Scientific Research Publishing

Journal of Computer and Communications, 2018, 6, 287-298
http://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Embedding and Extracting Digital Watermark Based on DCT Algorithm

Haiming Li, Xiaoyun Guo

School of Computer Science and Technology, Shanghai University of Electric Power, Shanghai, China
Email: lhm@shiep.edu.cn, xioayuu@163.com

How to cite this paper: Li, H.M. and Guo, X.Y. (2018) Embedding and Extracting Digital Watermark Based on DCT Algorithm. *Journal of Computer and Communications*, **6**, 287-298.
https://doi.org/10.4236/jcc.2018.611026

Received: September 15, 2018
Accepted: November 25, 2018
Published: November 28, 2018

Abstract

The principle of digital watermark is the method of adding digital watermark in the frequency domain. The digital watermark hides the watermark in digital media, such as image, voice, video, etc., so as to realize the functions of copyright protection, and identity recognition. DCT for Discrete Cosine Transform is used to transform the image pixel value and the frequency domain coefficient matrix to realize the embedding and extracting of the blind watermark in the paper. After success, the image is attacked by white noise and Gaussian low-pass filtering. The result shows that the watermark signal embedded based on the DCT algorithm is relatively robust, and can effectively resist some attack methods that use signal distortion to destroy the watermark, and has good robustness and imperceptibility.

Keywords

Digital Watermark, DCT Algorithm, White Noise, Gaussian Low-Pass Filtering, Robustness, Imperceptibility

1. Introduction

Digital watermarking is an effective digital product copyright protection and data security maintenance technology. It uses a digital marker to hide it in digital products such as digital images, documents, and videos to prove its copyright. And as evidence to prosecute illegal infringement, it thus becomes an effective means of intellectual property protection and digital media security [1]. Digital watermarking hides watermarks in digital media (images, voice, video, etc.) to enable hiding the functions of transmission, storage, annotation, identification, and copyright protection [2]. If there is no robustness requirement, the processing of watermark and information camouflage technology is completely consistent [3]. In most cases, we want to add information that is invisible or in-

visible; in some specific situations where visible digital watermarks are used, the copyright protection mark is not required to be hidden, and it is desirable that the attacker does not destroy the quality of the data itself. The watermark cannot be removed. Therefore, we can summarize functions of digital watermarking technology into two aspects. On the one hand, it can be used to prove the original author's ownership of his work as evidence for the identification and prosecution of illegal infringement; on the other hand, the author can also realize the work by detecting and analyzing the watermark in his digital product [4].

In this paper, the two-dimensional discrete cosine transform is used to realize the embedding and extracting of the digital watermarking algorithm. The forward DCT is used to convert the image block information into the coefficient frequency domain matrix, and then the inverse DCT is used to transform the watermarked coefficient matrix into the image block. This paper begins with a detailed introduction to the basic knowledge related to digital watermarking and classical algorithms, and briefly describes the DCT transforms that will be used in this paper. After that, the traditional algorithms are improved accordingly. According to the algorithm, in the intermediate frequency the watermark is embedded in the coefficient to realize the adaptive embedding of the watermark. At the end of the paper, the performance of the watermarking system is analyzed and evaluated. After the embedding and extraction, the two methods of attack and detection are performed. If the watermarked image cannot be seen and the watermark is still identifiable, the watermark is proved to be robust and imperceptible.

2. Digital Water Mark

2.1. Digital Watermark Meaning and Characteristics

Digital Watermarking technology hides some information that has special meanings into digital media information such as text files, digital audio, video, images, etc. through certain embedded algorithms, and requires that the embedded watermark does not cause the appearance of the original data. And the change of size does not affect the use value. When the watermark extraction detected, the hidden information cannot be lost. In order to make digital watermarks a trusted application system for digital product copyright protection and integrity identification, embedded information entered into digital products must have the following basic characteristics:

1) Concealment: After embedding the watermark, it will not affect the digital work itself, there is no obvious quality degradation, and it can be perceived by people.
2) Security and reliability: The embedded information and the embedded location are encrypted and hidden, so that the illegal interceptor cannot obtain relevant information.
3) Robustness: The way digital products suffer from some illegal or vandalism is usually signal processing such as channel noise interference, filtering, edge

enhancement, jitter, A/D and D/A conversion, clipping, displacement, Scale changes, multiple sampling and lossy compression coding. After such a processing operation, the watermark must be able to be distinguished and recognized.

4) Watermark capacity: Under the premise of ensuring multimedia quality, it is possible to embed the author information of the work or the authentication code of the product as much as possible. Only in this way can the function of the watermark system be reflected in the event of a dispute.
5) Low error rate: The probability of detection errors in watermark detection must be quite low, so that the performance of such a watermark system can be truly guaranteed.

2.2. Common Watermarks

1) Visible watermark: The watermark can be seen, representing a kind of copyright information. It is mainly applied to the image, there are also applications in video and audio, and audible watermarks in audio.
2) Invisible watermark: This watermark is more widely used. When viewing an image or video, the watermark is imperceptible and largely retains the value of the digital work. But when there are problems like copyright disputes that are difficult to solve, as long as the watermark can be extracted, the complicated problem becomes very simple.
3) Robust watermark: mostly used to identify information. Its purpose is to protect the digital copyright after it has been processed (filtered, noisy, replaced, compressed, etc.) and various malicious attacks.
4) Plaintext watermark: The original data must be detected when it is detected. Its advantage is strong robustness. However, due to the dispersion of network propagation information, the practical value of this watermark in the application process is not broad.
5) Airspace watermark: Look for unimportant image bits in the carrier file, and then directly superimpose the watermark information into the algorithm. The aspect is very simple, but the robustness is not very strong.
6) Frequency domain watermark: The carrier file is mathematically transformed so that it is converted from the time domain to the spatial domain, and then the watermark information is embedded, and finally the inverse transform is performed. At this time, the watermark already exists in any place of the carrier file. The mathematical transformation here is generally discrete cosine transform (DCT), discrete Fourier transform (DFT), discrete wavelet transform (DWT) and other algorithms.

3. Watermarking Algorithm

When the spatial domain algorithm is applied to the digital watermarking technology, when the digital artwork embedded in the watermark is subjected to some common attacks, the watermark signal embedded therein is easily lost. In

view of this situation, the researchers have proposed the idea of embedding the watermark in the transform domain. From the time domain to the transform domain, mainly through some mathematical transformations, these mathematical transformations have discrete cosine transform (DCT) and discrete fourier transform (DFT). At this time, some frequency domain coefficients of the image are embedded in the watermark information. For this change, it means that the signal of the watermark information may be released to any place in the entire image space, and then the transformed frequency domain image is transformed into a time domain watermarked carrier. After passing this series of transformations, the watermark signal will not be removed so easily.

3.1. Principle

Adding digital watermark principle in frequency domain: Adding digital watermark in frequency domain means transforming image into frequency domain by some transform such as Fourier transform, discrete cosine transform and wavelet transform, adding the watermark to the image in frequency domain and then transform the image into a spatial domain by inverse transform. Compared with airspace means, the frequency domain means is more occult and more resistant to attack.

3.2. Advantage

The watermark information is trapped in the low frequency coefficient, which is sensitive to the human eye, which will cause a significant drop in the quality of the carrier image; embedding the high frequency coefficient will cause serious damage to the watermark information embedded therein. Therefore, based on the DCT domain watermark embedding intermediate frequency coefficients, a good compromise between watermark transparency and robustness is achieved. Based on the image watermarking algorithm of DCT transform domain, the original image is firstly subjected to 8×8 block DCT transform. Then, the method of exchanging intermediate frequency coefficients is used, which is commonly used in traditional algorithms to improve the embedding of binary watermarks, so that the larger value of the system is larger after the system is exchanged, and the smaller value is smaller, thereby obtaining stronger robustness.

3.3. DCT

DCT (DCT for Discrete Cosine Transform): The DCT for Discrete Cosine Transform is a transform associated with the Fourier transform, which is similar to the DFT for Discrete Fourier Transform, but uses only real numbers. The discrete cosine transform is equivalent to a discrete Fourier transform of approximately twice the length. This discrete Fourier transform is performed on a real function, because the Fourier transform of a real function is still a real function, in some variants, it need to move the input or output position by half a unit [5].

The two-dimensional DCT is taken as an example.

- By using the mapping transformation method, the image compression is achieved by transforming each pixel in the image from one space to another, and the signal is transformed from the spatial domain to the frequency domain after DCT. It's a method of orthogonal transformation. It is a special case in the image processing that is widely used in the Fourier transform. The expanded function is a real function, and then discretized, that is a discrete cosine transform.
- Like the Fourier transform, there are two kinds of positive and inverse transformations.

Positive DCT: from spatial domain to frequency domain; inverse DCT: from frequency domain to spatial domain.

3.4. Specific Formula

1) FDTC (positive transformation):

$$\mathrm{f}(u,v)=c(u)c(v)\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}\mathrm{F}(x,y)\cos\frac{\pi(2x+1)\mathrm{u}}{2M}\cos\frac{\pi(2y+1)v}{2N} \tag{1}$$

$u=0,1\ \cdots\ M-1,\ v=0,1\ \cdots\ N-1$

2) IDCT (inverse transformation):

$$F(\mathrm{x},y)=\sum_{u=0}^{M-1}\sum_{v=0}^{N-1}c(u)c(v)f(u,v)\cos\frac{\pi(2x+1)u}{2M}\cos\frac{\pi(2y+1)v}{2N} \tag{2}$$

$x=0,1\ \cdots\ M-1\ y=0,1\ \cdots\ N-1$

3) Simplified formula

$$F(u,v)=Af(x,y)A^{T} \tag{3}$$

when $M=N$, the DCT transform can be expressed as a matrix multiplied form, where A is in the for

$$A=\begin{bmatrix}\sqrt{1/N}[& 1 & 1 & \cdots & 1\\ \sqrt{2/N}[& \cos(\pi/2N) & \cos(3\pi/2N) & \cdots & \cos\left((2N-1)\pi/2N\right)\\ \sqrt{2/N}[& \cos(\pi/2N) & \cos(6\pi/2N) & \cdots & \cos\left((2N-1)\pi/2N\right)\\ \vdots & \vdots & \vdots & \vdots & \vdots\\ \sqrt{2/N}[& \cos\left((N-1)\pi/2N\right) & \cos\left((N-1)3\pi/2N\right) & \cdots & \cos\left((N-1)(2N-1)\pi/2N\right)\end{bmatrix} \tag{4}$$

1) $f(x,y)$ is a digital image matrix of $M*N$ and the spatial sampled value, that is the pixel value of the point (x,y), which is the coordinates of the input 8 × 8 pixels.

2) $F(x,y)$ is the frequency domain sampled value, and the coordinates of the output 8 × 8 transform result.

4. Watermark Embedding

- The image matrix $f(x,y)$ which need to be embedded in the watermark is divided into 8 × 8 image blocks, and the image block is subjected to DCT transformation to obtain a frequency domain coefficient matrix $F(u,v)$.

- Selecting algorithm to determine frequency domain coefficients and then to make the watermark embedded, that is the selected frequency domain coefficients are modified to form a new frequency domain coefficient matrix. There are two basic methods for modifying the coefficients, as shown in formula (5) and formula (6):

$$\textbf{\textit{Addition principle}} \quad F' = F + a * W \tag{5}$$

$$\textbf{\textit{Multiplication principle}} \quad F' = F * (1 + a * W) \tag{6}$$

Among:

"***F***" in the formula denotes the frequency domain coefficient before modification

"***F***" denotes the modified frequency domain coefficient

"***W***" denotes the embedded watermark information

"***a***" denotes the embedded strength of the watermark, and "***a***" determines the amplitude of the frequency domain coefficient to be modified.

- Perform IDCT on the new frequency domain coefficient matrix $F'(u,v)$ to obtain an 8 × 8 image block containing the watermark, and replace the original image block to obtain the watermarked image $m(x,y)$.

Figure 1 is a watermark embedded block diagram.

5. The Extracting of the Watermark

Watermark Extraction Algorithm

- The extraction of watermark is the inverse process of the watermark embedding algorithm [6]. The image $m(x,y)$ containing the watermark and the original image $f(x,y)$ are respectively DCT transformed to obtain the frequency domain coefficient matrix $M(u,v)$ and $M'(u,v)$.
- The selected frequency domain coefficients are modified to form a new frequency domain coefficient matrix. Modify the coefficient formula (7):

$$N(p,q) = \left(M(u,v) - M'(u,v)\right) / b \tag{7}$$

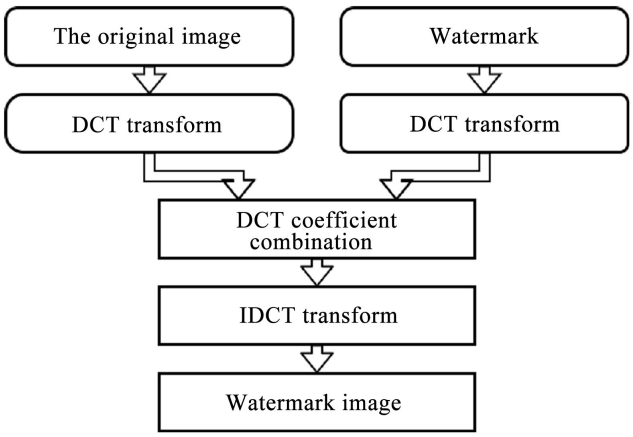

Figure 1. Watermark embedding block diagram.

- Perform IDCT on the new frequency domain coefficient matrix $N(p,q)$ to obtain an 8 × 8 image block containing a watermark, and replace the original image block to obtain an image $n(p,q)$ containing the watermark.

Figure 2 is a Watermark extraction block diagram.

6. Watermark Attack Detection

The so-called attack on the watermark refers to the destruction of the watermark, including smearing, shearing, scaling, rotation, compression, noise addition, filtering, and the like. Digital blind watermarking is not only about agility, but also defensive. The imperceptibility and robustness of digital blind watermarks are mutually exclusive [7].

6.1. White Noise

Image noise causes random signal interference during image acquisition or transmission, hindering people's understanding and analysis of the image. Image noise is often viewed as a multidimensional random process, so the method of describing noise can be borrowed from the description of a random process. White noise refers to the noise energy contained in a band of equal bandwidth over a wide frequency range. It is a random signal or stochastic process with a constant power spectral density. In other words, the power of this signal is the same in each frequency band. Since white light is a mixture of monochromatic lights of various frequencies (colors), the property of this signal with a flat power spectrum is called "white". This signal is therefore also referred to as white noise [8] [9].

6.2. Gaussian Low-Pass Filtering

Gaussian filtering is a linear smoothing filter that is suitable for eliminating Gaussian noise and is widely used in the noise reduction process of image processing. In layman's terms, it's the process of weighted averaging of the entire image, the value of each pixel is obtained by weighted averaging of itself and other pixel values in the neighborhood [8].

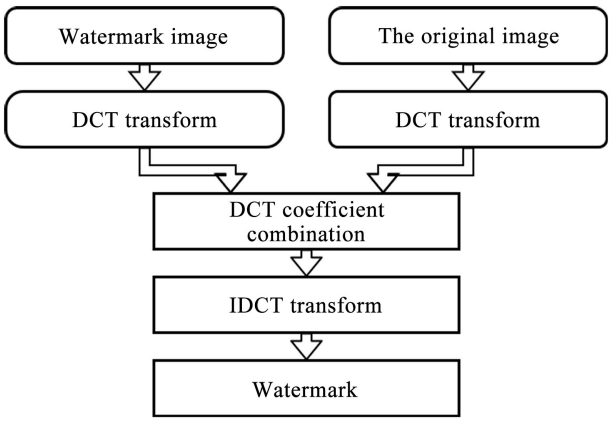

Figure 2. Watermark extraction block diagram.

Low-pass filtering is used to smooth the image. The goal of the low-pass filter is to reduce the rate of change of the image. For example, replace each pixel with the mean of the pixels around the pixel. This makes it possible to smooth and replace areas where the intensity changes significantly [10] [11]. The difference between low-pass filtering and Gaussian filtering is that in low-pass filtering, the weight of each pixel in the filter is the same, that is, the filter is linear. The weight of the pixels in the Gaussian filter is proportional to the distance from the center pixel.

6.3. Attack Detection

6.3.1. Testing

Digital watermarks have many features, but the basic features are as follows:

- Imperceptibility: The so-called imperceptible refers to the meaning of two aspects, one refers to the invisibility of the human eye, and the other refers to the statistical method cannot recover the watermark pattern of our embedded side.
- Robustness: Robustness refers to a system that can maintain certain performance characteristics under certain parameter changes, such as attacks and input errors. It can be classified into stable robustness and performance robustness [12]. In the specific context of this article, robustness refers to the ability to detect watermarks from watermarked images after noise attacks, low-pass high-pass filtering, geometric distortion, etc. Robustness for watermarks. It is a very important feature.
- Validity, effectiveness is mainly for the watermark system, it is a probability value, which characterizes the ability of us to detect the watermark. Of course, the larger the value, the better. But when it is closer to 100%, the more we have to sacrifice on other features, the more we have a trade-off, and sometimes we sacrifice some effectiveness based on our focus [13].

Fair algorithm comparison and performance evaluation between different digital watermarking systems are of great significance for the standardization of digital watermarks and the practical application of watermarks [14]. The key to performance evaluation of the watermarking system is to establish an evaluation benchmark. The criteria for evaluating the watermark system include not only the evaluation of robustness, but also the subjective or quantitative evaluation of the distortion introduced by the watermark processing [15] [16]. In other words, there needs to be a trade-off between the robustness and invisibility of the watermark.

6.3.2. Image and Watermark

In this paper, the robustness of the first feature of digital watermarking is tested. White noise and Gaussian low-pass filtering are selected as the attack. The watermarked image is extracted and compared with the unaffected watermark.

- Original image and watermark as shown in **Figure 3** and **Figure 4**
- Adding the watermarked image and the extracted watermark

As follows, the DCT is successfully used to embed the watermark. Compared with the original image, the difference is not substantial, and the shape and obvious features of the watermark are not visible, and it has good imperceptibility. A watermarked image can extract a relatively complete watermark.

Watermarked image and the extracted watermark are as shown in Figure 5 and Figure 6:

- Gaussian low-pass filtering attack

After the filtering attack, the image curve is smooth and the ambiguity is high, but the watermark is still completely extracted, and the watermark is clearly visible, indicating that the robustness is better after being filtered and attacking the watermark image.

Gaussian filtering and gaussian filtering are as shown in Figure 7 and Figure 8.

- White noise attack

As shown in the figure below, after the white noise attack on the image, the image is somewhat distorted, but the watermark is still extracted more completely. It shows that the image is still robust and robust after attacking the watermark image with white noise.

As shown below Figure 9 and Figure 10:

Figure 3. Original image.

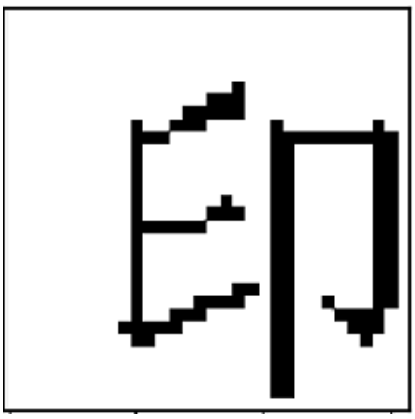

Figure 4. Original watermark.

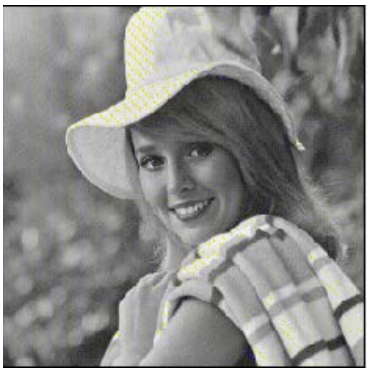

Figure 5. Watermarked image.

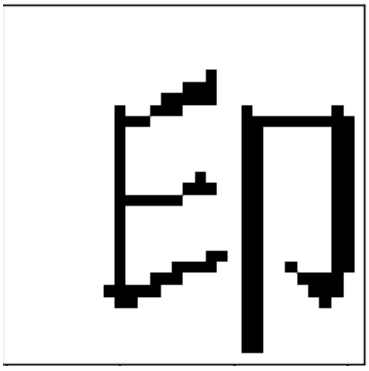

Figure 6. The extracted watermark.

Figure 7. Gaussian filtering.

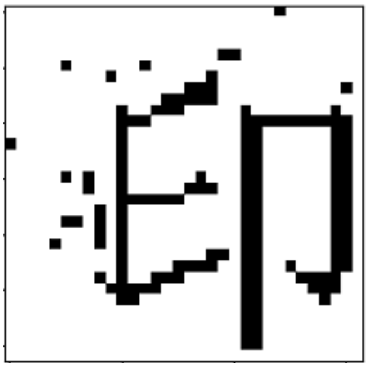

Figure 8. Gaussian filtering (Gaussian).

Figure 9. White noise.

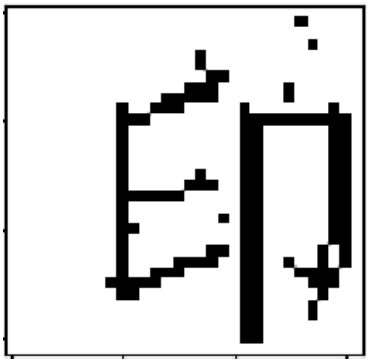

Figure 10. Extracted watermark (white noise).

7. Conclusion

Fair algorithm comparison and performance evaluation between different digital watermarking systems are of great significance for the standardization of digital watermarks and the practical application of watermarks. The key to performance evaluation of the watermarking system is to establish an evaluation benchmark. The criteria for evaluating the watermark system include not only the evaluation of robustness, but also the subjective or quantitative evaluation of the distortion introduced by the watermark processing. So there needs to be a trade-off between the robustness and invisibility of the watermark. The watermarking signal embedded in the watermarking algorithm based on DCT domain is robust and can effectively resist some attack methods that use signal distortion to destroy watermark. The robustness is good; the embedded watermark cannot be recognized, and the watermark image is not distinct from the original image, and is not perceptible. An algorithm for blind watermarking is implemented.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Huang, F.Y. (2004) Digital Watermarking Technology Based on Transform Domain

and Image Compression Coding. University of Electronic Science and Technology of China, Chengdu.

[2] Wang, H. (2016) Research on Digital Image Blind Watermarking Algorithm Based on DCT Domain. *Modern Vocational Education*, No. 14, 76-77.

[3] Yang, J.H. (2006) Research and Implementation of Digital Image Watermarking Algorithm Based on Frequency Domain. Southeast University, Nanjing.

[4] Han, W. (2006) Research on Digital Video Security Monitoring System. Shanghai Jiaotong University, Shanghai.

[5] Zhang, H.Y. (2004) Image Compression Based on DCT. *National Youth Communication Conference*, Chongqing, 1246-1251.

[6] Wei, W.Y. (2010) Adaptive Image Watermarking Algorithm Based on Wavelet Contrast. *Computer Engineering and Applications*, **46**, 89-90.

[7] Yang, D. (2014) Attack Methods and Evaluation of Digital Watermarking. *Computer Programming Techniques & Maintenance*, No. 3, 53-57.

[8] Minichino, J. (2016) OpenCV 3 Computer Vision: Python Language Implementation. 2nd Edition, Mechanical Industry Press, Beijing.

[9] He, X.H. (2005) Image Communication. Xi'an University of Electronic Science and Technology Press, Xi'an.

[10] Bao, X.X. and He, D.J. (2007) Color Image Watermarking Algorithm Based on DCT. *Microelectronics & Computer*, **24**, 91-93.

[11] Wang, B., Chen, Q. and Deng, F. (2004) Digital Watermarking Technology. Xidian University Press.

[12] Chen, C. (2003) Computer Image Processing Technology and Algorithm. Tsinghua University Press, Beijing.

[13] Huang, F., Guan, Z. and Wu, X. (2006) Research on Blind Watermarking Algorithm Based on Discrete Cosine Transform. *Journal of Huazhong University of Science and Technology* (*Natural Science*), **34**, 17-19.

[14] Jiang, B. (2006) A Blind Watermarking Algorithm Based on Positive and Negative Discrimination of DCT Coefficients. *Shanxi Electronic Technology*, No. 3, 57-58.

[15] Zhang, J. (2006) An Algorithm for Improving Watermark Robustness in DCT Domain. *Journal of Computer Applications and Software*, **23**, 100-101.

[16] Wang, J., Dai, Y. and Wang, Z. (2005) A Blind Watermarking Algorithm for Interpolating Frequency Coefficients in DCT. *Journal of Nanjing University of Science and Technology* (*Natural Science*), **29**, 9-13.