Optica Applicata, Vol. LIII, No. 2, 2023
DOI: 10.37190/oa230210

Digital watermarking scheme based on curvelet transform and multiple chaotic maps

YI XIAO[1], YA-CHEN XU[2], NAN-RUN ZHOU[2], ZHEN-RONG LIN[1,*]

[1]Department of Computer Science & Technology, Nanchang University, Nanchang 330031, Jiangxi, China

[2]Department of Electronic Information Engineering, Nanchang University, Nanchang 330031, Jiangxi, China

*Corresponding author: zrlin@ncu.edu.cn

The rapid development of digital products brings security issues. Digital watermarking technology is an important means to handle these problems. To enhance the imperceptibility of watermark and locate the possible tampering as well, a digital watermarking scheme based on curvelet transform is presented by combining with multiple chaotic maps. The host image is decomposed into three parts, *i.e.*, coarse layer, detail layer and fine layer, with curvelet transform, and a robust watermark is embedded into the coarse layer for copyright protection of digital products. In addition, an authentication watermark is embedded into the fine layer to detect and locate the illegal changes. Simulation results show that the proposed digital watermarking scheme possesses acceptable robustness and security.

Keywords: digital watermarking, curvelet transform, multiple chaotic maps.

1. Introduction

With the rapid development of computer multimedia technology, the security and the authenticity of digital contents are becoming increasingly important. The digital watermarking technology to hide a certain kind of information, *i.e.*, watermark, in the digital products is an effective solution to secure transmission, storage and identification. A qualified digital watermarking scheme should be of good imperceptibility and robustness.

The applications of digital watermarking have been widely investigated [1,2]. Images are the most common type of digital content transmitted on the internet. Generally, there are two categories of image watermarking schemes: spatial domain schemes and transform domain ones. In the spatial domain schemes, the watermark information is usually embedded by directly modifying the pixel value of host image, such as the least significant bit method, which is imperceptible and easy to implement; however the robustness is weak [3]. While in the transform domain watermarking schemes, before embedding the watermark, different mathematical transforms are performed on the host images, such as discrete cosine transform (DCT), discrete wavelet transform (DWT),

discrete Fourier transform (DFT), fractional Fourier transform (FrFT), and their combinations [4]. Then the watermark information is embedded in the middle or the low frequency part of the image in the transform domain. ERNAWAN and KABIR designed a robust image watermarking scheme, which modifies certain coefficients to construct watermarked image instead of inserting the watermark bits directly to achieve higher invisibility and robustness [5]. WU *et al*. presented an imperceptible digital watermarking algorithm based on 4-level DWT, DCT and SVD, which could resist JPEG compression attack, and various noise attacks [6]. HAMIDI *et al*. raised a robust blind image watermarking scheme based on the DFT-DCT, where Arnold transform is adopted to scramble the watermark and then to enhance the security of the scheme [7]. LANG and ZHANG proposed a novel blind digital image watermarking algorithm based on the FrFT, which is very robust to JPEG compression noise attacks and image manipulation operation [8]. ERNAWAN *et al.* put forward an adaptive scaling factor based on the selected DWT-DCT coefficients related to the image content and proposed a watermarking scheme with a set of rules involving the adaptive scaling factor [9]. To address the limited utilization areas and the insufficient in blindness of grayscale watermarking schemes, GUL proposed a blind robust color image watermarking method based on DWT and DCT [10].

In addition, curvelet transform (CT) has good approximation performance for multivariable functions with linear singularity, and can describe the curve edge of the image well. When being applied to digital watermarking, curvelet transform can make the host image retain high PSNR after being embedded a watermark [11–13]. AHMED *et al*. studied an attack resistant watermarking technique by combining CT with robust principal component analysis [11]. KIM *et al*. raised a watermarking scheme with CT to enhance imperceptibility and robustness [12]. KUKREJA *et al*. proposed a copyright protection scheme based on CT, which creates meaningful shares to provide better security and handles false positive cases efficiently [13].

In this paper, a digital watermarking scheme based on the curvelet transform and the multiple chaotic maps will be introduced. A robust watermark scrambled by the multiple chaotic maps is embedded into the low frequency (LF) coefficient matrix of the host image in the CT domain. While an authentication watermark constructed by the chaotic sequence is embedded into the high frequency (HF) coefficients of the CT to detect any unauthorized tamper.

The rest of the paper is organized as the following sections. The watermark embedding and extracting scheme is introduced in Sec. 2. Simulation results and performance analysis are given in Sec. 3. Finally, a brief conclusion is reached in Sec. 4.

2. Digital watermarking algorithm based on curvelet transform and multiple chaotic maps

2.1. Embedding method of watermark information

The embedding process of robust watermark is as follows.

Step 1. The curvelet transform is performed on the host image **H** to obtain the coarse layer composed of low frequency coefficient matrix **C**, detail layer composed of medium and high frequency coefficient matrix **D**, and fine layer involving high frequency coefficient matrix **T**.

Step 2. Two chaotic sequences X and Y are generated by iterative calculation according to Eqs. (1) and (2) with the keys k_1, k_2, k_3, k_4 and k_5, and then they are converted into 2D matrices **X** and **Y**, respectively. After sorting each row in **X** or **Y**, the position matrices $\mathbf{P}_1$ and $\mathbf{P}_2$ are obtained.

$$X_{n+1} = \begin{cases} \left(\dfrac{X_n}{\alpha} + \beta \sin \pi X_n + c\right) \bmod 1, & 0 \le X_n < \alpha \\ \left(\dfrac{X_n}{\alpha}\dfrac{1}{0.5-\alpha} + \beta \sin \pi X_n + c\right) \bmod 1, & \alpha \le X_n < 0.5 \\ \left(\dfrac{1-X_n}{\alpha} + \beta \sin \pi (1-X_n) + c\right) \bmod 1, & 0 \le 1-X_n < \alpha \\ \left(\dfrac{1-X_n}{\alpha}\dfrac{1}{0.5-\alpha} + \beta \sin \pi (1-X_n) + c\right) \bmod 1, & \alpha \le 1-X_n < 0.5 \end{cases} \tag{1}$$

$$Y_{n+1} = \eta Y_n (1 - Y_n) \tag{2}$$

Step 3. The corresponding row of the original watermark image $\mathbf{W}_1$ is selected according to the first column of $\mathbf{P}_2$, then $\mathbf{W}_1$ is scrambled according to each line of $\mathbf{P}_1$ to generate $\mathbf{W}_2$. Similarly, the corresponding row of the $\mathbf{W}_2$ is selected according to the first column of $\mathbf{P}_1$, then $\mathbf{W}_2$ is scrambled according to each line of $\mathbf{P}_2$ to produce the scrambled matrix **W**.

Step 4. The scrambling matrix **W** is embedded into matrix **C** to obtain matrix **C′**. The embedding process adopts the additive embedding rule.

$$C'(m, n) = C(m, n) + \omega W(m, n) \tag{3}$$

where $C(m, n)$ is the element of matrix **C** at position (m, n), while $W(m, n)$ is the element of matrix **W** at position (m, n), ω is the embedding strength, $C'(m, n)$ is the element of embedded matrix **C′** at position (m, n).

The generation and embedding process of authentication watermark is as follows.

Step 1. The chaotic sequence Z is produced by iterating Eq. (4) with k_6 and k_7, and then it is processed with the following methods to obtain a new sequence Z_1. If the element of Z is greater than 0.5, the element is modified to 1; On the contrary, it is modified to 0. Next, Z_1 is transformed into a 2D matrix $\mathbf{Z}_1$ as the authentication watermark.

$$Z_{n+1} = \mu \sin \pi Z_n \tag{4}$$

Step 2. The authentication watermark $\mathbf{Z}_1$ is added to matrix $\mathbf{T}$ by the half division method. The specific rule is constructed as

$$T'(m,n) = \begin{cases} T(m,n), & g(m,n) \geq 0.5, \quad Z_1(m,n) = 1 \\ T(m,n) + 0.5, & g(m,n) < 0.5, \quad Z_1(m,n) = 1 \\ T(m,n) - 0.5, & g(m,n) \geq 0.5, \quad Z_1(m,n) = 0 \\ T(m,n), & g(m,n) < 0.5, \quad Z_1(m,n) = 0 \end{cases} \tag{5}$$

where

$$g(m,n) = T(m,n) - \lfloor T(m,n) \rfloor \tag{6}$$

The host image $\mathbf{H}_1$ embedded with robust watermark and authentication one can be obtained by the inverse curvelet transform. The watermark embedding process is shown in Fig. 1.

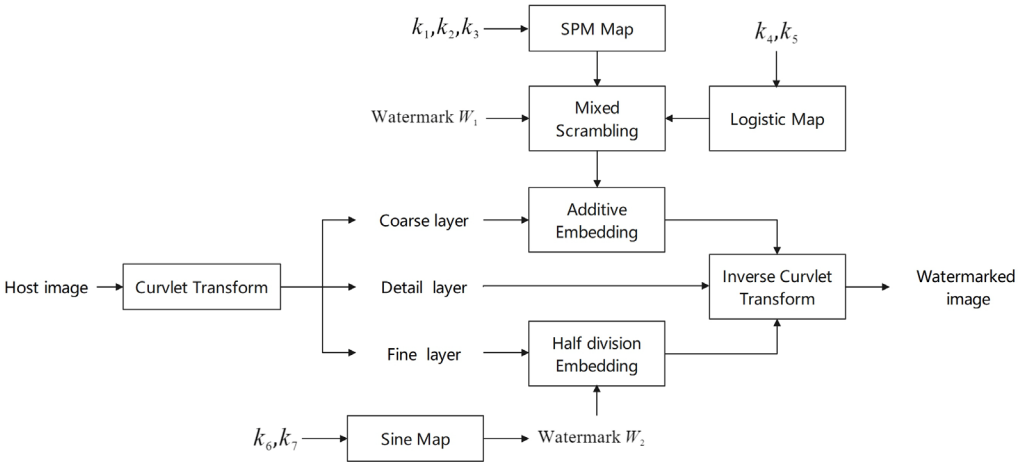


Fig. 1. Watermark embedding process.

2.2. Watermark extraction method

The watermark extraction process is in the following.

Step 1. The curvelet transform is performed on the host image $\mathbf{H}_1$ to obtain the low -frequency part $\mathbf{C}_1$, medium high-frequency part $\mathbf{D}_1$ and high-frequency part $\mathbf{T}_1$. Then the scrambled watermark $\mathbf{W}'$ is extracted as

$$W'(m,n) = \frac{C_1(m,n) - C(m,n)}{\omega} \tag{7}$$

Step 2. The robust watermark $\mathbf{W}_1'$ is obtain by performing inverse scrambling on the extracted watermark $\mathbf{W}'$.

Step 3. A new authentication watermark $\mathbf{Z}_1'$ is obtained with the following process on $\mathbf{T}_1$.

$$Z_1'(m, n) = \begin{cases} 1, & g_1(m, n) \geq 0.5 \\ 0, & g_1(m, n) < 0.5 \end{cases} \tag{8}$$

where

$$g_1(m, n) = T_1(m, n) - \lfloor T_1(m, n) \rfloor \tag{9}$$

Step 4. The authentication watermarks $\mathbf{Z}_1$ and $\mathbf{Z}_1'$ are XORed to obtain a tamper detection matrix $\mathbf{M}$. A zero matrix $\mathbf{Z}_2$ with the same size as the host image is defined. If $M(m, n) = 0$, it means the host image has not been tampered with, then the corresponding element of $\mathbf{Z}_2$ in the image does not change. If $M(m, n) = 1$, the host image has been tampered with, the element at the corresponding position in $\mathbf{Z}_2$ will be modified to 1. The watermark extraction process is shown in Fig. 2.

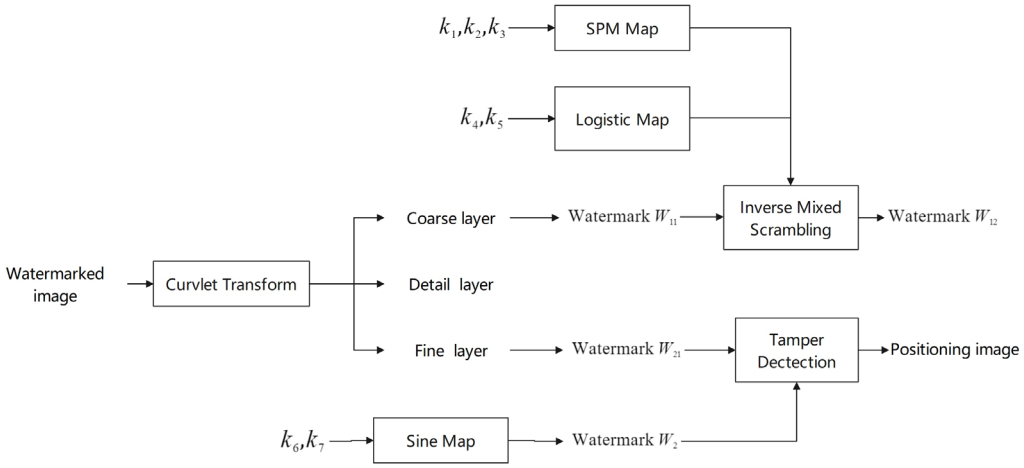


Fig. 2. Watermark extraction process.

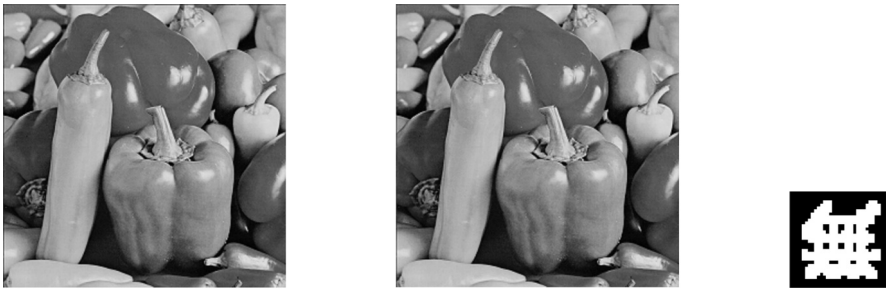
3. Simulation results and performance analysis

3.1. Imperceptibility

The proposed scheme is simulated by MATLAB with two test images *Peppers* and *Boat* of size 512×512 and watermark images of size 32×32. The embedding and extraction results of the watermark images are shown in Table 1 and Fig. 3. Figures 3(a1) and (b1)

T a b l e 1. PSNR value of watermarked images and NC value of extracted watermarks.

Host image	*Peppers*	*Boat*
PSNR	71.0336	71.0172
NC	1	1



(a1) (a2) (a3)

(b1) (b2) (b3)

Fig. 3. Embedding and extraction of watermark. (a1), (b1) The host images, (a2), (b2) the watermarked images, and (a3), (b3) are the watermark images after extraction.

are the host images, (a2) and (b2) are the watermarked images, (a3) and (b3) are the watermark images after extraction. The peak signal to noise ratio (PSNR) and normalized correlation (NC) are used to measure the similarity of original watermarks and extracted watermarks, which could evaluate the imperceptibility of proposed scheme in a more objective way. After being embedded with the watermark image, the PSNR value of the host image is more than 70 dB, which indicates that the information distortion between the watermarked image and the original one is very small. Thus the digital watermarking scheme has good imperceptibility.

3.2. Histogram

Figure 4 shows the histograms of images *Peppers* and *Boat* before and after being embedded with the watermark. Figures 4(a1) and (b1) are the histograms of original images. Figures 4(a2) and (b2) are the histograms of watermarked images. It can be seen that the histograms of the original host image and the watermarked image are indistinguishable to human eyes, and one can hardly obtain watermark information from the watermarked image. Therefore, the digital watermarking scheme has great advantages in resisting the histogram attack.

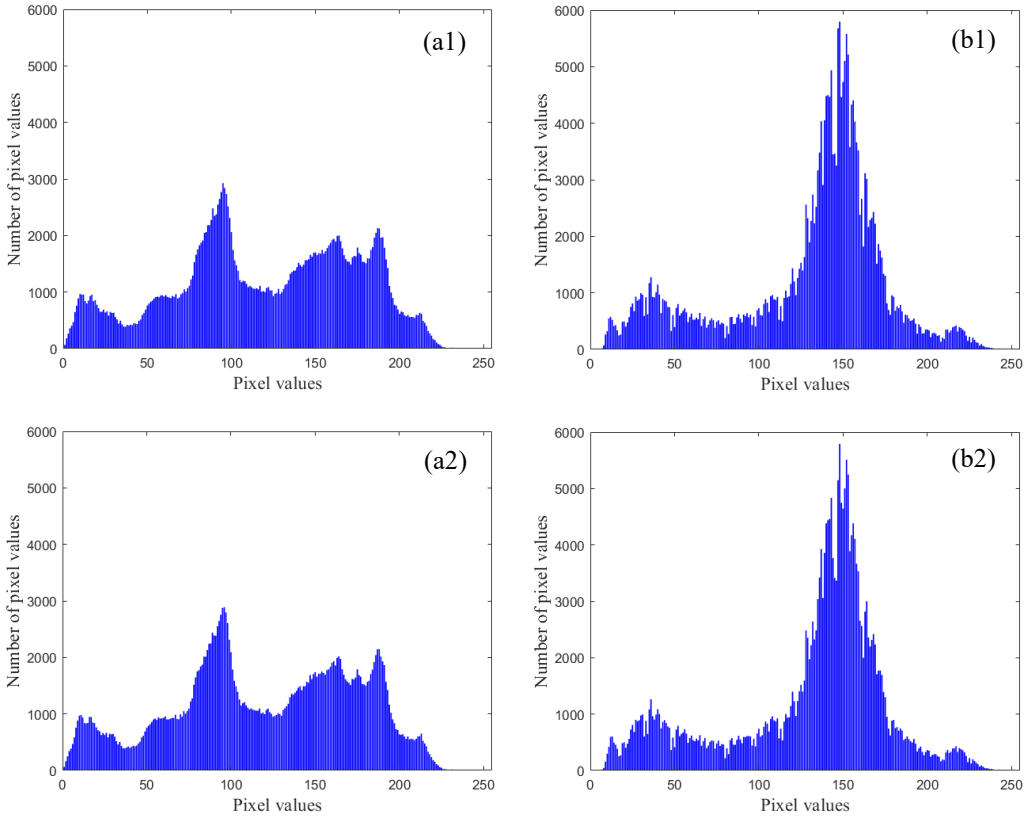


Fig. 4. Histograms of host images before and after being embedded in the watermark: (a1) original image *Peppers*, (b1) original image *Boat*, (a2) watermarked image *Peppers*, and (b2) watermarked image *Boat*.

3.3. Robustness

3.3.1. Key sensitivity

To enhance the security of the watermarking scheme, the chaotic scrambling method is adopted to scramble the watermark image. To analyze the security of the key, the original correct keys $\alpha = 0.1$, $\beta = 0.1$, $C = 5$, $X_0 = 0.6742$, $\eta = 4$, and $Y_0 = 0.6742$ are added the step $d = 0.01$ in turn. Then the watermark is extracted with a key slightly modified and five other correct keys, respectively. Six groups of simulation tests are carried out according to the above methods. Figure 5(a) is the extracted watermark image with the correct keys, and Figs. 5(b)–(g) are the extracted watermark images with a key slightly modified and the other five correct keys. The result shows that it is impossible to obtain the original watermark information from the watermark image extracted with the wrong key. Therefore the proposed digital watermarking algorithm is very sensitive to keys.

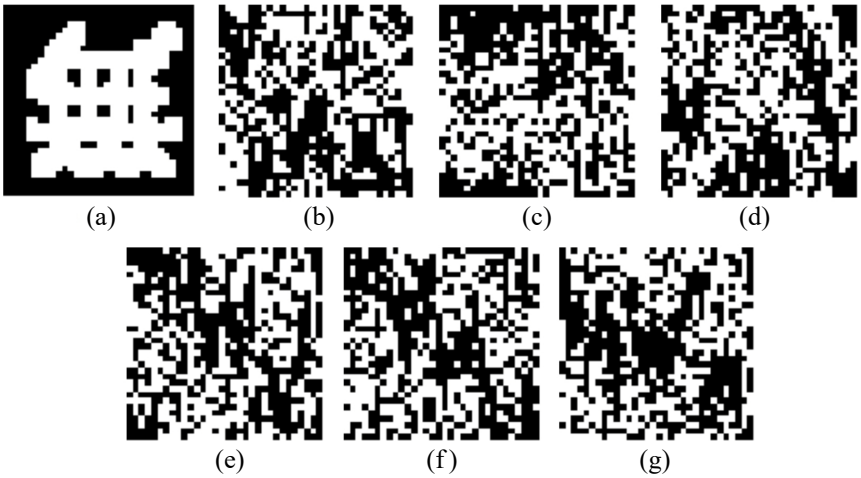


Fig. 5. Extracted watermark images with: (a) correct keys, (b) $\alpha + 10^{-15}$, (c) $\beta + 10^{-15}$, (d) $c + 10^{-14}$, (e) $X_0 + 10^{-15}$, (f) $\eta + 10^{-15}$, and (g) $Y_0 + 10^{-15}$.

3.3.2. Cutting attack

The watermarked image is cut with different degrees, and the watermark image is extracted from the cut image. Figure 6 shows the watermarked images subject to different degrees of cutting attacks and the corresponding extracted watermark image. Figures 6(a)–(c) and (d)–(f) are the watermarked images subject to 1/16, 1/8 and 1/4 cutting attacks, respectively. Figures 6(a1)–(f1) are the watermark images extract-

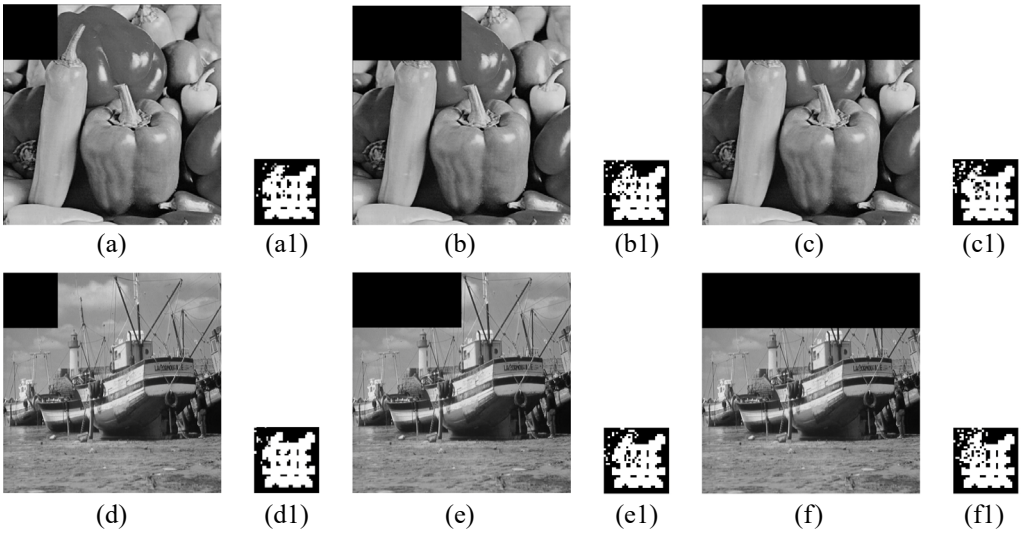


Fig. 6. Host image and corresponding extracted watermark after cutting attack. (a)–(c) and (d)–(f) The watermarked images subject to 1/16, 1/8 and 1/4 cutting attacks, respectively. (a1)–(f1) The watermark images extracted from the corresponding cut images.

T a b l e 2. NC values after cutting attack.

Cutting rate	*Peppers*	*Boat*
1/16	0.9795	0.9856
1/8	0.9610	0.9692
1/4	0.9487	0.9487

ed from the corresponding cut images. Table 2 shows the NC values of the extracted watermark. The NC values are all greater than 0.94, which means that the extracted watermark image is very similar to the original watermark image. Therefore, the proposed digital watermarking scheme can resist the cutting attack.

3.3.3. Noise attack

The watermarked images are attacked by white Gaussian noise with a variance of 0.005 and salt-and-pepper noise with a density of 0.01, respectively, and then the corresponding watermark images are extracted from the watermarked images with noise. Figure 7 shows the watermarked images after being added noise, and the corresponding extracted watermark images. It can be seen that the information of the original watermark image can still be obtained from the extracted watermark image. Table 3 lists the corresponding NC values of the extracted watermark images. As is shown, the digital watermarking scheme has a certain ability to resist noise attack.

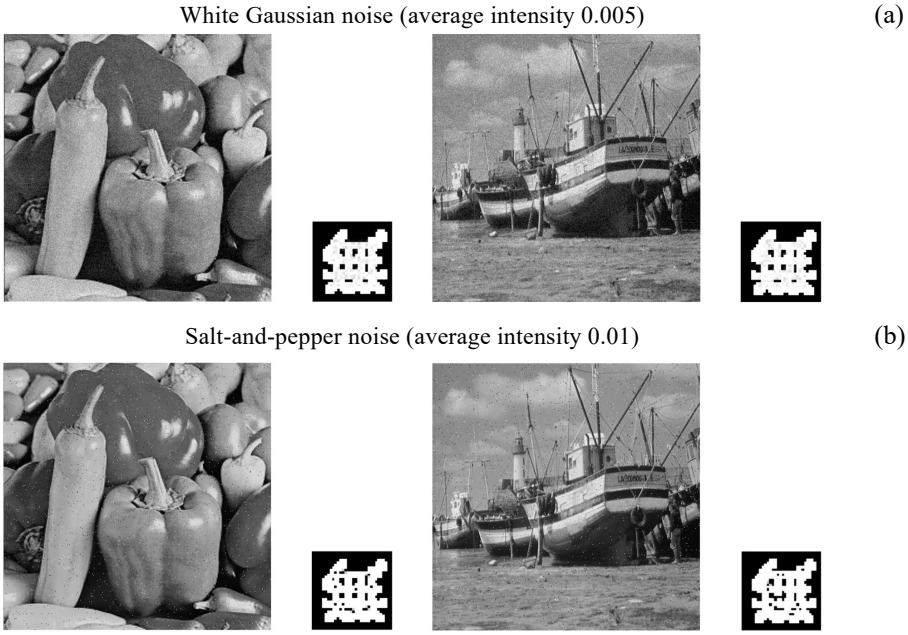


Fig. 7. Host image and corresponding extracted watermark after noise attack. (a) White Gaussian noise (average intensity 0.005). (b) Salt-and-pepper noise (average intensity 0.01).

T a b l e 3. NC values after noise attack.

Test image	White Gaussian noise (average intensity 0.005)	Salt-and-pepper noise (average intensity 0.01)
Peppers	0.9026	0.9532
Boat	0.8952	0.9610

3.3.4. JPEG compression attack

To test the ability of the proposed algorithm to resist the JPEG compression attack, the watermarked images are compressed with different compression ratios, and then the watermark images are extracted from the compressed images. Figure 8 shows the watermarked images and the corresponding extracted watermark image after compression. Figures 8(a)–(c) and (d)–(f) are the watermarked images after JPEG compression with a ratio of 30%, 60% and 90%, respectively. Figures 8(a1)–(f1) are the watermark images extracted from the corresponding images after JPEG compression. It can be seen that the original watermark information can still be obtained from the extracted

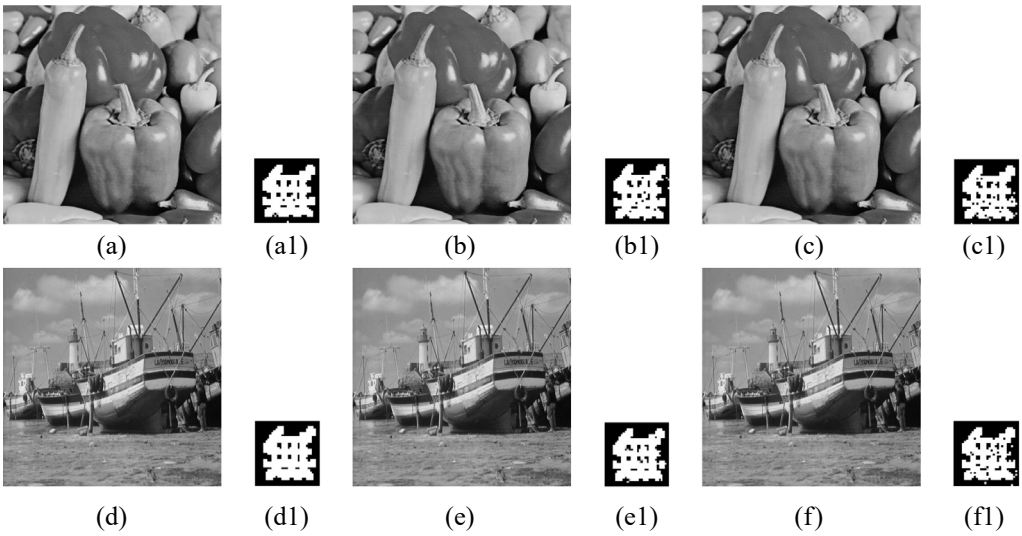


Fig. 8. Host image and corresponding extracted watermark after JPEG compression attack. (a)–(c) and (d)–(f) The watermarked images after JPEG compression with a ratio of 30%, 60% and 90%, respectively. (a1)–(f1) The watermark images extracted from the corresponding images after JPEG compression.

T a b l e 4. NC values after the JPEG compression attack.

Compression ratio	*Peppers*	*Boat*
30%	0.9959	0.9962
60%	0.9836	0.9877
90%	0.9754	0.9671

watermark after the JPEG compression attack. Table 4 lists the NC values of the watermark image extracted from the watermarked image after different degrees of compression. The NC values are all greater than 0.96, indicating that the extracted watermark is similar to the original watermark. It is obvious that the digital watermarking scheme can frustrate the JPEG compression attack.

3.3.5. Other attacks

In this section, the performances of the proposed watermarking scheme against some other typical image processing attacks are tested. Figure 9 shows the watermarked images and the corresponding extracted watermark images under various image processing attacks. Figures 9(a)–(e) are the test results of histogram equalization, image brightening, image darkening, contrast enhance and contrast weaken, respectively.

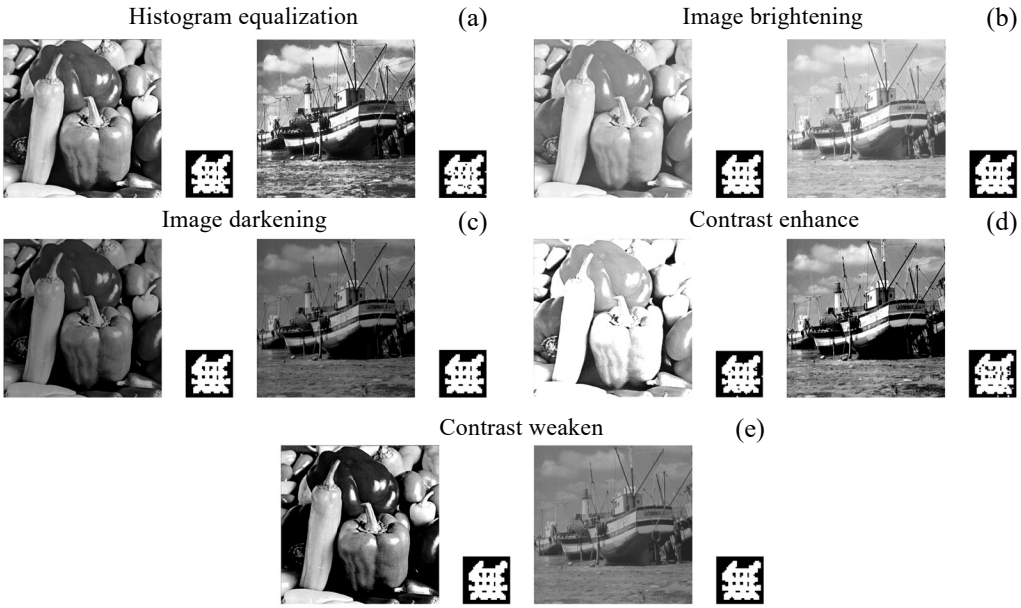


Fig. 9. Host image and corresponding extracted watermark after other attacks. (a) Histogram equalization, (b) image brightening, (c) image darkening, (d) contrast enhance, and (e) contrast weaken.

T a b l e 5. NC values of other attacks.

Attacks	*Peppers*	*Boat*
Histogram equalization	0.9856	0.9897
Image brightening	1	1
Image darkening	1	1
Contrast enhance	0.9825	0.9792
Contrast weaken	1	1

Table 5 presents the NC values of the watermark image extracted from the watermarked images under different attacks. The proposed digital watermarking scheme can resist the above attacks and has good robustness.

3.3.6. Position detection

To verify the tamper detection and positioning function of the proposed scheme, the watermarked image *Peppers* is selected to be tested three times. In the first test, the test image is cut square. In the second test, the test image is cut rectangular. In the third test, the Chinese character *Wang* is added to the test image. The results of the three tests are shown in Fig. 10. After different tampering of the watermarked image, the position and the pattern displayed in the location matrix are essentially identical. Thus, the proposed digital watermarking scheme has a strong positioning ability.

Fig. 10. Result of positioning detection.

3.4. Comparison

To further demonstrate the robustness of the proposed digital watermark scheme, the simulation result of image *Peppers* is listed in Table 6. In [8], the watermark information is embedded in the DCT low frequency sub-band, which significantly affects the visual quality of the host image. Therefore, the imperceptibility of this scheme is not satisfactory, and the PSNR value is relatively low. While in the proposed scheme, the watermark information is embedded in the low frequency (LF) coefficient of curvelet transform, which ensures the invisibility of the scheme, and the PSNR value is relatively high. The scheme in [14] performs well in resisting the salt-and-pepper noise attack. In [15], the watermark is constructed by modifying the maximal singular value of the singular value matrix. The maximal singular value of the image will change greatly in the case of image brightness and contrast gradient change. At this time, it is hard to

T a b l e 6. Normalized correlation coefficients with proposed algorithm and some typical works.

Attack	[8]	[14]	[15]	Proposed algorithm
None	0.9698	1	1	1
Salt-and-pepper noise attack (0.01)	0.9399	0.9986	0.9634	0.9630
JPEG compression (60%)	0.9601	0.8263	1	0.9856
Cutting attack 1/16	0.9449	0.9724	0.9736	0.9920
White Gaussian noise (0.005)	0.8963	0.8017	0.9543	0.8550
Histogram equalization	0.9663	0.9731	0.6165	0.9918
Image brightening	0.9698	0.9660	0.6393	1
Image darkening	0.9698	0.9787	0.6545	1
Contrast enhance	0.9454	0.9367	0.5341	0.9875
Contrast weaken	0.9698	0.9828	0.6047	1
PSNR (dB)	36.9	40.0	40.3	70.9

extract the watermark information with this scheme. Therefore, the digital watermarking scheme is robust enough.

3.5. Efficiency

The equipment parameters of this experiment are as follows: Inter(R) Core (TM) i5-6500 CPU@3.20GHz, 4GB RAM, simulation platform, *i.e.*, MATLAB 9.0.0.341360(R2016a). Host image *Peppers* of size 512×512 and watermark images of size 32×32 are employed in the simulation. The simulation results are listed in Table 7. Watermark encryption time and watermark decryption time are those required to scramble and reverse the watermark image with multiple chaotic maps, while watermark embedding time and watermark extraction time are those spent on performing the curvelet transform, embedding the scrambled watermark and corresponding reverse operation. It can be seen that the processing time of the digital watermarking scheme is acceptable.

T a b l e 7. Execution time (second).

Encryption time	Decryption time	Embedding time	Extraction time
13.1	12.8	6.1	6.5

4. Conclusion

A digital watermarking scheme is proposed based on the curvelet transform. To guarantee the security of watermark information, the watermark image is scrambled with multiple chaotic maps. And the curvelet transform is performed on the host image to obtain the LF coefficient matrix **C** and HF coefficient matrix **T**. Then the scrambled watermark image is embedded into the matrix **C** with the additive embedding rule, while the authentication watermark generated by chaotic sequence is embedded into

matrix **T** with the half division method. Finally, the host image with robust watermark and authentication watermark is obtained by the inverse curvelet transform. It is verified that the proposed watermarking scheme has good robustness, high security, and shares an accurate positioning function. Future works can make full use of machine learning or new encryption approach to achieve better performance [16, 17].

Acknowledgements
This work is supported by the National Natural Science Foundation of China (Grant No. 61861029).

References

[1] LYDIA E.L., RAJ J.S., SELVAM R.P., ELHOSENY M., SHANKAR K., *Application of discrete transforms with selective coefficients for blind image watermarking*, Transactions on Emerging Telecommunications Technologies **32**(2), 2021: e3771. https://doi.org/10.1002/ett.3771

[2] HAN D., ZHANG J., LIU Y., WU P., SUN Y., *Real-time feedback watermarking authentication scheme for streaming media*, Multimedia Tools and Applications **79**(17), 2020: 12699–12725. https://doi.org/10.1007/s11042-020-08646-7

[3] VAN SCHYNDEL R.G., TIRKEL A.Z., OSBORNE C.F., *A digital watermark*, [In] *Proceedings of 1st International Conference on Image Processing*, Vol. 2, IEEE, 1994: 86–90. https://doi.org/10.1109/ICIP.1994.413536

[4] 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: 30251–30267. https://doi.org/10.1007/s11042-018-6128-9

[5] ERNAWAN F., KABIR M.N., *A robust image watermarking technique with an optimal DCT-psychovisual threshold*, IEEE Access **6**, 2018: 20464–20480. https://doi.org/10.1109/ACCESS.2018.2819424

[6] 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: 22727–22747. https://doi.org/10.1007/s11042-020-08987-3

[7] HAMIDI M., EL HAZITI M., CHERIFI H., EL HASSOUNI M., *Hybrid blind robust image watermarking technique based on DFT-DCT and Arnold transform*, Multimedia Tools and Applications **77**(20), 2018: 27181–27214. https://doi.org/10.1007/s11042-018-5913-9

[8] LANG J., ZHANG Z.G., *Blind digital watermarking method in the fractional Fourier transform domain*, Optics and Lasers in Engineering **53**, 2014: 112–121. https://doi.org/10.1016/j.optlaseng.2013.08.021

[9] ERNAWAN F., ARIATMANTO D., FIRDAUS A., *An improved image watermarking by modifying selected DWT-DCT coefficients*, IEEE Access **9**, 2021: 45474–45485. https://doi.org/10.1109/ACCESS.2021.3067245

[10] GUL E., *A blind robust color image watermarking method based on discrete wavelet transform and discrete cosine transform using grayscale watermark image*, Concurrency and Computation: Practice and Experience **34**(22), 2022: e6884. https://doi.org/10.1002/cpe.6884

[11] AHMED R., RIAZ M.M., GHAFOOR A., *Attack resistant watermarking technique based on fast curvelet transform and robust principal component analysis*, Multimedia Tools and Applications **77**(8), 2018: 9443–9453. https://doi.org/10.1007/s11042-017-5128-5

[12] KIM W.H., NAM S.H., KANG J.H., LEE H.K., *Robust watermarking in curvelet domain for preserving cleanness of high-quality images*, Multimedia Tools and Applications **78**(12), 2019: 16887–16906. https://doi.org/10.1007/s11042-018-6879-3

[13] KUKREJA S., KASANA G., KASANA S.S., *Curvelet transform based robust copyright protection scheme for color images using extended visual cryptography*, Multimedia Tools and Applications **79**(35), 2020: 26155–26179. https://doi.org/10.1007/s11042-020-09130-y

[14] Bi H., Li X., Zhang Y., Xu Y., *A blind robust watermarking scheme based on CT and SVD*, [In] *IEEE 10th International Conference On Signal Processing Proceedings*, IEEE, 2010: 881–884. https://doi.org/10.1109/ICOSP.2010.5656038

[15] Su Q., Wang G., Zhang X., Lv G., Chen B., *A new algorithm of blind color image watermarking based on LU decomposition*, Multidimensional Systems and Signal Processing **29**(3), 2018: 1055–1074. https://doi.org/10.1007/s11045-017-0487-7

[16] Gong L.H., Luo H.X., *Dual color images watermarking scheme with geometric correction based on quaternion FOFMMs and LS-SVR*, Optics and Laser Technology, 2023. https://doi.org/10.1016/j.optlastec.2023.109665

[17] Zhou N.R., Tong L.J., Zou W.P., *Multi-image encryption scheme with quaternion discrete fractional Tchebyshev moment transform and cross-coupling operation*, Signal Processing **211**, 2023: 109107. https://doi.org/10.1016/j.sigpro.2023.109107

Received August 25, 2022
in revised form September 28, 2022