A robust watermarking hybrid algorithm for color image

Mengli Song[1], *Huijun* Wang[2], *Jianbin* Wu[1,*], *Xinrong* Yan[2], *Linfeng* Yuan[2], and *Yameng* Tu[1]

[1]College of Physics Science and Technology, Central China Normal University, Wuhan, 430079, China
[2]Wuhan Maritime Communication Research Institute, Wuhan, 430079, China

Keywords: Color image, Watermarking, Layered embedding, Robustness.

Abstract. In order to improve the anti-attack performance of the watermark to meet the requirements of copyright protection and content forensics. This paper proposes a digital watermarking hybrid algorithm based on color images. The specific process is to adopt the idea of multi-algorithm layered embedding, choose the algorithm based on discrete cosine transform (DCT) algorithm, discrete wavelet transform_singular value decomposition (DWT_SVD) algorithm, and hologram algorithm, these three algorithms with robust complementary functions, then embed the same watermark image into the color image R, G and B layers to complete the watermark embedding. Compared with the single-algorithm embedded watermark, the hybrid algorithm can achieve blind extraction, at the same time, the algorithm has better robustness and can resist more types and higher intensity attacks. In the process of digital image transmission, the integrity of the watermark information of the carried picture can be guaranteed to achieve copyright protection, content forensics and other purposes.

1 Introduction

The concept of “What You See Is What You Get (WYSIWYG)” no longer holds true. With rapid growth of multimedia technology, computer networks are subjected to malicious attacks. Privacy and security of information are the most promising issues in our digital life. Therefore, digital watermarking technology[1][2] has an increasingly research value[3][4]. It originate from the spatial watermarking algorithm which proposed by Tirkel [5] in 1993. Then Van schyndel et al.[6] put forward the concept of digital watermarking and gives a specific implementation method, but this method has poor anti-attack ability.

Cox [7] proposed a digital watermarking algorithm based on global image transformation. This method embeds watermark into the transformation domain, which has

* Corresponding author: wujianbin@mail.ccnu.edu.cn

good robustness, but can not achieve blind extraction. On this basis, Tan et al. [8] proposed an image blind watermarking algorithm based on Discrete Wavelet Transform (DWT), which can realize the blind extraction of watermarks. Halima NB [9] proposed an algorithm based on block discrete cosine transform (DCT), which achieved a good balance between invisibility and robustness.

There are many types of attacks but the functional of a single algorithm are limited. Therefore, many scholars have begun to study the techonlogy, which using multi-algorithm to embedded watermarking. Santhi et al. [10] proposed a watermark embedding method using DWT, DCT and SVD for color images. The most significant coefficients are selected for the embedding of the watermark for different known attacks and found to be the method is robust except for rotation attacks. A secure and robust watermarking method based DWT and DCT is presented by Zhao et al. [11] the method is robust for known attacks. In addition, the security of the watermark is enhanced by using logistic chaotic encryption to encrypt the mark. Amit [12] proposed a multi-watermarking technology, which based on DWT, DCT and SVD, and has higher performance in terms of robustness, security and capacity.

Different from the above algorithm, in order to improve the robustness of the watermarking algorithm and adapt to the application needs of forensic and copyright services, a robust watermarking hybrid strategy for color images based on the idea of multi-watermark layered embedding is proposed in this paper. The experimental results show that our method is imperceptible and robust for different known attacks. Thereby ensuring the integrity of the watermark information in the transmission process to achieve the purposes of forensics and copyright protection.

2 Related work

In general, There are many kinds of attacks will be encountered during image transmission. According to the types of attacks, they are broadly classified in two types: image processing attacks and geometric attacks [13], such as adding noise, JPEG compression, low-pass filtering, quantization, histogram specification, image sharpening and geometric transformation. In this case, the visual quality of the hidden watermark and the robustness of the extracted image watermark were evaluated by determining Peak Signal-to-Noise Ratio (PSNR) and NC values respectively.

NC measures the similarity between the extracted watermark and the original watermark. The formula is as follows:

$$NC = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} w(i,j)w'(i,j)}{\sqrt{\sum_{i=1,j=1}^{i=m,j=n} w^2}\sqrt{\sum_{i=1,j=1}^{i=m,j=n} w'^2(i,j)}} \tag{1}$$

The evaluation indicator of PSNR is usually expressed in decibels (DB) and represents the change of image quality before and after watermark embedding. Generally, the larger of number, the better of invisibility of the watermark algorithm. And the formula is as follows:

$$PSNR = 10\lg\frac{M * N * MAX(I^2(a,b))}{\sum_{a=1}^{M}\sum_{b=1}^{N}(I(a,b)-I'(a,b))^2} \tag{2}$$

Where M and N denotes the number of rows and columns of the image, and $I(a,b)$ and $I'(a,b)$ respectively represent the pixel gray value of the image before and after the watermark is embedded.

We have done preliminary experiments to confirm that DWT_SVD algorithm [13] have excellent robustness when faced JPEG compression attacks, flip attacks, rotation attacks, size scaling attacks. The next digital watermarking algorithms is based on DCT transformation [14], which has strong robustness to histogram adjustment and sharpening attacks. The hologram algorithm for Gaussian white noise attacks, salt and pepper noise attacks, size scaling, JPEG compression and other strong attacks have strong robustness. In a word, the above three watermarking algorithms have complementary characteristics in robustness.

3 Hybrid algorithm embedding and extraction

In this experiment, the watermark image W selects a $64*64$ "China" binary image, and the carrier image I selects a $512*512$ Lena color image. The algorithm implementation steps are as follows:

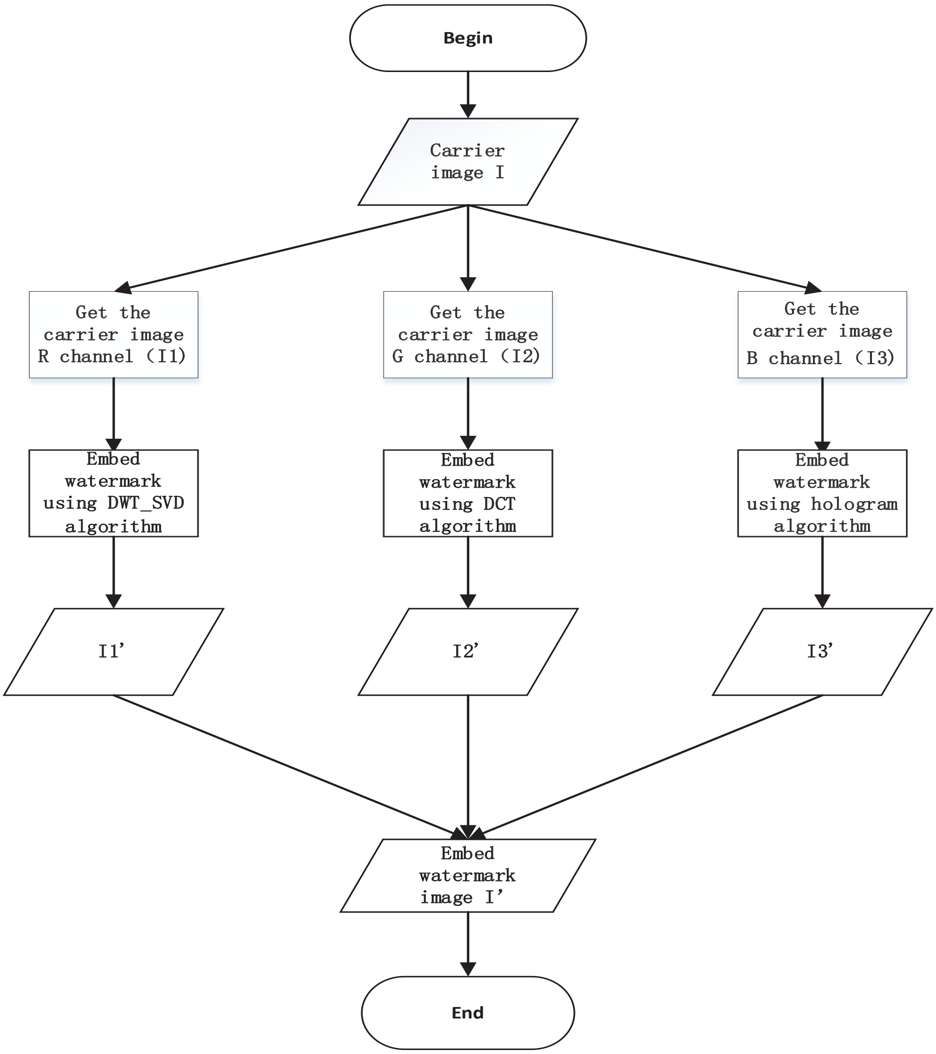

Begin
Carrier image I
Get the carrier image R channel (I1)
Get the carrier image G channel (I2)
Get the carrier image B channel (I3)
Embed watermark using DWT_SVD algorithm
Embed watermark using DCT algorithm
Embed watermark using hologram algorithm
I1'
I2'
I3'
Embed watermark image I'
End

Fig. 1. Watermark embedding flow chart.

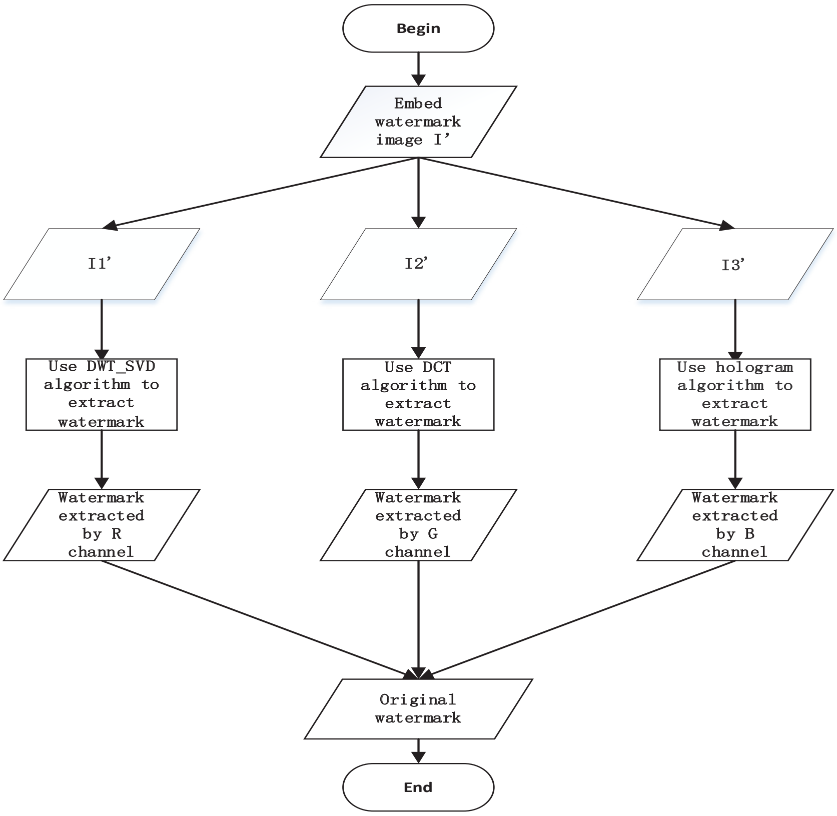

Begin
Embed watermark image I'
I1'
I2'
I3'
Use DWT_SVD algorithm to extract watermark
Use DCT algorithm to extract watermark
Use hologram algorithm to extract watermark
Watermark extracted by R channel
Watermark extracted by G channel
Watermark extracted by B channel
Original watermark
End

Fig.2. Watermark extraction flow chart.

Step 1: Read watermark W and carrier image I .

Step 2: Obtain the R, G, and B component matrices of I , and write them as $I1$， $I2$， $I3$.

Step 3: Using the DWT_SVD algorithm proposed above, the watermark image W is embedded in the R component $I1$ matrix of the carrier image. The difference here is that $I1$ is subjected to a three-level wavelet transform here, and the singular values of the watermark image after the scrambling are embedded in three levels The singular value of the wavelet transform $LL2$ component.

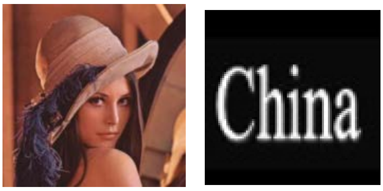
Step 4: Using the DCT algorithm to embed the watermark image W in the G component $I2$ of the carrier image. The specific method is to generate two normally distributed random arrays $K1$ and $K2$, perform $8*8$ block DCT transformation on the carrier image, and select 8 diagonal coefficients of each DCT block to embed 1bit watermark information. Finally, the $8*8$ block DCT inverse transformation is performed on the DCT coefficients embedded in the watermark to obtain the embedded watermark image $I2'$.

Step 5: The watermark image W is embedded in the B component $I3$ of the carrier image using a hologram algorithm. The main method is to superimpose the singular value coefficients of the Fourier hologram Arnold scrambling to the singular value coefficients of the carrier image secondary wavelet decomposition low-frequency component $LL2$ with the additive rule, reconstruct the low-frequency component, and then perform the secondary wavelet inverse transform to get the embedded watermark image $I3'$.

Step 6: Write the three components of R, G, and B embedded with watermark information into image I', which is the carrier image with embedded watermark.

4 Experimental results and analysis

The experiment selects a $64*64$ binary image of "China" as the watermark image, which is denoted as W. Choosing $512*512$ Lena color image as the carrier image, and it is marked as I. As shown in Figure 3a) and 3b), They represent carrier image and watermark image respectively.



a) Carrier image b) Watermark image

Fig. 3. Carrier image and watermark image.

In order to balance the robustness and invisibility of the watermarking algorithm, It is necessary to combine the spectral characteristics of HVS, setting the embedding intensity of the DWT_SVD sub-algorithm, DCT sub-algorithm, and hologram sub-algorithm to 0.2, 22, and 1.0, respectively. The carrier image with embedded watermark is shown in Figure 4.

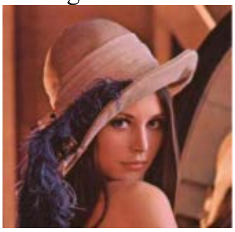
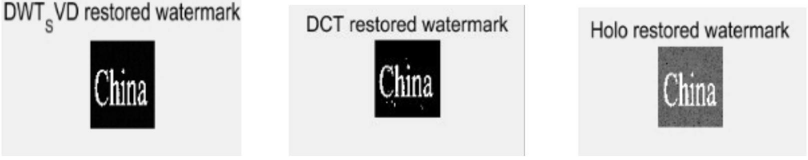


Fig. 4. Image with watermark embedded in hybrid algorithm.

The PSNR value of the above picture is 37.9095, which is not discernible with the naked eye from the original carrier image.

When the watermarked image is not attacked, the extracted watermark image is shown in Figure 5a), Figure 5b) and Figure 5c).

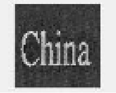
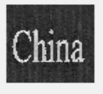
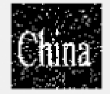
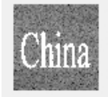
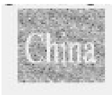
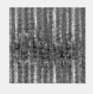
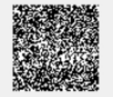
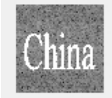
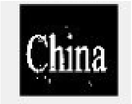
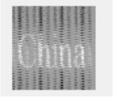
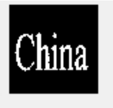
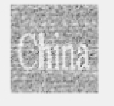
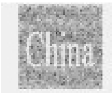
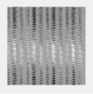
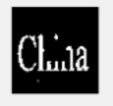
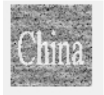
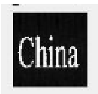
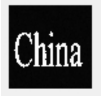
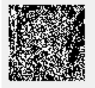
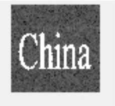
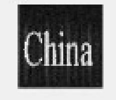
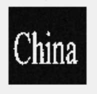
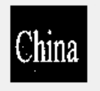
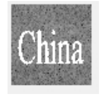
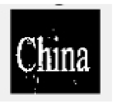
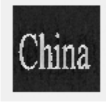
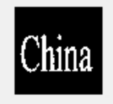
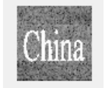


a) DWT_SVD restored watermark b) DCT restored watermark c) holographic algorithm restored watermark

Fig. 5. Watermark extracted without attack.

In the above three pictures, the first one is the R component of the image using the DWT_SVD algorithm to extract the watermark, which is extracted with $NC = 0.9998$. The watermark extracted from the G component of the second image $NC = 0.9979$, which uses the DCT algorithm. And $NC = 0.9329$ of the last image, which extracted from the B component of the image by using the holographic algorithm.

Table 1. Gaussian white noise attack.

Attack	hybrid algorithm	DWT_SVD algorithm	DCT algorithm	hologram algorithm
Gaussian white noise (V= 0.01)	 NC=0.9558	 NC=0.9875	 NC=0.8585	 NC=0.7050
Gaussian white noise (V= 0.1)	 NC=0.6990	 NC=0.5419	 NC=0.6462	 NC=0.7028
Crop the upper left corner of the image 1/16	 NC=0.9893	 NC=0.6759	 NC=0.9993	 NC=0.6223
Crop image center 1/16	 NC=0.6336	 NC=0.5556	 NC=0.9322	 NC=0.6575
JPEG compression (QF=90)	 NC=0.9983	 NC=0.9989	 NC=0.6192	 NC=0.7189
JPEG compression (QF=30)	 NC=0.9857	 NC=0.9890	 NC=0.9878	 NC=0.7038
Image sharpening	 NC=0.9836	 NC=0.9896	 NC=0.9993	 NC=0.6910

As shown in Table 1, It is clearly that the watermark can be extracted effectively by three single algorithms when the Gaussian white noise attack intensity is *0.01*, and in the hybrid algorithm, The watermark with the highest NC value is selected as the final result. However, the watermark extracted by the single DCT algorithm and the DWT_SVD algorithm can no longer distinguish the information content when the attack strength increases to *0.1*, but if the watermark is embedded with the hybrid algorithm, then the B component of the color image can be extracted after being the same attacked.

When 1/16 of the image center is cropped, the watermark image embedded using the DCT transform algorithm and the DWT_SVD algorithm are all destroyed. However, the watermark image extracted by the DCT transform algorithm in the G component is clearly distinguishable when using a hybrid algorithm. What's more , the NC value is above 0.9, but it can't resist cutting that the watermark image is also cut off by *1/16* of the center. Although the NC value of the B component hologram algorithm is not high, but the extracted watermark information is complete and clear. Therefore, in the face of strong attacks, the watermark information extracted by the hybrid algorithm can be compared each other, then choose the best one.

Table 2. Detailed comparative of the proposed scheme and the existing schemes.

Metric	Zhao et al.[11]	Amit et al.[12]	Smith LC et al.[15]	Proposed Method
Transform domain	DWT+DCT	DWT+SVD+DCT	DWT+SVD	DWT_SVD+DCT+Hologram algorithm
Host image	$512*512$	$512*512$	$512*512$	$512*512$
Watermark image	$64*64$	$64*64$	$256*256$	$64*64$
Embedded subhand	the low frequency sub-image LLn	the low frequency band (LL3) and vertical frequency band (LH2)	All	low frequency band LL2 and color images components of G, and B

Table 3. Comparison for 64 bit image watermark size.

Attacks	Zhao et al.[11]	Amit et al. [12]	Smith LC et al.[15]	Proposed Method
JPEG(*QF=80*)	*0.9767*	*0.9882*	-	*0.9962*
JPEG(*QF=40*)	-	*0.9819*	-	*0.9833*
JPEG(*QF=20*)	*0.8635*	*0.9872*	-	*0.9769*
Salt&Peppers(*d=0.01*)	*0.5473*	*0.9579*	*0.9270*	*0.9805*
Salt&Peppers(*d=0.02*)	-	*0.8696*	*0.9030*	*0.9397*
Gaussian noise (*V=0.01*)	*0.5473*	*0.8184*	*0.8760*	*0.9558*
Gaussian noise (*V=0.02*)	*0.4657*	*0.6740*	*0.8410*	*0.8040*
Median Filtering [3 3]	-	*0.9790*	*0.9720*	*0.9746*
Resize 1.3x	-	*0.9906*	-	*0.9986*
Gaussian Lowpass filter ([5 5], 0.5)	-	*0.9865*	*0.856*	*0.9977*

On the contrary, clear watermark information can be extracted from the R and B components of the hybrid algorithm. In general, the three sub-algorithms embedded in the three components of color images R, G, and B, when faced with most attacks, if there is a algorithm can resist, the effectiveness of the embedded watermark can be guaranteed. Perform simulations on the proposed algorithm and the algorithms in [11][12][15]. Table 3 shows the specific descriptions and simulation parameters. Table 4 shows the NC performance of the proposed method is compared with other reported techniques [11][12][15], which also use multiple algorithms to embed the watermark.Referring the table it can be inferred that the NC values as obtained by proposed method vary in the range from *0.8040* to *0.9977*. The maximum NC value has been obtained by the proposed method is *0.9977* with image Gaussian Lowpass filter ([5 5], 0.5) . However, the minimum NC value is *0.8040* for Gaussian noise ($M = 0, V = 0.02$). The NC values of watermarked images are higher than other methods except for JPEG (*QF=20*) extected by Amit Kumar Singh et al. [12]. Compared with other reported techniques, it can be clearly seen that the robustness of proposed algorithm is better.

5 Conclusion

In order to realize a robust watermarking hybrid algorithm for color images, different algorithms are used to embed the same watermark image in the R, G, and B components of the color image. Some experimental results are given in this paper. The experimental results and analysis show that the layered embedding of the hybrid algorithm can effectively improve the robustness of the watermark. Meanwhile, the proposed algorithm can resist more types and higher intensity attacks. In this way, we can ensure the integrity of the watermark information and achieve the purpose of tracking digital products. On one hand, it can successfully solve the copyright certification problems of digital products at different stages such as release and sales. On the other hand, because of each algorithm has different extractions of watermark when faced with attack, the extracted multiple watermarks can also reference between each other.In addition, compared with grayscale images, color images are spread more widely on the Internet. Therefore, this promising algorithm can be applied to practical scenes and more realistic and in line with actual application circumstances.

Furthermore, the common digital watermarking algorithm can be improved which based on DCT transform and hologram algorithm, then the two algorithms are respectively embedded to G and B components respectively. In this case, in order to realize the blind extraction of the watermark, the watermark image is extracted without the original data.The improved hologram sub-algorithm used in this paper not only solves the problem of carrier image quality degradation, but also improves the ability to resist noise and filter attacks In addition, the hologram has an encryption function, which greatly enhances the security of the algorithm. At the same time, it has greater potential value in achieving enhanced robustness and watermark security. Besides, these watermarks can also be effectively extracted in the distribution and utilization of medical or other security documents.

This work was supported by the National Natural Science Foundation of China [Grant no. U1736121] and Wuhan Maritime Communication Research Institute [Grant no. KCJJ2019-2]. Independent research funding for central universities (30106200571).

References

1. Wuyoung Z, Chen J, Yufeng Z. Global resynchronization-based image watermarking resilient to geometric attacks. Comput Electr Eng 2018;67(1):182–94.
2. Ayesha SK, Masilamani V. A novel digital watermarking scheme for data authentication and copyright protection in 5G networks. Comput Electr Eng 2018;72:614–30.
3. Y.G. Wang, D. Xie, B.B. Gupta, A study on the collusion security of LUT-based client-side watermark embedding, IEEE Access 6 (2018) 15816–15822.
4. Brij B. Gupta et al, Handbook of Computer Networks and Cyber Security, Springer, 2020.
5. A Z Tirkel, G A Rankin, R M Van Schyndel, W J Ho, NRA Mee. Electronic Watermark. Digital Image Computing[J], Technology and Applications DICTA 93. Sidney: Maquarie University, 1993: 666-673.
6. R. G. Van Schyndel, A. Z. Tirkel, C. F. Osborne. A Digital Watermark.International Conference on Image Processing, IEEE Press,1994.
7. Cox I J,Kilian J,Leighton F T,Shamoon T. Secure spread spectrum watermarking for multimedia[J]. IEEE transactions on image processing : a publication of the IEEE Signal Processing Society,1997,6(12).
8. Tan Linglong, He Yihong, Wu Fengzhi, et al. A Blind Watermarking Algorithm for Digital Image Based on DWT. 2020, 1518(1):012068.

9. Halima N B, Hosam O. Embedding image ROI watermark into median DCT coefficients[J]. International Review on Computers & Software, 2015, 10(6):643.
10. V.Santhi, and A Thangavelu," DC Coefficients Based Watermarking Technique for color Images Using Singular Value Decomposition", International Journal of Computer and Electrical Engineering, Vol.3, No.1, pp. 8-16, February, 2011.
11. M Zhao and Y Dang, "Color Image Copyright Protection Digital Watermarking Algorithm Based on DWT & DCT",4th International Conference on Wireless Communications, Networking and Mobile Computing, Dalian, pp.1-4, 12-14 Oct. 2008
12. Amit Kumar Singh, Basant Kumar, Sanjay Kumar Singh, et al. Multiple watermarking technique for securing online social network contents using Back Propagation Neural Network. 2018, 86:926-939.
13. Haiming Li, Xiaoyun Guo. "Embedding and Extracting Digital Watermark Based on DCT Algorithm. 2019, 2019
14. Na Na Zhang, Li Yu, Xiao Fang Yang. Research of Digital Image Watermarking Robustness Algorithm Based on DCT. 2014, 3181:3171-3174.
15. Smith L C, Turcotte D L, Isacks B L. Stream flow characterization and feature detection using a discrete wavelet transform[J]. Hydrological Processes, 2015, 12(2):233-249.