Optica Applicata, Vol. LI, No. 4, 2021
DOI: 10.37190/oa210411

Digital watermarking algorithm based on 4-level discrete wavelet transform and discrete fractional angular transform

JING-YOU LI[1, 2], CHUN-HUI ZHAO[2*], GUANG-DA ZHANG[1]

[1]School of Computer and Control Engineering, Qiqihar University, Qiqihar 161006, China

[2]School of Information & Communication Engineering, Harbin Engineering University, Harbin 150001, China

[*]Corresponding author: zhaochunhui@hrbeu.edu.cn

Nowadays, there are many watermarking algorithms based on wavelet transform. The simple one is to insert directly the watermark into the wavelet transform coefficients. However, most of the existing watermarking schemes can only resist traditional signal processing attacks, such as image compression, noise and filtering. When the watermarked image is subject to geometric transformations, especially rotation attack, it is hard to detect the watermark successfully. In this paper, a digital watermarking algorithm is proposed based on 4-level discrete wavelet transform and discrete fractional angular transform. To enhance the security of the algorithm, the watermark is scrambled with the simplicity of Arnold transform and chaos-based mix optical bistability model, since the chaos is pseudorandom and sensitive to the initial values. And the watermark is embedded into the medium frequency sub-band of the 1-level wavelet decomposition according to the Harris feature point detection. Simulation results show that the proposed digital watermarking algorithm by combining 4-level discrete wavelet transform with discrete fractional angular transform could resist rotation attack and other common attacks.

Keywords: digital watermarking algorithm, mix optical bistability, Harris feature point detection, discrete wavelet transform, discrete fractional angular transform, singular value decomposition.

1. Introduction

In recent years, with the rapid development of the Internet technology, information has been frequently changed, copied and disseminated over Internet. Over the past century, a large number of reversible data hiding methods have been proposed. LIAO and SHU put forward successively a method to evaluate the complexity of image blocks to reduce average extracted-bit error rate [1], and a quadtree-based value ordering method to improve the embedding performance [2]. LIU *et al*. designed a double image encryption algorithm based on Arnold transform and discrete fractional angular trans-

form (DFAT) to enhance the security [3]. Sui *et al*. proposed a double-image encryption scheme based on the discrete multiple-parameter fractional angular transform and two -coupled logistic map to enhance the security of the cryptosystem [4]. Digital watermarking technology could provide an effective tool or solution for copyright protection. Digital watermarking was widely adopted to hide copyright information in files [5]. The general model of digital watermarking system can be divided into two stages, *i.e*., embedding and detection. In the watermarking embedding stage, the main goal is to find a good compromise between invisibility and robustness. In the detection stage, it is of significant importance to minimize the possibility of false judgment and loss judgment, and then the existence of watermark can be judged by the test results based on statistical principle.

Generally, image watermarking schemes could be grouped into two categories: watermarking schemes in the spatial domain and watermarking schemes in the transform domain [6]. Spatial domain techniques have not been widely used because of their poor robustness against attacks [7]. While in transform domain watermarking schemes, the stronger robustness can be achieved since the watermark data are indirectly modulated by some coefficients in the transform domain [8], such as fractional Fourier transform (FrFT) [9], discrete wavelet transform (DWT) [10], discrete cosine transform (DCT) [11], singular value decomposition (SVD) [12], *etc*.

To achieve higher security, people preferred to adopt the transform domain watermarking methods. Gao *et al*. presented a novel digital image watermarking scheme combined 2D chirp signal with additive and rotational invariant qualities of 2D-FrFT [13]. Since the DWT has the characteristics of multi-resolution decomposition to offer better robustness [14], Chetan and Nirmala suggested an integer wavelet-based watermarking algorithm for embedding the compressed version of the watermark logo to improve the robustness of the watermarking scheme [15]. Subsequently, Hu *et al*. studied a windowed vector modulation scheme incorporating with distortion compensation in the DWT domain to improve the imperceptibility and robustness of blind audio watermarking [16]. However, due to the limited function of the DWT or the DCT, it is difficult to further improve the performance of watermarking schemes. The SVD has been widely applied to image compression and digital watermarking with its strong stability. Ali and Ahn proposed a watermarking scheme based on DWT and SVD [17]. Even if the watermark image is seriously distorted after various attacks, the watermark can still be recognized. Fazli and Moeini put forward a robust digital watermarking method based on DWT, DCT and SVD to resist various attacks [18]. With the development of digital watermarking technology, scrambling technology also has new applications. For example, scrambling techniques including Arnold transform and chaotic sequence are frequently employed to encrypt the watermark [19–22]. A case in point, Singh proposed an enhanced asymmetric optical image encryption scheme in the fractional Hartley transform domain to enhance the security of watermarking algorithm [23]. And Zhou *et al*. investigated a new image encryption algorithm by using a discrete frac-

tional angular transform and Arnold transform in image bit planes to improve security and robustness [24].

A new watermarking scheme based on the 4-level DWT is designed by combining SVD, discrete fractional angular transform and Harris feature point detection. And Arnold transform and the chaos sequence based on the mix optical bistability model are employed to improve the security of the watermarking algorithm. Since the spatial-frequency localization characteristics of the DWT, the high processing speed of discrete fractional angular transform and the stability characteristics of SVD, the imperceptibility and robustness of the watermark can be significantly improved.

The rest of this paper is arranged as follows. In Section 2, some fundamental encryption tools are introduced. In Section 3, the watermark embedding scheme and the extracting one of the proposed digital watermarking algorithm are described in detail. Simulation results and performance analyses are given in Section 4. Finally, the work is summarized in Section 5.

2. Theoretical background

2.1. Discrete fractional angular transform

To a certain extent, discrete fractional angular transform is derived from discrete Fourier transform, which can be expressed by matrix multiplication as [25]:

$$\mathbf{T} = \mathbf{V}\mathbf{D}\mathbf{V}^{\mathrm{T}} \tag{1}$$

where $\mathbf{V}$ and $\mathbf{D}$ represent the eigenvector matrix and the eigenvalue matrix of discrete fractional angular transform, respectively. $\mathbf{V}^{\mathrm{T}}$ is the transpose of the matrix $\mathbf{V}$. The discrete fractional angular transformation can also be defined as:

$$\mathbf{A}_N^{\alpha,\beta} = \mathbf{V}_N^{\alpha}\mathbf{D}_N^{\beta}(\mathbf{V}_N^{\beta})^{\mathrm{T}} \tag{2}$$

where α and β express the fractional order and the angular matrix, respectively. $(\mathbf{V}_N^{\beta})^{\mathrm{T}}$ is the transpose of the matrix $\mathbf{V}_N^{\beta}$. The eigenvector matrix of the transformation is mainly affected by the angle β. If $\mathbf{V}_N$ is an orthogonal matrix, the following orthogonal matrix can be used to construct the eigenvector matrix of discrete fractional angular transform.

$$\mathbf{V}_2^{\beta} = \begin{bmatrix} \cos\beta & \sin\beta \\ -\sin\beta & \cos\beta \end{bmatrix} \tag{3}$$

$$\mathbf{V}_{2N+1} = \begin{bmatrix} \mathbf{V}_N & \mathbf{V}_N & \mathbf{V}_0^{\mathrm{T}} \\ \mathbf{V}_0 & \mathbf{V}_0 & \sqrt{2} \\ -\mathbf{V}_N^{\mathrm{Z}} & \mathbf{V}_N^{\mathrm{Z}} & \mathbf{V}_0^{\mathrm{T}} \end{bmatrix} \tag{4}$$

where the matrix $\mathbf{V}_N^{\mathrm{Z}}$ is the flipping matrix of the matrix $\mathbf{V}_N$, and the matrix $\mathbf{V}_0$ is a zero vector. The matrix $\mathbf{V}_0^{\mathrm{T}}$ is the transpose of the matrix $\mathbf{V}_0$. And these eigenvectors can be obtained by a simple recursion as [26]

$$\lambda_N^{\alpha} = \{1, \exp(-i2\pi\alpha), \exp(-i4\pi\alpha), \ldots, \exp(-i2(N-1)\pi\alpha)\} \tag{5}$$

2.2. Discrete wavelet transform

Wavelet transform is a major breakthrough in Fourier transform. And wavelet analysis has been widely employed in watermark scheme. Discrete wavelet transform (DWT) is obtained by the discretization of the scale and the displacement of continuous wavelet transform according to the power of 2 [27]. From the perspective of filtering, Fig. 1 exhibits that the original image signal $x[n]$ is decomposed by discrete wavelet filtering along the line and column, and the filtering results of even subscript are extracted through low-pass filter $h[n]$ and high-pass filter $g[n]$, respectively.

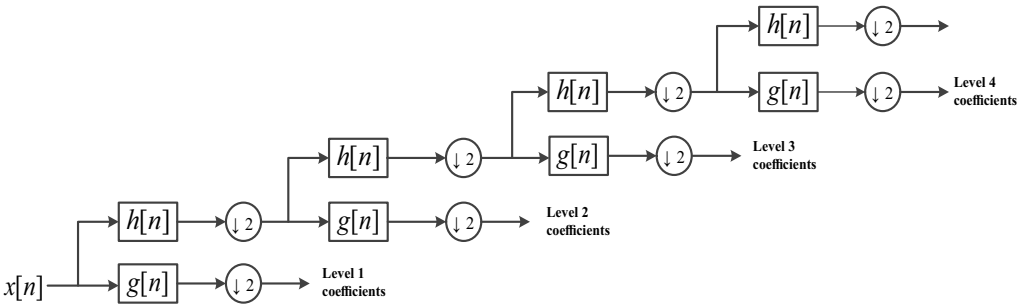


Fig. 1. The structure of the 4-level wavelet decomposition.

2.3. Chaos sequence based on mix optical bistability model

To solve the periodicity problem of Arnold transformation, the chaos sequence based on mix optical bistability model is introduced. The iterative equation is generated from the Gibbs optical bistable system with a long time delay.

$$X_{n+1} = 4\sin^2(X_n - 2.6) \tag{6}$$

The watermark scrambling steps are as follows.

Step 1. The watermark image matrix of size $N \times N$ is transformed into the row vector **A**.

Step 2. The initial value or key is substituted into the iterative sequence to yield a chaos sequence of length $N \times N$.

Step 3. The chaos sequence is sorted and the position vector **numy** of the sequence number in the original sequence is recorded.

Step 4. The position vector **numy** is utilized to reorder **A**, and then the result is transformed into an $N \times N$ matrix, which is the image matrix after scrambling and encryption.

3. Watermarking scheme based on 4-level DWT and DFAT

3.1. Watermark embedding scheme

The image watermark embedding scheme (see Fig. 2) is described as follows.

Step 1. The watermark image is scrambled with chaos and Arnold transform. Then the DWT is performed on the scrambled watermark to obtained the sub-bands: **ILL**, **IHL**, **ILH** and **IHH**.

Step 2. The original image **I** of size $N \times N$ is partitioned into four sub-bands **LL**, **HL**, **LH** and **HH** with the DWT. **LH** is selected for the later step by the Harris feature point detection.

Step 3. The low frequency bands **LH**, $\mathbf{HH}_1$ and $\mathbf{HH}_2$ are partitioned into sub-bands: $\mathbf{LL}_1$, $\mathbf{HL}_1$, $\mathbf{LH}_1$ and $\mathbf{HH}_1$; $\mathbf{LL}_2$, $\mathbf{HL}_2$, $\mathbf{LH}_2$ and $\mathbf{HH}_2$; $\mathbf{LL}_3$, $\mathbf{HL}_3$, $\mathbf{LH}_3$ and $\mathbf{HH}_3$, respectively. $\mathbf{HH}_3$ is selected for the sequential step.

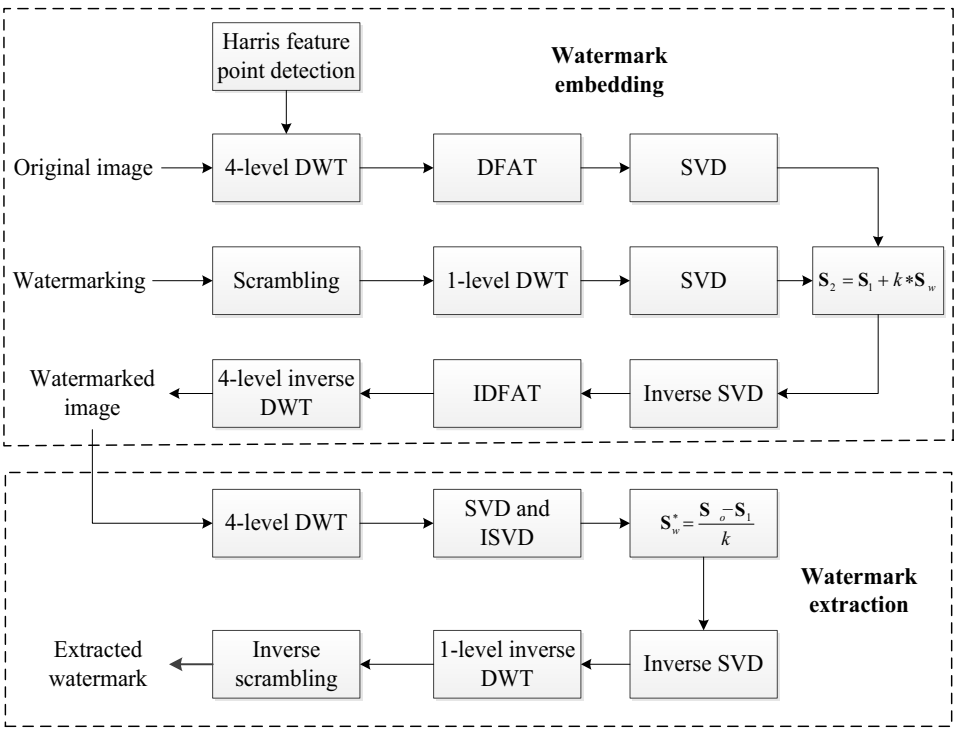


Fig. 2. The process of embedding and extracting watermark.

Step 4. The sub-band $\mathbf{HH}_3$ is encrypted with the DFAT to obtain the encrypted band $\mathbf{J}_1$.

Step 5. The SVD is performed on $\mathbf{J}_1$ and **IHH** to obtain the singular value arrays $\mathbf{S}_1$ and $\mathbf{S}_w$, respectively, and the orthogonal vectors are saved.

$$[\mathbf{U}_1, \mathbf{S}_1, \mathbf{V}_1] = \mathrm{SVD}(\mathbf{J}_1) \tag{7}$$

$$[\mathbf{U}_\mathrm{w}, \mathbf{S}_\mathrm{w}, \mathbf{V}_\mathrm{w}] = \mathrm{SVD}(\mathbf{ILL}) \tag{8}$$

Step 6. The watermark is embedded in the singular value $\mathbf{S}_1$ with the scaling factor k controlling the watermark embedding strength.

$$\mathbf{S}_2 = \mathbf{S}_1 + k \cdot \mathbf{S}_\mathrm{w} \tag{9}$$

Step 7. After obtaining all the information **S** of the embedded image, the inverse SVD is carried out on **S** and a new matrix $\mathbf{J}_2$ can be acquired by the IDFAT.

$$[\mathbf{U}, \mathbf{S}, \mathbf{V}] = \mathrm{SVD}(\mathbf{S}_2) \tag{10}$$

Step 8. By combining with other high frequency sub-bands, the image containing watermark information is obtained by the inverse 4-level DWT.

The scaling factor k, the singular value matrix $\mathbf{S}_1$ of the cover image, the left and the right singular vectors $\mathbf{U}_\mathrm{w}$ and $\mathbf{V}_\mathrm{w}$ of the watermark image and the left and the right singular vectors **U** and **V** of the embedded watermark image are all kept as keys for watermark extraction.

3.2. Watermark extraction scheme

The extraction process of watermark scheme (see Fig. 2) is as follows.

Step 1. In the same way, the 4-level DWT is performed on the watermarked image to obtain the sub-band $\mathbf{OHH}_3$.

Step 2. The SVD is carried out on the sub-band $\mathbf{OHH}_3$ to acquire the diagonal matrix $\mathbf{S}_\mathrm{ow}$.

$$[\mathbf{U}_\mathrm{ow}, \mathbf{S}_\mathrm{ow}, \mathbf{V}_\mathrm{ow}] = \mathrm{SVD}(\mathbf{OHH}_3) \tag{11}$$

Step 3. The inverse SVD is executed on $\mathbf{S}_\mathrm{ow}$ to acquire a new diagonal matrix $\mathbf{S}_\mathrm{o}$ with the left and the right singular vectors **U** and **V**.

$$\mathbf{S}_\mathrm{o} = \mathbf{U} \times \mathbf{S}_\mathrm{ow} \times \mathbf{V}^\mathrm{T} \tag{12}$$

Step 4. With the singular value matrix $\mathbf{S}_1$ of the original image and the scaling factor k, the diagonal matrix $\mathbf{S}_\mathrm{w}^*$ of the scrambling watermark can be gained.

$$\mathbf{S}_\mathrm{w}^* = \frac{1}{k}(\mathbf{S}_\mathrm{o} - \mathbf{S}_1) \tag{13}$$

Step 5. The inverse SVD is used to obtain the new sub-band $\mathbf{ILL}^*$ of the watermark, and the scrambling watermark image can be obtained with the inverse DWT.

$$\mathbf{ILL}^* = \mathbf{U}_w \times \mathbf{S}_w^* \times \mathbf{V}_w^T \tag{14}$$

Step 6. The watermark is extracted with the inverse scrambling based on chaos and the Arnold transform.

4. Simulation results and analyses

4.1. Simulation results

In the experiment, the gray-scale images *Baboon*, *Peppers* and *Couple* with 512 × 512 pixels are regarded as the cover images, and the gray-scale image with 64 × 64 pixels is considered as watermark. The results of test images without attacks are shown in Fig. 3. The keys of Arnold transform and chaos sequence based on the mix optical bistability model adopted in these simulations are chosen as 25 and 5, respectively. Double keys can improve the security of watermarking algorithms. The parameters α and β of the DFAT are given as 0.1234 and 4.5357, respectively. It is difficult to realize the real-time signal processing due to the large amount of calculation of the eigenvectors of discrete

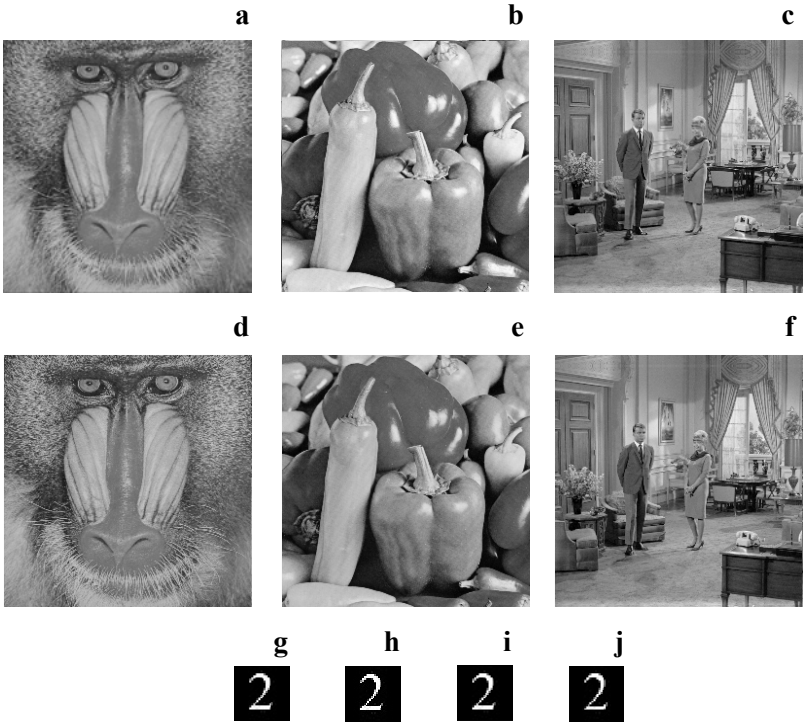


Fig. 3. Experiment results: (**a**) *Baboon*, (**b**) *Peppers*, (**c**) *Couple*; (**d**) watermarked *Baboon*, (**e**) watermarked *Peppers*, (**f**) watermarked *Couple*; (**g**) original watermark, (**h**–**j**) extracted watermark, respectively.

T a b l e 1. PSNR and NC values of the watermarked images.

	Cover image		
	Baboon	*Peppers*	*Couple*
PSNR [dB]	54.6735	54.6165	54.7353
NC	1.0000	1.0000	1.0000

Fourier transform (DFT). The DFAT can determine all eigenvectors of DFT by a simple iterative transform of one parameter. Therefore, the DFAT can process the signal quickly and has the mathematical properties similar to the DFT, such as linearity, unitarity, index additivity, multiplicity and Parseval energy conservation.

To evaluate the approximation degree between the watermarked image and the original one, the peak signal-to-noise ratio (PSNR) and the normalized correlation (NC) are adopted. PSNR shows the imperceptibility of the watermark, while NC evaluates the robustness of the extracted watermark. Generally, if the PSNR value is more than 40 dB, the imperceptibility can be guaranteed. Table 1 shows the PSNR values (dB) of different watermarked images. Therefore, the proposed watermarking scheme can display the excellent imperceptibility.

4.2. Various attack analyses

4.2.1. JPEG compression attack

Figure 4 indicates the results of JPEG compression attack on different watermarked images and the corresponding extracted watermarks. And Table 2 shows the NC values of different watermarked images with the distinct compression factors. These results indicate that the extracted watermark image under the JPEG compression attack is sig-

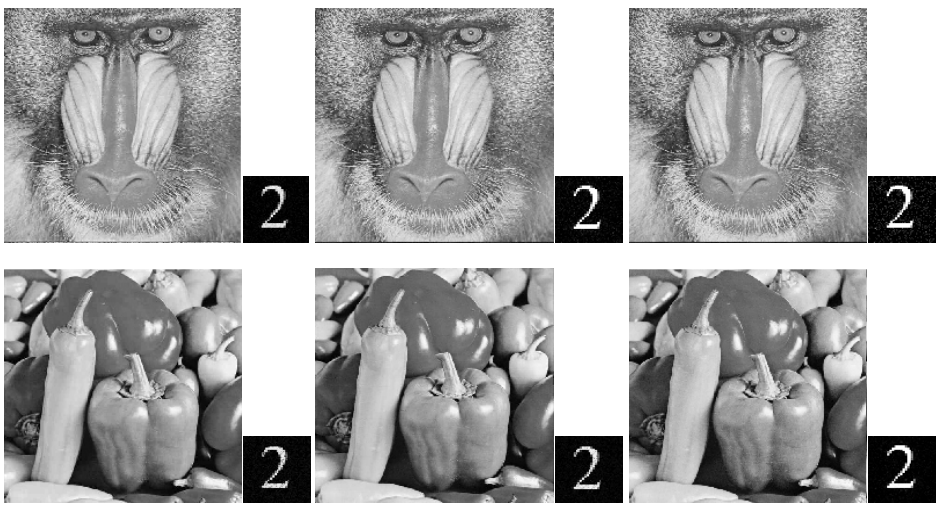


Fig. 4. JPEG compression attack with compression factors 30%, 60%, 90%: (**a**) *Baboon*, (**b**) *Peppers*, and (**c**) *Couple*. Extracted watermarks are also shown.

Fig. 4. Continued.

T a b l e 2. NC values of different watermarked images with different compression factors.

	Cover image		
	Baboon	*Peppers*	*Couple*
30%	0.9928	0.9749	0.9765
60%	0.9881	0.9890	0.9938
90%	0.9577	0.9975	0.9997

nificantly correlated with the original watermarking image. Under the compression conditions, the watermark image could still clearly extract from the watermarked image. Thus, the proposed watermark scheme could resist the JPEG compression attack to some extent.

4.2.2. Cutting attack

The results of the watermarked images and the corresponding extracted watermarks under different degrees of cutting on different cover images are given in Fig. 5. And

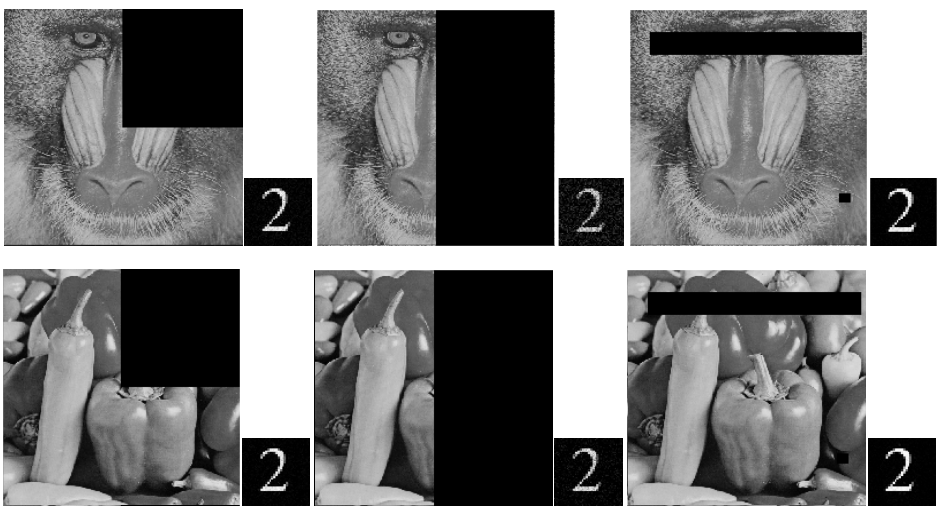


Fig. 5. Watermarked images with irregular cutting, quarter cutting and half cutting: (**a**) *Baboon*, (**b**) *Peppers*, and (**c**) *Couple*. Extracted watermarks are also shown.

c

Fig. 5. Continued.

T a b l e 3. NC values of different watermarked images with different cutting degrees.

	Cover image		
	Baboon	*Peppers*	*Couple*
Irregular cutting	0.9974	0.9992	0.9995
Quarter cutting	0.9903	0.9968	0.9923
Half cutting	0.8798	0.9776	0.9696

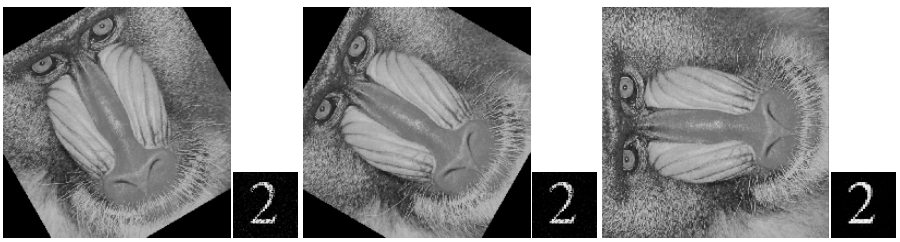
Table 3 indicates that the NC values of the extracted watermark from different cutting attack are as high as 0.90 and even higher. Although the NC values are decrease with the increase of the cutting area, the extracted watermark images could be still recognized by human eyes. Therefore, the watermark scheme based on the 4-level DWT and DFAT could resist the quarter cutting attack.

4.2.3. Rotation attack

The watermarked images and the corresponding extracted watermarks after rotation attack are demonstrated in Table 4 and Fig. 6. Under the rotation attack with 30°, 60°,

T a b l e 4. NC values of different watermarked images with different angles.

	Cover image		
	Baboon	*Peppers*	*Couple*
30°	0.9386	0.9843	0.9962
60°	0.9556	0.9860	0.9930
90°	0.9959	0.9818	0.9818



a

Fig. 6. Rotation attack on distinct watermarked images with 30°, 60°, and 90°: (**a**) *Baboon*, (**b**) *Peppers*, and (**c**) *Couple*. Extracted watermarks are also shown.

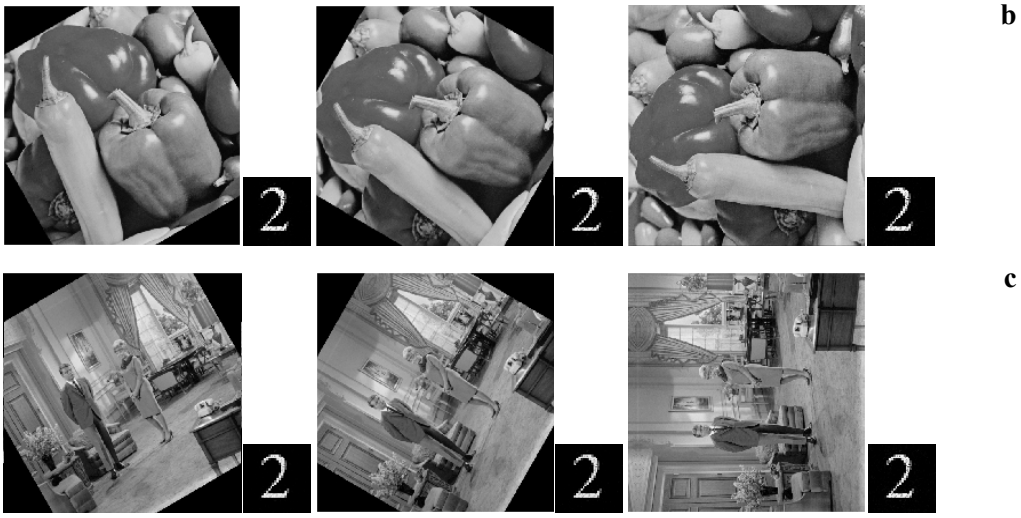


Fig. 6. Continued.

and 90°, the extracted watermark can satisfy the visual characteristics of the human. In the field of image processing, Harris feature point detection usually has the advantages of rotation invariability and angle invariability. As shown in Fig 7, the feature point information of different cover images will not change under the rotation attack.

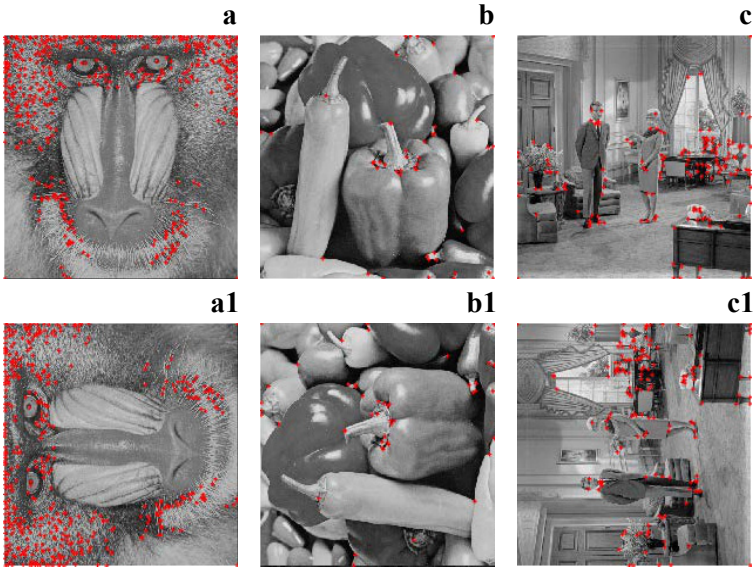


Fig. 7. Information graph of Harris feature point detection after rotation attack: (**a**) original cover image *Baboon*, (**a1**) watermarked image under rotation attack with 90°; (**b**) original cover image *Peppers*, (**b1**) watermarked image under rotation attack with 90°; (**c**) original cover image *Couple*, (**c1**) watermarked image under rotation attack with 90°.

Experimental results also indicate that this scheme based on 4-level DWT and DFAT could resist rotation attack effectively.

4.3. Results analyses

The attacks on watermarking system can be divided into conventional signal processing attacks and geometric attacks. The signal processing attacks consist of image compression, image enhancement, noise, filtering, *etc*. The effect of geometric attack on the watermarking system is different from the signal processing attacks. The main function of the signal processing attack is to weaken the energy of watermark, while the main purpose of geometric attack is to destroy the synchronization of watermark embedding and extraction. Table 5 shows that the NC values of noise attack, especially under the Gaussian noise attack, are not good. Since the synchronization of watermark embedding and extraction depends on these feature points and the information of the feature point is destroyed by noise attack, the similarity between the extracted watermark image and the original watermark image would be decreased.

Besides the noise attacks, the NC values under other signal processing attacks could be acceptable. In the field of image processing, Harris feature point detection usually has the advantages of rotation invariability and perspective invariability. Consequently, the results of the resistance with the rotation attack are reasonable. Since the wavelet transform has localization characteristics in both spatial domain and transform domain, the watermark scheme has excellent robustness in the cutting attack of the local geometric attack.

T a b l e 5. NC values of the proposed scheme on different cover images with various attacks.

Attacks	Cover image		
	Baboon	*Peppers*	*Couple*
No attack	1.0000	1.0000	1.0000
JPEG compression (30%)	0.9928	0.9749	0.9765
JPEG compression (60%)	0.9881	0.9890	0.9938
JPEG compression (90%)	0.9577	0.9975	0.9997
Gaussian low-pass filtering (0.5)	0.9763	0.9942	0.9931
Gaussian noise (0.05)	0.5980	0.5479	0.5429
Salt and pepper noise (0.05)	0.8641	0.7284	0.7163
Irregular cutting	0.9974	0.9992	0.9995
Quarter cutting	0.9903	0.9968	0.9923
Half cutting	0.8798	0.9776	0.9696
Rotation (30°)	0.9386	0.9843	0.9962
Rotation (60°)	0.9556	0.9860	0.9930
Rotation (90°)	0.9959	0.9818	0.9818
Image brightening	0.9983	0.9995	0.9994
Image darkening	0.9960	0.9989	0.9986

In summary, the proposed watermark scheme based on 4-level DWT and DFAT can resist various attacks, and according to the similarity between the extracted watermark image and the original watermark image, it is proved that the scheme has good robustness.

4.4. Comparison with the existing works

To further reflect the advantages of the proposed digital watermarking scheme based on 4-level DWT and DFAT, the comparison results with the previous methods are displayed in Table 6. To compare fairly, the same cover image and the same watermark image are chosen. Based on DWT, DCT and SVD, the algorithm in Ref. [28] improved the robustness against common watermark attacks and rotation attack. In Ref. [29], a more robust watermarking scheme based on 4-level DWT, DCT and SVD was designed, while the ability to resist the half cutting attack and rotation attack is not good. In this paper, a digital watermarking scheme based on 4-level DWT, DFAT and SVD is proposed. Since the DCT can help concentrate the image energy and is beneficial to resist the signal processing attack, the NC values of the proposed watermark scheme in the resistance of the noise attack are worse than those of Refs. [28] and [29]. However, the proposed watermarking scheme combining with Harris feature point detection could still achieve acceptable results in resisting other attacks, particularly the rotation attack.

T a b l e 6. The NC values of the existing schemes.

Attacks	NC [28]	NC [29]	Proposed NC
No attack	0.9995	0.9992	1.0000
JPEG compression (60%)	0.9770	0.9964	0.9749
Gaussian low-pass filtering (0.5)	0.9806	0.9978	0.9942
Gaussian noise (0.05)	0.9079	0.9388	0.5479
Salt and Pepper noise (0.05)	0.9230	0.9554	0.7284
Quarter cutting	0.9931	0.9801	0.9968
Half cutting	0.9742	0.6232	0.9776
Rotation (30°)	0.9775	0.2354	0.9843
Image brightening	0.9988	0.9991	0.9995
Image darkening	0.9978	0.9982	0.9989

5. Conclusion

This paper proposes a digital watermarking algorithm based on the 4-level discrete wavelet transform and the discrete fractional angular transform. The 1-level decomposition sub-bands with few feature points are chosen by the Harris feature point detection. Wavelet transform can classify the image with the help of multi-resolution features. And the discrete fractional angular transform only adopts a parameter to determine its all eigenvectors via a simple iteration, which greatly speeds up the signal processing. Simula-

tion results demonstrate that the digital watermarking algorithm has strong resistance to geometric attack and other attacks. Admittedly, it has weak resistance to noise attack. There is still room for improvement on this algorithm in the future work.

Acknowledgement – This work is supported by the National Natural Science Foundation of China (grant No. 61172159), and the Research Foundation of the Education Department of Heilongjiang Province (grant No. 135509115).

References

[1] Liao X., Shu C.W., *Reversible data hiding in encrypted images based on absolute mean difference of multiple neighboring pixels*, Journal of Visual Communication and Image Representation **28**, 2015, pp. 21–27, DOI: 10.1016/j.jvcir.2014.12.007.

[2] Di F.Q., Zhang M.Q., Liao X., Liu J., *High-fidelity reversible data hiding by Quadtree-based pixel value ordering*, Multimedia Tools and Applications **78**(6), 2019, pp. 7125–7141, DOI: 10.1007/s11042-018-6469-4.

[3] Liu Z.J., Gong M., Dou Y.K., Liu F., Lin S., Ahmad M.A., Dai J.M., Liu S.T., *Double image encryption by using Arnold transform and discrete fractional angular transform*, Optics and Lasers in Engineering **50**(2), 2012, pp. 248–255, DOI: 10.1016/j.optlaseng.2011.08.006.

[4] Sui L.S., Duan K.K., Liang J.L., *Double-image encryption based on discrete multiple-parameter fractional angular transform and two-coupled logistic maps*, Optics Communications **343**, 2015, pp. 140–149, DOI: 10.1016/j.optcom.2015.01.021.

[5] Lang J., Zhang Z.G., *Blind digital watermarking method in the fractional Fourier transform domain*, Optics and Lasers in Engineering **53**, 2014, pp. 112–121, DOI: 10.1016/j.optlaseng.2013.08.021.

[6] Xiao D., Chang Y.T., Xiang T., Bai S., *A watermarking algorithm in encrypted image based on compressive sensing with high quality image reconstruction and watermark performance*, Multimedia Tools and Applications **76**(7), 2017, pp. 9265–9296, DOI: 10.1007/s11042-016-3532-x.

[7] Belazi A., Abd El-Latif A.A., Diaconu A.V., Rhouma R., Belghith S., *Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms*, Optics and Lasers in Engineering **88**, 2017, pp. 37–50, DOI: 10.1016/j.optlaseng.2016.07.010.

[8] Xia C., Guan Q.X., Zhao X.F., Zhao C.D., *Highly accurate real-time image steganalysis based on GPU*, Journal of Real-Time Image Processing **14**(1), 2018, pp. 223–236, DOI: 10.1007/s11554-016-0600-4.

[9] Tang L.L., Huang C.T., Pan J.S., Liu C.Y., *Dual watermarking algorithm based on the fractional Fourier transform*, Multimedia Tools and Applications **74**(12), 2015, pp. 4397–4413, DOI: 10.1007/s11042-013-1531-8.

[10] Benrhouma O., Hermassi H., Abd El-Latif A.A., Belghith S., *Chaotic watermark for blind forgery detection in images*, Multimedia Tools and Applications **75**(14), 2016, pp. 8695–8718, DOI: 10.1007/s11042-015-2786-z.

[11] Das S., Banerjee M., Chaudhuri A., *An improved video key-frame extraction algorithm leads to video watermarking*, International Journal of Information Technology **10**(1), 2018, pp. 21–34, DOI: 10.1007/s41870-017-0054-3.

[12] Jia S.L., *A novel blind color images watermarking based on SVD*, Optik **125**(12), 2014, pp. 2868–2874, DOI: 10.1016/j.ijleo.2014.01.002.

[13] Gao L., Qi L., Wang Y.J., Chen E.Q., Yang S.Y., Guan L., *Rotation invariance in 2D-FRFT with application to digital image watermarking*, Journal of Signal Processing Systems **72**(2), 2013, pp. 133–148, DOI: 10.1007/s11265-012-0722-2.

[14] Abd El-Latif A.A., Abd-El-Atty B., Hossain M.S., Elmougy S., Ghoneim A., *Secure quantum steganography protocol for fog cloud Internet of things*, IEEE Access **6**, 2018, pp. 10332–10340, DOI: 10.1109/ACCESS.2018.2799879.

[15] CHETAN K.R., NIRMALA S., *An efficient and secure robust watermarking scheme for document images using Integer wavelets and block coding of binary watermarks*, Journal of Information Security and Applications **24**–**25**, 2015, pp. 13–14, DOI: 10.1016/j.jisa.2015.07.002.

[16] HU H.T., CHANG J.R., HSU L.Y., *Windowed and distortion-compensated vector modulation for blind audio watermarking in DWT domain*, Multimedia Tools and Applications **76**(24), 2017, pp. 26723–26743, DOI: 10.1007/s11042-016-4202-8.

[17] ALI M., AHN C.W., *An optimized watermarking technique based on self-adaptive DE in DWT-SVD transform domain*, Signal Processing **94**, 2014, pp. 545–556, DOI: 10.1016/j.sigpro.2013.07.024.

[18] FAZLI S., MOEINI M., *A robust image watermarking method based on DWT, DCT, and SVD using a new technique for correction of main geometric attacks*, Optik **127**(2), 2016, pp. 964–972, DOI: 10.1016/j.ijleo.2015.09.205.

[19] TAN Y.L., ZHAO Y.Q., *Digital watermarking image compression method based on symmetric encryption algorithms*, Symmetry **11**(12), 2019, article 1505, DOI: 10.3390/sym11121505.

[20] ROY S., PAL A.K., *A robust blind hybrid image watermarking scheme in RDWT-DCT domain using Arnold scrambling*, Multimedia Tools and Applications **76**(3), 2017, pp. 3577–3616, DOI: 10.1007/s11042-016-3902-4.

[21] LUO A.W., GONG L.H., ZHOU N.R., ZOU W.P., *Adaptive and blind watermarking scheme based on optimal SVD blocks selection*, Multimedia Tools and Applications **79**(1–2), 2020, pp. 243–261, DOI: 10.1007/s11042-019-08074-2.

[22] TIAN C., WEN R.H., ZOU W.P., GONG L.H., *Robust and blind watermarking algorithm based on DCT and SVD in the contourlet domain*, Multimedia Tools and Applications **79**(11–12), 2020, pp. 7515–7541, DOI: 10.1007/s11042-019-08530-z.

[23] SINGH H., *Nonlinear optical double image encryption using random-optical vortex in fractional Hartley transform domain*, Optica Applicata **47**(4), 2017, pp. 557–578, DOI: 10.5277/oa170406.

[24] ZHOU Z.H., YU J., LIA Q.H., GONG L.H., *Image encryption combining discrete fractional angular transform with Arnold transform in image bit planes*, Optica Applicata **48**(2), 2018, pp. 225–236, DOI: 10.5277/oa180206.

[25] LIU Z.J., AHMAD M.A., LIU S.T., *A discrete fractional angular transform*, Optics Communications **281**(6), 2008, pp. 1424–1429, DOI: 10.1016/j.optcom.2007.11.012.

[26] ZHOU N.R., XIA HOU W.M., WEN R.H., ZOU W.P., *Imperceptible digital watermarking scheme in multiple transform domains*, Multimedia Tools and Applications **77**(23), 2018, pp. 30251–30267, DOI: 10.1007/s11042-018-6128-9.

[27] ROY S., PAL A.K., *A hybrid domain color image watermarking based on DWT–SVD*, Iranian Journal of Science and Technology, Transactions of Electrical Engineering **43**(2), 2019, pp. 201–217, DOI: 10.1007/s40998-018-0109-x.

[28] ZHENG P.J., ZHANG Y.H., *A robust image watermarking scheme in hybrid transform domains resisting to rotation attacks*, Multimedia Tools and Applications **79**(25–26), 2020, pp. 18343–18365, DOI: 10.1007/s11042-019-08490-4.

[29] WU J.Y., HUANG W.L., XIA-HOU W.M., ZOU W.P., GONG L.H., *Imperceptible digital watermarking scheme combining 4-level discrete wavelet transform with singular value decomposition*, Multimedia Tools and Applications **79**(31–32), 2020, pp. 22727–22747, DOI: 10.1007/s11042-020-08987-3.

Received November 21, 2020
in revised form December 25, 2020