A Novel Robust Blind Digital Image Watermarking Scheme Against JPEG2000 Compression

Zheng Hui[(✉)] and Quan Zhou

Xi'an Institute of Space Radio Technology, Xi'an 710000, Shaanxi, China
358971616@qq.com

Abstract. In this paper, a novel robust blind digital image water marking scheme is proposed by jointly using discrete wavelet transform (DWT), stationary wavelet transform (SWT), discrete cosine transform (DCT) and singular value decomposition (SVD). Firstly host image is decomposed by DWT and the obtained approximation coefficient is portioned into non-overlapping blocks. For each block, SWT is applied to affine redundant low frequency sub-bands which are subsequently processed by DCT and SVD. Watermark bit is embedded through quantifying the obtained greatest singular value. Extraction of proposed scheme is blind without any referring to the original image or watermark. Experimental result show that watermarked image is visually invisible of which peak signal to noise ratio (PSNR) is above 44 dB. Besides, by comparing with other DWT-SVD robust watermarking approaches, proposed scheme significantly outperforms in robustness against JPEG2000 compression. Performance of proposed scheme is also superior or competitive against other attacks such as rotation, filter or scaling.

Keywords: Blind image watermarking · Discrete wavelet transform · Stationary wavelet transform · Singular value decomposition · JPEG2000

1 Introduction

With the popularization and ripeness of the Internet, efficient storage management, rapid transmission and sharing, and real-time analysis and processing of digital multimedia data have gradually become an indispensable part of people's daily life. Due to the openness and compatibility of Internet, it's simple and convenient for people to access and obtain digital resources. However, under such circumstance, security of digital media has been greatly threatened and challenged for numerous digital products being copied, tampered and spread without the permission of copyrights' owners. Through illegal copying, huge profits have been made by criminals, which heavily threaten the development of digital media industry.

Digital watermarking, as an efficient authentication approach for copyright protection, is an important brunch of information security. Digital image is a key part of digital multimedia resources, thus digital image watermarking has been the essential aspects of watermarking technology. Digital watermarking protects the copyright of digits images by embedding watermarks into host images. In the implement of

copyright protection, the visual quality of watermarked image should not be significantly reduced; on the other hand, watermarking information should be robust of which most part can be detected and extracted after interference and attacking.

Since to deliver raw image greatly challenges storage and transmission bandwidth, it's necessary to have digital images compressed. JPEG2000 is discrete wavelet based still-image compression standard proposed by Joint Photographic Expert Group (JPEG). Taking advantages of discrete wavelet transform (DWT) and EB2COT encoding, JPEG2000 supports multi-resolution progressive representation and outperforms JPEG standard in reconstruction quality and compression ratio. However, in most scenes, JPEG2000 is applied as lossy compression scheme which brings distortion to watermarked image. In this paper, we focus in designing an efficient watermarking scheme against JPEG2000 compression.

According to the embedding domain of host images, digital image watermarking can be roughly categorized into two aspects, namely the spatial domain watermarking and the transform domain watermarking. Generally, digital watermarking in spatial domain is implemented by directly altering pixels within host image, which is characterized by simplicity and low computational complexity. The least significant bit substitution (LSB) [1] is a classic spatial domain watermarking algorithm implement by replacing host images' LSB with watermarking bits. Other typical spatial watermark includes pixel value differencing (PVD) [2], exploiting modification direction (EMD) [3] and reversible approaches such as histogram shifting (HS) [4] and difference expansion (DE) [5].

However, spatial watermark is not robust enough to resist attacks such as affine transformation or image compression in most scenes. Therefore research focusing on watermarking withstands compression has been continuously worked out for decades [6, 7]. The transform domain based watermarks is one of the efficient schemes resists to digital image compression. Compared with spatial domain watermarking, watermarks embedded in transform domain, such as discrete Fourier transform (DFT) [8, 9], discrete cosine transform (DCT) [10–12], discrete wavelet transform (DWT) [13, 14] and singular vale decomposition (SVD) [15–17] exploits better performance in both imperceptivity and robustness.

As mentioned, characteristics of mentioned transforms make them eligible for robust watermarking—most energy of natural signals (including images) is concentrated in low frequency coefficient and correlation between DCT coefficients is very low; DWT is a multi-resolution analysis in both spatial domain and frequency domain which characterizes the local properties in both domains; in addition, SVD is a powerful numeric tools for watermarking which effectively withstands attacks like geometric transform and noise. Therefore, research of robust watermarking [18–21] in hybrid domains involving DWT, DCT and SVD has been continually proposed in recent years which combines advantages of each transform. In Zear et al. [18], a back propagation Neural Network (BPNN) is applied in the watermark extraction phase to compensate the distortion induced by various attacks. In Fazli et al. [19], a watermarking scheme is proposed by combing DWT, DCT and SVD. The host image is firstly into four non-overlapping blocks and a 64 bit/128 bit binary watermark is embedded into each block four times respectively to enhance robustness. However, their approach is non-blind and its watermarking capacity is limited. In [21], Hu et al.

embeds multiple watermarking bits into host images by adjusting feature parameters obtained from DWT-SVD-DCT domain via the progressive quantization index modulation technique, which effectively withstands JPEG2000 compression attack.

Despite the mentioned transforms—DWT, DCT and SVD, another transform called stationary wavelet transform (SWT) is induced in this paper to implement robust watermarking scheme. SWT is an improved wavelet transform version aimed at overcoming the shortage of translation-invariance of DWT by removing down-samplers and up-samplers in original DWT algorithm. The salient features of SWT are redundancy and translation invariance. In this article, host image is firstly decomposed by 1-level DWT to obtained four sub-bands $[LL, LH, HL, HH]$. Then LL is portioned into 4×4 non-overlapping blocks, for each block a 1-level SWT is applied to obtain the low approximation coefficients LL_{SWT}. DCT and SVD are successively executed in LL_{SWT}, watermarking bits are embedded into the largest singular value via quantization.

The rest of this paper is organized as follows. In Sect. 2 describes the algorithm of both embedding and extraction algorithm. In Sect. 3, we gave out the experimental results and comparison between proposed Scheme and prior works. Eventually conclusion is presented in Sect. 4.

2 Proposed Blind Watermarking Scheme

2.1 Watermarking Embedding

The detailed embedding process of proposed scheme is given as follow:

(1) Using Haar wavelets, one-level 2-dimension DWT is applied on host image I. Therefore, four sub-bands are obtained namely LL, LH, HL and HH. Size of each sub-band will be $M/2 \times N/2$ Considering the demand of watermarking robustness, the embedding will be executed in sub-band LL.

$$[LL, LH, HL, HH] = \mathrm{DWT}(I) \qquad (1)$$

(2) Then the obtained LL is portioned into 4×4 non-overlapping block $LL(m, n)$ of which total amount is $M/8 \times N/8$. Each sub-block is decomposed by 2-dimension SWT; therefore a newly generated sub-band is obtained with size being the same as $LL(m, \mathrm{n})$

$$LL = \bigcup_{m}^{M/8} \bigcup_{n}^{N/8} LL(m, n) \qquad (2)$$

$$[A, H, V, D] = \mathrm{SWT}(LL(m, n)) \qquad (3)$$

(3) Then each stationary wavelet approximation A is transformed by DCT to obtain new coefficients A^{DCT} then apply SVD to A^{DCT}, therefore a singular value matrix **S** is acquired.

$$A^{DCT} = \text{DCT}(A) \tag{4}$$

$$[U, S, V] = \text{SVD}(A^{DCT}) \tag{5}$$

(4) According to formulas (5) and (6), watermarking bits $b \in \{0, 1\}$ is embedded into the maximum singular value $S(1, 1)$

$$S_W(1, 1) = round\left(\frac{S(1, 1) - d(b)}{\delta}\right)\delta + d(b) \tag{6}$$

Where, δ denotes quantization step, $d(0)$ is the quantization dither which is a random value within interval $[0, \delta]$ and $d(1) = d(0) + \delta/2$.

(5) Then calculate the watermarked A_W^{DCT} as follow:

$$A_W^{DCT} = U * S_W * V^T \tag{7}$$

(6) Inverse DCT and SWT operation is successively applied to 4×4 non-overlapping blocks, therefore the watermarked $LL_W(m, n)$ sub-band is obtained:

$$A_W = \text{Inverse\_DCT}(A_W^{DCT}) \tag{8}$$

$$LL_W(m, n) = \text{Inverse\_SWT}(A_W, H, V, D) \tag{9}$$

(7) These modified $LL_W(m, n)$s are put back to relevant position; therefore the watermarked approximation coefficient LL_W is obtained. Then apply inverse DWT transform by using Haar filter to LL_W and the rest detailed sub-bands which remain unchanged to acquire watermarked image I_W

$$LL_W = \bigcup_{m}^{M/8} \bigcup_{n}^{N/8} LL_W(m, n) \tag{10}$$

$$I_W = \text{Inverse\_DWT}(LL_W, LH, HL, HH) \tag{11}$$

2.2 Watermarking Extraction

The watermark extraction is basically the inverse operation against embedding process that contains similar operations, which are:

(1) By using Haar wavelet, two dimension DWT transform is applied to the watermarked image I_W, therefore a series of decomposed coefficients are obtained according to:

$$[LL_W, LH_W, HL_W, HH_W] = \text{DWT}(I_W) \tag{12}$$

(2) Divide acquired approximation sub-band LL_W into 4×4 non-overlapping blocks $LL_W(m, n)$s of which amount is $M/8 \times N/8$. Each sub-block is decomposed by 2-demsion SWT, therefore newly generated sub-bands are obtained with size being the same as $LL_W(m, n)$.Similarly, DCT and SVD operation are also successively applied to obtained singular value

$$LL_W = \bigcup_{m}^{M/8} \bigcup_{n}^{N/8} LL_W(m, n) \tag{13}$$

$$[A_W, H_W, V_W, D_W] = \mathrm{SWT}(LL(m, n)) \tag{14}$$

$$A_W^{DCT} = \mathrm{DCT}(A_W) \tag{15}$$

$$[U_W, S_W, V_W] = \mathrm{SVD}(A_W^{DCT}) \tag{16}$$

(3) To extract the watermark bit b, firstly the modified maximum singular value $S_W(1, 1)$ is modulated by a pair of quantization dither $d(i), i \in \{0, 1\}$ respectively:

$$e_i = round\left(\frac{S_W(1, 1) - d(i)}{\delta}\right)\delta + d(i) \tag{17}$$

Then b will be extracted according to the comparison of distance derived by demodulation in (17), which is

$$b = \arg\min_{i \in \{0,1\}}(S_W(1, 1) - e_i)^2 \tag{18}$$

Based on (18), the modulated $e_i, i \in \{0, 1\}$ of which distance is less will be judged as proper watermark bit as index $i_{\min}$ as $b = i_{\min}$.

3 Experimental Results

In this paper, five 512×512 gray-scale image namely are served as host images, namely 'Lena', 'Pepper', 'Boat', 'Jet' and 'Tiffany'. In addition, a binary logo with size 64×64 is used as watermark. The watermarking logo is 20 times Arnold transformed before embedding. Host images and watermarking logo are displayed as follow:

(a)   (b)   (c)   (d)   (e)

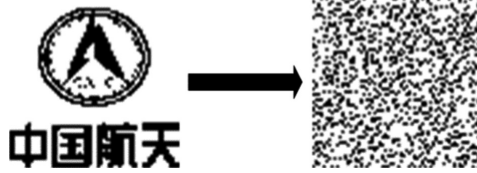**Fig. 1.** Host images: (a) Lena; (b) Pepper; (c) Boat; (d) Jet; (e) Tiffany

Fig. 2. Watermarking logo and its permutation by Arnold transform

3.1   Index of Quality Evaluation

In order to evaluate performance of proposed watermarking scheme, two metrics are induced namely peak signal to noise ratio (PSNR) and bit error rate (BER), among which PSNR indicates the imperceptivity of proposed scheme which is the variation between original host image and BER evaluates the robustness of extracted watermark under various attack types (Figs. 1 and 2).

PSNR between image I_1 and I_2 with size $M \times N$ is defined as below:

$$\text{PSNR} = 10 \log_{10} \left(\frac{255}{\text{MSE}} \right) (dB) \tag{19}$$

Where, MSE denotes the mean square error of which definition is as follow:

$$\text{MSE} = \frac{1}{MN} \sum_{x=1}^{M} \sum_{y=1}^{N} (I_1(x, y) - I_2(x, y))^2 \tag{20}$$

Definition of BER between $m \times n$ sized original watermark w and extracted w^* is shown as follow:

$$\text{BER} = \sum_{x=1}^{m} \sum_{y=1}^{n} \frac{(w(x, y) \oplus w^*(x, y))}{mn} \tag{21}$$

Where, $\oplus$ is exclusive or operation.

3.2   Selection of Quantization Step δ

As described in Sect. 2, it figures out that relation between imperceptivity of water-marked image and robustness of watermark is a compromise both affected by quantization step δ; which is greater δ enhances the robustness of watermark, yet impacts the invisibility of watermarked host images negatively.
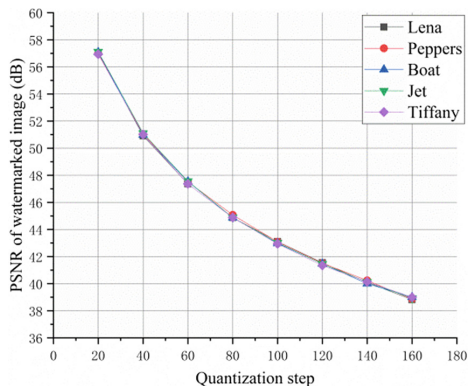
Fig. 3. Curves of watermarked images PSNR varying with different quantization steps
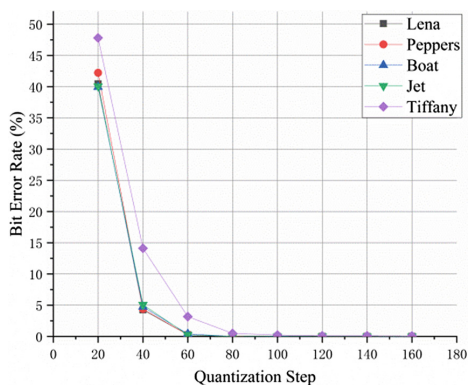

Fig. 4. Bit error rate of extracted watermark under JPEG 2000 compression with compression ratio set to 4

Figure 3 illustrates the trend how PSNR of watermarked images varies with different quantization steps. Figure 4 indicates the BERs of the extracted watermarks in case of JPEG2000 compression of which compression ratio (CR) is 4. From Fig. 4, it figures out that when quantization step $\delta \geq 80$ BERs of extracted watermarks of test images is very close to zero ($\leq 0.1\%$). The improvement in BER is very slight when step δ keeps increasing. However, performance of extracted watermarks' BERs deteriorates when quantization step $\delta \leq 60$. Moreover, from Fig. 3, it points out that when δ equals 80 the average PSNR of watermarked images is approximately 46 dB, which according to Human Vision System (HVS) [22], is excellent in vision quality and extremely invisible. Therefore, we intensively set quantization step $\delta = 80$ to achieve a trade-off between imperceptivity and robustness of proposed watermarking scheme.

3.3   Experimental Results and Comparison with Prior Works

In order to evaluate proposed scheme, a series of prior watermarking scheme of which watermark scales are all 4096 bits is induced as comparative groups, including Su et al. [17], Patra et al. [12] and Hu et al. [21]. In [17], watermark bits are embedded into non-overlapping blocks of host image by modifying some elements within U component of SVD decomposition. In [12], Patra et al. employs a Chinese Remainder Theorem-based (CRT) technology to embed watermark bits into DCT domain of host images. Hu et al. [21] embeds multiple watermarking bits into host images by adjusting obtained feature parameters from DWT-SVD-DCT domain via the progressive quantization index modulation technique, which effectively withstands JPEG2000 compression attack.

Table 1. Resulting PSNR (dB) of watermarked images for different schemes

Images	Watermarking schemes			
	Su et al. [17]	Patra et al. [12]	Hu et al. [21]	The proposed
Lena	41.55	42.49	43.60	44.88
Peppers	39.35	42.12	42.78	45.07
Boat	37.36	42.47	42.96	44.87
Jet	36.21	42.50	42.71	44.90
Tiffany	35.99	42.33	42.65	44.88

Table 1 indicates PSNR resulting from various watermarking schemes. It's obvious that PSNR achieved by proposed scheme is approximately 44.90 dB, which is significantly higher than other three approaches. Furthermore, unlike Su et al. PSNR achieved by different varies very slight for proposed scheme, which is, relevance of watermarked image quality to specific images is very little. Overall, imperceptivity of proposed algorithm stays in a relatively high level.

Subsequently, in order to test the robustness of proposed scheme, some types of attacks are taken into consideration, which are displayed in Table 2:

Attacks applied in this article mainly focus on JPEG2000 compression with a range of different compression ratio. Besides, other types of attack including noise, filter, rotation, scaling and pixels intensity variation are also explored to test the robustness of proposed scheme. Comparison between our work and prior research is displayed in Table 3.

Table 3 displays the average BER of extracted watermarks for test images under various types of attack, from which we can tell, proposed scheme significantly outperforms the other three works against JPEG2000 standard with all compression ratio employed. Besides, robustness of proposed scheme also has superiority under Median filter, scaling and rotation attack. However, not all of BER obtained by proposed algorithm is statistically competitive, for example, performance against Gaussian filter and pixels intensity variation is just general among four schemes and proposed scheme underperforms among all four works against salt & pepper noise. Figure 5 presents the extracted watermark visually.

Table 2. Attack types applied

Index	Attack type	Description
1–3	JPEG2000 compression	JPEG2000 compression with compression ratio of {2, 4, 8} is successively applied
4	Salt & pepper noise (1%)	Watermarked images are corrupted by salt & pepper noise with 1% intensity
5	Median filter (3×3)	Water marked images are filtered by a 3×3 median mask
6	Gaussian filter (3×3)	Watermarked images are filtered by a 3×3 Gaussian mask
7	Scaling	Watermarked images are shrunk into 256×256, then enlarged back to 512×512
8	Rotation	Watermarked images are rotated by $\pi/4$,then rotated back by $-\pi/4$
9	Cropping	Left upper corners with 256×256 pixels of watermarked images are cropped
10	Brighten	Intensity of watermarked images is added by 20
11	Darken	Intensity of watermarked images is subtracted by 20

Table 3. Average BER (%) of extracted watermarks for various schemes

Attack Type	Watermarking scheme			
	Su et al. [17]	Patra et al. [12]	Hu et al. [21]	The proposed
None	0	0	0	0
1	1.82	3.76	0	0
2	7.95	10.41	0.66	0.02
3	27.93	20.98	7.78	1.07
4	11.61	20.17	22.60	25.88
5	27.18	27.96	9.35	7.30
6	11.77	17.49	0.40	4.66
7	23.45	24.50	4.24	1.29
8	25.76	35.75	22.29	17.43
9	12.01	12.34	12.55	6.81
10	0.22	15.82	0.08	1.12
11	1.5	17.11	1.41	6.08

Fig. 5. Extracted watermark under various types of attack (a) None; (b–d) JPEG2000 compression with CR = 2, 4, 8; (e) Salt & pepper noise; (f) Median filter; (g) Gaussian filter; (h) Scaling; (i) Rotation; (j) Cropping; (k) Brighten; (h) Darken;

4   Conclusion

In this paper, we propose a novel robust blind watermarking scheme by jointly using DWT, SWT, DCT and SVD. The robustness is guaranteed by taking advantages of multi-resolution analysis offered by DWT, the translation invariance provided by SWT and the algebraic invariance furnished by SVD. Host images is firstly decomposed by DWT. Subsequently the approximation coefficient LL is portioned into non-overlapping blocks. For each block, SWT is applied to obtain the redundant low frequency coefficient LL_{SWT}. After successively applying DCT and SVD, multiple watermarks are embedded into the obtained greatest singular value of LL_{SWT} blindly using quantization. Experimental results show that the watermarked image is visually invisible of which peak signal to noise ratio (PSNR) is above 44 dB. Besides, by comparing with other DWT-SVD robust watermarking approaches, proposed scheme significantly outperforms in robustness against JPEG2000 compression. Performance of proposed scheme is also superior or competitive against other attacks such as rotation, filter or scaling.

References

1. Muhammad, K., Sajjad, M., Mehmood, I., Rho, S., Baik, S.W.: A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image. Multimed. Tools Appl. **75**, 14867–14893 (2016). https://doi.org/10.1007/s11042-015-2671-9

2. Sahu, A.K., Swain, G.: An optimal information hiding approach based on pixel value differencing and modulus function. Wirel. Pers. Commun. (2019). https://doi.org/10.1007/s11277-019-06393-z

3. Kieu, T.D., Chang, C.-C.: A steganographic scheme by fully exploiting modification directions. Expert Syst. Appl. **38**, 10648–10657 (2011). https://doi.org/10.1016/j.eswa.2011.02.122

4. Chen, H., Ni, J., Hong, W., Chen, T.-S.: Reversible data hiding with contrast enhancement using adaptive histogram shifting and pixel value ordering. Signal Process. Image Commun. **46**, 1–16 (2016). https://doi.org/10.1016/j.image.2016.04.006

5. Vinoth Kumar, C., Natarajan, V.: Hybrid local prediction error-based difference expansion reversible watermarking for medical images. Comput. Electr. Eng. **53**, 333–345 (2016). https://doi.org/10.1016/j.compeleceng.2015.11.033

6. Wu, H., Huang, J.: Secure JPEG steganography by LSB$^{+;}$ matching and multi-band embedding. In: 2011 18th IEEE International Conference on Image Processing. pp. 2737–2740. IEEE, Brussels (2011). https://doi.org/10.1109/ICIP.2011.6116235

7. Wu, H.-T., Liu, Y., Huang, J., Yang, X.-Y.: Improved steganalysis algorithm against motion vector based video steganography. In: 2014 IEEE International Conference on Image Processing (ICIP), pp. 5512–5516. IEEE, Paris (2014). https://doi.org/10.1109/ICIP.2014.7026115

8. Cedillo-Hernandez, M., Garcia-Ugalde, F., Nakano-Miyatake, M., Perez-Meana, H.: Robust watermarking method in DFT domain for effective management of medical imaging. Signal Image Video Process. **9**, 1163–1178 (2015). https://doi.org/10.1007/s11760-013-0555-x

9. Urvoy, M., Goudia, D., Autrusseau, F.: Perceptual DFT watermarking with improved detection and robustness to geometrical distortions. IEEE Trans. Inf. Forensics Secur. **9**, 1108–1119 (2014). https://doi.org/10.1109/TIFS.2014.2322497

10. Hsu, L.-Y., Hu, H.-T.: Robust blind image watermarking using crisscross inter-block prediction in the DCT domain. J. Vis. Commun. Image Represent. **46**, 33–47 (2017). https://doi.org/10.1016/j.jvcir.2017.03.009

11. Liu, S., Pan, Z., Song, H.: Digital image watermarking method based on DCT and fractal encoding. IET Image Process. **11**, 815–821 (2017). https://doi.org/10.1049/iet-ipr.2016.0862

12. Patra, J.C., Phua, J.E., Bornand, C.: A novel DCT domain CRT-based watermarking scheme for image authentication surviving JPEG compression. Digit. Signal Process. **20**, 1597–1611 (2010). https://doi.org/10.1016/j.dsp.2010.03.010

13. Keshavarzian, R., Aghagolzadeh, A.: ROI based robust and secure image watermarking using DWT and Arnold map. AEU Int. J. Electron. Commun. **70**, 278–288 (2016). https://doi.org/10.1016/j.aeue.2015.12.003

14. Singh, A.K., Dave, M., Mohan, A.: Multilevel encrypted text watermarking on medical images using spread-spectrum in DWT domain. Wirel. Pers. Commun. **83**, 2133–2150 (2015). https://doi.org/10.1007/s11277-015-2505-0

15. Makbol, N.M., Khoo, B.E., Rassem, T.H.: Security analyses of false positive problem for the SVD-based hybrid digital image watermarking techniques in the wavelet transform domain. Multimed. Tools Appl. **77**, 26845–26879 (2018). https://doi.org/10.1007/s11042-018-5891-y

16. Vaishnavi, D., Subashini, T.S.: Robust and invisible image watermarking in RGB color space using SVD. Procedia Comput. Sci. **46**, 1770–1777 (2015). https://doi.org/10.1016/j.procs.2015.02.130

17. Su, Q., Niu, Y., Zhao, Y., Pang, S., Liu, X.: A dual color images watermarking scheme based on the optimized compensation of singular value decomposition. AEU Int. J. Electron. Commun. **67**, 652–664 (2013). https://doi.org/10.1016/j.aeue.2013.01.009

18. Zear, A., Singh, A.K., Kumar, P.: A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine. Multimed. Tools Appl. **77**, 4863–4882 (2018). https://doi.org/10.1007/s11042-016-3862-8
19. 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**, 964–972 (2016). https://doi.org/10.1016/j.ijleo.2015.09.205
20. Dong, H., He, M., Qiu, M.: Optimized gray-scale image watermarking algorithm based on DWT-DCT-SVD and chaotic Firefly algorithm. In: 2015 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery. pp. 310–313. IEEE, Xi'an (2015). https://doi.org/10.1109/CyberC.2015.15
21. Hu, H.-T., Hsu, L.-Y.: Exploring DWT–SVD–DCT feature parameters for robust multiple watermarking against JPEG and JPEG2000 compression. Comput. Electr. Eng. **41**, 52–63 (2015). https://doi.org/10.1016/j.compeleceng.2014.08.001
22. Panetta, K., Gao, C., Agaian, S.: Human-visual-system-inspired underwater image quality measures. IEEE J. Ocean. Eng. **41**, 541–551 (2016). https://doi.org/10.1109/JOE.2015.2469915