Watermarking method based on discrete wavelet transform

Bing He[a], Xinru Dai[b], Kuai Yu[a], Ye Ma[a], Yuanyuan Bai[b], Ying Wen[b,c*]
[a] State Grid Shanghai Extra High Voltage Company, Shanghai 200063, China; [b] School of Communication and Electronic Engineering, East China Normal University, Shanghai 200241, China; [c] Avcon Information Technology Co., Ltd., Shanghai, China

ABSTRACT

Improving the invisibility and robustness of watermarking, increasing the embedding capacity of watermarking and reducing the complexity of watermarking algorithms are becoming hot topics and difficulties in the research of watermarking algorithms nowadays. In this paper, we propose a digital watermarking technique based on discrete wavelet transform for the protection of author's copyright. First, the watermark is pre-processed, specifically, then the Arnold transform is used for encryption to ensure the security of watermark. Then the wavelet coefficients are obtained by discrete wavelet transform of the original image. Finally, the watermark information is embedded into the wavelet coefficients of the image. The watermark embedding experiments indicate that the algorithm is reversible and the invisibility of watermark is excellent. The watermark extraction experiments demonstrate that our method has strong robustness to against various external attacks.

Keywords: UAV, image watermarking, discrete cosine transform, wavelet transform

1. INTRODUCTION

By the end of 2020, the transmission operation and inspection centre of the State Grid Corporation of Shanghai have stored a total of 350,000 inspection photos. There is a technical blind spot in how to cooperate with the relevant image intelligence recognition units to ensure that the grid company's image data is not illegally transmitted or used. Since the invisibility and robustness of watermarking cannot be achieved simultaneously, balancing the invisibility and robustness of watermarking algorithms while minimizing the complexity of the algorithm is the main difficulty of watermarking algorithms today. Reena et al.[1] proposed a reversible watermarking algorithm based on adaptive edge sensing interpolation (AESI). Liu et al.[2] proposed a watermarking technique based on discrete cosine transform (DCT)[3], discrete wavelet transform (DWT)[4] and Canny edge detection operator to improve the robustness. DWT-FRFT watermarking algorithm[5] solved the problem of non-smooth signal with low algorithm complexity but not high robustness in the face of noise attack. Saini[6] used lifting wavelet transform (LWT) instead of DWT[7]. Narima et al.[8] used DWT and singular value decomposition, wavelet transform for retinal images and singular value decomposition for their LL sub-bands. Eduardo et al.[9] proposed a watermarking technique based on an improved seam carving technique to provide robustness against removal attacks. Yong et al.[10] proposed a robust blind watermarking scheme based on quaternion decomposition. Meanwhile, with the continuous development of deep learning, some scholars have applied neural networks to image watermarking techniques. Makram et al.[11] proposed a full convolutional neural network based denoising attack, which effectively preserves the detailed structure of the original image while removing noise and improves the robustness.

In this paper, a watermarking method based on discrete wavelet transform is designed to address the shortcomings of the existing technology. First, the watermark is disordered using the Arnold[12] transform, and the wavelet coefficients are obtained from the second-stage discrete wavelet transform of the image. Then the watermark image is embedded in the low-frequency part LL2 of the wavelet coefficients using the state coding method. The random number in the discrete wavelet transform and the disorder count in the disorder process are stored as two keys, and then the watermark image is obtained by reconstructing the second-level wavelet with the watermark information embedded in it. The watermark is extracted by inverse operation. After obtaining the watermark information from the low-frequency coefficients according to the key, the extracted coefficients containing the watermark information are inverse-Arnold transformed to extract the watermark. The proposed method improves the invisibility, robustness and security of the watermark.

* ywen@cs.ecnu.edu.cn

Third International Conference on Computer Science and Communication Technology (ICCSCT 2022)
edited by Yingfa Lu, Changbo Cheng, Proc. of SPIE Vol. 12506, 1250635
 · 0277-786X · doi: 10.1117/12.2661826

2. METHOD

The main process of the proposed method consists of three steps: watermark image and original image pre-processing, embedding of watermark and extracting of Watermark. Overall structure of the proposed method is shown in Figure 1.

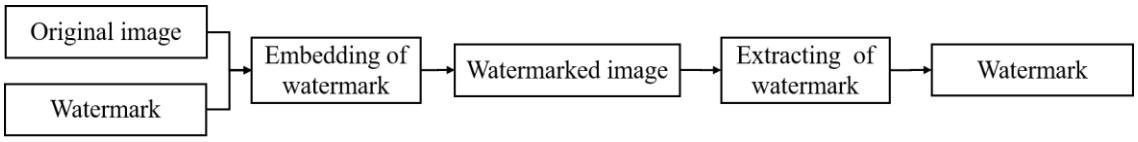


Figure 1. An overview of the proposed method.

2.1 Pre-processing

2.1.1 Pre-processing of the Watermark. In our proposed method, the watermark image is transformed into a binary image firstly. Then the Arnold transform is applied to the processed watermark to encrypt it. Since the Arnold transform is periodic, the original image can be reproduced by continuing to use the Arnold transform. The formula for the two-dimensional Arnold transformation of a digital watermark image:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & b \\ a & ab+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod(N) \tag{1}$$

where x_n and y_n are the pixel positions in the image before the transformation, x_{n+1} and y_{n+1} are the pixel positions after the transformation. *a*, *b* are the transformation parameters, *n* is the number of current transformations.

2.1.2 Pre-processing of the original image. Since digital images are discrete signals, the proposed method uses the Haar[13] wavelet transform. Haar wavelet transform has two significant functions: scaling function $\varphi(x)$ (the father wavelet) and wavelet function (the mother wavelet). V_j is the space spanned by the following equation:

$$\sum_{k \in Z} a_k \varphi(2^j x - k), a_k \in R \tag{2}$$

Since each V space can be decomposed into a V space and a W space of a lower order. Therefore, any scaling function f_j in V_j can be decomposed into the following summation:

$$f_j = w_{j-1} + w_{j-2} + \cdots + w_0 + f_0 \tag{3}$$

The above wavelet decomposition is applied to the original signal. The wavelet transform result of the first level will divide the image into four parts: LL, LH, HL, HH. In this paper, the original image is processed by a two-level wavelet transform, which makes the information stored in the low-frequency part relatively more important. The structure of the two-level wavelet decomposition is shown in Figure 2.

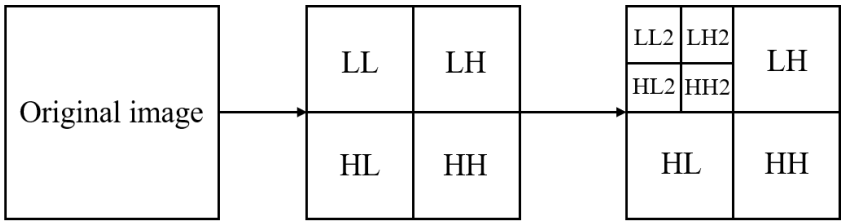


Figure 2. Second level wavelet decomposition.

2.2 Embedding of the watermark

The wavelet coefficients are obtained by applying a second level wavelet transform to a RGB component of the original image. The watermark image after Arnold transform is embedded in the low-frequency part LL2 of the wavelet coefficients using the state encoding method. Moreover, the disorder count is then stored as the key to recover the watermark image:

$$z = \mathrm{mod}(LL2, m) \tag{4}$$

$$LL_2' = \begin{cases} LL2 + m/4 - z, W = 0 \,\&\, z < 3m/4 \\ LL2 + 5m/4 - z, W = 0 \,\&\, z \geq 3m/4 \\ LL2 - m/4 - z, W = 1 \,\&\, z < m/4 \\ LL2 + 3m/4 - z, W = 1 \,\&\, z \geq m/4 \end{cases} \tag{5}$$

2.3 Extracting of the watermark

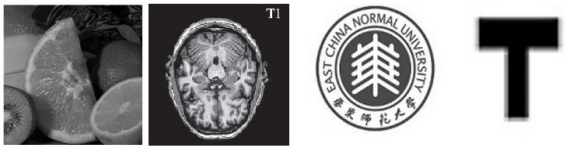
The proposed watermark extraction process is based on the watermark embedding algorithm, which extracts the watermark information from the embedded image. Firstly, the image with the watermark embedded is input along with two keys: the disorder count and the random number seed. Then a second level wavelet transform is applied to one of the RGB components of the watermarked image. The keys are used to extract the coefficients to which the watermark information has been added. Finally, the extracted coefficients containing the watermark information are inverse-Arnold transformed by the key to extract the watermark:

$$z = \mathrm{mod}(LL2', m) \tag{6}$$

$$W' = \begin{cases} 0, z < m/2 \\ 1, z \geq m/2 \end{cases} \tag{7}$$

3. EXPERIMENTS

Two original images and two watermarks were used for the experiments. The fruit image and the brain image were used for the original image, and the ECNU image and the T image were used for the watermark image, as shown in Figure 3.



(a) fruit (b) brain (c) ECNU (d) T

Figure 3. Original image and watermark.

3.1 Experimental simulation of basic watermarking algorithms

In this experiment, we test the performance of various watermark embedding algorithms. The performance of watermarked images is measured by invisibility and robustness. The invisibility is quantified by the Peak Signal to Noise Ratio (PSNR). Robustness refers to the quality of the watermark that can be extracted after the image has resisted various external attacks. The robustness is generally evaluated quantitatively by using the normalization coefficient (NC).

Our paper compares the least significant bit (LSB) watermarking algorithm, the DCT watermarking algorithm, and the DWT watermarking algorithm. The PSNR results of the watermarked images by each algorithm are shown in Table 1. Comparing the three sets of experimental results, the LSB algorithm achieves the highest peak signal-to-noise ratio of the watermarked images. The results of the robustness experiments are shown in Tables 2-4. In terms of performance against external attacks, the DWT algorithm achieves the highest average NC, indicating that it can resist many external attacks with strong robustness. The LSB algorithm has the lowest average NC. Therefore, a large amount of watermark information will be lost and the watermark information can no longer be extracted. In addition, the DCT algorithm has

good invisibility and can extract the original watermark effectively, but the computational complexity of the discrete cosine transform is relatively high. In general, DWT is the most robust and fastest algorithm.

Table 1. Comparison of watermark invisibility.

	LSB	DCT	DWT
PSNR of watermarked image	79.1617	45.3987	42.6746

Table 2. Normalization coefficient table of LSB.

	No attacks	White noise	Pepper noise	Gaussian noise	Clipping
NC	1	0.61339	0.98218	0.61781	0.99088
	Rotation	Gaussian filtering	Median filtering	Scaling	Compression
NC	0.66051	0.60559	0.79217	0.83414	0.89510

Table 3. Normalization coefficient table of DCT.

	No attacks	White noise	Pepper noise	Gaussian noise	Clipping
NC	1	0.80297	0.81417	0.80554	0.98802
	Rotation	Gaussian filtering	Median filtering	Scaling	Compression
NC	0.66051	0.60559	0.79217	0.98948	0.60353

Table 4. Normalization coefficient table of DWT.

	No attacks	White noise	Pepper noise	Gaussian noise	Clipping
NC	0.98471	0.91368	0.78982	0.84668	0.98579
	Rotation	Gaussian filtering	Median filtering	Scaling	Compression
NC	0.94718	0.95258	0.98604	0.98433	0.98383

3.2 Experimental simulation of the proposed watermarking method

Table 5 and Figure 4 show the experimental results and watermark extraction results of the discrete wavelet transform based on the Arnold transform under various external attacks. It can be seen that the DWT algorithm based on Arnold transform proposed in this paper has a much better performance in embedding and extracting watermarks compared with the previous methods, and can effectively against a variety of external attacks. Meanwhile, in the field of security, the proposed discrete wavelet transform with Arnold transform can protect the watermark preferably. Figure 4 shows that the quality of the watermark extracted from the images embedded by this algorithm after various attacks is high.

Table 5. Normalization coefficient table of the proposed method.

	No attacks	White noise	Pepper noise	Gaussian noise	Clipping
NC	1	0.92441	0.79817	0.85477	0.99729
	Rotation	Gaussian filtering	Median filtering	Scaling	Compression
NC	0.96143	0.97187	0.99971	1	1

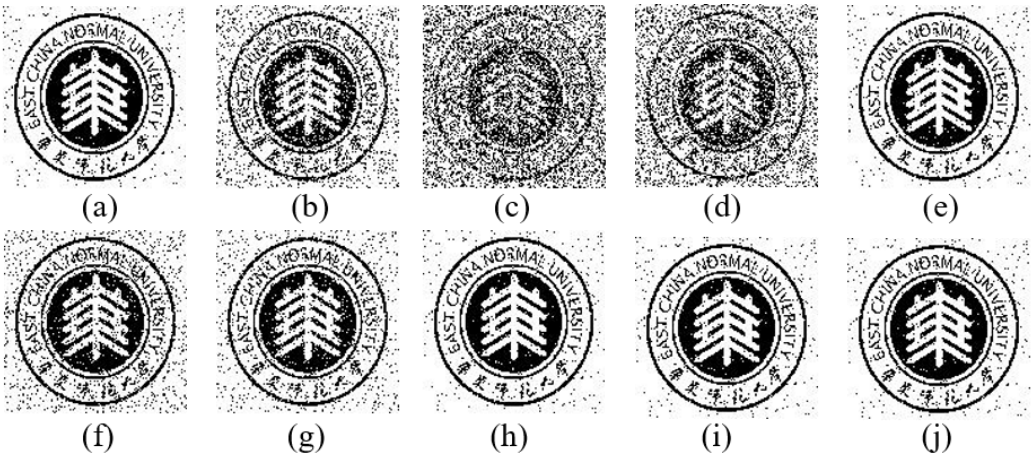


Figure 4. Experimental results of the proposed method for watermarking against external attacks: (a) The direct watermark extraction; (b)-(j) The extraction after adding white noise, pepper noise, gaussian noise, clipping, rotation, gaussian filtering, median filtering, scaling and compression respectively.

4. CONCLUSION

In this paper, an improved image watermarking algorithm is proposed, which greatly improves the invisibility, robustness and security of the watermarking algorithm. The experimental watermarking algorithm is based on the discrete wavelet transform, which greatly reduces the complexity of the algorithm and increases the running speed.

The proposed watermark embedding method transforms the watermark image by using the Arnold method. The low frequency part of the wavelet coefficients is selected to embed the Arnold transformed watermark information. The coefficients embed with the watermark information are reconstructed with a second level wavelet to obtain a watermark image. Then a second wavelet transform is applied to the RGB components of the embedded image. The coefficients with the watermark information are extracted from the low frequency coefficients according to the random number seed. Finally, the extracted coefficients containing watermark information are inverse-Arnold transformed by the disorder count to extract the watermark.

ACKNOWLEDGMENTS

This work was supported in part by Shanghai Science and Technology Project (21XD1430600); Shanghai Municipal Science and Technology Committee of Shanghai Outstanding Academic Leaders Plan (21XD1430600); Fundamental Research Funds for the Central Universities.

REFERENCES

[1] Reena, T. and Sucharitha, M., “Reversible watermarking using adaptive edge sensing interpolation,” Materials Today: Proceedings, 11(27), 55-62(2020).
[2] Liu, Y., Xu, W. and Zhu, T., “Color image watermarking algorithm based on lifting wavelet transform and discrete cosine transform,” Science Technology and Engineering, 20(10), 4056-4060(2020).
[3] Sun, S. and Wang, Q., “Digital watermarking embedding algorithm based on discrete cosine transform coefficient decomposition,” Journal of Harbin Institute of Technology, 33(5), 6(2001).
[4] Zhang, P. and Li, H., “A harmonic analysis method based on discrete wavelet transform,” Transactions of China Electrotechnical Society, 27(3), 8(2012).
[5] Gong, C., “Digital image watermarking algorithm based on DWT and FRFT,” Modern Computers, 42(29), 55-58(2020).
[6] Saini, M., “LWT based hybrid digital watermarking scheme in YCbCr colour space,” Inter. Conf. on Intelligent Circuits and Systems (ICICS), 320-328(2018).

[7] Rani, A., Bhullar, A. K. and Dangwal, D., "A scheme using discrete wavelet transform," Procedia Computer Science, 70(1), 603-609(2015).
[8] Narima, Z. and Amine, K., "A DWT-SVD based robust digital watermarking for medical image security," Forensic Science International, 110(320), 69-77(2021).
[9] Eduardo, F. and Kevin, R., "Seam carving based visible watermarking robust to removal attacks," Journal of King Saud University–Computer and Information Sciences, 48(26), 253-260(2021).
[10] Yong, C. and Zhi, G. J., "A new structure-preserving quaternion QR decomposition method for color image blind watermarking," Signal Processing, 10(185), 80-88(2021).
[11] Makram, W. and Jean-François, C., "Using deep learning for image watermarking attack," Signal Processing: Image Communication, 11(90), 60-69(2021).
[12] Qi, D., Zou, J. and Han, X., "A new class of scrambling transform and its application in image information concealing," Science in China: Science of Technology, 30(5), 440-235(2000).
[13] Di, J. Z., [Wavelet Analysis Principle], Science Press, (2010).