International Journal of Innovative
Computing, Information and Control
Volume **19**, Number **6**, December **2023**

 ISSN 1349-4198
pp. **1847–1859**

RESEARCH ON WATERMARKING ALGORITHM BASED ON IMPROVED ARNOLD PERMUTATION AND ADAPTIVE EMBEDDING POSITION

Wenjie Meng[1,*], Qiumei Zheng[2] and Fenghua Wang[2]

[1]Library Information Technology Department
[2]College of Computer Science and Technology
China University of Petroleum (East China)
No. 66, West Changjiang Road, Huangdao District, Qingdao 266580, P. R. China
{ zhengqm; fenghuawang }@upc.edu.cn
[*]Corresponding author: mengwj@upc.edu.cn

Received March 2023; revised July 2023

Abstract. *This paper proposes an adaptive watermarking algorithm for copyright protection that addresses the limitations of existing techniques, including low anti-attack ability, fixed embedding strength, and single watermark size. The algorithm selects locations with rich image information in the four high-frequency sub-bands of an image for watermark embedding, effectively enhancing the robustness of the watermark. To address the issue of watermark algorithms being limited to a single-size watermark image, the proposed algorithm adaptively selects the number of watermark embedding blocks based on the size of the watermark image, enabling multi-size watermark embedding. Additionally, the improved Arnold algorithm is utilized to encrypt the watermark image, enhancing the watermark's security. Experimental results demonstrate that the proposed algorithm ensures the robustness of the watermarking process while addressing the fixed image size issue, enabling multi-size watermark embedding.*
Keywords: Watermarking algorithm, Arnold permutation, Embedding position

1. **Introduction.** The rapid development of electronic resources has brought greater challenges in copyright protection of digital libraries. Watermarking technology achieves copyright protection by embedding image-related information in the original image.

Currently, many robust watermarking algorithms are transformed domain algorithms [1-8]. First, the image is converted to the frequency domain, and the frequency domain coefficients are processed according to certain rules to complete the watermark embedding. Typically, methods such as Discrete Wavelet Transform (DWT) [1,5], discrete Tchebichef transform [2], discrete lifting wavelet transform [3], discrete cosine transform [6], and non-subsampled discrete wavelet transform [7,8] are selected to process the image before embedding the watermark. Such algorithms require more computational complexity but allow for embedding more information and provide higher resistance to attacks than spatial domain algorithms. [9-12] designed watermarking algorithms based on discrete wavelet transform, which embeds watermark information in the low-frequency part and has certain capabilities to resist noise, filtering, and other attacks. However, the DWT transform performs downsampling during signal processing, which results in the discrete wavelet transform not having shift invariance and limited resistance to geometric attacks. Zhang and Lu [13] provided an audio watermark algorithm based on Discrete Fourier Transform (DFT) peak detection, which can commendably defend synchronous attacks

DOI: 10.24507/ijicic.19.06.1847

like Time Scale Modulation (TSM) and pitch shifting. Sharma et al. [14] proposed Redundant Discrete Wavelet Transform (RDWT) for image processing and selected low frequency as the watermark embedding location, but the algorithm's resistance to geometric attacks is still not ideal. This is due to the limitations of the directional filter type of the wavelet transform, which limits the representation of image direction information and thus limits the algorithm's resistance to attacks. At the same time, the embedding location of the algorithm is in the low-frequency part, which does not contain the direction and contour information of the image and also hinders the algorithm's ability to resist geometric attacks.

Therefore, watermarking algorithms based solely on single-band embedding are not yet perfect in terms of robustness. This is because image transformations have redundancy, resulting in a large amount of useless information in each frequency band, with only some regions containing useful information. Embedding the watermark into the entire sub-band cannot fully utilize the information obtained after the transformation, which limits the algorithm's ability to extract the watermark when faced with attacks. Therefore, to improve the robustness of the algorithm, it is necessary not only to choose the appropriate frequency band but also to select the location that can fully represent the effective information in the image for watermark embedding. In our previous work [15], a Discrete Wavelet Transform and Non-Subsampled Contourlet Transform (DWT-NSCT) watermarking algorithm combined with geometric correction was proposed. By combining geometric correction techniques with transform domain algorithms, this algorithm uses the translation invariance, multiscale, and multidirectional properties of the NSCT transform to perform NSCT transformation on the approximate sub-band obtained after DWT transformation, and selects high-frequency sub-bands containing more directional contour information as the watermark embedding area. At the same time, the Zernike moments are used to rotate the image for further optimization of the algorithm. The experiments show that the algorithm has strong robustness against both conventional attacks and geometric attacks. However, this algorithm only selects one directional sub-band for watermark embedding and does not fully utilize the directional information obtained after NSCT, which reduces its robustness against rotation attacks, and it can only embed a watermark image of a single size.

To address the above-mentioned issues, this paper further improves the watermarking algorithm and proposes an adaptive embedding position watermarking algorithm. Based on the NSCT transform of the DWT-transformed approximation sub-band, this algorithm fully utilizes image information to construct watermark embedding positions through a block-based algorithm, ensuring the algorithm's ability to extract watermarks under various attacks. At the same time, the algorithm's flexibility is enhanced by using the block-based approach to achieve multi-size watermark embedding. The improved Arnold encryption is also used to encrypt images and improve the algorithm's security.

The remainder of the paper is structured as follows. In Section 2, related theories are discussed. The improved adaptive watermarking algorithm with Arnold scrambling and block-based strategy is described in Section 3. Experiments and results are shown in Section 4. Conclusions are drawn in Section 5.

2. **Related Theory.**

2.1. **Improved Arnold watermark encryption algorithm.**

Arnold scrambling [15] is commonly used to pre-process the watermark image, mapping the old positions to new positions for an $M \times M$ sized image, transforming the meaningful information contained in the image into a meaningless image.

To improve the Arnold scrambling algorithm, a Zigzag scanning technique is combined. Before encrypting the image with Arnold scrambling, the image is first scanned using the Zigzag method, and then the one-dimensional data is reconstructed, as shown in Figure 1.

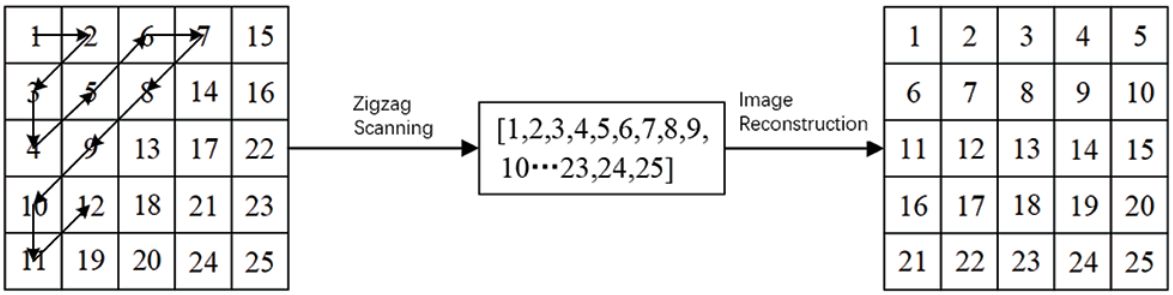


FIGURE 1. Zigzag scan

The encryption of the image in this algorithm is achieved by performing K rounds of Arnold scrambling on the scanned and reconstructed image. The algorithm only needs to store the key for Arnold scrambling, but it achieves the effect of double encryption. The encryption process is shown in Figure 2.

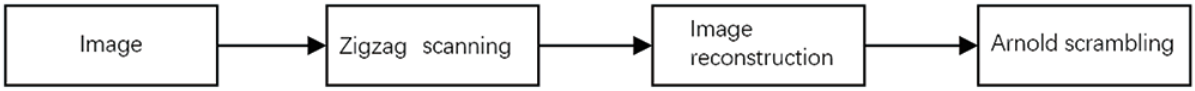


FIGURE 2. Encryption process

The decryption process of the image is exactly the opposite of the encryption process. The process is shown in Figure 3.

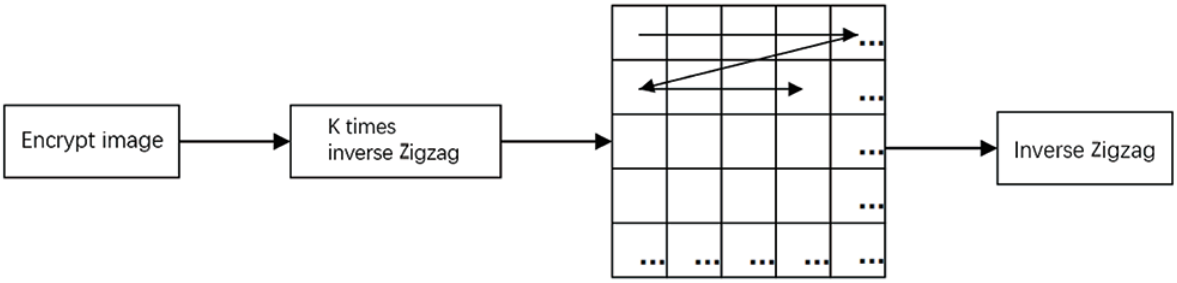


FIGURE 3. Decode process

2.2. **Watermark embedding position selection.** In our previous algorithm [15], the embedding position of the algorithm was fixed, which was not conducive to ensuring the security of the algorithm. Moreover, the direction information of the transformed image was not fully utilized, resulting in the algorithm having good anti-rotation attack capability only based on geometric correction. Therefore, this paper proposes a watermark embedding position selection algorithm. Based on the size of the watermark image, sub-blocks are selected in four directional sub-bands to determine the embedding position of the watermark, as shown in Figure 4.

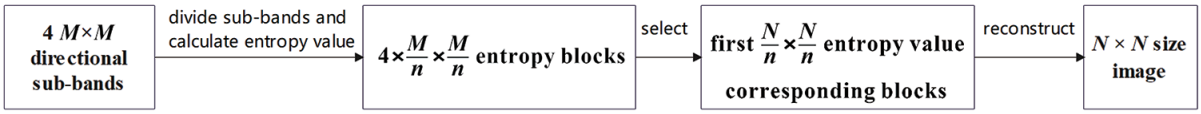


FIGURE 4. Embedded location selection process

2.3. **NSCT.** NSCT [16] is a fast transform that can effectively approximate image features and capture image features well. It consists of two parts: Non-Subsampled Pyramid (NSP) and Non-Subsampled Directional Filter Bank (NSDFB). NSP decomposes the image into multiple scales, while NSDFB decomposes the high-frequency portion into multiple directions, making NSCT transform have translation invariance, multi-scale and multi-directional characteristics.

3. Improved Adaptive Watermarking Algorithm with Arnold Scrambling and Block-Based Strategy.

3.1. **Watermark embedding.** The watermark embedding algorithm can be divided into 7 steps, as shown in Figure 5, which are described as follows.

Step 1: Host image processing. Firstly, the image is subjected to spatial transformation, and then the luminance Y is selected for DWT processing. The low-frequency part obtained is subjected to two-layer non-subsampled contourlet transform. Four directional subbands are selected for watermark embedding after the transform.

Step 2: Selection of embedding positions. According to the watermark embedding position selection algorithm introduced in Section 2.2, the specific processes are as follows.

1) Divide sub-bands and calculate entropy value. Divide the four directional sub-bands of size $M \times M$ into non-overlapping blocks of size $n \times n$ to obtain $4 \times M/n \times M/n$ image blocks and calculate the entropy value for each block, as shown in Equation (1).

$$E_i = Entropy(X_i) \quad i = 1, 2, \ldots, 4 \times M/n \times M/n \tag{1}$$

where X represents the image block. Sort all the entropy values according to the order of the sub-blocks, and associate the obtained entropy values with the corresponding block order, and save the array (E_i, i).

2) Sort the entropy values in descending order and obtain a new sequence of entropy values that correspond to the original block sequence, as shown in Equation (2).

$$(E_i', A) = sort(E_i, descend) \quad i = 1, 2, \ldots, 4 \times M/n \times M/n \tag{2}$$

where $sort(E_i, descend)$ represents the descending sorting operation, E_i' and A represent the sorted entropy value sequence and the corresponding position values before sorting, respectively. The first $(N/n)^2$ entropy values corresponding to image blocks are selected as the watermark embedding positions according to the size of the $N \times N$ watermark image.

3) Reconstruct the $(N/n)^2$ image blocks obtained into an image of size $N \times N$. The sub-blocks containing relatively more information are selected from the four directional subbands, and then the image is reconstructed. The selected sub-blocks are rearranged into an image block I with the same size as the watermark image.

Step 3: Watermark image processing. The image is processed using the improved encryption algorithm in Section 2.1 to obtain the encrypted watermark image W, and the key K is saved.

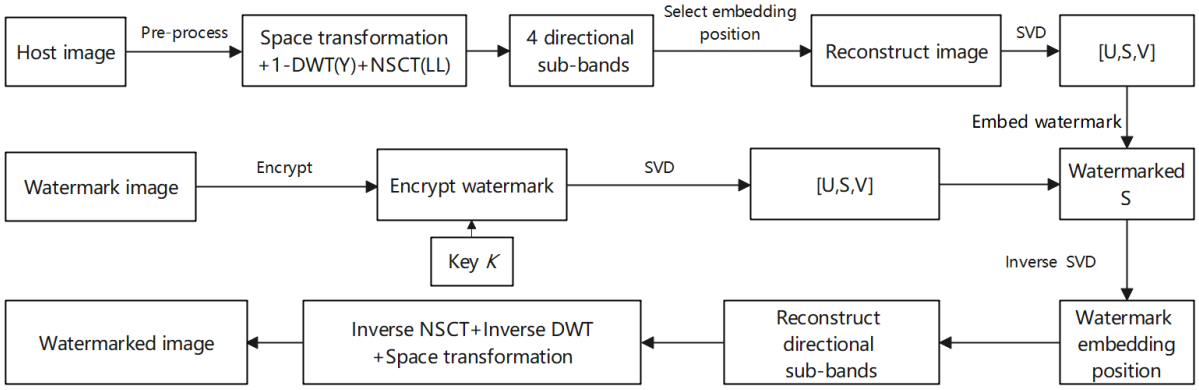


FIGURE 5. Watermarking embedding process

Step 4: Singular value decomposition. The image block I and the watermark image W obtained are subjected to SVD decomposition, as shown in Equations (3) and (4):

$$SVD(I) = U_1 S_1 V_1^T \tag{3}$$

$$SVD(W) = U_2 S_2 V_2^T \tag{4}$$

Step 5: Watermark embedding. The watermark singular value matrix obtained in the previous step is added to the image singular value matrix using an additive approach, as shown in Equation (5):

$$S' = S_1 + factor \times S_2 \tag{5}$$

where, the *factor* represents the watermark embedding strength, which is solved using the PSO-GWO algorithm.

Perform inverse SVD decomposition on the watermarked singular value matrix S' with U_1 and V_1 to obtain the watermarked image block I_m, as shown in Equation (6):

$$I_m = U_1 \times S' \times V_1^T \tag{6}$$

Step 6: Reconstruction of watermarked directional sub-bands. In Step 2, $(N/n)^2$ blocks of size $N \times N$ were selected from the four directional sub-bands of size $M \times M$, and watermarked using the block-based strategy. After watermark embedding, the watermarked directional sub-bands are reconstructed based on the original block order matrix A corresponding to the $(N/n)^2$ blocks with the highest entropy. First, the watermarked image block I_m is non-overlapping partitioned into $n \times n$ sub-blocks, which are then arranged in left-to-right and top-to-bottom order. The $(N/n)^2$ watermarked sub-blocks are matched with their corresponding original sub-blocks using the original block order matrix saved in Step 2. The watermarked sub-blocks are then used to replace the corresponding sub-bands in the original frequency domain using Equation (7). Finally, four directional sub-bands containing the watermark are obtained.

$$\begin{cases} a = \dfrac{A[i]-1}{\frac{M}{n} \times \frac{M}{n}} + 1 \\ b = (A[i]-1) \bmod \left(\dfrac{M}{n} \times \dfrac{M}{n} \right) + 1 \end{cases} \quad i = 1, 2, 3, \ldots, \frac{M}{n} \times \frac{M}{n} \tag{7}$$

Here, a represents the index of the directional subband, and b represents the position of the sub-block in the corresponding directional subband.

Step 7: Perform inverse NSCT transform, inverse DWT transform, and spatial transformation on the image to obtain the watermarked image.

3.2. **Watermark extraction algorithm.** The watermark extraction process is shown in Figure 6 and includes three steps as follows.

Step 1: Preprocessing. Similar to the watermark embedding process, the image is first spatially transformed, and then the luminance component Y is selected for a 1-level DWT transformation. The resulting low-frequency subband is subjected to a 2-level non-subsampled contourlet transform, and the watermark embedding position selection algorithm is used to obtain the watermarked image block I_{mm}.

Step 2: The image block is subjected to SVD decomposition, and the watermark image is extracted using the saved S_1, U_2, V_2, and *factor* values, as shown in Equations (8) and (9):

$$SVD(I_{mm}) = U_m \times S_m \times V_m^T \tag{8}$$

$$I_w = U_2 \times \frac{(S_m - S_1)}{factor} \times V_2^T \tag{9}$$

Step 3: The image is decrypted using the decryption algorithm with the key K, as described in Section 2.1. The decrypted watermark image is obtained.

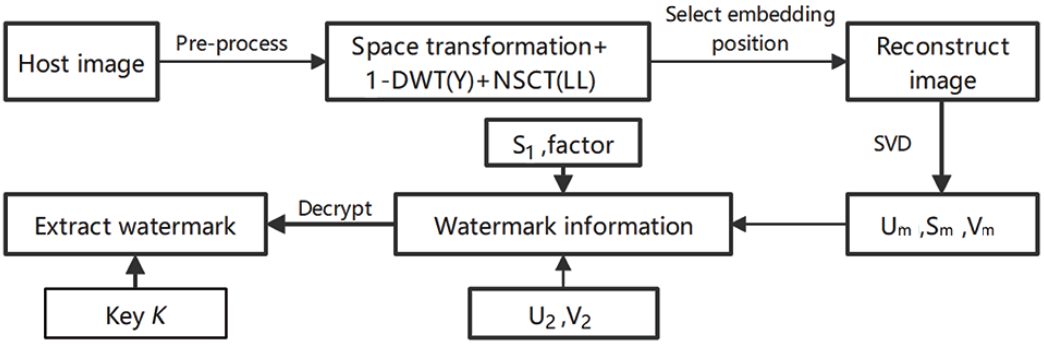


FIGURE 6. Watermarking extraction process

4. **Experimental Results and Analysis.** To comprehensively test the performance of the watermarking algorithm, this paper selected 3 512×512 host images and 2 watermark images as verification images for experiments, as shown in Figure 7. These host images combine numerous intricate elements, smooth areas, shadows, textures, etc. They are very suitable for testing watermark image processing algorithms. The watermark images are selected from commonly used logos and letter-type images.

(a) Lena (b) Airplane (c) Flower (d) LOGO (e) C

FIGURE 7. The host images and watermark images

4.1. **Block size analysis.** In this paper, the algorithm performs non-overlapping block partitioning of the directional subbands with a size of $n \times n$ when selecting the watermark embedding position. A certain number of blocks are selected for reconstruction to obtain the watermark embedding position. The block size directly affects the anti-attack ability of the watermark algorithm, especially its anti-filtering ability. Moreover, when selecting the embedding blocks, it is necessary not only to partition and read the four directional subbands, but also to calculate the entropy value of each block. Therefore, the block size directly affects the running time of the algorithm. To obtain the optimal block size, experiments were conducted on the 512×512 Lena image and the 128×128 LOGO image, and different block sizes, such as 4×4, 8×8, and 16×16, were selected to implement the watermark embedding. Finally, the running time and robustness of the algorithms with different block sizes were evaluated, as shown in Table 1.

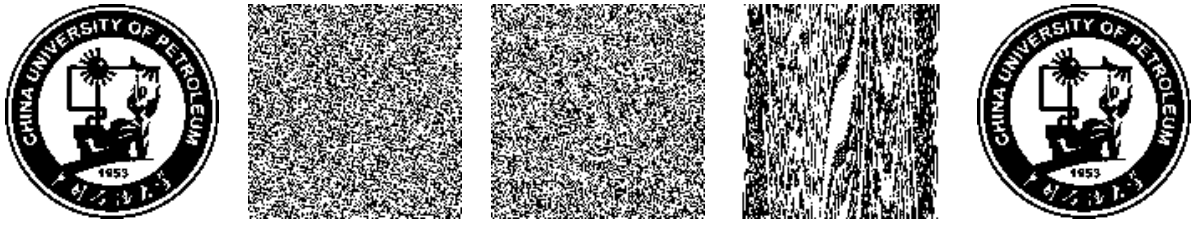
Table 1. Block size test results

Chunk size	Run time (seconds)	Robustness
4×4	4.705	0.9887
8×8	2.58	0.9929
16×16	2.32	0.9870

The robustness in Table 1 refers to the average NC value obtained from extracting watermarks from watermarked images after various types and intensities of filtering, noise, rotation, translation, and other attacks in different block embedding algorithms. As shown in the table, the robustness generally increases with the increase of block size, and the running time of the watermark algorithm decreases. However, it can be seen that compared with the watermark algorithm using 8×8 blocks, the watermark algorithm using 16×16 blocks did not significantly reduce the time and had lower average NC values. Therefore, based on the above analysis, the block size of 8×8 is selected for the watermark algorithm to embed watermarks into the image.

4.2. **Security analysis.** The security of watermark algorithms should be high in addition to the requirements of invisibility and robustness. The encryption process of the watermark using the algorithm in Section 2.1 solves the problem that the Arnold scrambling algorithm can be cracked by brute force. The encryption and decryption process of the LOGO image is shown in (b)-(e) of Figure 8.

As shown in Figure 8, Figure 8(a) is the original LOGO image, 8(b) is the image obtained by encrypting the image with the key K, 8(c) is the image obtained by decrypting 8(b) with the wrong key, and 8(d) and 8(e) are the decrypted images obtained by using the



(a) LOGO (b) Encrypted (c) Wrong key (d) Wrong decryption (e) Correct decryption

Figure 8. The watermark encryption

correct key and the conventional and improved Arnold algorithms, respectively. It can be seen from the figure that the improved Arnold encryption algorithm solves the problem of brute-force cracking of the conventional Arnold algorithm, and has higher security than the conventional Arnold encryption algorithm. Furthermore, without increasing the number of keys, it achieves the effect of double encryption.

4.3. **Invisibility analysis.** Two watermarked images of size 128 × 128, denoted as Figures 7(d) and 7(e), were embedded into the original images of size 512 × 512 shown in Figures 7(a)-7(c) using the watermark embedding algorithm. The resulting watermarked images are shown in Figure 9.

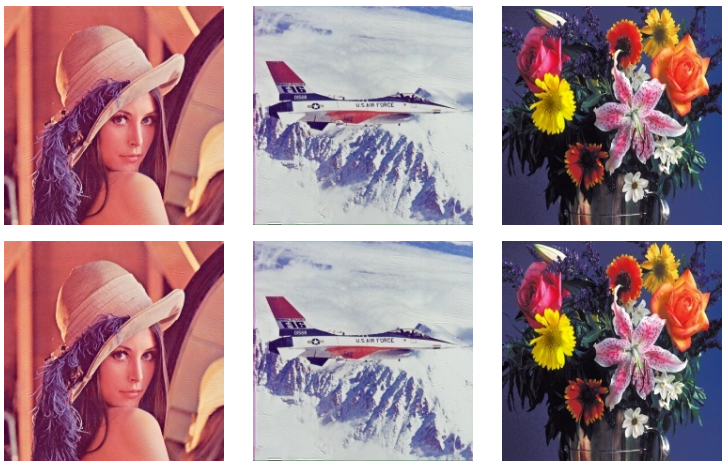


FIGURE 9. Watermark embedding effect

In Figure 9, two rows represent the image results after adding LOGO, and C watermarks, respectively. It can be observed that the images have remained largely unchanged before and after watermark embedding. To objectively measure the impact of the added watermark information on the images, the PSNR values were calculated for the above images, and the test results are shown in Table 2.

TABLE 2. The experiment result of imperceptibility

PSNR (dB)	UPC	LOGO	C
Lena	40.0091	40.2828	40.0094
Airplane	40.5254	40.6077	40.4507
Flower	40.0018	40.7294	40.2236

From Table 2, it can be seen that the PSNR values calculated after watermark embedding are all above 40 dB, which is higher than the threshold set by the optimized algorithm. Combined with the watermark embedding effect in Figure 9, it can be concluded that the proposed watermark algorithm has good invisibility.

4.4. **Robustness analysis.** The host images with a size of 512 × 512 in Figures 7(a)-7(c) and the watermark image with a size of 128 × 128 in Figure 7(d) were selected. The chosen three host images have different textures and feature information; thus, the algorithm was tested on these three images to verify the robustness. The watermarked images were subjected to various attacks, including salt-and-pepper noise attacks with intensities of 0.001, 0.01, 0.1, 0.3, and 0.5, Gaussian filtering attacks with filter windows of size 2 × 2, 3 × 3, and 5 × 5, JPEG compression attacks with different intensities, as

well as scaling, cropping, and rotation attacks. The extracted NC value of the watermark under high-intensity noise attack is basically 1, indicating that the extracted watermark is consistent with the original image. Although some of the NC values obtained under scaling, Gaussian filtering, and other attacks are not ideal, they are also generally around 0.9. The proposed algorithm exhibits good resistance to various attacks on the three selected images.

In addition, the proposed algorithm was objectively analyzed using NC values and BER values. When subjected to noise attacks of intensity from 0.01 to 0.5, the NC values of the watermarks extracted by this algorithm are all above 0.999, and the Bit Error Rate (BER) is less than 0.001. When the watermark image is C, lossless extraction is achieved, indicating that the algorithm has strong robustness against noise attacks. The NC values of the watermarks extracted after JPEG compression attacks, as well as after shear and scaling attacks, also reached over 0.99. By fully utilizing the feature information of the image, the algorithm has strong anti-rotation attack capability, with most of the NC values above 0.99. The NC values also reached 0.98 when facing Gaussian and median filtering attacks, but slightly decreased when encountering Wiener filtering of intensity 3×3. This is because the block algorithm used by this algorithm to extract the embedding location of the watermark has slightly weaker robustness against filtering attacks, but still able to extract effective watermark images. In addition, this algorithm also shows strong robustness against contrast adjustment, sharpening, and translation attacks.

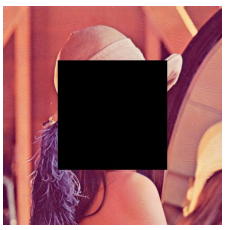
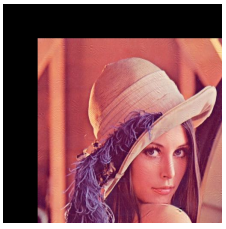
Compared with the algorithm in [15], the watermark embedding position selection algorithm of this algorithm automatically determines the number of embedding blocks based on the size of the watermark. Therefore, this watermark algorithm can change the size of the watermark image according to actual needs, making the algorithm more flexible. To verify that the algorithm has robustness against watermark images of different sizes, the Lena image with a size of 512×512 was selected as the host image, and C images with sizes of 32×32, 64×64, 128×128, and 256×256 were embedded, respectively. The results of the attack tests on the obtained images are shown in Table 3.

As shown in Table 3, the proposed algorithm successfully embeds watermarks of different sizes. The NC values obtained for watermark sizes of 64×64 and 128×128 are

Table 3. Different size watermarks were extracted and compared with NC values.

Attack type	Attack strength	32×32	64×64	128×128	256×256
Gaussian filter	$[2, 2]$	0.9985	0.9996	0.9998	0.9855
Median filter	$[2, 2]$	0.9970	0.9994	0.9999	0.9828
Wiener filtering	$[2, 2]$	0.9970	0.9991	0.9980	0.9406
Gaussian noise	0.01	1.0000	1.0000	1.0000	1.0000
Salt-and-pepper noise	0.01	1.0000	1.0000	1.0000	1.0000
Speckle noise	0.01	1.0000	1.0000	1.0000	1.0000
Sharpening	0.8	0.9977	1.0000	1.0000	1.0000
JPEG	40	0.9970	0.9996	0.9999	0.9905
Translation	0.25	0.9977	0.9994	0.9999	0.9624
Rotation	45°	0.9802	0.9998	1.0000	1.0000
Top-left cropping	128×128	0.9992	1.0000	1.0000	0.9996
Center cropping	128×128	0.9992	0.9998	1.0000	0.9999

TABLE 4. Extracted watermarks under different attacks

Attack type	Lena	LOGO	C
Contrast adjustment 20%			
Crop 256 × 256			
Gaussian filtering 3 × 3			
Salt and pepper noise 0.5			
JPEG 60			
Translation 80			
Rotation 45°			

slightly higher than those for other sizes. When the watermark size is 32×32, the NC values are above 0.98, and the algorithm shows strong robustness. When the watermark size is increased to 256×256, the NC values slightly decrease after filtering and scaling attacks, but they are still above 0.96 and the watermarks can be extracted clearly.

To observe the effectiveness of the watermark extracted by the algorithm under various types of attacks, the extracted watermarks after the attacks are visually presented. In this section, Figure 7(a) Lena image is chosen as the host image, and Figure 7(d) LOGO image, and Figure 7(e) C image are selected as watermark information for visual presentation. The extraction results are shown in Table 4.

From Table 4, it can be observed that the image quality significantly degrades after being subjected to attacks. The damage is particularly severe when compared to the original image, especially after crop, translation, and rotation attacks. In these cases, not only are the pixel positions altered, but also a portion of the image information is lost. Despite these conditions, the watermark image remains clear and effective, containing all the original image information. This indicates that our proposed algorithm possesses strong resilience against attacks. Overall, the proposed algorithm demonstrates good robustness.

4.5. **Comparative analysis.** In designing image watermarks for solving copyright issues, robustness is the most important feature of the algorithm. To further verify that our algorithm has stronger robustness, we conducted a comparative analysis with other advanced algorithms, including Wang and Zhao [12], Sharma et al. [14], and Singh et al. [17], and the results are shown in Table 5.

Table 5. Comparison of NC values of different algorithms for watermark extraction

Attack type	Attack strength	**Our**	Singh et al. [17]	Wang and Zhao [12]	Sharma et al. [14]
Gaussian filter	$[3, 3]$	0.9999	0.9640	0.9878	0.9959
Median filter	$[3, 3]$	0.9984	0.9880	0.9971	0.9955
Gaussian noise	0.01	0.9999	0.9360	–	0.9914
Salt-and-pepper noise	0.01	1.0000	0.9710	0.9868	0.9916
Speckle noise	0.01	0.9999	0.9720	0.9955	0.9899
Sharpening	0.8	0.9999	–	0.9891	0.9914
JPEG	40	0.9995	–	–	0.9960
Scaling	0.25	0.9994	–	0.9938	0.9948
Rotation	45°	0.9997	0.9840	0.3928	–
Cropping	256×256	0.9998	0.9160	–	0.9648

According to Table 5, it can be seen that the NC values of the watermark extracted by the proposed algorithm are better than those of Wang and Zhao [12] and Sharma et al. [14] algorithms, which use a single band for embedding, under various attacks. The NC value of the proposed algorithm is 0.6 higher than that of Wang and Zhao [12] under rotation attack. Compared with Singh et al. [17], which also uses a block-based approach for watermark embedding, the proposed algorithm shows significant improvement in resisting rotation, shearing, and noise attacks. Therefore, compared with other algorithms, the proposed algorithm has demonstrated excellent resistance to various attacks.

Table 6 presents a comparison of the BER values obtained by extracting the watermark using the proposed algorithm and those obtained by Islam et al. [3], Wang and Zhao [12], and Ma et al. [18] algorithms under the same attacks.

Table 6. Comparison of the BER of different algorithms

Attack type	Attack strength	**Our**	Islam et al. [3]	Wang and Zhao [12]	Ma et al. [18]
Gaussian filter	[3, 3]	0.0006	0.0043	0.0087	0.0039
Median filter	[3, 3]	0.0026	0.1477	0.0097	0.0104
Gaussian noise	0.001	0.0000	–	0.0001	0.0151
Salt-and-pepper noise	0.01	0.0000	0.0778	0.0093	0.0191
Speckle noise	0.01	0.0000	0.0548	0.0131	0.0156
JPEG	50	0.0001	0.0180	–	0.0052
Scaling	0.25	0.0002	–	0.0068	0.0658
Rotation	45°	0.0000	–	0.7780	0.0216

As shown in Table 6, the BER values for watermark extraction using our algorithm are lower than those of other algorithms under different attacks, indicating a high accuracy of watermark extraction and good robustness of our algorithm.

5. **Conclusion.** This paper proposes an adaptive embedding location watermarking algorithm for copyright protection. The image is subjected to discrete wavelet transform and non-subsampled contourlet transform, and the four directional components obtained are processed in non-overlapping 8×8 blocks based on the redundancy characteristics of frequency domain transforms. Based on the watermark size and sub-block information, the sub-blocks are reconstructed to obtain the watermark embedding location, making the algorithm robust and capable of embedding watermark images of various sizes, thus improving the algorithm's flexibility. The watermark image is encrypted using an improved Arnold scrambling method to enhance the algorithm's security.

In the copyright-oriented adaptive watermarking algorithm proposed in this paper, due to the use of block-based reconstruction to obtain the embedding positions for watermarking, the algorithm's performance is slightly compromised when facing high-intensity filtering attacks. Therefore, the future direction is to investigate how to resist the impact of block-based manipulation without compromising watermarking performance.

REFERENCES

[1] N. Zermi, A. Khaldi, R. Kafi et al., A DWT-SVD based robust digital watermarking for medical image security, *Forensic Science International*, vol.320, 110691, 2021.

[2] R. K. Senapati, S. Srivastava and P. Mankar, RST invariant blind image watermarking schemes based on discrete Tchebichef transform and singular value decomposition, *Optik – International Journal for Light and Electron Optics*, vol.45, no.4, pp.3331-3353, 2020.

[3] M. Islam, A. Roy and R. H. Laskar, SVM-based robust image watermarking technique in LWT domain using different sub-bands, *Neural Computing & Applications*, vol.32, pp.1379-1403, 2020.

[4] H.-Y. Fan, Z.-M. Lu and Y. Liu, The digital image watermarking scheme using low frequency construction and histogram, *International Journal of Innovative Computing, Information and Control*, vol.16, no.1, pp.367-384, 2020.

[5] D. K. Mahto and A. K. Singh, A survey of color image watermarking: State-of-the-art and research directions, *Computers & Electrical Engineering*, vol.93, no.3, 107255, 2021.

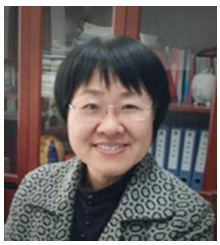
[6] R. Thanki, S. Borra, V. Dwivedi et al., An efficient medical image watermarking scheme based on FDCuT-DCT, *Engineering Science and Technology, an International Journal*, vol.20, no.4, pp.1366-1379, 2017.

[7] R. Thanki, A. Kothari and S. Borra, Hybrid, blind and robust image watermarking: RDWT-NSCT based secure approach for telemedicine applications, *Multimedia Tools and Applications*, vol.80, no.18, pp.27593-27613, 2021.

[8] K. L. Hua, B. R. Dai, K. Srinivasan et al., A hybrid NSCT domain image watermarking scheme, *EURASIP Journal on Image & Video Processing*, vol.2017, no.1, pp.1-17, 2017.
[9] I. A. Ansari and M. Pant, Multipurpose image watermarking in the domain of DWT based on SVD and ABC, *Pattern Recognition Letters*, vol.94, pp.228-236, 2017.
[10] S. P. Vaidya, Fingerprint-based robust medical image watermarking in hybrid transform, *The Visual Computer*, pp.1-16, 2022.
[11] H. Gao and Q. Chen, A robust and secure image watermarking scheme using SURF and improved Artificial Bee Colony algorithm in DWT domain, *Optik – International Journal for Light and Electron Optics*, vol.242, 166954, 2021.
[12] B. Wang and P. Zhao, An adaptive image watermarking method combining SVD and Wang-Landau sampling in DWT domain, *Mathematics*, vol.8, no.5, 691, 2020.
[13] X.-Q. Zhang and Z.-M. Lu, Discrete Fourier transform peak detection based robust audio watermarking against time scale modulation and pitch shifting, *International Journal of Innovative Computing, Information and Control*, vol.16, no.6, pp.1973-1985, 2020.
[14] S. Sharma, H. Sharma and J. B. Sharma, An adaptive color image watermarking using RDWT-SVD and artificial bee colony based quality metric strength factor optimization, *Applied Soft Computing*, vol.84, 105696, 2019.
[15] Q. Zheng, Y. Chen and C. Lin, Contourlet watermarking algorithm based on geometric correction optimization, *Journal of Optoelectronics Laser*, vol.33, no.3, pp.330-336, 2022.
[16] T. Liu and T. Tan, An SVD-based water marking scheme for protecting rightful ownership, *IEEE Transactions on Multimedia*, vol.4, no.1, pp.121-128, 2002.
[17] P. Singh, A. K. Pradhan and S. Chandra, False-Positive-Free and geometric robust digital image watermarking method based on IWT-DCT-SVD, in *Advances in Communication and Computational Technology. ICACCT 2019. Lecture Notes in Electrical Engineering*, G. S. Hura, A. K. Singh and L. Siong Hoe (eds.), Singapore, Springer, 2019.
[18] B. Ma, L. Chang, C. Wang et al., Robust image watermarking using invariant accurate polar harmonic Fourier moments and chaotic mapping, *Signal Processing*, vol.172, 107544, 2020.

Author Biography

Wenjie Meng received her B.Sc. degree in Communication Engineering and M.Sc. degree in Computer Application Technology from China University of Petroleum (East China), China, in 2004 and 2007, respectively. Currently she works in Library Information Technology Department at China University of Petroleum (East China). Her research interests include image processing, information resource construction, and big data applications.



Qiumei Zheng is Professor of College of Computer Science and Technology at China University of Petroleum (East China). She received the B.S. degree from East China Petroleum Institute, Dongying, China, in 1986. She received the M.E. degree from China University of Petroleum (East China), Dongying, China, in 1999. Her research interests lie in watermarking, and image processing.

Fenghua Wang received the Ph.D. degree from Xi'an Jiaotong University, Xi'an, China, in 2009. Currently he works in College of Computer Science and Technology at China University of Petroleum (East China). His research interests include digital watermarking, pattern recognition, and computer vision.