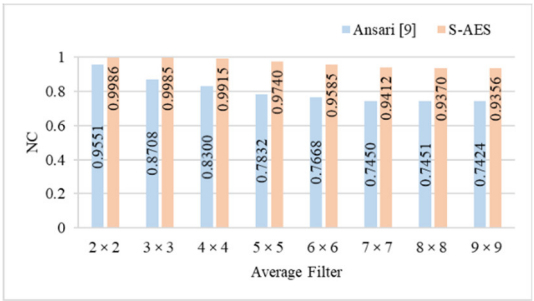
4.2.2. Comparative Analysis

Optimization of Embedding Strength Comparison

We embed "UPC" into "Lena" using the embedding strength optimized by the proposed method and the method presented in [9]. We then perform eight types of attacks on watermarked images. The comparison of NC values is presented in Figure 9.



(**a**)



(**b**)

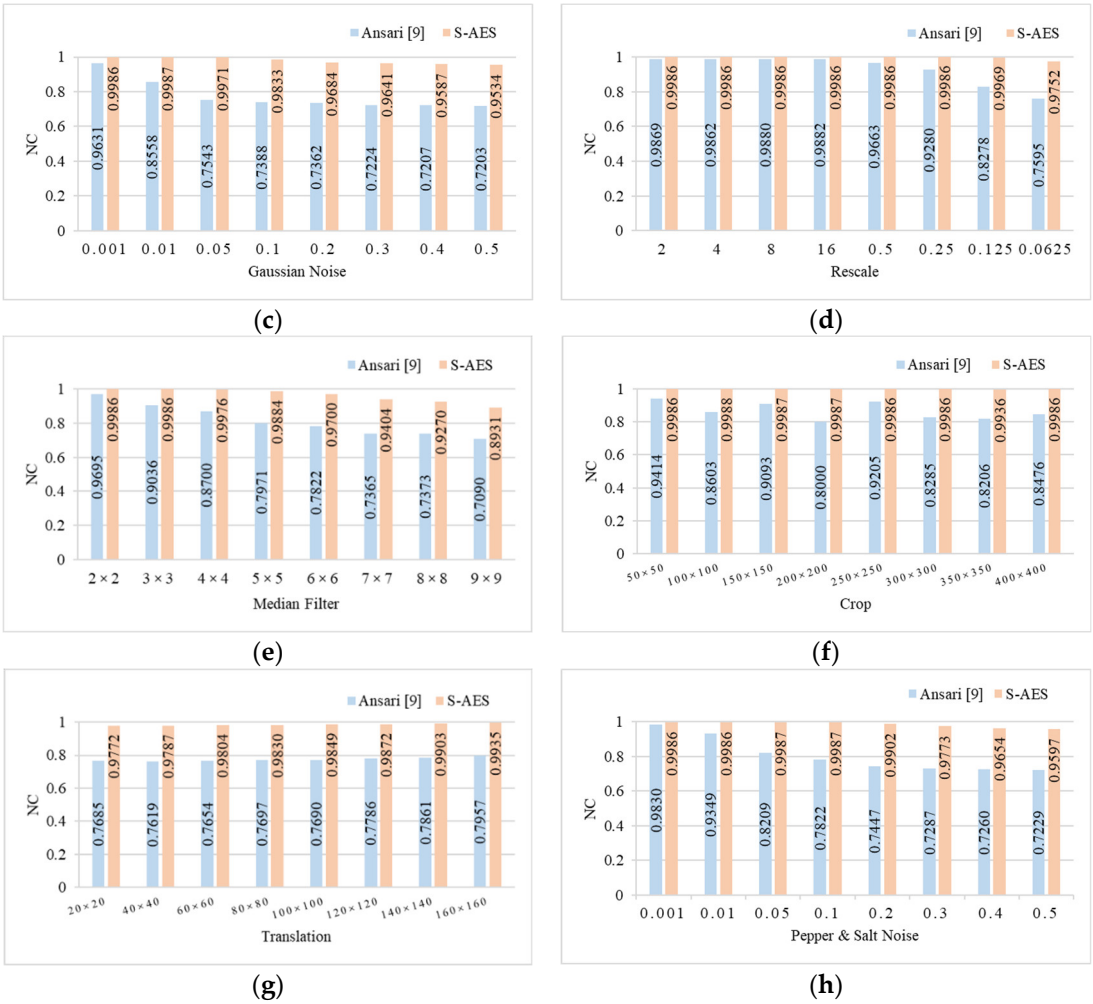


Figure 9. Comparison of NC values under different attacks. (**a**) Rotation. (**b**) Average filter. (**c**) Gaussian noise. (**d**) Rescale. (**e**) Median filter. (**f**) Crop. (**g**) Translation. (**h**) Pepper and salt noise.

It is evident from Figure 9 that the robustness is stronger using the embedding strength optimized by the proposed objective function than [9]. Notably, the NC values decrease more slightly as compared to [9] when the attack intensity increases. Therefore, the proposed algorithm is more robust.

Comparison of Robustness

In order to test the stronger robustness of S-AES, the NC values of the extracted watermark are compared with [9] under attacks with the same parameters. In addition, we also perform comparison with [13,15,17,21,22]. The results are presented in Table 6.

Table 6. Comparison of NC values under attacks with the same parameters.

Attacks	Parameters	S-AES	Ansari [9]	Vali [21]	Makbol [22]	Sharma [15]	Mandanpour [17]	Wang [13]
Contrast adjustment	20%	0.9940	0.5806	-	-	-	-	-
Crop	128 × 128	0.9986	-	-	0.9801	-	0.9400	-
	256 × 256	0.9966	-	0.9686	-	0.9659	-	-
Center Crop	128 ×128	0.9970	-	-	0.9200	-	-	-
Gaussian filter	[3,3]	0.9986	0.9898	0.9832	0.9874	0.9959	0.9900	0.9959
	[5,5]	0.9986	-	0.9899	-	0.9958	0.9900	-
	0.001	0.9986	0.9105	0.9838	0.9810	0.9965	0.9900	0.9983

Gaussian noise	0.01	0.9986	-	0.9304	0.9712	0.9914	0.9800	-
	0.5	0.9400	-	0.8181	-	0.9082	-	-
JPEG 2000 compression	5:1	0.9986	-	-	-	0.9963	-	-
	12:1	0.9986	0.9393	-	-	-	-	-
	20:1	0.9986	-	-	-	0.9959	-	-
JPEG compression	10%	0.9986	-	0.9733	-	0.9954	0.9900	-
	30%	0.9986	-	0.9241	0.9930	0.9957	0.9900	0.9982
	50%	0.9986	0.9706	0.9938	0.9811	0.9960	0.9900	-
	90%	0.9986	-	0.9740	-	0.9962	0.9900	-
Average filter	[2,2]	0.9986	-	-	-	0.9955	-	0.9030
	[3,3]	0.9984	0.8353	0.9496	0.9796	0.9948	0.9700	-
	[5,5]	0.9714	-	-	-	0.9917	0.9000	-
Median filter	[2,2]	0.9986	-	-	0.9802	0.9958	0.9900	-
	[3,3]	0.9986	0.9357	0.9716	0.9800	0.9955	0.9800	0.9971
	[5,5]	0.9856	-	0.9603	-	0.9945	0.9600	-
Motion blur	$\theta = 4$，$l = 7$	0.9984	0.9575	-	-	-	0.7700	-
Pepper and salt noise	0.01	0.9986	-	0.9688	0.9841	0.9916	0.9900	0.9868
	0.1	0.9969	-	0.8924	0.9220	0.9832	0.9600	-
	0.3	0.9632	-	0.8227	0.9353	-	-	-
Rescale	0.5 times	0.9986	-	0.9470	0.9808	0.9948	0.9800	-
	0.25 times	0.9986	0.9803	0.8289	0.9680	0.9903	0.8900	0.9977
	2 times	0.9986	-	0.9705	-	-	0.9900	-
	4 times	0.9986	0.9941	-	-	0.9961	-	-
Rotation	45°	0.9932	-	0.9851	0.9779	-	0.9600	0.3928
	−50°	0.9818	-	0.9820	-	-	0.9200	-
Speckle noise	0.001	0.9986	0.9803	0.9953	-	0.9964	0.9900	-
	0.01	0.9986	-	0.9666	0.9903	0.9899	0.9900	0.9955
	0.1	0.9979	-	0.9210	0.9578	0.9813	0.9700	-
Translation	[10,10]	0.9985	-	0.9715	-	0.9895	0.9900	-
	[20,20]	0.9746	-	-	0.9380	0.9814	0.9800	-
	[10,20]	0.9984	-	-	-	0.9894	-	-
	[20,35]	0.9855	-	-	-	0.9853	-	-
	[50,50]	0.9985	-	0.9880	-	0.9728	0.9500	-
Weiner filter	[2,2]	0.9986	-	-	-	0.9960	-	-
	[3,3]	0.9986	0.9695	0.9940	0.9901	0.9953	-	-
	[5,5]	0.9967	-	0.9533	-	0.9943	-	-
Histogram equalization	-	0.9974	-	0.9721	0.9532	0.9725	0.9800	0.8176

In Table 6, we can see that the NC values of S-AES are larger than [9] under the same attacks. S-AES has stronger robustness than other algorithms for compression and geometric attacks, such as crop and rescale. In most cases, S-AES has stronger robustness than other algorithms under translation attacks. The NC values of S-AES are slightly lower than [15] under the filter attack a larger window size. This is because S-AES uses NSST to select the embedding position.

Under the attacks with the same parameters, we compare the BER of S-AES with methods presented in [13,14,18,35]. The results are presented in Table 7.

Table 7. Comparison of the BER under attacks with the same parameters.

Attacks	Parameters	S-AES	Ma [35]	Wang [13]	Islam [14]	Liu [18]
Crop	10%	0.0015	-	-	-	0.0052
Center crop	10%	0.0012	-	-	-	0.0160

Gaussian filter	[3,3]	0.0020	-	0.0087	0.0039	0.0246
JPEG compression	20%	0.0020	0.0065	-	-	-
	30%	0.0020	0.0065	0.0007	0.0098	-
	50%	0.0020	0.0052	-	0.0059	-
	90%	0.0020	-	-	-	0.0024
Average filter	[3,3]	0.0021	-	0.1187	0.0664	0.0248
Median filter	[3,3]	0.0020	0.0104	0.0097	-	0.0125
Pepper and salt noise	0.01	0.0020	-	0.0093	0.0488	-
Rescale	256 × 256	0.0020	0.0658	0.0068	-	0.0466
	1024 × 1024	0.0020	0.0052	-	-	-
Rotation	5°	0.0035	0.0091	-	0.0352	-
	15°	0.0059	0.0078	-	-	0.1354
	25°	0.0061	0.0117	-	-	0.0936
	35°	0.0046	0.0195	-	-	-
	45°	0.0052	0.0216	0.7780	-	-
Speckle noise	0.01	0.0020	0.0191	0.0131	-	-
Histogram equalization	-	0.0009	-	0.3524	0.0156	-

It is evident from the comparison of the BER presented in Table 7 that the S-AES algorithm has better robustness.

We compared the NC values of the extracted watermark with [15,24] under multiple attacks. The results are shown in Table 8.

Table 8. Comparison of NC values under multiple attacks.

Multiple attacks	**S-AES**	**Sharma [15]**	**Lakrissi [24]**
Pepper and salt noise (0.2) + JPEG compression (30%)	0.9907	0.9868	-
Histogram equalization + Rotation (5°)	0.9861	0.9626	-
Sharpen + Gaussian filter ([3,3])	0.9966	-	1
Gaussian noise (0.2) + crop (25%)	0.9719	0.9613	-
Sharpen + Average filter ([5,5])	0.9956	0.9940	-
Rescale (0.5) + JPEG compression (50%)	0.9986	-	0.9816
Gaussian noise (0.01) + JPEG compression (50%)	0.9987	-	0.9633
Weiner filter ([5,5]) + Translation (10)	0.9983	0.9899	-
Average filter ([5,5]) + Rotation (5°)	0.9985	0.9910	-
Pepper and salt noise (0.2) + Gaussian noise (0.2)	0.9653	0.9678	-
Gaussian noise (0.01) + Gaussian filter ([3,3]) + JPEG compression (50%)	0.9986	-	0.9800
Pepper and salt noise (0.01) + contrast adjustment (20%) + JPEG compression (50%)	0.9984	-	0.8798

According to Table 8, most of the NC values of S-AES are larger than those in [15] and [24]. Therefore, S-AES has the ability to resist multiple attacks effectively.

The aforementioned experimental results show that S-AES has the capacity to resist not only single attacks but also multiple attacks. Furthermore, S-AES has stronger robustness compared with the existing algorithms.

4.3. False Positive Problem

In order to test the false positive problem, the watermarked image "Lena" is embedded with the "UPC" watermark used as a disputed image. "Logo" is used as a false watermark. The extracted results are presented in Figure 10.

(**a**) (**b**) (**c**)

Figure 10. Result of the false positive problem. (**a**) Disputed image. (**b**) False watermark. (**c**) Extracted watermark.

Figure 10 shows that the watermark cannot be extracted successfully using side information of the false watermark. This indicates that S-AES overcomes the false positive problem.

According to the aforementioned experiments, S-AES has good imperceptibility and strong robustness for single attacks and multiple attacks. It also overcomes the false positive problem.

5. Conclusions

In this work, we propose an adaptive embedding strength watermarking algorithm based on shearlets' capture directional features (S-AES). The multiscale and multidirectional characteristics of NSST are used to improve the watermarking algorithms in the domain of DWT. This enables the algorithm to resist common attacks and geometric attacks effectively. S-AES fully considers the watermarking characteristics of imperceptibility and robustness and optimizes the embedding strength using the proposed objective function, achieving maximum robustness under the premise of satisfying imperceptibility. As compared with other algorithms, S-AES has a greater ability to resist high intensity attacks. We embedded the principle components enclosing the unique features of the watermark into the host image to overcome the false positive problem. Even if someone provides a wrong singular matrix obtained from a false watermark, it cannot extract the watermark successfully using side information of the false watermark. The robustness of S-AES decreases slightly under average and median filter attacks with a larger window size. This can be improved in the future. In addition, S-AES can also be extended to the field of video watermarking.

Author Contributions: Conceptualization, Q.Z. and N.L.; methodology, N.L.; writing—original draft preparation, N.L.; writing—review and editing, N.L. and F.W. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Natural Science Foundation of China, grant number 51274232; the Natural Science Foundation of Shandong Province of China, grant number ZR2018MEE004; and the Fundamental Research Funds for the Central Universities, grant number 19CX02030A.

Acknowledgments: The authors would like to sincerely thank the anonymous reviewers for their valued comments and constructive suggestions, which significantly improved the quality of this paper.

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

References

1. Najafi, E.; Loukhaoukha, K. Hybrid secure and robust image watermarking scheme based on SVD and sharp frequency localized contourlet transform. *J. Inf. Secur. Appl.* **2019**, 44, 144–156.
2. Arumugham, S.; Rajagopalan, S.; Rayappan, J.B.B.; Amirtharajan, R. Tamper-resistant secure medical image carrier: An IWT–SVD–Chaos–FPGA combination. *Arab. J. Sci. Eng.* **2019**, 44, 9561–9580.
3. Bhinder, P.; Singh, K.; Jindal, N. Image-adaptive watermarking using maximum likelihood decoder for medical images. *Multimed. Tools Appl.* **2018**, 77, 10303–10328.

4. Huang, Y.; Niu, B.N.; Guan, H.; Zhang, S.W. Enhancing image watermarking with adaptive embedding parameter and PSNR guarantee. *IEEE Trans. Multimed.* **2019**, 21, 2447–2460.
5. Zhou, X.Y.; Cao, C.J.; Ma, J.X. An adaptive digital watermarking scheme based on support vector machines and optimized genetic algorithm. *Math. Probl. Eng.* **2018**, doi:10.1155/2018/2685739.
6. Kang, X.B.; Chen, Y.J.; Zhao, F.; Lin, G.F. Multi-dimensional particle swarm optimization for robust blind image watermarking using intertwining logistic map and hybrid domain. *Soft Comput.* **2019**, 24, 10561–10584.
7. Kuraparthi, S.; Kollati, M.; Kora, P. Robust optimized discrete wavelet transform-singular value decomposition based video watermarking. *Trait. Signal* **2019**, 36, 565–573.
8. Cui, X.C.; Niu, Y.Y.; Zheng, X.W.; Han, Y.S. An optimized digital watermarking algorithm in wavelet domain based on differential evolution for color image. *PLoS ONE* **2018**, 13, e0196306.
9. Ansari, I.A.; Pant, M. Multipurpose image watermarking in the domain of DWT based on SVD and ABC. *Pattern Recogn. Lett.* **2017**, 94, 228–236.
10. Zhang, Q.; Li, Y.; Wei, X. An improved robust and adaptive watermarking algorithm based on DCT. *J. Appl. Res. Technol.* **2012**, 10, 405–415.
11. Hamidi, M.; El Haziti, M.; Cherifi, H.; El Hassouni, M. Hybrid blind robust image watermarking technique based on DFT-DCT and Arnold transform. *Multimed. Tools Appl.* **2018**, 77, 27181–27241.
12. Abdulrahman, A.K.; Ozturk, S. A novel hybrid DCT and DWT based robust watermarking algorithm for color images. *Multimed. Tools Appl.* **2018**, 78, 17027–17049.
13. Wang, B.W.; Zhao, P. An adaptive image watermarking method combining SVD and Wang-Landau sampling in DWT domain. *Mathematics* **2020**, 8, 691.
14. Islam, M.; Roy, A.; Laskar, R.H. SVM-based robust image watermarking technique in LWT domain using different sub-bands. *Neural Comput. Appl.* **2020**, 32, 1379–1403.
15. Sharma, S.; Sharma, H.; Sharma, J.B. An adaptive color image watermarking using RDWT-SVD and artificial bee colony based quality metric strength factor optimization. *Appl. Soft Comput.* **2019**, 84, 105696.
16. Gao, X.B.; Lu, W.; Tao, D.C.; Li, X.L. Image quality assessment based on multiscale geometric analysis. *IEEE Trans. Image Process.* **2009**, 18, 1409–1423.
17. Mardanpour, M.; Chahooki, M.A.Z. Robust transparent image watermarking with Shearlet transform and bidiagonal singular value decomposition. *AEU Int. J. Electron. Commun.* **2016**, 70, 790–798.
18. Liu, X.Y.; Wang, Y.F.; Du, J.Y.; Liao, S.H.; Lou, J.T.; Zou, B.J. Robust hybrid image watermarking scheme based on KAZE features and IWT-SVD. *Multimed. Tools Appl.* **2019**, 78, 6355–6384.
19. Araghi, T.K.; Abd Manaf, A.; Araghi, S.K. A secure blind discrete wavelet transform based watermarking scheme using two-level singular value decomposition. *Expert Syst. Appl.* **2018**, 112, 208–228.
20. 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.
21. Vali, M.H.; Aghagolzadeh, A.; Baleghi, Y. Optimized watermarking technique using self-adaptive differential evolution based on redundant discrete wavelet transform and singular value decomposition. *Expert Syst. Appl.* **2018**, 114, 296–312.
22. Makbol, N.M.; Khoo, B.E.; Rassem, T.H.; Loukhaoukha, K. A new reliable optimized image watermarking scheme based on the integer wavelet transform and singular value decomposition for copyright protection. *Inform. Sci.* **2017**, 417, 381–400.
23. Ali, M.; Ahn, C.W.; Siarry, P. Differential evolution algorithm for the selection of optimal scaling factors in image watermarking. *Eng. Appl. Artif. Intell.* **2014**, 14, 15–26.
24. Lakrissi, Y.; Saaidi, A.; Essahlaoui, A. Novel dynamic color image watermarking based on DWT-SVD and the human visual system. *Multimed. Tools Appl.* **2017**, 77, 13531–13555.
25. Yadav, N. DWT-SVD-WHT watermarking using varying strength factor derived from means of the WHT coefficients. *Arab. J. Sci. Eng.* **2018**, 43, 4131–4143.
26. Araghi, T.K.; Abd Manaf, A. An enhanced hybrid image watermarking scheme for security of medical and non-medical images based on DWT and 2-D SVD. *Future Gener. Comp. Syst.* **2019**, 101, 1223–1246.
27. Li, Y.W.; Song, W.; Zhao, X.B.; Wang, J.; Zhao, L.Z. A novel image tamper detection and self-recovery algorithm based on watermarking and chaotic system. *Mathematics* **2019**, 7, 955.
28. Zhao, J.; Xu, W.S.; Zhang, S.L.; Fan, S.S.; Zhang, W.R. A strong robust zero-watermarking scheme based on shearlets' high ability for capturing directional features. *Math. Probl. Eng.* **2016**, 2016, 2643263.
29. Wang, X.Y.; Liu, Y.N.; Li, S.; Yang, H.Y.; Niu, P.P. Robust image watermarking approach using polar harmonic transforms based geometric correction. *Neurocomputing* **2016**, 174, 627–642.
30. Thanki, R.; Borra, S.; Dwivedi, V.; Borisagar, K. An efficient medical image watermarking scheme based on FDCuT–DCT. *Eng. Sci. Technol.* **2017**, 20, 1366–1379.
31. Moosazadeh, M.; Ekbatanifard, G. A new DCT-based robust image watermarking method using teaching-

learning-based optimization. *Optik* **2019**, 47, 28–38.
32. Tan, Y.; Qin, J.H.; Xiang, X.Y.; Ma, W.T.; Pan, W.Y.; Xiong, N.N. A Robust Watermarking Scheme in YCbCr Color Space Based on Channel Coding. *IEEE Access* **2019**, 7, 25026–25036.
33. Rakheja, P.; Vig, R.; Singh, P. An asymmetric watermarking scheme based on random decomposition in hybrid multi-resolution wavelet domain using 3D Lorenz chaotic system. *Optik* **2019**, 198, 163289.
34. Zebbiche, K.; Khelifi, F.; Loukhaoukha, K. Robust additive watermarking in the DTCWT domain based on perceptual masking. *Multimed. Tools Appl.* **2018**, 77, 21281–21304.
35. Ma, B.; Chang, L.L.; Wang, C.P.; Li, J.; Wang, X.Y.; Shi, Y.Q. Robust image watermarking using invariant accurate polar harmonic Fourier moments and chaotic mapping. *Signal Process.* **2020**, 172, 107544.