ISSN 2706-6827 Vol. 3, Issue 17: 1-7, DOI: 10.25236/IJFS.2021.031701

Embedding and Extraction of Color Image Digital Watermark Based on Quaternion Fourier Transform

Yongqiang Ma[1,2*], Wei Sun[1], Jing Bian[1], Jianli Zhang[1,2], Dexi Chen[1,2],Juan Wu[1,2]

[1]School of Computer Science, Jining Normal University, Wulanchabu 012000, China
[2]Center for International Education, Philippine Christian University, Manila 1006, Philippines
nsd-myq@126.com
**Corresponding author*

Abstract: *With the rapid development of computer and network technology, digital products, especially color digital images, can be popularized on the Internet, but because of their easy access and large-scale copying characteristics, their copyright protection has become increasingly difficult, and piracy and infringement and other issues are becoming more and more serious. Therefore, watermarking technology has increasingly attracted people's attention. Whether it is using digital or color images as host graphics or watermarking materials, it has become one of the hottest watermarking technologies. This article intends to explore the method of embedding and extracting the color image digital watermark using quaternion Fourier transform, and theoretically analyzes the quaternion representation, quaternion Fourier transformation, and logarithmic polar coordinate transformation of color images. And select the middle and low frequency area of the final real part of the quaternion Fourier transform as the embedding area, and carry out the method and process of watermark embedding and extraction. The simulation results show that, in the most typical attack form, the above-mentioned dynamic watermark embedding and extraction algorithm can not only effectively combat filtering attacks and noise intrusion, but also has absolute advantages in combating shear damage.*

Keywords: *Quaternion, Fourier Transform, Color Image, Digital Watermark*

1. Introduction

Due to the vigorous development of computer network technology and multimedia technology, information processing technology and communication technology have also attracted increasing attention. The ability to use the Internet to quickly transmit images, sounds, videos, and other signals makes it easier and faster to save, publish, and distribute multimedia signals [1-2]. Especially in recent years, the dissemination of multimedia information has become more and more colorful. People can publish some important information and works through the Internet for e-commerce. However, when the Internet was opened up, while providing convenience for people, it also brought about some serious security problems: the leakage of personal secrets and even state secrets, copyright infringement of works, illegal misappropriation in e-commerce, and so on. Therefore, how to ensure the security of these confidential information is an urgent issue [3-4].

Scholars at home and abroad have given a variety of watermarking algorithms, including discrete cosine transform, discrete wave transform, unique value decomposition, inverse wave transform, and multi-directional wave transform. Among them, DCT conversion is one of the methods in the field of frequency domain conversion. The image information is divided into high frequency and low frequency areas in different frequency bands, and the main image information is in the high and low frequency areas of the image [5-6]. On the basis of the original DCT method, some researchers have provided a blind watermarking algorithm for DCT coefficients based on the difference between blocks. The watermark embedding range above is defined by calculating the difference between adjacent blocks in a certain area. , In the algorithm, an image block on the adjacent block is selected, and the value of the DCT coefficient is modified to achieve the purpose of embedding the watermark. Compared with the original DCT transform method, this algorithm is more powerful [7-8]; some scholars have proposed a fixed watermarking method, which combines two frequency field methods. This is the weakness of wavelet transform and has an inverse Displacement and deformation. Using the robustness of SVD, the watermark image used in the article is directly embedded into the unique value of the redundant

ISSN 2706-6827 Vol. 3, Issue 17: 1-7, DOI: 10.25236/IJFS.2021.031701

waveform conversion subband. This allows the algorithm to achieve a higher capacity and a better sense of subtlety, while the watermark is integrated into a higher security [9-10]. Some researchers have proposed a new Contourlet color image watermarking algorithm. Directional wave transformation is also called anisotropic particle transformation. Compared with the fixed transformation direction of particle transformation, the transformation can be performed in any direction and information is received in each direction of the image [11-12]. The research results of predecessors provide a theoretical basis for the research of this article.

Based on a large number of references related to "quaternion Fourier transform", "digital watermarking", etc., based on the quaternion theory, the characteristics of digital watermarking technology, and common image watermarking attacks, this paper envisages watermark embedding and the method and process of acquisition, and a simulation test was carried out.

2. Embedding and Extraction of Color Image Digital Watermark Based on Quaternion Fourier Transform

2.1 Quaternion Theory

(1) Quaternion representation of color image

In the RGB color space, any color can be represented by a 3D vector, so each pixel can also be represented by a pure quadratic imaginary number. The three components of R, G, and B are used as the coefficients of i, j, and k respectively, and the color image can be represented by a quadratic array. This allows the entire color image to be processed instead of editing three gray scale images as before.

$$q = a + bi + cj + dk \tag{1}$$

$$f(x, y) = R(x, y)i + G(x, y)j + B(x, y)k \tag{2}$$

(2) Fourier transform of quaternion

In image processing, the Fourier transforms we use are all discrete types

$$F(u,v) = \frac{1}{\sqrt{MN}} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} e^{-u_1 2\pi \frac{mu}{M}} f(m,n) e^{-u_2 2\pi \frac{nv}{N}} \tag{3}$$

$$f(m,n) = \frac{1}{\sqrt{MN}} \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} e^{u_1 2\pi \frac{mu}{M}} F(u,v) e^{u_2 2\pi \frac{nv}{N}} \tag{4}$$

(3) Logarithmic polar coordinate transformation

The formula for the log-polar transformation of coordinates (x, y) is

$$x = e^{\rho} \cos\theta, y = e^{\rho} \sin\theta (0 \le \theta \le 2\pi) \tag{5}$$

In the formula, ρ and θ respectively represent the polar diameter and polar angle in the polar coordinate system.

2.2 Features of Digital Watermarking

(1) Security

Security means that the watermark information embedded in the carrier data is not easy to be detected by humans, nor is it easy to be deleted, tampered with or forged; on the other hand, this is sensitive information and appropriate identification marks. The watermark can only be accessed with permission, that is, only authorized users can search, export or modify the watermark in order to achieve the purpose of copyright protection. In addition, as the vector watermark data changes, the watermark information should also change accordingly. By doing so, when the vector watermark data changes, the watermark information can be extracted and the vector data can be judged according to the change of the watermark information. Cryptography is the most standard method of protecting watermarks.

ISSN 2706-6827 Vol. 3, Issue 17: 1-7, DOI: 10.25236/IJFS.2021.031701

(2) Concealment

The concealment of digital watermark information is also called imperceptibility or fidelity. This mainly refers to the watermark carrier data after the watermark is integrated through the watermark technology, which should have the same visual effect as before the watermark is merged. In other words, you may not notice the subtle changes in the carrier data after the watermark is embedded, and may have the same meaning as the carrier data before and after the watermark is embedded. In addition, the integration of watermark information should not affect the shape and content of the vector, that is, after the integration of the watermark, the vector can be used normally. The most perfect situation is that the original carrier and the carrier with the water indicator are visually identical, or the difference is too small to be perceived by the human eye.

(3) Robustness

Robustness is one of the most important characteristics of watermarking algorithms. This mainly means that the watermark information embedded in the carrier data can resist various common processing operations and attacks. Even if the intruder maliciously attacks the watermark data or performs illegal operations such as blurring, sharpening, noise attack, filtering attack, geometric attack, etc., the built-in watermark information is reliable to a certain extent. Not only can the watermark information be smoothly extracted from the watermark carrier after the attack, but the watermark detection algorithm can detect the change of the watermark after the attack.

(4) Low error rate

In theory, users cannot extract watermarks from non-watermark carriers, but after performing certain attacks or other operations on the original data of non-watermark operators, users can retrieve the watermark information. This phenomenon is a watermark error. Error rate refers to the ability to extract watermarks from body data that does not contain watermarks. Digital watermarking technology requires a low error rate, in other words, no matter what the type of attack or processing, the watermark information cannot be extracted, or the possibility of watermark extraction is very small.

2.3 Common Image Watermark Attack Methods

(1) Remove the attack

This type of attack is also called brute force attack, which destroys the watermark, mainly destroying the robustness of the watermark. The specific idea of removing the attack is to achieve the purpose of removing or removing the watermark of the highlighted image data without affecting the normal use of the image, and to reduce the extent of the watermark vector data. The vector is the watermark of the destructive wave.

(2) Represents an attack

This means that the attack will not immediately eliminate or reduce the new watermark embedded in the watermark image, but will combine the fuzzy watermark technology to prevent the watermark detector from detecting the appearance of the new watermark. Therefore, the demonstrating attacker can often use the simple change of the watermark to an offline aligned image to fool the automatic watermark detector. This type of attack is mainly in the research field of geometric feature attacks such as flipping, compression, shearing, and radial transformation.

(3) Explain the attack

Explaining an attack is different from expressing an attack and removing an attack. Instead, it tries to make crawlers detect false watermarks or watermark data, which is a protocol-level attack. The above attack changes the unreliable value of image pixels. It needs to analyze the watermark to protect the target. This kind of attack is usually called a misleading attack, which modifies the target image and the original watermark. Digital watermarking has some risks in normal copyright protection.

(4) Legal attacks

Legal attacks usually deny the legitimacy of the watermark user without considering the technology. In different jurisdictions, there may be different understandings of property. At the same time, a legal attack may also involve the credit between the user and the attacker, as well as various information. In addition to this, there may be other conditional factors, such as the comparison of social status between the owner and the intruder, the evaluation of relevant experts, and the debate strength of the judges on both sides, and so on. There is no doubt that legal attacks are more difficult to understand and learn

ISSN 2706-6827 Vol. 3, Issue 17: 1-7, DOI: 10.25236/IJFS.2021.031701

than technical attacks. As a starting point, the first thing to do is to introduce reasonable legal regulations to provide users with a reasonable protective watermark. The most reliable watermark integration solution requires professional watermark destruction, and it makes sense to reduce the reliability of the watermark owner through litigation.

3. Experiment

3.1 Embedding of Watermark Information

The color image can be represented by pure quaternion, so the corresponding quaternion matrix is transformed into ordinary quaternion matrix after QFT

$$F(u,v) = A(u,v) + B(u,v)i + C(u,v)j + D(i,v)k \tag{6}$$

The analysis shows that the real part after quaternion Fourier transform satisfies the following formula, where M and N are the size of the image.

$$A(u,v) = -A(M-u, N-v) \tag{7}$$

If the frequency domain table corresponding to the pure quaternion after QFT remains unchanged, the actual part of the pure quaternion obtained after the IQFT inverse transformation procedure is still zero. In formula (7), if the actual part of the color image after QFT has symmetry, the actual part is taken as the embedding area, and the watermark information is embedded symmetrically according to formula (7). And we can see that the real part of the new quaternion is zero after the inverse transformation. Therefore, the real embedded information will not be lost after IQFT, and the visual error caused by the embedded information will propagate in the entire image, which is not easy to cause subjective perception.

The specific embedded flowchart is shown in Figure 1.

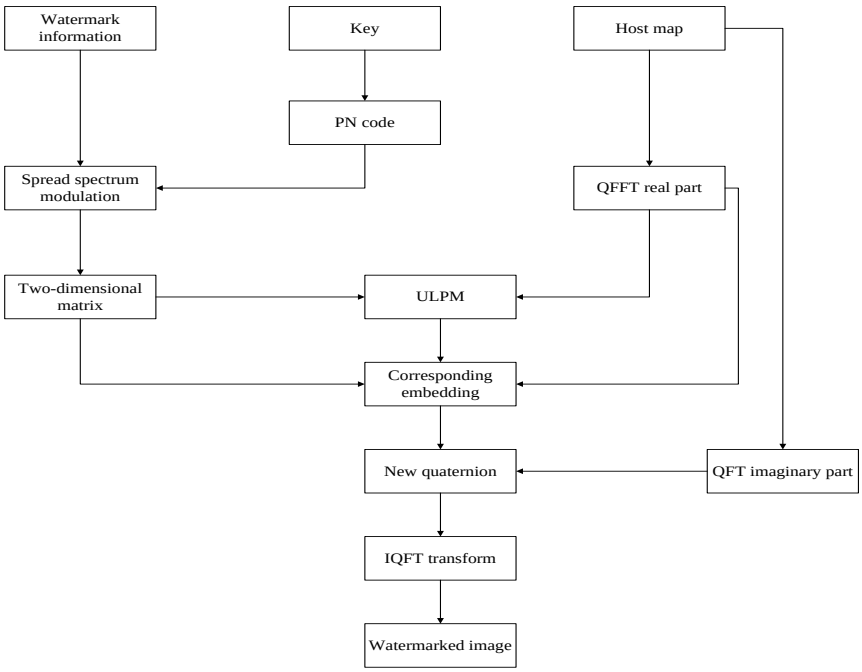

Figure 1: Watermark embedding flowchart

According to the logarithmic polar coordinate theory, the medium and low frequency range is selected as the embedding area of the watermark. After the quaternion Fourier transform is performed on the color image, the polar coordinate logarithm base is selected as follows

$$a = 2^{\frac{1}{M}} \tag{8}$$

Choose to find the corresponding point in the polar coordinate system in the frequency domain Cartesian coordinate system to embed the watermark.

ISSN 2706-6827 Vol. 3, Issue 17: 1-7, DOI: 10.25236/IJFS.2021.031701

$$l_1 = ceil\left(\log_a \frac{r}{R}\right) + \frac{M}{2}$$
$$l_2 = ceil\left(\frac{N \times \theta}{\pi}\right) \tag{9}$$

M is the number of sampling points along the polar radial direction, and N is the number of sampling points along the polar angle direction.

3.2 Extraction of Watermark Information

(1) Correlation coefficient

The digital watermark in this article uses an extraction algorithm based on correlation coefficients. The formula for calculating the correlation coefficient between vectors P and Q is (10)

$$c(P,Q) = \frac{1}{N}\sum_i P(i)Q(i) \tag{10}$$

At present, in the fields of communication, signal processing/detection, image registration, target tracking, etc., many related problems can be solved through related methods. The correlation coefficient algorithm makes it easier to detect, but the value found depends largely on the width of the embedded information. Therefore, most of the current algorithms use the normalized correlation coefficient method to solve this problem.

$$\rho(w,\hat{w}) = \frac{\sum_{i=1}^{N_w} w(i)\hat{w}(i)}{\sqrt{\sum_{i=1}^{N_w} w^2(i)}\sqrt{\sum_{i=1}^{N_w} \hat{w}^2(i)}} \tag{11}$$

Among them, w(i) represents the embedded watermark information.

(2) Extraction of watermark

The watermark extraction process is shown in Figure 2.

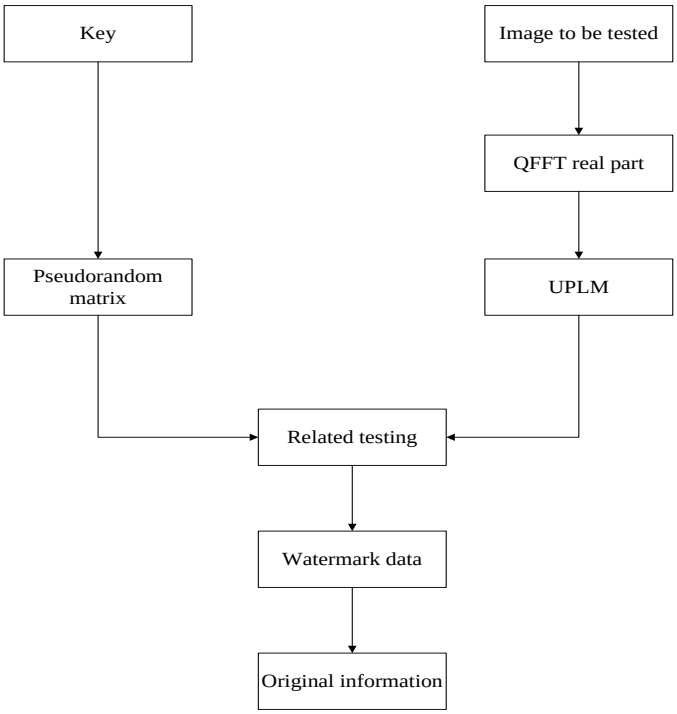

Figure 2: Watermark extraction process

ISSN 2706-6827 Vol. 3, Issue 17: 1-7, DOI: 10.25236/IJFS.2021.031701

Perform discrete quaternion Fourier transform on the image contained in the watermark to find the real part and move it around the DC element of the real part. Before using the extraction function, first add a watermark to edit the picture. In the actual part of the spectrum image, the rotation angle can be analyzed and an appropriate reversible transformation can be performed to achieve correction; in the case of a zoom attack on the pixel, the pixel will be restored to its original pixel size. After that, the Cartesian coordinate value corresponding to the LPM value is found through the coordinate correlation equation (9) proposed, the key and the pseudo-random matrix are correlated with (l_1, l_2), and the extracted minimum correlation coefficient is restricted to obtain the original watermark data. The scrambled matrix is then restored to the original embedded signal through the Arnold reverse redirection method, and the original watermark signal is obtained blindly.

4. Discussion

In order to test the performance of the algorithm in this paper, the original host image selected in this paper is a 512x512 color image, and the watermark is a 64x64 binary image, which meets the requirements of maximizing the length of the watermark, and checks the embedding and extraction effects of the watermark. The experimental results are shown in Table 1.

Table 1: *Experimental results of watermarking attacks*

Attack form	Experimental results	
	NC value	PSNR/dB
Gaussian noise	0.97	33.08
Median filter	0.71	36.47
Cut 1/16	0.98	41.81
Gaussian low pass	0.98	40.98

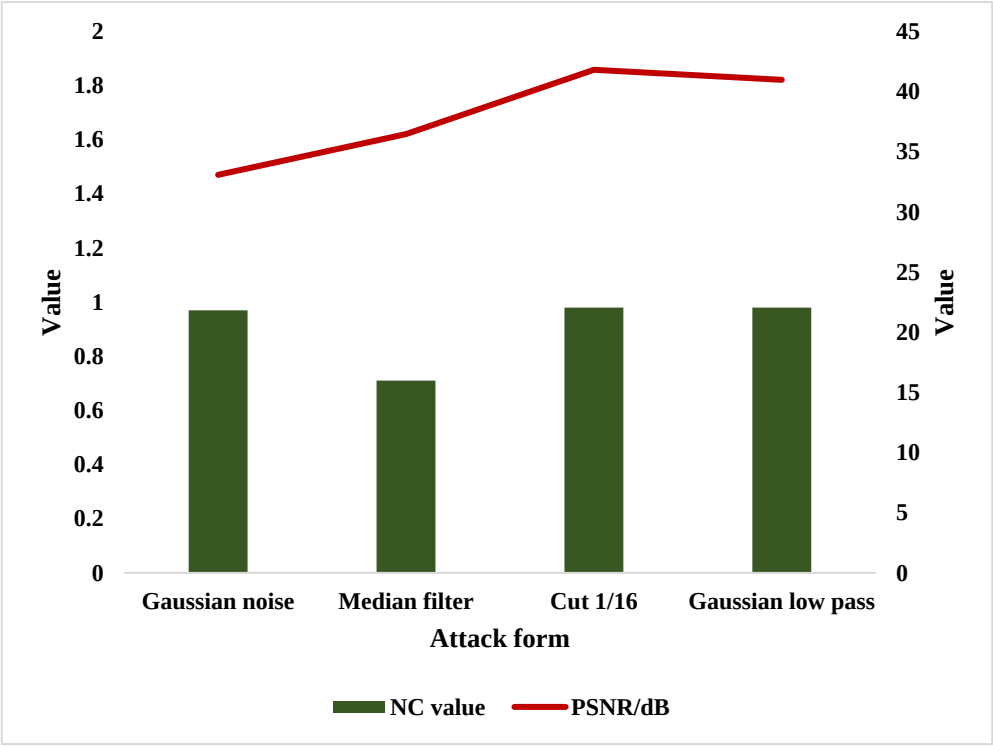

Figure 3: Experimental results of watermarking attacks

It can be seen from Figure 3 that in the most typical attack form, by using the watermark embedding and extraction algorithm described above, it can not only resist filtering and noise attacks, but also has an absolute advantage in anti-cutting. Even when it is attacked, the invisibility of the embedded watermark can be guaranteed, and the watermark extraction effect is also very ideal.

ISSN 2706-6827 Vol. 3, Issue 17: 1-7, DOI: 10.25236/IJFS.2021.031701

5. Conclusions

The color image digital watermarking technology based on quaternion Fourier transform not only has strong application value and development prospects, but the methods and skills in the research process also provide an effective reference for other related technologies. At present, this technology has become one of the research hotspots in the field of information security. Many domestic researchers have carried out fruitful work in this field and have achieved many meaningful research and application results.

Acknowledgments

This work was supported by Research Program of Science and Technology at Universities of Inner Mongolia Autonomous Region (NJZZ20246).

References

[1] Sharma S S, Chandrasekaran V. A robust hybrid digital watermarking technique against a powerful CNN-based adversarial attack [J]. Multimedia Tools and Applications, 2020, 79(43):32769-32790.

[2] Li H Guo X. Embedding and Extracting Digital Watermark Based on DCT Algorithm [J]. Journal of Computer & Communications, 2018, 06(11):287-298.

[3] Ma Z, Jiang M, Huang W. Trusted forensics scheme based on digital watermark algorithm in intelligent VANET[J]. Neural Computing and Applications, 2020, 32(6):1665-1678.

[4] Xiao Y, Gao G. Digital Watermark-Based Independent Individual Certification Scheme in WSNs [J]. IEEE Access, 2019, PP (99):1-1.

[5] Li H, Guo X. Embedding and Extracting Digital Watermark Based on DCT Algorithm [J]. Journal of Computer & Communications, 2018, 06(11):287-298.

[6] Moreno R, M Graña, Ramik D M, et al. Image Segmentation on the Spherical Coordinate Representation of the RGB Color Space [J]. Iet Image Processing, 2018, 6(9):1275-1283.

[7] Zhao B, Fang L, Zhang H, et al. Y-DWMS: A Digital Watermark Management System Based on Smart Contracts [J]. Sensors, 2019, 19(14):3091-3092.

[8] Gonzalez-Lee M , Vazquez-Leal H , Gomez-Aguilar J F , et al. Exploring the Cross-Correlation as a Means for Detecting Digital Watermarks and Its Reformulation Into the Fractional Calculus Framework[J]. IEEE Access, 2018, PP (99):1-1.

[9] Veni M, Meyyappan T. Digital image Watermark embedding and extraction using oppositional fruit Fly algorithm [J]. Multimedia Tools and Applications, 2019, 78(19):27491-27510.

[10] Niu P P, Wang X Y, Yang H Y, et al. A blind watermark algorithm in SWT domain using bivariate generalized Gaussian distributions [J]. Multimedia Tools and Applications, 2020, 79(19):13351-13377.

[11] Hemdan E D. An efficient and robust watermarking approach based on single value decompression, multi-level DWT, and wavelet fusion with scrambled medical images[J]. Multimedia Tools and Applications, 2021, 80(2):1749-1777.

[12] Wang X Y, Zhang S Y, Wang L, et al. Locally Optimum Image Watermark Decoder by Modeling NSCT Domain Difference Coefficients with Vector based Cauchy Distribution [J]. Journal of Visual Communication and Image Representation, 2019, 62(JUL.):309-329.