# The digital watermarking technology research based on DCT coefficient

**ZhAO Lian-qing [1], LV Zheng-quan[2]**

*School of Electric and Electronic engineering , North China Electric Power University, Beijing 102206*

*1.zhaolianqing@163.com , 2.lvzhengq@163.com*

**Abstract:** Using discrete cosine transform and Arnold transform , It realized the digital image information hiding. we analyze the relationship of the embedded watermark image with the host image, but also with the peak signal to noise ratio of the host image and the embedded watermark image. Besides that, we analyze the algorithm's robustness and invisibility for the geometric attack as well as white Gaussian noise attack .

**Keywords:** Digital watermarking; DCT; Arnold transform; Watermark strength

## 1 Introduction

In recent years, digital watermarking for copyright protection of digital products and authentication technologies has become a research hotspot. It is generally believed that Digital watermarking should have the following characteristics [1]:

No-perceiving: the non-perception is a means of visual or hearing impairment's non-sensory, which means that the observer can't detect the change of vector data embedded into the watermark data in the term of the visual and hearing .The most ideal situation is that the watermark with the original vector are visually identical and the vast majority of the watermarking algorithm can meet the requirements.

Proven: the watermark should be able to be copyright-protected digital products providing full attribution of reliable evidence. Watermarking algorithm can be used to embed the owner of the relevant information (such as number of registered users, product logo or meaningful language, etc.) in the object to be protected, and extract information when we want. Watermarking can be used to determine whether the object should be protected and be able to monitor the protected data transmission, the authenticity of identification and control of illegal copies.

Robustness: robustness refers to that the watermark should be able to bear the substantial physical and geometric distortion, including the intentional (such as malicious attacks) or unintentionally (such as image compression, filtering, printing, scanning and copying, noise pollution, the size change, etc.).Obviously, after these operations, the robust watermarking algorithm should be able to extract watermark from vector data embedded watermark or to prove the existence of a watermark. A robust watermark should be done if an attacker tried to delete the watermark which will lead to total destruction of the watermark vector. Because of the characteristics that the watermarking depends heavily on the application, an appropriate evaluation criteria is decided by a specific application. A lot of types of digital watermarking may not have these characteristics, or only have some of these characteristics.

Discrete cosine transform of digital watermarking technology is a transform-domain algorithms. First, the original data using the DCT transform, the hidden information for Arnold transform getting scrambling image, then we embed the scrambling image, at last DCT inverse transform and Arnold transform should be used to extract embedded information. For the algorithm, if we choose suitable watermark strength, it can basically meet the three conditions above.

## 2 Discrete Cosine Transform

Images are two-dimensional data, we have only carried out the description of discrete cosine transform for two-dimensional .

$$F(\mu,\nu)=\frac{1}{N}\sum\sum f(x,y)\cos\frac{(2x+1)\mu\pi}{2N}\bullet\cos\frac{(2y+1)\nu\pi}{2N} \quad (1)$$

In the equation: $f(x,y)$ is on behalf of a two-dimensional element for spatial domain, where $x,y=0,1,2,\cdots,N-1$; $F(\mu,\nu)$ is on behalf of a element of the transform coefficient array. The array is

N×N[2];

For example，if N=8, we can get the coefficient of the

DCT $\mathbf{A}$

$$\mathbf{A}=\begin{bmatrix} 0.354 & 0.354 & 0.354 & 0.354 & 0.354 & 0.354 & 0.354 & 0.354 \\ 0.490 & 0.416 & 0.278 & 0.098 & -0.098 & -0.278 & -0.416 & -0.490 \\ 0.462 & 0.191 & -0.191 & -0.462 & -0.462 & -0.191 & 0.191 & 0.462 \\ 0.416 & -0.098 & -0.490 & -0.278 & 0.278 & 0.490 & 0.098 & -0.416 \\ 0.354 & -0.354 & -0.354 & -0.354 & -0.354 & -0.354 & -0.354 & -0.354 \\ 0.278 & -0.490 & -0.098 & 0.416 & -0.416 & -0.098 & 0.490 & -0.278 \\ 0.191 & -0.462 & -0.462 & -0.191 & -0.191 & -0.191 & 0.462 & 0.191 \\ 0.098 & -0.278 & -0.416 & -0.490 & 0.490 & -0.416 & 0.278 & -0.098 \end{bmatrix} \quad \textbf{(2)}$$

For the equation (1) ,we can get the following equations **(3)**,**(4)**:

$$\mathbf{F}(\mu,v)=\mathbf{A}\mathbf{f}(x,y)\mathbf{A}^{\mathbf{T}} \qquad \textbf{(3)}$$

$$\mathbf{f}(x,y)=\mathbf{A}^{\mathbf{T}}\mathbf{F}(\mu,v)\mathbf{A} \qquad \textbf{(4)}$$

For the equation(4),it is the two-dimensional data space of the inverse transform. Because a few of coefficients can characterize the signal[3], we can use the nature to embed the information into the vector data. For the watermark image and vector data, the DCT is used and by changing the coefficients which the human cannot detect the variation, the information will be hided. As the following, the process will be shown in front of us.

## 3 Specific Implementation

Various transform methods are used to deal with the original watermark carriers, and a large number of data can be embedded into the original watermark carriers which will not lead to the naked eye to detect. Taking into account the human visual system (HVS) characteristics, which have different characteristics in the local nature of the region in the guarantees of non-visibility, under the premise that allows superposition of different signal intensity. So we can put the original image block in order to overlay the watermark different intensity, namely on the original gray image in accordance with the size of block, and then carried out on each piece of DCT transform [4-5]. The original vector images in non-overlapping 8 × 8 block DCT transform, the operation function using the MATLAB environment has provided the sub-block DCT transform function [6]. Figure 1 is a complete flow of the watermark, including the watermark image scrambling, embedding and extraction. We will carry out them out.

### 3.1 Scrambling Watermark Image and The Restoration

For the embedded watermark image, we will use the

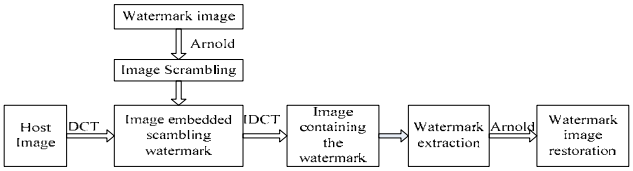


**Figure 1 Digital Image Watermarking overall flow**

Arnold transform, so that they are certain confidentiality and robustness.

#### 3.1.1 Arnold algorithm

Arnold transform is made by the Russian mathematician Vladimir I. Arnold. A N × N two-dimensional digital image of Arnold transform is defined as:

$$\begin{bmatrix} x' \\ y' \end{bmatrix}=\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix}(\mathrm{mod}\, N) \qquad \textbf{(5)}$$

Where $x,y\in\{0,1,2,3\cdots N-1\}$ is a coordinate before the transform, mod is the modulus operator. Digital image can use the matrix transform to achieve the purpose of information scrambling.

Because of Arnold algorithm's the cyclical, we do not have to worry about scrambling image problem that can not be restored. Arnold transform cyclical is related with the size of the image, but not directly proportional. Such as a size of 128×128 images' period of Arnold transform is 96, a size of 240×240 images' period of Arnold transform is 60. Table 1 gives a different N value corresponding to the cycle [7].

**Table 1 Arnold scrambling algorithm N value with its cycle T**

| N | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|
| T | 4 | 3 | 10 | 12 | 8 | 6 |
| N | 16 | 32 | 64 | 128 | 256 | 512 |
| T | 12 | 24 | 49 | 96 | 192 | 384 |

#### 3.1.2 Arnold transform authentication

We used a 32 ×32 bmp map used as a watermark embedding, as shown in figure 2:

Comparison of figures 2 and 4, we can see that a cycle after Arnold transform the scrambling image can be fully restored. But the premise is that we know

**Figure 2 Watermark image**

**Figure 3 For 10 times transform the watermark image**

**Figure 4 For 24 times transform the watermark image**


978-1-935068-01-3 © 2009 SciRes.

the transform's number, which means we obtain the key conditions, and then it can resume the image, which playing a role in the information encryption.

### 3.2 Embedded Images

First of all, reading the host image and watermark image respectively, the host image is divided into 8×8 blocks, and then using DCT to transform each piece. While for the watermark image, it determines whether to embed the information .If the grey level of the pixel is 0 ,then the coefficient subtracts a number , contrarily the coefficient adds a number.

Specific flow as follows:

(1): The original image is divided into 8 small pieces of eight;

(2): One for each DCT transform, if the grey level of the watermark information is 0 ,then flag = -1,else flag = 1; DCT transform coefficients add (1 + flag× $\alpha$ ); flag is just a sign and $\alpha$ is embedment strength.

(3): For the image adjusted, we use the inverse transform DCT to each block.

Following the above, we will get the image embedded the scrambling information of the watermark image.

### 3.3 Watermark Images Extracted

Extracted watermark images are the inverse process of watermark embedding. For the embedded images and the original host image, the DCT transform is used firstly, and then the corresponding values for division, if the result is more than one, corresponding to the location of the gray level of 0, else 1. So that we can restore a picture of the information embedded in the host image.

Specific flow as follows:

(1): Dividing the embedded watermark image into blocks.

(2): For each small piece for DCT transform, the coefficients obtained divide the original host image DCT transform coefficients , then minus 1, if the result is greater than 0 ,then the corresponding value for the location is 1, else 0, so that you can access binary watermark image.

### 3.4 Watermark Image Restoration

The images are extracted after Arnold transformed image, we will cycle to Arnold transform to restore the image. For example, image 32×32 bmp picture, Arnold transform cycle is 24.We have adopted the change of number of 10,then if we want to restore the image, 14 times Arnold transform will needed. 3.1.2 has been verified. We will not explain it in this part.

## 4 Experiment and Verification

### 4.1 Watermark Strength for the Watermark Extraction

For the experiment, we used 256×256 grayscale ncep.bmp, the size of the embedded watermark image is 32×32 , as shown in Figure 5.


**(a)Host image** **(b)Watermark image**

**Figure 5 Host image and watermark image ((a) host image, (b) watermark image)**

First of all, in the absence of any attack, we analyze the relevance of the strength of watermark embedding with the image extracted from the host image, as well as with the nature of no-perceiving for the image embedded watermark' no. Figure 6 when $\alpha$ = 0.02, the information obtained as well as the embedded watermark images.


**(a) Image embedded watermark (b) Extracted watermark image**

**Figure 6 Image embedded watermark without any attraction( $\alpha$ =0.02)((a) Image embedded watermark (b) Extracted watermark image)**

For the variation between the embedded watermark image and original image , we used *PSNR* (peak signal to noise ratio) to measure its characteristic of perception. *PSNR* calculation formula is as follows:

$$PSEN = 10 * \log\left(\frac{(2^N - 1)^2}{MSE}\right) \quad \textbf{(6)}$$

$$MSE = \frac{\sum_{n=1}^{Framesize}(I^n - P^n)}{Framesize} \quad \textbf{(7)}$$

In the equation**(7)**, *MSE* is the mean square error between the original image and the image processed . Formula symbols are adopted the usage of MATLAB. 8 bits expression as the maximum 255, $N$ = 8. $I$ refers to the first n months pixel values for the original image, and $P$ means the first $n$ months pixel value for the image processed. *Framesize* refers to the image size, *PSNR*'s unit is the dB. Therefore the greater the *PSNR* value, the less the *MSE* , which is meaning the Less distortion.

Calculated by MATLAB , we have obtained the following data, as shown in table 2.

**Table 2 Relationship between $\alpha$ and $\rho$ , as well as *PSNR***

| $\alpha$ | 0. 005 | 0. 01 | 0. 02 | 0. 03 |
|---|---|---|---|---|
| $\rho$ | 0. 9874 | 1 | 1 | 1 |
| *PSNR*(dB) | 49. 6205 | 44. 3505 | 38. 6982 | 35. 3652 |

$\rho$ : the correlation coefficient; $\alpha$ : embedment strength

From Table 2, with the embedded intensity increased, $\rho$ is growing and the extraction of the watermark image is closer to the original image, but a watermark image host has a greater distortion, leading the non-perception poor. This requires us to select the embedding strength with a reasonable value. In the absence of any attack, by the circumstances, we may wish to select $\alpha$ =0.02 to achieve the best watermark effect.

## 4.2 Digital watermarking Robustness analysis

### 4.2.1 Gaussian white noise attack

Gaussian white noise with mean 0, standard deviation 0.01.

(1) $\alpha$ =0.03

The images obtained from the experiment shown in figure 7.

Calculated by MATLAB, we got the $\rho$ =0.4259,

Calculated by MATLAB, we got the $\rho$ =0.2039, *PSNR*=35.3652dB,the watermark can't be recognized. The information of the watermark is lost all.

(2) $\alpha$ =0.05

The images obtained from the experiment shown in figure 8.

**(a) Image embedded watermark (b) Extracted watermark image**

**Figure 7 $\alpha$ =0.03 Image embedded watermark and the restored watermark((a) Image embedded watermark (b) Extracted watermark image)**

**(a) Image embedded watermark (b) Extracted watermark image**

**Figure 8 $\alpha$ =0.05 Image embedded watermark and the restored watermark((a) Image embedded watermark (b) Extracted watermark image)**

*PSNR*=31.1392dB.The watermark can be recognized but not clearly.

(3) $\alpha$ =0.1

The images obtained from the experiment shown in figure 9.

**(a) Image embedded watermark (b) Extracted watermark image**

**Figure 9 $\alpha$ =0.1 Image embedded watermark and the restored watermark((a) Image embedded watermark(b) Extracted watermark image)**

Calculated by MATLAB, we got the $\rho$ =0.5376, *PSNR*=25.4032dB.The watermark can be recognized .But we can detect the scrambling watermark obviously.

From above, this digital watermarking algorithm for the Gaussian noise attack is weak . Once the embedded watermark with lower intensity, it is hard to restore to the original embedded watermark information. But once the embedded strength becomes



978-1-935068-01-3 © 2009 SciRes.

great, the embedded image can be easily observed by the human eyes. So we should select the appropriate intensity $\alpha$ in order to satisfy the embedded watermark image robustness and non-perception simultaneously.

### 4.2.2 Geometric Attack

When $\alpha$ =0.03, we analyze the effects of geometric attacks for digital images.

(1)Image embedded a watermark image without the right-down part:

**(a)Image embedded watermark without the right-down part (b)watermark exacted from the image**

**Figure 10 The lower right corner of the shear((a)Image embedded watermark without the right-down part (b)watermark exacted from the image)**

Calculated by MATLAB, for the extracted watermark image and embedded image $\rho$ =0.8614.

(2)Image embedded a watermark image without the left-up part:

**(a)Image embedded watermark without the right-down part (b)watermark exacted from the image**

**Figure 11 The lower right corner of the shear((a)Image embedded watermark without the up-down part (b)watermark exacted from the image)**

Calculated by MATLAB, for the extracted watermark image and embedded image , $\rho$ =0.9489. It can fully extract the watermark information.

From above, it can be seen that the watermark algorithm has very good anti-geometric offensive.

## 5 Summary

The watermark information to be embedded into the host image first use Arnold transform to scramble the information ,which playing the role of encryption to hide information, divide the host image into blocks, and then for each block' DCT transform, the watermark information embedded into the DCT transform coefficients, and then after DCT inverse transform information eventually will be embedded into the host image. After inverse process of extracting the watermark information for Arnold cycle eventually transform to extract the watermark information.

In addition, we analyze anti-Gaussian noise and geometric attacks' ability. It certificated that for the Gaussian noise ,when embedding strength to a certain degree ,we can extract the watermark meeting the requirements basically., but *PSNR* is low, the performance of non-perception is bad. For the geometric attack, this algorithm has good performance. At the same time we also analyzed the intensity with the extraction of embedded watermark image and the watermark image the link between relevance, pointing out that a reasonable selection of the embedded watermark strength to balance the robustness and non-sensory.

## References

[1] Yang Song. Wen Qiao-yan. Digital watermarking attacks and experimental analysis[DB/OL]. http://www.paper.edu.cn

[2] Ruan Qianqi.Digital Image Processing Study[M].Beijing:Publishing House of Electronics Industry,2007.102~104.

[3] Luo Junhui,Luo Yongjiang,Bai Yicheng etc. matlab7.0 in Image Processing Applications[M].Beijing:China Machine Press.56~57.

[4] Sun Sheng-he，Lu Zhe-ming，Liu xia-mu. Digital watermarking technology and its application[M]. Science Press.2004.

[5] Wang Li-na,Guo Chi,Li Peng. Information Hiding Technology Experiment Tutorial[M].WuHan University Press.2004.

[6] He Meijuan,Jing Xiao-jun. Based on the DCT transform domain general shear resistance of the Image Digital Watermarking attack[DB/OL]. http://www.paper.edu.cn.

[7] HUANG Fang-yuan .Image Scrambling Based on Arnold Transforming and Implementation[J]. Journal of Guizhou University (Natural Sciences),2008.5,Vo.l 25 No. 3.P277-288.