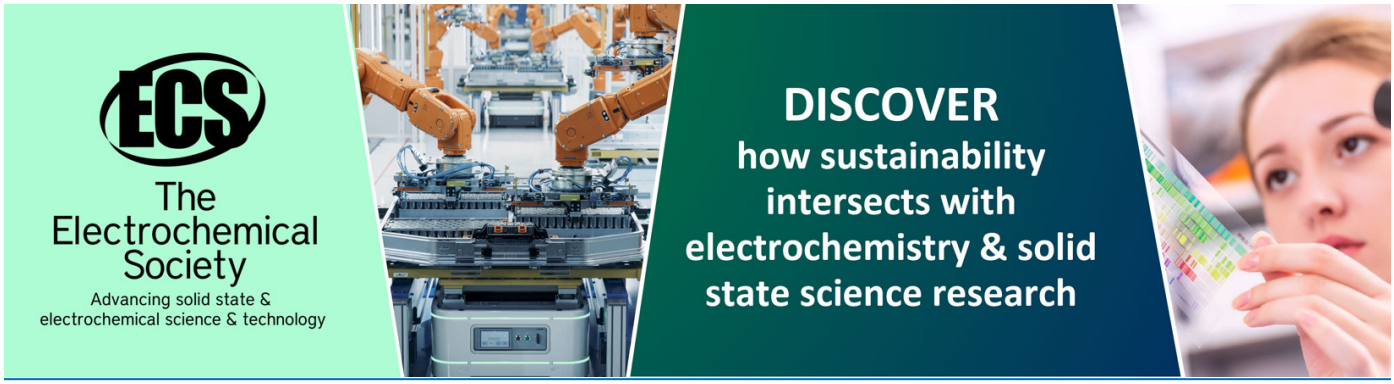
A Blind Watermarking Algorithm for Digital Image Based on DWT



A Blind Watermarking Algorithm for Digital Image Based on DWT

Linglong Tan[1, *], Yihong He[2], Fengzhi Wu[3] and Dong Zhang[4]

[1]Electronic communication engineering college, Anhui Xinhua University, Hefei, 230088, China
[2]School of Computers, Guangdong University of Technology, Guangzhou, 510006, China
[3]Department of Mechanical Engineering, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, US
[4]School of land science and technology, China University of Geosciences, Beijing, 100089, China

[*]E-mail: tanlinglong@axhu.edu.cn

Abstract. In order to improve the robustness of digital image watermarking algorithms, the digital image blind watermarking algorithm proposed in this paper embeds watermark information in a reasonable position. First, scramble the watermark information and embed the random signal into the low-frequency domain of the image. On the one hand, it can effectively prevent attacks on the watermark system and enhance the security of the system, disperse as much as possible. In the watermark embedding process, a method based on the wavelet transform domain is used. The original image is not required to participate in the watermark extraction process, and the blind watermark function is implemented. In order to verify the effectiveness of the algorithm, the watermarked image is subjected to filtering, scaling, noise, cropping and rotation attacks, and the peak signal-to-noise ratio and normalized correlation coefficient are used to quantitatively evaluate the watermarked image. Experimental results show that the algorithm can resist a variety of attacks, and has good imperceptibility and robustness.

1. Introduction

At present, there are many publicly available digital watermarking algorithms, which are generally divided into two types: spatial domain and transform domain. Among them, the spatial domain watermarking algorithm adds a watermark directly to the data. This watermarking technology can embed a large amount of information, but its resistance to attack is poor. In the transform domain watermarking algorithm, the watermark information is scattered over the entire frequency spectrum, which cannot be recovered by ordinary filtering methods, and has strong resistance to attack.DWT is a multi-resolution analysis method of time-scale (time-frequency domain) signals. It has the ability to characterize signals in the time and frequency domains. The advantage of the DWT watermarking algorithm is that the watermark detection is performed according to the subband hierarchically expanded watermark sequence. If the watermark sequence that is detected first meets the requirements of the similar function of the watermark, the detection is terminated. Otherwise, continue to find the

next subband extended watermark sequence until a peak occurs in the similarity function or all subband search ends[1,2].

2. Wavelet decomposition and reconstruction

The image is a two-dimensional signal. The wavelet decomposition of the image can be regarded as one-dimensional wavelet transform of the rows and columns of the image. The digital image is divided into 4 frequency bands after wavelet decomposition, namely horizontal direction, vertical direction, diagonal direction and low-frequency part. Among them, the low-frequency part can be further divided into more detailed high-frequency data. The image energy is mainly concentrated in the low-frequency part, which is an approximate sub-picture of the original image, which has strong anti-interference ability and good stability. The other three subbands represent the edge details of the original image in the horizontal, vertical, and diagonal parts. The characteristic of multi-resolution image decomposition based on wavelet transform is that the decomposed image has good spatial direction selectivity, which is in good agreement with human visual characteristics[3].

Let the original image be $f(x,y)$ and decompose it in the first layer to get the formula 1.

$$\begin{aligned} LL_1(m,n) &=< f(x,y), \psi^0(x-2m, y-2n) > \\ LH_1(m,n) &=< f(x,y), \psi^1(x-2m, y-2n) > \\ HL_1(m,n) &=< f(x,y), \psi^2(x-2m, y-2n) > \\ HH_1(m,n) &=< f(x,y), \psi^3(x-2m, y-2n) > \end{aligned} \tag{1}$$

The second-order decomposition is performed on the LL_1 subband, and the decomposition process is similar to formula 1.

If the wavelet decomposition is realized by a filter, the original image $f(x,y)$ is filtered by a low-pass filter and a high-pass filter along the rows and columns, respectively, and the filtering result of the even-numbered subscript is left. Wavelet reconstruction and wavelet decomposition have the opposite process. In the extracted rows and columns, a column or a row of zero elements is inserted into two adjacent columns or two adjacent rows,as shown in Figure 1.Wavelet reconstruction and wavelet decomposition are basically the opposite process, except that the decomposition part is two-to-one extraction rows and columns, and the reconstruction part is to insert a column (or row) of zero elements into two adjacent columns (or rows).

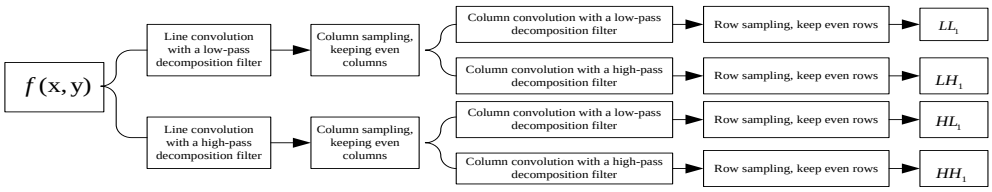


Figure 1. Schematic diagram of wavelet decomposition data flow

3. Algorithm Design

The blind watermarking algorithm of binary image based on wavelet transform proposed in this paper first scrambles the watermarked image and turns the watermark into a seemingly chaotic signal, thereby improving the anti-attack ability of the watermarking system. Secondly, a method based on wavelet transform domain is adopted in the watermark embedding process to ensure the imperceptibility and robustness of the watermark. Third, the original image is not needed in the watermark extraction process, and the blind watermark function is implemented.

3.1. Arnold Scrambling Algorithm

To ensure the security of the watermark, the watermark needs to be encrypted before being embedded. Scrambling is a simple and commonly used encryption method. The scrambling process is to use certain rules to scramble the position or color of pixels in the image, and turn the image into a chaotic,

unrecognizable image. By scrambling the correlation between watermarkable image pixels and dispersing the distribution of error bits, the robustness of the watermarking system is improved[4].Among the many scrambling algorithms, the Arnold scrambling algorithm is simple and the scrambling effect is significant. Arnold scrambling replaces the pixel information of point (x, y) in the image with point (x', y'), and performs N times of Arnold substitution on a digital image of order N, the disorder results is formula 2.

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}^n \begin{bmatrix} x \\ y \end{bmatrix} \bmod N, \quad x, y \in \{0, 1, \ldots, N-1\} \tag{2}$$

Use formula 2 to scramble the image to get a scrambled image. An Arnold transform is equivalent to scrambling the image. In general, multiple iterations are required to obtain a satisfactory result. Arnold scrambling is used to transform the original meaningful image into a meaningless image similar to white noise to achieve the initial hiding of information. Using the number of scrambling as the key of the watermark system can also increase the security and confidentiality of the system. Because the pixels of a digital image are limited, when the image is repeatedly Arnold transformed, the original image will eventually be restored, that is, Arnold has periodicity. For any given $N > 2$, the period m is the minimum natural number n for which formula (3) is established.

$$\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}^n (\bmod \quad N) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{3}$$

3.2. Embedding and Extraction of Watermark

The low-frequency part of the wavelet transform concentrates the main energy of the image and is the most important part of the visual effect. Embedding the watermark in this part can easily cause image distortion. However, from the perspective of robustness, embedding the watermark in the most important areas of vision can improve the anti-attack ability of the image. In this paper, after performing a two-level wavelet transform on the original image, we choose to approximate the subgraph coefficient $cA2$, modify it, and embed the watermark information. Then, two-level wavelet reconstruction and binarization are performed to obtain a binary image containing a watermark, and the watermark is embedded. The original image is subjected to two-level wavelet decomposition to obtain detailed sub-pictures at different resolution levels. A low-frequency sub-picture coefficient $cA2'$ is selected. The watermark image matrix is formed by each pixel of the binary watermark image. The scrambled binary value is obtained by the Arnold function. Watermark information W. The low-frequency subgraph coefficient $cA2'$ is used to modify the approximation subgraph coefficient, and the watermark image after Arnold scrambling is embedded into the approximation subgraph coefficient cA2 by using formula (4).

$$cA2' = cA2 + \alpha W \tag{4}$$

Among them, α is the watermark embedding strength. The Haar wavelet reconstruction is performed on the sub-embedded approximation sub-image. The grayscale image after embedding the watermark is binarized to obtain a binary image containing the watermark. In this paper, a blind watermarking algorithm is used. The original image is not required to participate in the extraction process. First, the binary image containing the watermark is subjected to the second-order wavelet decomposition to obtain the detailed sub-pictures and approximation sub-pictures at different resolution levels. Then from the logical table generated when embedding the watermark and the approximate subgraph coefficients containing the watermark, the embedded scrambled watermark is obtained. Then use the Arnold function to iteratively complete the restoration of the watermark image[5,6].

4. Algorithm performance evaluation

The evaluation of the impact of digital watermarks is mainly evaluated from two aspects: the robustness of the watermark and the distortion caused by the embedded watermark on the image.

Because the image is distorted when it is embedded in watermarks or subjected to various attacks, there is a certain difference between the extracted watermark and the original watermark. In order to evaluate the impact of digital watermarking, this paper selects the peak signal-to-noise ratio (PSNR) to evaluate the deviation error between the embedded image and the original image. Generally speaking, the larger the peak signal-to-noise ratio value, the better the image quality is maintained.The normalized correlation coefficient (NC) is selected to evaluate the similarity between the extracted watermark and the original watermark signal. For robust watermarks, the larger the correlation coefficient, the better, and for the vulnerable watermark, the smaller the correlation coefficient, the better.

$$PSNR = 10 \times \lg \frac{mn \times \max(I_{i,j}^2)}{\sum (I_{i,j} - \hat{I}_{i,j})^2} \tag{5}$$

$$NC = \frac{\sum W_i \hat{W}}{\sqrt{\sum W_i^2} \sqrt{\sum \hat{W}_i^2}} \tag{6}$$

5. Experimental verification

In order to verify the effectiveness of the algorithm, this paper uses the color image of 512×512 as the original image, as shown in Figure 2, and the watermark image is a binary image of 64×64, as shown in Figure 3.The coefficient matrix after the second-order wavelet decomposition of the original image is shown in Figure 4. The low-frequency coefficient matrix in the upper left corner concentrates the main capabilities of the original image and is an approximation subgraph of the original image. Perform 23 Arnold scrambling transforms on the original watermark image to obtain an irregularly garbled image, as shown in Figure 5. The scrambled watermark image is embedded in the secondary wavelet coefficients, and the watermarked image is obtained by inverse wavelet transform. As shown in Figure 6, the PSNR value is calculated to be 40.7406, which indicates that the image quality after embedding the watermark is maintained well.

Figure 2. Original image

Figure 3. Watermark image

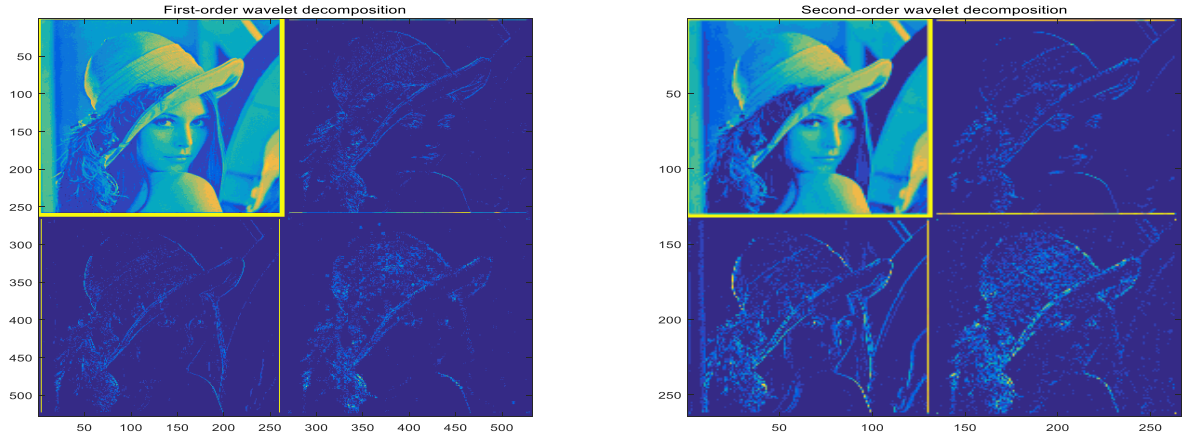


Figure 4. Second-level wavelet decomposition of the original image

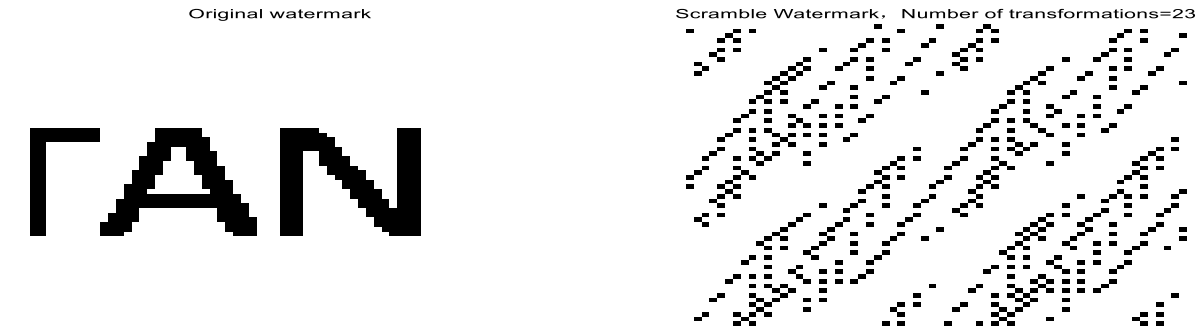


Figure 5. Arnold scrambled watermark image

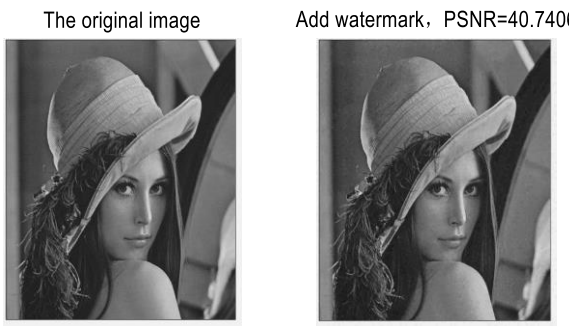


Figure 6. Original image after adding watermark

Figure 7. Influence of noise attack on wavelet watermark

In order to verify the robustness of the watermarking algorithm, the anti-attack ability of the watermarked image under the following attacks is detected below. Manic attack: Add salt and pepper noise to the image containing the watermark. The watermark image and detection result after the manic addition are shown in Figure 7; Filter attack: 3×3 smooth filtering is performed on the image containing the watermark. The filtered watermark image and detection result are shown in Figure 8; Cropping attack: After cutting the upper left part of the image containing the watermark, Figure 9 shows the cropped watermark image and the corresponding watermark detection results; Scaling attack: After reducing the watermarked image by 0.5 times and then by 2 times, the attacked watermark image and watermark detection results are shown in Figure 10.Rotating attack, rotate the image containing the watermark by 45 degrees and then extract the watermark. The result is shown in Figure 11.The above experimental results show that when the digital image watermarking algorithm based on wavelet transform proposed in this paper is subjected to some simple and geometric attacks, the interference of various attacks on the watermark recovery is obvious, but the algorithm can still detect the embedded watermark more reliably. It shows that this algorithm can basically guarantee the imperceptibility, robustness and security of the watermark, and implements the blind detection function.

6. Summary

This paper proposes a digital image blind watermarking algorithm in the wavelet domain. Using the masking ability of the human visual system for brightness and texture, the scrambled watermark is embedded into the low-frequency part of the image to ensure the adaptive ability of the embedded watermark. In order to meet people's requirements for visual perception of image quality, the robustness and security of watermarking algorithms are greatly improved. Perform some simple and geometric attack experiments on images containing digital watermarks, and analyze the degree of watermark impact from the perspective of vision, peak signal-to-noise ratio, and normalized correlation coefficient. The experimental results show that the image quality of the proposed

watermark algorithm decreases after being attacked, but it can still extract identifiable watermark images from the image.

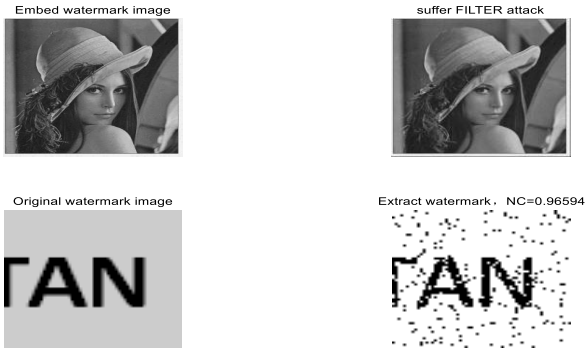


Figure 8. Impact of Filter Attacks on Wavelet Watermarking

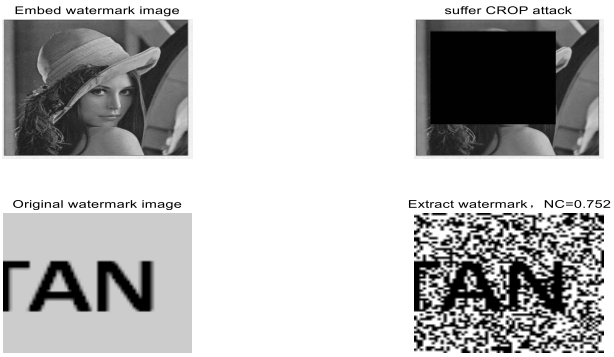


Figure 9. Effect of cropping attack on watermark image

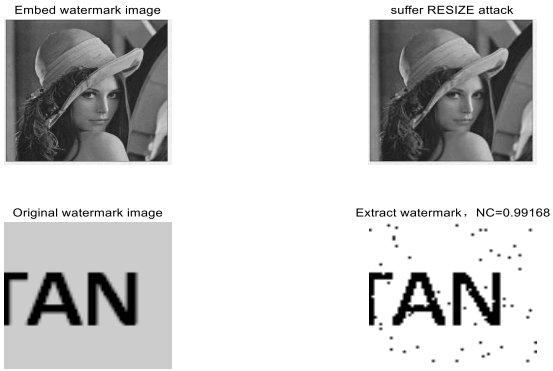


Figure 10. Impact of scaling attacks on watermarked images

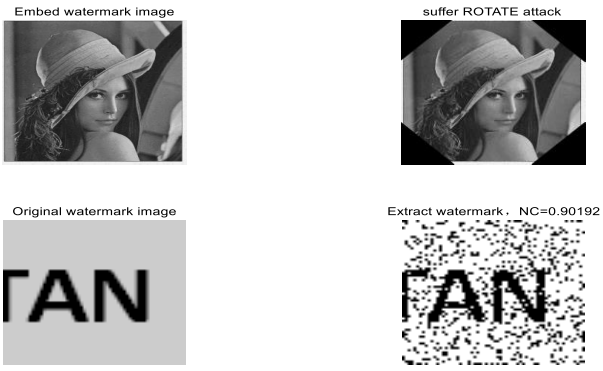


Figure 11. The effect of rotation attack on the watermark image

Acknowledgments
This work was supported by the Scientific Research Project of Anhui Natural Science Research Project No. KJ2017A628, the Quality Engineering Project No.2015zy073 and the backbone Teacher Project No.2018xgg04.

References

[1] Hung-Jui Ko, Cheng-Ta Huang, Gwoboa Horng, Shiuh-Jeng WANG. Robust and blind image watermarking in DCT domain using inter-block coefficient correlation[J]. Information Sciences,2019.
[2] Swaraja K, Meenakshi K, Padmavathi Kora. An optimized blind dual medical image watermarking framework for tamper localization and content authentication in secured telemedicine[J]. Biomedical Signal Processing and Control,2020,55.
[3] Lei Chen, Jiying Zhao. Quality evaluation of DIBR 3D images based on blind watermarking[J]. Multimedia Systems,2019,25(3).
[4] Aniruddha Kanhe, Aghila Gnanasekaran. A Blind Audio Watermarking Scheme Employing DCT – HT – SD Technique[J]. Circuits, Systems, and Signal Processing,2019,38(8).
[5] Yung-Yao Chen, Kuan-Yu Chi. Cloud image watermarking: high quality data hiding and blind decoding scheme based on block truncation coding[J]. Multimedia Systems,2019,25(5).
[6] Jie Wu, Xiaohu Ma. An improved blind watermarking method based on SWT and LU decomposition[P]. International Conference on Digital Image Processing, 2019.