An improved color image watermarking algorithm based on DWT

Zhaoting Wang[1*], Hongqin Wu[2], Yuying Ma[3]

ShanDong University of Engineering and Vocational Technical, Jinan 250200, China

[1]*Correponding author: sdwzt513@163.com
[2]e-mail: 2530387097@qq.com
[3]e-mail: 532228103@qq.com

Abstract. Aiming at the poor robustness and transparency of color image watermarking algorithm, this paper proposes an improved color image watermarking algorithm based on DWT. The watermark image and the original image are transformed by DWT, and the embedding position of the watermark is adjusted according to the frequency sensitivity and color sensitivity of human visual system, so as to improve the robustness and transparency of the watermark algorithm. At the same time, the technology also uses Arnold scrambling encryption to ensure the security of the watermark. The simulation results show that the improved color image algorithm based on DWT proposed in this paper can effectively improve the transparency and robustness of the watermark, while ensuring the security of the watermark.

Keywords: Color Image, Digital watermark, DWT, Image Scrambling

1 Introduction

With the continuous development of network technology, digital information products have developed rapidly. However, there are also some problems, such as digital information transmission and copyright protection of digital products [1-2]. Faced with this situation, digital watermarking technology developed rapidly at the end of the 20th century. This technology is different from traditional encryption technology, which makes up for the shortcomings of traditional encryption technology that the information content is destroyed after the password is cracked. At the same time, digital watermarking technology can also resist some conventional operations, such as encryption, decryption, compression and cutting [3-5]. Digital watermarking technology mainly embeds the information to be hidden into the digital carrier through some special treatments, and ensures that the embedded information will not be detected by the human visual system (HVS) on the premise that the embedded information will not damage the use value of the original carrier. Image-based digital watermarking technology has been deeply studied, and most of the algorithms have good transparency and some robustness such as anti-noise and low-pass filtering.

G. Guan et al. (eds.), *Proceedings of the 2023 3rd International Conference on Education, Information Management and Service Science (EIMSS 2023)*, Atlantis Highlights in Computer Sciences 16,
https://doi.org/10.2991/978-94-6463-264-4_91

Digital watermarking algorithm based on discrete wavelet transform (DWT) domain has been deeply studied because of its good time-frequency characteristics and multi-resolution characteristics [6-7]. This kind of algorithm can not only describe the local characteristics of the signal, but also embed the watermark into different resolution layers, thus improving the transparency of the watermark. At the same time, DWT is more in line with the characteristics of human visual system, and is compatible with JPEG and video compression, which makes the watermark have better anti-compression performance. Yang Hongying [8] and others put forward a watermark embedding scheme for color images. In this scheme, the color images are transformed by DWT to obtain texture sub-blocks, and then the scrambled watermark images are embedded into texture blocks. Experiments show that the watermark image generated by this scheme has good effect. Liang Xin [9] combines the advantages of DWT technology and matrix singular value decomposition to propose a digital watermarking algorithm for color images based on DWT, which shows strong robustness to common attacks. Song[10] and others put forward a watermark mixing algorithm to improve the robustness of the watermark. This algorithm combines the discrete cosine transform (DCT) algorithm, discrete wavelet transform _ singular value decomposition (DWT_SVD) algorithm and holographic algorithm, and embeds the same watermark image into the tricolor components of the color image by using the complementarity of these three algorithms. Compared with single watermarking algorithm, this algorithm can realize blind extraction and has good robustness. However, the calculation process of this algorithm is complicated and there are many uncontrollable factors. At present, there are many watermarking algorithms based on DWT domain, but few have good robustness and transparency at the same time. Based on this, this paper proposes an improved color image watermarking algorithm based on DWT, which combines the advantages of DWT transform and human visual system and can effectively enhance the robustness and transparency of the image.

2 Improve color image watermarking algorithm

2.1 Digital Watermark Embedding Algorithm for Color Images

In order to enhance the transparency and robustness of color image watermark, this paper proposes a digital watermark embedding algorithm based on DWT. The embedding process is shown in Figure 1, and the embedding steps are as follows:

(1) The watermark image is separated into three primary colors, and the color watermark image is decomposed into three components, namely, SR, SG and SB. The structure of the color watermark image is scrambled by Arnold transform, and the scrambled three components are respectively transformed by DWT to obtain the wavelet coefficients of the three primary colors.

(2) The original color image is separated by three primary colors, and the color image is decomposed into three components, namely ZR, ZG and ZB, and then the wavelet coefficients of the three primary colors are obtained by DWT transform.

(3) Before the scrambled watermark image is embedded in the original image, a threshold T is set in advance to select the position where the watermark is embedded in the original image. Firstly, the energy value of the green component in the watermark image is calculated, and then compared T. When the energy value of the green component in the watermark image exceeds the threshold, the green component of the watermark image is embedded in the high frequency region of the original image, while the blue component and the red component are embedded in the low frequency region of the original image. On the contrary, when the energy value of the green component is lower than the threshold, the green component of the watermark image is embedded in the low-frequency region of the original image, while the blue component and the red component are embedded in the high-frequency region of the original image.
(4) Through DWT inverse transformation, the three primary colors embedded with watermark are regenerated.
(5) The three primary colors are merged to obtain a color image embedded with watermark.

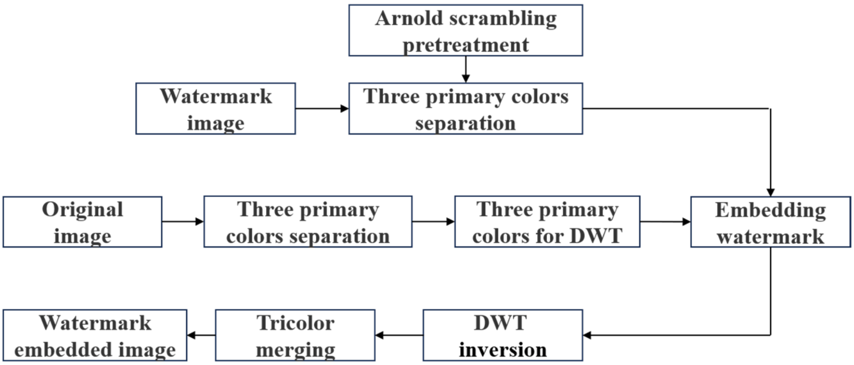

Fig. 1. Watermark embedding process

2.2 Extraction of Digital Watermark from Color Image

The watermark is extracted from the color image with watermark through DWT inverse transformation. The watermark extraction process is shown in Figure 2, and the steps are as follows:

(1) The original image is separated by three primary colors, and the discrete wavelet coefficients of the original image are obtained by DWT transform of the three primary colors respectively.
(2) The watermark embedded image is separated into three primary colors, and the discrete wavelet coefficients of the image with watermark are obtained by DWT transform.
(3) Subtracting the discrete wavelet coefficient of the original image from the discrete wavelet coefficient of the watermark embedded image to obtain the discrete wavelet coefficient of the watermark image.

(4) DWT inverse transform is performed on the discrete wavelet coefficients of the watermark image, then Arnold inverse transform is performed, and finally the three primary colors are merged to obtain the watermark image. Arnold inverse transform can effectively eliminate image color confusion, thus effectively extracting and processing the watermark in the image.

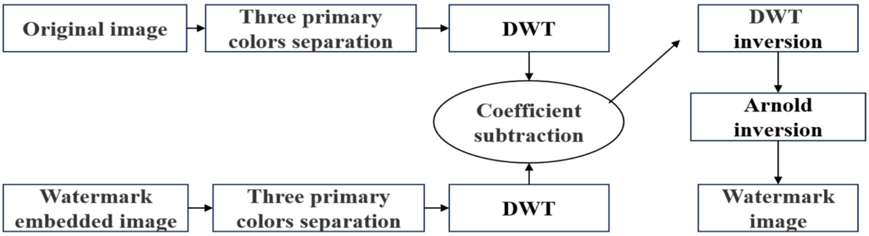

Fig. 2. Watermark extraction process

3 Experimental simulation results and analysis

3.1 Embedding and Extraction of Watermark

In this paper, 256×256 color image is selected as the original carrier image, as shown in Figure 3(a), and 64×64 color badge image is used as the original watermark image, as shown in Figure 3(b). Haar wavelet is used in wavelet transform, and the simulation experiment is carried out under Matlab7.0 and WindowsXP. In this paper, we not only evaluate the algorithm by vision, but also use Peak Signal-to-Noise Ratio (PSNR) to evaluate the difference between the watermark embedded image and the original carrier image and the effectiveness of extracting the watermarked image after various attacks, and use Normalized Correlation Coefficient (NC) to quantitatively analyze the similarity between the extracted watermark image and the original watermark image. PSNR and NC are defined as follows:

$$PSNR = 10\lg \frac{3 * M * N * \max(I^2(i,j,k))}{\sum_{i=1}^{M}\sum_{j=1}^{N}\sum_{k=1}^{3}(I(i,j,k) - I'(i,j,k))^2} \tag{1}$$

$$NC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\sum_{k=1}^{3} W'(i,j,k) \times W(i,j,k)}{\sum_{i=1}^{M}\sum_{j=1}^{N}\sum_{k=1}^{3} W(i,j,k)^2} \tag{2}$$

Among them, $I(i,j,k)$ represents the pixel value of the original carrier image. $I'(i,j,k)$ represents the pixel value of the watermark embedded image. $W(i,j,k)$

represents the pixel value of the original watermark image. $W'(i,j,k)$ Represents the pixel value of the extracted watermark image.

In order to ensure the security of the watermark image, the original watermark image is scrambled and encrypted, as shown in Figure 3(c). Then, the energy of the green component in the watermark image is calculated, and the calculation result is compared with the preset threshold T, and different embedding methods are selected according to the comparison result. Set the threshold T to 0.05. Through calculation, the energy value of the green component of the watermark image is 0.0104, which is lower than the threshold T, so this paper embeds the green component of the watermark image into the low frequency region of the original image, and the blue and red components into the high frequency region of the original image. Figure 3(d) shows the image after embedding the watermark. From the comparison between Figure 3(a) and Figure 3(d), it can be seen that it is difficult to distinguish the difference between the watermark embedded image and the original carrier image with naked eyes. Further, the peak signal-to-noise ratio of the watermark embedded image and the original carrier image is calculated to be 40.9821dB. The results show that the embedded watermarking algorithm in this paper has good transparency. Without any attack, the watermark image is extracted from the watermark embedded image, and the extracted watermark image is shown in Figure 3(e). Comparing the original watermark image Figure 3(b) and the extracted watermark image Figure 3(e), it can be seen that there is almost no visual difference between the extracted watermark image and the original watermark image, and the normalized correlation coefficient between the extracted watermark image and the original watermark image is calculated to be 1. The results show that the watermark extraction algorithm proposed in this paper is feasible without any attack.

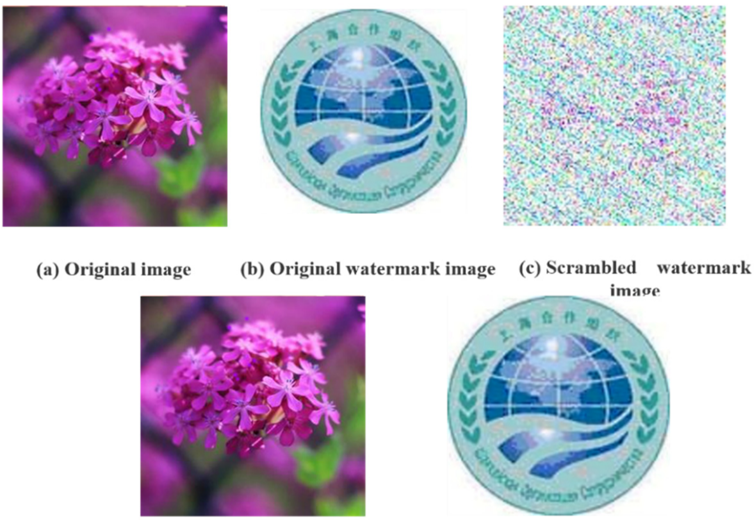

Fig. 3. Embedding and extraction of watermark

3.2 Performance test of watermarked images

In order to evaluate the robustness of the watermarking algorithm proposed in this paper, this paper carries out a variety of different attack tests on watermark embedded image, including JPEG compression, cropping and noise addition.

JPEG compression attack.

JPEG is a widely used method in image compression, so whether the watermarking system is robust to JPEG compression is an important criterion to measure the success of a watermarking algorithm. Fig. 4 shows the watermark embedded image and the extracted watermarked image after being attacked by JPEG compression with quality factor QF=80 and quality factor QF=40, respectively. As can be seen from Figure 4, the JPEG compression attack has little effect on the vision of the watermark embedded image, and the similarity between the extracted watermark image and the original watermark image is high, which shows that the algorithm in this paper has good resistance to JPEG compression attack.

(a) JPEG Compression Attack (QF=80)　　(b) JPEG Compression Attack (QF=40)

Fig. 4. Watermark embedded image and extracted watermark image after JPRG compression attack

Shear attack.

The image embedded with watermark may be subjected to various cutting operations when it is used, so this paper tests the cutting attack on the watermark embedded image. Because the extraction algorithm requires the scale of the image to be detected, this paper displays the cut part as a white image. Fig. 5 shows the watermark embedded image and the extracted watermarked image respectively after the watermark embedded image is subjected to 1/16th, 1/4th and 1/2 shearing attacks. With the increase of the cropped part of the watermark embedded image, the loss of watermark information increases accordingly. However, because the algorithm embeds the watermark in the transform domain and the watermark information is scattered on all pixels, the overall effect of the extracted watermark image is still good. When the watermark embedded image is cut off by 1/16, the watermark information can be extracted completely.

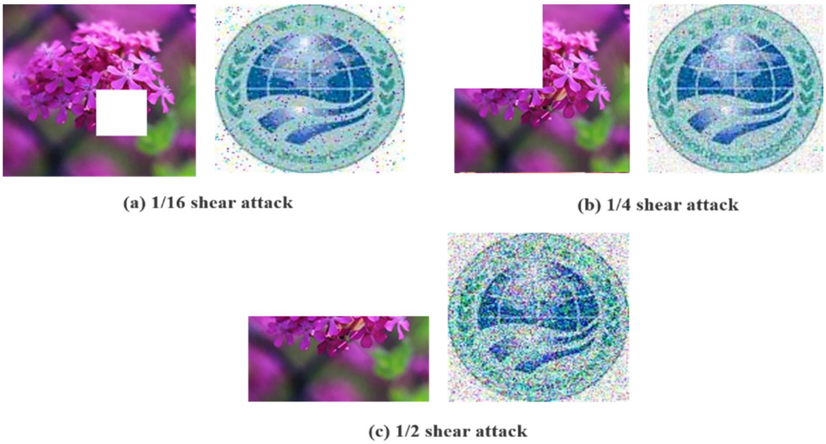

Fig. 5. Watermark embedded image and extracted watermark image after shear attack

Noise attack.

In the process of image transmission, it is often subject to all kinds of interference and noise. Fig. 6 shows the watermark embedded image and the extracted watermarked image respectively after being attacked by salt and pepper noise with noise densities of d=0.01 and d=0.05 and Gaussian noise with average value of m=0 and variance of v=0.005. From Figure 6(a) and Figure 6(b), it can be seen that the extracted watermark image can be clearly recognized after the watermark embedded image is attacked by salt and pepper noise. The results show that the algorithm in this paper has good robustness to salt and pepper noise attacks. It can be seen from Figure 6(c) that the visual effect of the extracted watermark image is poor after Gaussian noise attack, but it can also be recognized, indicating that the algorithm has some resistance to Gaussian noise attack, but it is worse than salt and pepper noise attack.

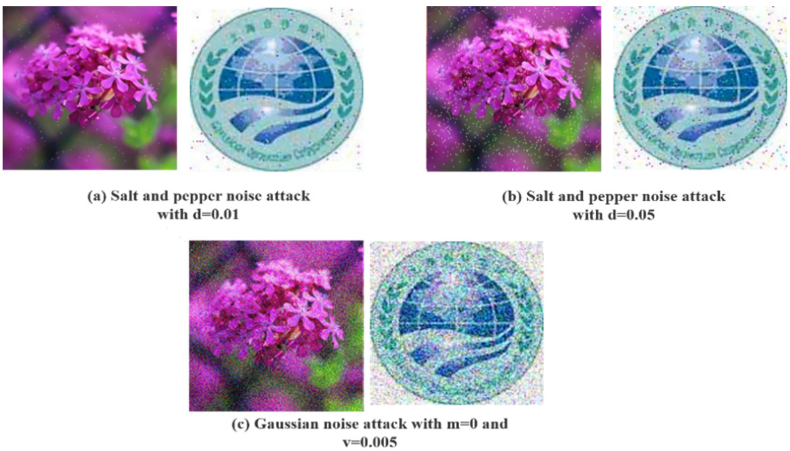

Fig. 6. Watermark embedded image and extracted watermark image after noise attack

In order to quantitatively describe the ability of this algorithm to resist foreign attacks, this paper calculates the PSNR values of the watermark embedded image and the original carrier image after various attacks, and the NC values of the watermarked image and the original watermark image after various attacks, as shown in Table 1. It can be seen from the table that the PSNR value calculated by JPEG compression attack is the highest, and the algorithm in this paper has the best resistance to JPEG compression attack, followed by noise attack. Compared with salt and pepper noise attack, the PSNR value of Gaussian noise attack is lower. The cropping attack determines the PSNR value according to the number of cropping parts. The more cropping, the more image distortion and the lower PSNR value. But on the whole, this algorithm can effectively resist the common attacks in image processing. The NC value reflects the similarity between the extracted watermark image and the original watermark image. The NC values of the watermark embedded image after JPEG compression attack, noise attack and cropping attack are all greater than 0.8. The results show that the algorithm in this paper has good robustness to common image processing attacks.

Table 1. Experimental results of DWT-based watermarking algorithm against various attacks

Image attack type	PSNR	NC
JPEG compression (QF=80)	36.0381	0.8731
JPEG compression (QF=40)	31.3718	0.8201
Shear 1/16	20.4228	0.9803
Shear 1/4	18.2853	0.8764
Shear 1/2	13.6383	0.8176
Salt and pepper noise (d=0.01)	25.3969	0.9743
Salt and pepper noise (d=0.05)	22.8015	0.9017
Gaussian noise (m=0, v=0.005)	18.0931	0.8361

4 Conclusions

Aiming at the poor robustness and transparency of color image watermarking embedding algorithm, this paper proposes an improved color image watermarking algorithm based on DWT. The algorithm is based on DWT transform, and uses the frequency sensitivity and color sensitivity of human visual system to adjust the embedding position of watermark. The simulation results show that the algorithm has good transparency, and can effectively resist JPEG compression attacks, cropping attacks and noise attacks, and has good robustness.

References

1. Marzieh., Amini., Hamidreza., et al. (2018）A Channel-Dependent Statistical Watermark Detector for Color Images. IEEE Transactions on Multimedia, 21(1):65-73. https://doi.org/10.1109/TMM.2018.2851447.
2. Liu, X.L., Lin, C.C., Yuan, S.M. (2016) Blind Dual Watermarking for Color Images' Authentication and Copyright Protection. IEEE Transactions on Circuits and Systems for Video Technology, 1047-1055. https://doi.org/10.1109/TCSVT.2016.2633878.
3. Goléa, N.E.H., Seghir, R., Benzid, R. (2010) A bind RGB color image watermarking based on singular value decomposition. In:IEEE/ACS International Conference on Computer Systems & Applications. Cheng du. 1-5. https://doi.org/10.1109/AICCSA.2010.5586967.
4. Hu, H.T., Hsu, L.Y., Chou, H.H. (2020) An improved SVD-based blind color image watermarking algorithm with mixed modulation incorporated. Information Sciences, 519:161-182. https://doi.org/10.1016/j.ins.2020.01.019.
5. Zhang, F., Luo, T., Jiang, G., et al. (2019) A novel robust color image watermarking method using RGB correlations. Multimedia Tools and Applications, 78(14):20133-20155. https://doi.org/10.1007/s11042-019-7326-9.
6. Jiang, Z.T., Chen, W. (2016) Zero-watermarking algorithm for color images based on DWT-DCT-SVD. Microelectronics & Computer, 33(08):107-111. https://doi.org/10.19304/j.cnki.issn1000-7180.2016.08.023.
7. Abdulrahman, A.K., Ozturk, S. (2019) A novel hybrid DCT and DWT based robust watermarking algorithm for color images. Multimedia Tools and Applications, 78(12):17027-17049. https://doi.org/10.1007/s11042-018-7085-z.
8. Yang, H.Y., Wang, X.Y., Zhao,Y., et al. (2004) Digital lmage Watermarking Based on Streak Blockin the Discrete Wavelet Domain. Microelectronics & Computer, (07):106-109. https://doi.org/10.3969/j.issn.1000-7180.2004.07.028.
9. Liang, X. (2019) Study of Digital Watermark Algorithm on Color lmage Based on DWT and SVD. Computer & Digital Engineering, 47(08):2014-2017. https://doi.org/CNKI:SUN:JSSG.0.2019-08-036.
10. Song, M., Wang, H., Wu, J., et al. (2021) A robust watermarking hybrid algorithm for color image. Mathc Web of Conferences, 336(1):07012. https://doi.org/10.1051/matecconf/202133607012.