Multimedia Tools and Applications (2020) 79:30007–30021
https://doi.org/10.1007/s11042-020-09389-1

Blind watermarking scheme based on Schur decomposition and non-subsampled contourlet transform

Jing-You Li [1,2] · Chao-Zhu Zhang [1]

Received: 15 August 2019 / Revised: 14 June 2020 / Accepted: 21 July 2020 /
Published online: 13 August 2020

Abstract
An invisibility and blind watermarking algorithm based on Schur decomposition and non-subsampled contourlet transform is designed to protect copyright. The cover image is decomposed by the non-subsampled contourlet transform. And the low pass sub-band of the non-subsampled contourlet transform is divided into 8×8 non-overlapping blocks. Then each block is performed by the Schur decomposition and the watermark information is embedded by modifying the largest energy element in the Schur domain. Before embedding into the cover image, the original watermark is scrambled with logistic map and Arnold transform to ensure the security. Besides, a synchronization mechanism based on scale invariant feature transform is designed for resisting geometrical attacks. The proposed watermarking algorithm is evaluated with structural similarity index, peak signal to noise ratio and bit error rate. Experimental results demonstrate that the proposed watermarking scheme performs better in terms of invisibility, robustness and payload than other similar schemes.

Keywords Blind watermarking scheme · Schur decomposition · Non-subsampled contourlet transform · Logistic map · Arnold transform

1 Introduction

With the fast development of digital products, a series of urgent security issues such as the illegal copying and distortion of private information have been deeply concerned [17, 20, 41, 43]. Digital

✉ Jing-You Li
lijingyou99@163.com

Chao-Zhu Zhang
zhangchaozhu@hrbeu.edu.cn

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

[2] School of Communication & Electronic Engineering, Qiqihar University, Qiqihar 161006, China

watermarking is considered as an effective solution to these security issues [16, 25]. Generally, digital watermarking is achieved by embedding the private information into the host image [12, 14]. Invisibility, robustness, security and payload are necessary for an excellent watermarking scheme [2, 13, 26, 35]. The invisibility in a watermarking algorithm refers to the cover image and the watermarked one should be similar enough to avoid being noticed. And the robustness of watermarks indicates that the watermark algorithm is able to resist against common attacks, such as JPEG compression, noise attacks and geometric attacks, etc. The security means that watermark extraction in a watermarking scheme relies on the secret key. The payload implies that the total amount of information can be hidden into the cover image. Generally, digital watermarking can be implemented in frequency domain and spatial domain [27, 39]. The watermarking schemes in the spatial domain generally embed the watermark by altering a set of pixel values of the cover image directly [3]. This kind of spatial domain watermarking algorithm with low complexity is easy to implement but fragile to most common attacks, for example JPEG compression and filtering. While the kind of frequency domain watermarking technique is achieved by modulating the frequency coefficients of the cover image, which can increase the invisibility and robustness [42]. The most popular watermarking techniques in the frequency domain are mainly based on mathematical transforms, such as discrete cosine transform (DCT) [5, 8], discrete Fourier transform (DFT) [4, 19, 34], discrete wavelet transform (DWT) [1, 22, 38] and contourlet transform (CT) [9, 10]. Because of marvelous spatial localization and multi-resolution characteristics of the discrete wavelet transform, the DWT is widely applied in the field of digital watermarking algorithms. Singh D et al. investigated a robust watermarking algorithm based on DWT-SVD and DCT, where watermark encoding is realized by the Arnold cat map [33]. Kang X B et al. proposed a robust and invisible blind watermarking technique by fusing DCT and SVD in the DWT domain, where the embedding strength is selected by the least-square curve fitting [15]. Contourlet transform makes up the directional limitation over wavelet transform and provides a multi-scale and multi-directional representation for high dimension signal with smooth contours [37]. Sadreazami H et al. designed a novel multiplicative watermarking scheme with the univariate and bivariate alpha-stable distributions in the contourlet transform domain [31]. Chen L et al. proposed a new blind image watermarking scheme based on CT and principal component analysis, which is robust to geometric attacks and compressions [6]. As an expansion of the traditional contourlet transform, the non-subsampled contourlet transform (NSCT) can effectively represent high dimension signal with more directional information. Niu P P et al. presented a non-blind watermarking algorithm by combining support vector regression with non-subsampled contourlet transform for color image to resist geometric distortions [28]. However, most of the above-mentioned schemes in the frequency domain embed a binary logo of size 32×32 into a 512×512 gray-scale image, thereby leading to low payload of the watermarking, unsatisfactory or imperfect robustness and invisibility. Especially, the security of the watermark is ignored in some watermarking schemes. To further simultaneously increase the performance of payload, robustness, invisibility and security, a new blind watermarking algorithm is presented by combining non-subsampled contourlet transform with Schur decomposition. To enhance the security, the original watermark is pre-scrambled by logistic chaotic map and Arnold transform. To reconstruct the watermarked image more efficiently and enhance the hiding capacity, the cover image is decomposed by the two level non-subsampled contourlet transform. And the largest energy element of upper triangular Schur matrix is modified to embed the encrypted watermark sequence with a quantification technique. Then the invisibility of watermarked image is guaranteed by modifying only one element. Moreover, the performance of resisting geometrical attacks is improved by SIFT.

The style of this paper is organized as follows. The related fundamental theories are given in Section 2. The processes of watermark encryption, watermark embedding and watermark

decryption are introduced in Section 3. And the simulation results are discussed in Section 4. Finally, a short conclusion is drawn in Section 5.

2 Fundamental theories

2.1 Non-subsampled contourlet transform

Non-subsampled contourlet transform is an improvement over contourlet transform, which efficiently represents typical image with more directional information, including edges and smooth contours [7]. Besides, the non-subsampled contourlet transform is a redundant transform that can increase the capacity of the watermarking system. Usually, the non-subsampled contourlet transform is constructed in two stages: non-subsampled pyramid (NSP) and non-subsampled direction filter banks (NSDFB) [40]. Firstly, the NSP is used to ensure multi-scale property. Then NSDFB provide the directionality of the non-subsampled contourlet transform.

2.2 Schur decomposition

The Schur decomposition is an intermediate step of the singular value decomposition (SVD), which plays a very important role in mathematical linear algebra [18, 30]. The Schur decomposition of a real matrix Y is defined as

$$\mathrm{Y} = \mathrm{U} \times \mathrm{S} \times \mathrm{U}^{T}, \tag{1}$$

where the superscript T indicates the matrix transposition operation, and U and S are unitary matrix and upper triangular matrix, respectively.

Comparing with the SVD, the Schur decomposition has low computational complexity, which guarantees its successful applications in the field of digital watermarking. According to Table 1, the Schur decomposition only cost less than 1/3 of computing resources in comparison with SVD. Besides, the upper triangular matrix S has good stability. In this regard, the robustness can be improved when embedding the watermark into the matrix S. To guarantee the invisibility, the watermark information is embedded into the upper triangular matrix S with an optimal quantification in this paper.

2.3 Arnold transform and logistic map

The security of the proposed watermarking scheme is ensured by logistic chaotic map and Arnold transform [29, 32]. The Arnold transform is defined as

$$\begin{bmatrix} m' \\ n' \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} m \\ n \end{bmatrix} (\mathrm{mod} N), \tag{2}$$

Table 1 Time complexity for different matrix factorization techniques

Matrix factorization	Time complexity
Singular value decomposition	$O(11N^3)$
Schur decomposition	$O(8N^3/3)$

where a and b represent two positive numbers, N is the order of watermark and (m, n) denotes the pixel point.

Logistic chaotic map is defined as

$$g_{n+1} = \mu g_n(1-g_n), g_n \in (0, 1). \tag{3}$$

The bifurcation diagram of logistic chaotic map is shown in Fig. 1. It can be seen in it, the logistic map becomes chaotic when $\mu \in [3.57, 4]$.

In this paper, a chaotic sequence generated from Eq. (3) is converted to a binary sequence for watermark encryption. And three binary logos with different sizes are selected as test watermarks. Each of them is pre-scrambled by Arnold transform and logistic map. The encrypted watermarks are shown in Fig. 2 (a1)-(c1).

2.4 Scale invariant feature transform

To make up the weakness in resisting geometrical attack of traditional watermarking schemes, a synchronization mechanism based on the scale invariant feature transform (SIFT) is presented. SIFT is used to extract the distinctive features from typical images, which can be invariant to image scale and rotation [24]. The major stages of SIFT are listed as follows.

Step1 Scale-space extrema detection: The difference of Gaussian function (DOG) is used to identify the potential interest points that are invariant to scale and orientation.

Step2 Keypoint localization: In this stage, the detailed models at each candidate location are built to determine location and scale. And the keypoints are selected by measuring their stability.

Step3 Orientation assignment: One or more orientations are assigned to each keypoint location according to local image gradient directions. Besides, all future operations are

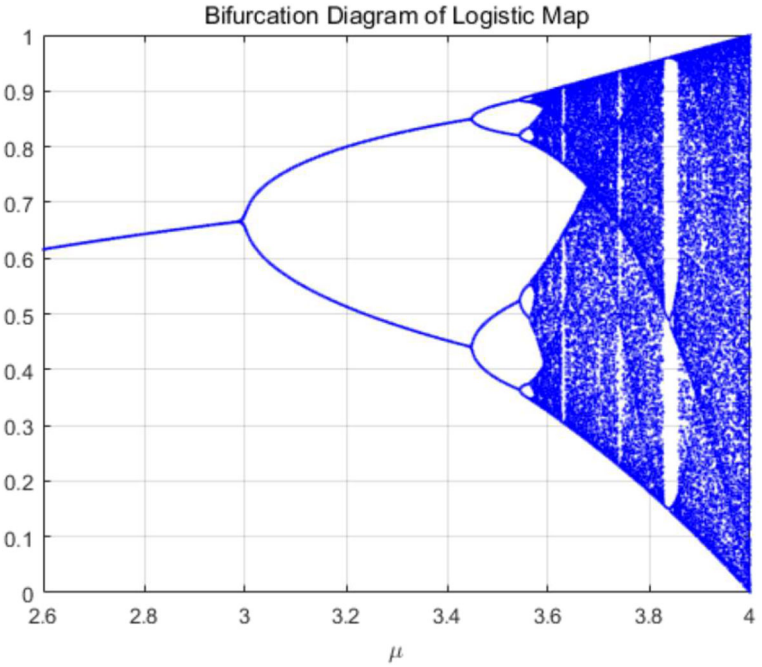


Fig. 1 The bifurcation diagram of logistic chaotic map

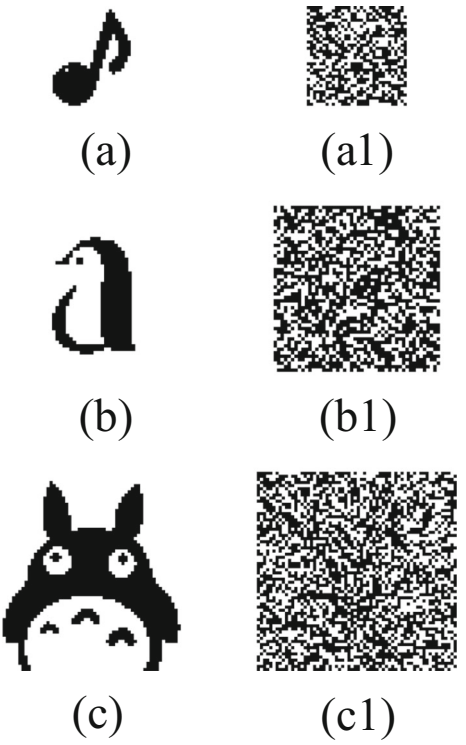


Fig. 2 Binary watermarks and their corresponding encrypted watermarks of difference sizes: (**a**) Watermark A of size 32 × 32; (**b**) Watermark B of size 48 × 48; (**c**) Watermark C of size 64 × 64; (a1) Scrambled image for watermark A; (b1) Scrambled image for watermark B; (c1) Scrambled image for watermark C

executed after transforming relative to the assigned orientation, scale and location for each feature, which can provide the invariance to these transformations.

Step4 Keypoint descriptor: The local image gradients are measured at the selected scale in the region around each keypoint.

Figure 3 shows the results of SIFT.

In this paper, the SIFT is applied to design a synchronization mechanism. Firstly, the keypoints in watermarked image and the attacked one are extracted and matched. Any two keypoints in watermarked image are connected for constructing directional vector D_1. The corresponding two keypoints in the attacked image are connected for constructing vector D_2. Let $D_1 = \overrightarrow{(x_1, y_1)}$ and $D_2 = \overrightarrow{(x_2, y_2)}$. Then the geometrical distortion parameters are obtained as follows.

(a) SIFT for scaling (b) SIFT for rotation and scaling

Fig. 3 Keypoints matching with SIFT algorithm

(1) The measured scale parameter *Ms* is generated by computing the scale radio of two directional vectors.

$$Ms = \frac{\sqrt{{x_1}^2 + {y_1}^2}}{\sqrt{{x_2}^2 + {y_2}^2}} \tag{4}$$

2 The measured rotation parameter *Mr* is obtained by calculating the angle of two vectors.

$$Mr = arccos \frac{x_1 x_2 + y_1 y_2}{\sqrt{{x_1}^2 + {y_1}^2}\sqrt{{x_2}^2 + {y_2}^2}} \tag{5}$$

3 Blind watermarking algorithm

The presented watermarking algorithm consists of watermark encryption, watermark embedding, watermark extraction and watermark decryption. The detailed procedures of the proposed watermarking method are described as follows and shown in Figs. 4 and 5.

3.1 Watermark encryption

Before embedding the watermark into the cover image, the original watermark is scrambled with Arnold transform and logistic map, respectively.

Step 1 By applying the Arnold transform on the original watermark W of size $N \times N$, the scrambled watermark image W* is generated.

Step 2 The scrambled watermark image W* is then converted into a binary sequence W_o^* of size $1 \times N^2$. Then the encrypted watermark sequence W_e is generated as

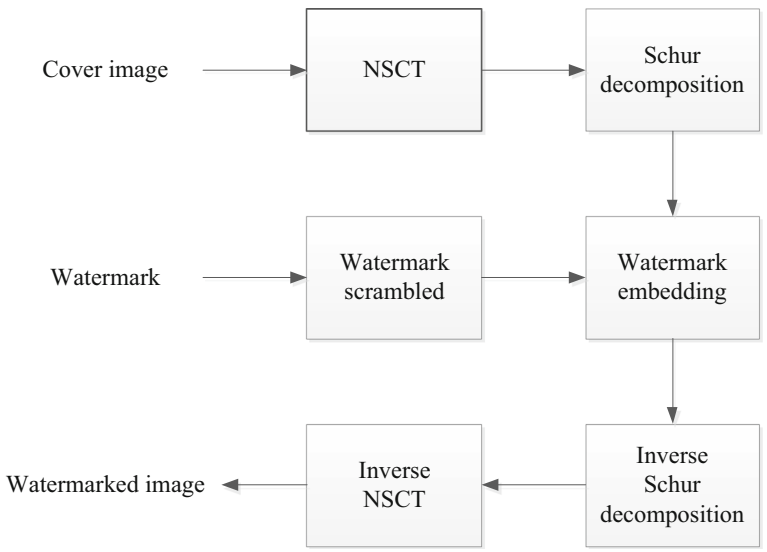


Fig. 4 Watermark embedding process

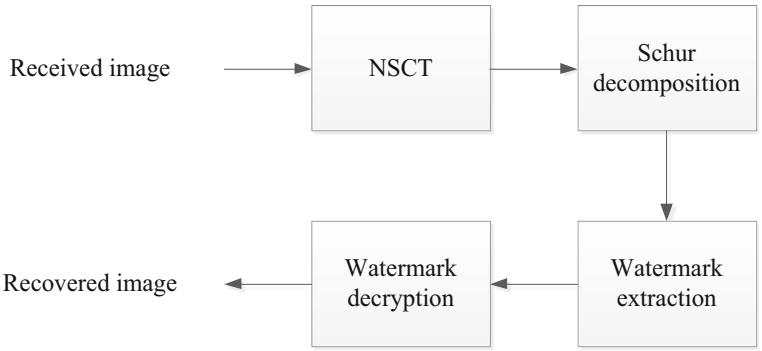


Fig. 5 Watermark extraction stage

$$W_e = W_o^* \oplus LB \tag{6}$$

where $\oplus$ is the XOR operation and LB is a binary sequence generated from Eq. (3).

3.2 Watermark embedding

Step 1 The cover image I is decomposed with a two-level non-subsampled contourlet transform to obtain a low pass sub-band and five directional sub-bands. To guarantee the robustness of the watermark, the low pass sub-band of non-subsampled contourlet transform is selected for watermark insertion.

Step 2 The low pass sub-band L of the non-subsampled contourlet transform is divided into some 8×8 non-overlapping blocks $B_i (i = 1, 2, \ldots, N)$.

Step 3 For each block

1 By applying the Schur decomposition on the non-overlapping block and the maximal value x in the upper triangular matrix is extracted.

$$[U, S] = \mathrm{Schur}(B) \tag{7}$$

$$x = S(1, 1) \tag{8}$$

where U and S are the results of Schur decomposition.

2 The encrypted watermark sequence is embedded by modifying the value of x as follows.

$$x' = \begin{cases} x - \lambda + \frac{1}{4}\sigma, W_e = 0 \& \lambda \in \left[0, \frac{3}{4}\sigma\right); \\ x - \lambda + \frac{5}{4}\sigma, \ W_e = 0 \& \lambda \in \left[\frac{3}{4}\sigma, \sigma\right); \\ x - \lambda - \frac{1}{4}\sigma, \ W_e = 1 \& \lambda \in \left[0, \frac{1}{4}\sigma\right); \\ x - \lambda + \frac{3}{4}\sigma, \ W_e = 1 \& \lambda \in \left[\frac{1}{4}\sigma, \frac{3}{4}\sigma\right). \end{cases} \tag{9}$$

In Eq. (9), x' is the modified value in the upper triangular matrix S, σ indicates quantification step and $\lambda = \mathrm{mod}\,(x, \sigma)$.

3 The modified matrix S^* is generated by replacing the largest energy element with x'.

$$S^*(1,1) = x'. \tag{10}$$

4 The altered coefficients block B^* is obtained by the inverse Schur decomposition.

$$B^* = US^*U'. \tag{11}$$

By repeating Step 3, the encrypted watermark sequence can be embedded into the low pass sub-band of the non-subsampled contourlet transform.

Step 4 The watermarked image I^* is obtained by the inverse non-subsampled contourlet transform.

3.3 Watermark extraction

Step 1 Two-level non-subsampled contourlet transform is applied on the received image I^*.

Step 2 The low pass sub-band of non-subsampled contourlet transform is segmented into some non-overlapping blocks.

Step 3 For each block:

1 The upper triangular matrix S^Δ is obtained by the Schur decomposition and its maximal value is extracted.

$$x^* = S^\Delta(1,1). \tag{12}$$

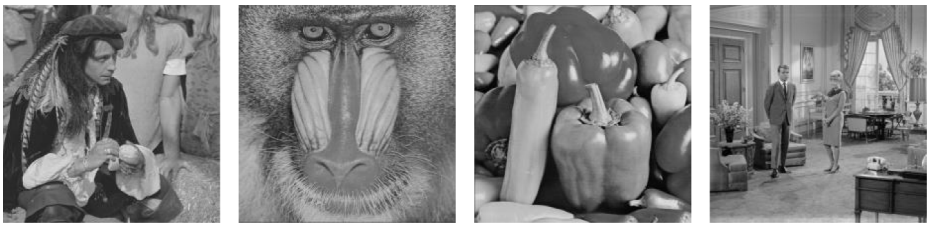
2 The encrypted watermark bit W_e' is extracted as follows. Suppose $\lambda^* = \mathrm{mod}\,(x^*, \sigma)$. If $\lambda^* < \frac{1}{2}\sigma$, then $W_e' = 0$. If $\lambda^* \geq \frac{1}{2}\sigma$, then $W_e' = 1$.

The encrypted watermark sequence W' can be extracted by repeating Step 3.

3.4 Watermark decryption

The watermark decryption is the inverse process of watermark encryption. Firstly, the XOR operation is applied on the extracted watermark sequence W' with a binary sequence LB.

$$W_d = W' \oplus LB. \tag{13}$$



(a) Man (b) Baboon (c) Peppers (d) Couple

Fig. 6 Cover images of size 512 × 512

Then the decrypted watermark W_d is reshaped and converted by Arnold transform to generate the recovered watermark image W_r of size $N \times N$.

4 Experiment results and analyses

To evaluate the performance of the presented watermarking algorithm, four gray images of size 512 × 512 are selected as test cover images, as shown in Fig. 6, i.e., 'Man', 'Baboon', 'Peppers' and 'Couple'. And three binary logos of different sizes shown in Fig. 2 (a)-(c) are chosen as the test watermarks. The parameters a, b, μ and g_0 in the watermark encryption stage are set as 1, 1, 3.611 and 0.5152, respectively. The quantification step is 70.

4.1 Invisibility analysis

Peak signal to noise ratio (PSNR) [23] and structural similarity index (SSIM) [11] are adopted to evaluate the invisibility of the proposed blind watermarking scheme. SSIM can measure the similarity of two images with same size.

$$\mathrm{SSIM}\left(\mathrm{I}, \mathrm{I}^{*}\right) = \frac{2\mu_{\mathrm{I}}\mu_{\mathrm{I}^{*}} + p_1}{\mu_{\mathrm{I}^{*}}^2 + \mu_{\mathrm{I}}^2 + p_1} \times \frac{2\sigma_{\mathrm{I}^{*}\mathrm{I}} + p_2}{\sigma_{\mathrm{I}^{*}}^2 \sigma_{\mathrm{I}}^2 + p_2} \tag{14}$$

where I and I* are original cover image and watermarked one, respectively; μ_{I} and $\mu_{\mathrm{I}^{*}}$ are the mean values of I and I*, respectively. The definition of PSNR is

(a) Man (b) Baboon (c) Peppers (d) Couple

Fig. 7 Results of four test images for embedding watermark A

Table 2 The invisibility of the presented watermarking scheme without attack

Cover image	Watermark A		Watermark B		Watermark C	
	PSNR (dB)	SSIM	PSNR (dB)	SSIM	PSNR (dB)	SSIM
Man	47.38	0.9954	43.50	0.9922	40.96	0.9878
Baboon	46.68	0.9962	43.18	0.9934	40.62	0.9906
Peppers	46.84	0.9928	43.14	0.9867	40.86	0.9816
Couple	46.84	0.9959	43.22	0.9920	40.73	0.9875
Mean	46.94	0.9951	43.26	0.9911	40.79	0.9869

$$\mathrm{PSNR} = 20\log\frac{255}{\sqrt{\mathrm{MSE}}} \tag{15}$$

$$\mathrm{MSE} = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\left[f(i,j) - \widehat{f}\left(i,j\right)\right]^2. \tag{16}$$

where f and $\widehat{f}$ denote original cover image and watermarked one of size $M \times N$. (i,j) represents the pixel position.

The result of the proposed watermarking method for embedding watermark A is shown in Fig. 7. And the PSNR and the SSIM values are compiled in Table 2. From Fig. 7, it can be

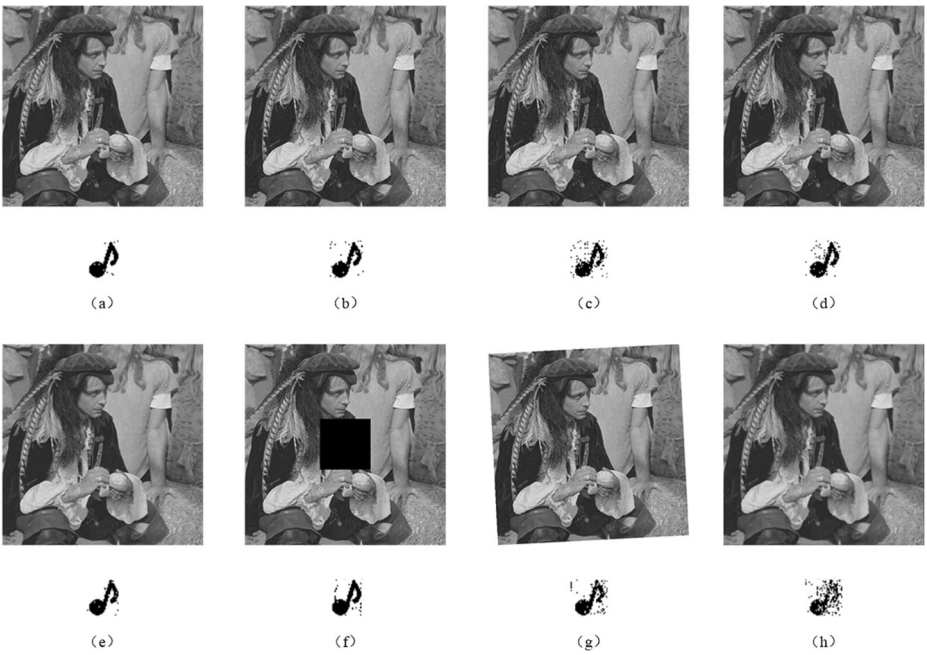


Fig. 8 The watermarked images under different attacks and their corresponding extracted watermarks: (**a**) JPEG compression (30%); (**b**) Gaussian noise 0.001; (**c**) Salt and Pepper noise 0.005; (**d**) Multiplicative noise 0.005; (**e**) Median filtering 3 × 3; (**f**) Cropping 1/16; (**g**) Rotation 3°; (**h**) Low pass filtering

Table 3 Experimental results under different attacks

Attacks	PSNR (dB)	BER
JPEG compression (30%)	31.84	0.0098
Gaussian noise (0.001)	30.36	0.0234
Salt and Pepper noise (0.005)	28.94	0.0742
Multiplicative noise (0.005)	29.33	0.0527
Median filtering 3×3	32.12	0.0127
Cropping 1/16	19.66	0.0313
Rotation 3^o	25.78	0.0541
Low pass filtering	27.90	0.1523

seen that there are no obvious differences between original cover images and watermarked ones. Besides, the corresponding watermarks can be recovered completely without attack.

As can be seen in Table 1, the average value of PSNR is larger than 40 dB and the SSIM is close to 1 even if a watermark of size 64×64 is embedded. And the PSNR value is larger than 46 dB for embedding a 32×32 watermark, which signifies the high invisibility of the watermarking algorithm since only one element of the upper triangular Schur matrix is modified during the watermark embedding.

4.2 Robustness analysis

The bit error rate (BER) is employed to show the performance of robustness. Figure 8 gives the results under various attacks and the bit error rate values are given in Table 3. As can be seen in Fig. 8, the recovered original watermark logo appears slight distortion under various attacks, which indicates the robustness of the proposed watermarking algorithm is acceptable.

To resist the geometrical attacks, a synchronization mechanism with SIFT is offered. The distortion parameters are measured and the attacked image is corrected according the measured parameters. Table 4 lists the measured geometric distortion parameters. The performance of resisting geometrical attacks is given in Fig. 9 and Table 5. It is shown that the measured parameters are closer to the actual values and the extracted watermark is clearly visible.

According to Table 6, the BER values under most of attacks are below than 0.1. In another word, the proposed blind watermarking scheme is robust for most common attacks as the low pass sub-band of the non-subsampled contourlet transform is selected for embedding watermark. Particularly, the original watermark can be extracted completely when suffering from JPEG compression (50%). And the performance for resisting Median filtering and Rotation is great.

Table 4 The measured parameters by SIFT

Attack	Man	Baboon	Peppers	Couple
	The measured parameter			
Scaling 0.8	0.8004	0.7982	0.8010	0.7990
Scaling 0.5	0.4989	0.5012	0.4991	0.4985
Rotating 5^o	4.97	5.02	4.94	4.99
Rotating 10^o	10.07	10.08	9.98	9.99

Fig. 9 Results of geometrical attacks: (**a**)-(**d**) Performances of resisting scaling (0.8); (**e**)-(**h**) Performance of resisting rotation (10^o)

4.3 Comparison

To verify the performance of the proposed blind watermarking scheme, comparative experiments with the typical algorithms [15, 21, 36] are executed. A binary logo of size 32×32 is selected as a test original watermark and a gray image of size 512×512 is chosen as a test cover image. The results are compared in Table 7. From Table 3, the BER values under most attacks are smaller than those with other algorithms, which means the robustness of the proposed watermarking scheme is better. And the presented watermarking method also performs better in terms of invisibility, since the PSNR is up to 47.38 dB. In [15], the low frequency sub-band of cover image in the DWT domain was selected for watermark insertion to guarantee the robustness, however a significant distortion of the watermarked image is inevitable since a multiplicative method is employed in the watermark insertion stage. The blind watermarking scheme based on quaternion singular value decomposition was presented to balance the transparency and the robustness with two threshold values [21], and it performs well in terms of invisibility but poor for filtering. Su Q T et al. designed a new color image

Table 5 Results for geometrical attacks

Attack	Man BER	Baboon	Peppers	Couple
Scaling 0.8	0.0664	0.1709	0.0361	0.1484
Scaling 0.5	0.1670	0.2412	0.1025	0.2617
Rotating 5^o	0.0703	0.0625	0.1006	0.1045
Rotating 10^o	0.1035	0.1641	0.0928	0.1797

Table 6 Experimental results under different attacks for embedding watermark A

Attacks	Parameter	Man BER	Baboon BER	Peppers BER	Couple BER
No attack	/	0	0	0	0
JPEG compression	70	0	0	0	0
	50	0	0	0	0
	30	0.0098	0.0029	0.0127	0.0215
Gaussian noise	0.001	0.0234	0.0127	0.0215	0.0195
	0.002	0.0977	0.0615	0.0869	0.0986
Salt and Pepper noise	0.005	0.0742	0.0654	0.0684	0.0703
	0.01	0.1621	0.1172	0.1338	0.1514
Multiplicative noise	0.005	0.0527	0.0693	0.0723	0.0537
	0.01	0.1289	0.1699	0.1543	0.1289
Median filtering	3 × 3	0.0127	0.0537	0.0001	0.0420
	5 × 5	0.0469	0.1123	0.0088	0.1064
Cropping	1/8	0.1211	0.0918	0.0654	0.1299
	1/16	0.0313	0.0454	0.0283	0.0215
Rotation	5°	0.0703	0.0625	0.1006	0.1045
Low pass filtering	/	0.1523	0.1846	0.0791	0.2422

watermarking algorithm based on the LU decomposition [36], which is good at resisting Salt and Pepper noise but is not robust for rotation and filtering attacks. Obviously, the proposed blind watermarking scheme is superior in terms of invisibility and robustness under most common attacks. In addition, the watermarking schemes in [15, 21] both embed a binary logo of size 32 × 32 into a 512 × 512 gray-scale image, thus the payload of these methods is 1024 bits, while the proposed blind watermarking method can embed a binary watermark of size 64 × 64 when the host gray images are same.

Bold data represents the better performance in terms of robustness; '-' indicates the watermark unable to be extracted.

Table 7 Comparison results among four watermarking schemes

Attacks	Parameter	Ref [15] BER	Ref [21] BER	Ref [36] BER	Presented BER
No attack	/	0	0	0	0
JPEG compression	70	0.0381	0.0859	0.2813	0
	50	0.0664	0.2148	0.3721	0
	30	0.1152	0.3281	0.4697	**0.0098**
Gaussian noise	0.001	0.1396	0.0645	0.2363	**0.0234**
	0.002	0.1934	0.1338	0.2588	**0.0977**
Salt and Pepper noise	0.005	0.1182	0.0420	0.0039	0.0742
	0.01	0.1943	0.0723	0.0098	0.1621
Multiplicative noise	0.005	0.1504	0.0566	0.2569	**0.0527**
	0.01	0.1855	0.1172	0.2939	**0.1133**
Median filtering	3 × 3	0.1162	0.4570	0.5576	**0.0127**
	5 × 5	0.2900	0.4746	0.5664	**0.0469**
Cropping	1/8	0.1250	0.0313	0.0947	0.1211
	1/16	0.0410	0.0205	0.0449	0.0313
Rotation	3°	–	–	–	**0.0541**
	5°	–	–	–	**0.0703**
Low pass filtering	/	0.2451	0.3262	0.4268	**0.1523**
PSNR (dB)		43.53	46.52	45.83	47.38
SSIM		0.9942	0.9977	0.9693	0.9954

5 Conclusions

Based on non-subsampled contourlet transform and Schur decomposition, a secure and blind watermarking algorithm is presented in this work. The cover image is decomposed with the two-level non-subsampled contourlet transform and its low pass sub-band is selected as watermark insertion to enhance the robustness. Before embedding into the cover image, the original watermark is scrambled with logistic chaotic and Arnold transform to provide an extra level of security. And the invisibility is ensured with a quantification technique. In the watermark extraction stage, the encrypted watermark sequence can be recovered without the host image. Experimental results demonstrate the proposed blind watermarking scheme is superior in terms of invisibility, robustness and payload in comparison with some typical watermarking algorithms. However, the performance against scaling and low pass filtering can be improved further.

Acknowledgements 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 nos. 12531767 and 12541872).

References

1. Abdulrahman AK, Ozturk S (2019) A novel hybrid DCT and DWT based robust watermarking algorithm for color images [J]. Multimed Tools Appl 78(12):17027–17049
2. Ahmaderaghi B, Kurugollu F, Del Rincon JM et al (2018) Blind image watermark detection algorithm based on discrete shearlet transform using statistical decision theory [J]. IEEE Transactions on Computational Imaging 4(1):46–59
3. Cancellaro M, Battisti F, Carli M et al (2011) A commutative digital image watermarking and encryption method in the tree structured Haar transform domain [J]. Signal Process Image Commun 26(1):1–12
4. Cedillo-Hernandez M, Garcia-Ugalde F, Nakano-Miyatake M, Perez-Meana H (2015) Robust watermarking method in DFT domain for effective management of medical imaging [J]. SIViP 9(5): 1163–1178
5. Chang TJ, Pan IH, Huang PS, Hu CH (2019) A robust DCT-2DLDA watermark for color images [J]. Multimed Tools Appl 78(7):9169–9191
6. Chen L, Zhao JY (2018) Contourlet-based image and video watermarking robust to geometric attacks and compressions [J]. Multimed Tools Appl 77(6):7187–7204
7. Da Cunha AL, Zhou J, Do MN (2006) The nonsubsampled contourlet transform: theory, design, and applications [J]. IEEE Trans Image Process 15(10):3089–3101
8. Ernawan F, Kabir MN (2018) A robust image watermarking technique with an optimal DCT-psychovisual threshold [J]. IEEE Access 6:20464–20480
9. Etemad S, Amirmazlaghani M (2018) A new multiplicative watermark detector in the contourlet domain using t location-scale distribution [J]. Pattern Recogn 77:99–112
10. Fan D, Wang Y, Zhu CW (2019) A blind watermarking algorithm based on adaptive quantization in Contourlet domain [J]. Multimed Tools Appl 78(7):8981–8995
11. Guo Y, Li BZ (2016) Blind image watermarking method based on linear canonical wavelet transform and QR decomposition [J]. IET Image Process 10(10):773–786
12. Horng S, Farfoura ME, Fan P et al (2014) A low cost fragile watermarking scheme in H.264/AVC compressed domain [J]. Multimed Tools Appl 72(3):2469–2495
13. Horng S, Rosiyadi D, Fan P et al (2014) An adaptive watermarking scheme for e-government document images [J]. Multimed Tools Appl 72(3):3085–3103
14. Horng S, Rosiyadi D, Li T et al (2013) A blind image copyright protection scheme for e-government [J]. J Vis Commun Image Represent 24(7):1099–1105
15. Kang XB, Zhao F, Lin GF, Chen YJ (2018) A novel hybrid of DCT and SVD in DWT domain for robust and invisible blind image watermarking with optimal embedding strength [J]. Multimed Tools Appl 77(11): 13197–13224

16. Khalifa A, Hamad S (2012) A robust non-blind algorithm for watermarking color images using multi-resolution wavelet decomposition [J]. Int J Comput Appl 37(8):33–39
17. Lai CC, Tsai CC (2010) Digital image watermarking using discrete wavelet transform and singular value decomposition [J]. IEEE Trans Instrum Meas 59(11):3060–3063
18. Li JZ, Yu CY, Gupta BB et al (2018) Color image watermarking scheme based on quaternion Hadamard transform and Schur decomposition [J]. Multimed Tools Appl 77(4):4545–4561
19. Liao X, Li K, Yin J (2017) Separable data hiding in encrypted image based on compressive sensing and discrete fourier transform [J]. Multimed Tools Appl 76(20):20739–20753
20. Liao X, Qin Z, Ding L (2017) Data embedding in digital images using critical functions [J]. Signal Process Image Commun 58:146–156
21. Liu F, Ma LH, Liu C, Lu ZM (2018) Optimal blind watermarking for color images based on the U matrix of quaternion singular value decomposition [J]. Multimed Tools Appl 77(18):23483–23500
22. Liu Y, Tang SY, Liu R et al (2018) Secure and robust digital image watermarking scheme using logistic and RSA encryption [J]. Expert Syst Appl 97:95–105
23. Liu H, Xiao D, Zhang R et al (2016) Robust and hierarchical watermarking of encrypted images based on compressive sensing [J]. Signal Process Image Commun 45:41–51
24. Lowe D (2004) Distinctive image features from scale-invariant keypoints. Int J Comput Vis 60(2):91–110
25. Luo AW, Gong LH, Zhou NR, Zou WP (2020) Adaptive and blind watermarking scheme based on optimal SVD blocks selection [J]. Multimed Tools Appl 79(1–2):243–261
26. Makbol NM, Khoo BE, Rassem TH (2016) Block-based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics [J]. IET Image Process 10(1):34–52
27. Mittal A, Moorthy AK, Bovik AC (2012) No-reference image quality assessment in the spatial domain [J]. IEEE Trans Image Process 21(12):4695–4708
28. Niu PP, Wang XY, Yang YP, Lu MY (2011) A novel color image watermarking scheme in nonsampled contourlet-domain [J]. Expert Syst Appl 38(3):2081–2098
29. Parah SA, Loan NA, Shah AA, Sheikh JA, Bhat GM (2018) A new secure and robust watermarking technique based on logistic map and modification of DC coefficient [J]. Nonlinear Dynamics 93(4):1933–1951
30. Rosiyadi D, Horng S, Lestriandoko NH, et al. (2015) A resistant digital image watermarking scheme based on masking model [C]. International Carnahan Conference on Security Technology, 1–4.
31. Sadreazami H, Ahmad MO, Swamy MNS (2014) A study of multiplicative watermark detection in the contourlet domain using alpha-stable distributions [J]. IEEE Trans Image Process 23(10):4348–4360
32. Shehab A, Elhoseny M, Muhammad K, Sangaiah AK, Yang P, Huang H, Hou G (2018) Secure and robust fragile watermarking scheme for medical images [J]. IEEE Access 6:10269–10278
33. Singh D, Singh SK (2017) DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection [J]. Multimed Tools Appl 76(11):13001–13024
34. Solachidis V, Pitas L (2001) Circularly symmetric watermark embedding in 2-D DFT domain [J]. IEEE Trans Image Process 10(11):1741–1753
35. Su QT, Liu DC, Yuan ZH et al (2019) New rapid and robust color image watermarking technique in spatial domain [J]. IEEE Access 7:30398–30409
36. Su QT, Wang G, Zhang XF et al (2018) A new algorithm of blind color image watermarking based on LU decomposition [J]. Multidim Syst Sign Process 29(3):1055–1074
37. Sun SL, Guo YN (2015) A novel image steganography based on contourlet transform and hill cipher. [J]. Journal of Information Hiding and Multimedia Signal Processing 6(5):889–897
38. Thakkar FN, Srivastava VK (2017) A blind medical image watermarking: DWT-SVD based robust and secure approach for telemedicine applications [J]. Multimed Tools Appl 76(3):3669–3697
39. Verma VS, Jha RK, Ojha A (2015) Significant region based robust watermarking scheme in lifting wavelet transform domain [J]. Expert Syst Appl 42(21):8184–8197
40. Zhang QY, Yang Z, Dou QY et al (2017) Robust hashing for color image authentication using non-subsampled contourlet transform features and salient features [J]. Journal of Information Hiding and Multimedia Signal Processing 8(5):1029–1042
41. Zhou NR, Luo AW, Zou WP (2019) Secure and robust watermark scheme based on multiple transforms and particle swarm optimization algorithm [J]. Multimed Tools Appl 78(2):2507–2523
42. Zhou Y, Wang J (2012) Image denoising based on the symmetric normal inverse Gaussian model and non-subsampled contourlet transform [J]. IET Image Process 6(8):1136–1147
43. Zhou NR, Xiahou WM, Wen RH et al (2018) Imperceptible digital watermarking scheme in multiple transform domains [J]. Multimed Tools Appl 77(23):30251–30267