# A Robust Digital Watermarking Algorithm Based On Pre-processing Method

Jingzhou Sun[1, a], Yizhen Cao[2, b], Yongbin Wang[3, c]

[1, 2, 3]School of computer, Communication university of china, Beijing, 100024, China

[a]sunjingzhou333@yahoo.com.cn, [b]caoyizhen@cuc.edu.cn, [c]ybwang@cuc.edu.cn

**Keywords:** Digital Watermark, Watermark Pre-processing, Watermark Algorithm, Robustness.

**Abstract.** In recent years, with the development of computer and networking technology, much more attention has been raised to digital watermark technology. The robustness and invisibility are two main indicators of the digital image watermarking system, and the combination of watermark pre-processing and embedding watermarking algorithm can improve the robustness and reduce error rate. In this paper, the algorithm can extract watermark without the original image, and realize a blind detection of watermark. The experimental results show that this algorithm is good at invisibility, and has good robustness to the attacks of down-sampling, noise, format converting, filtering.

## Introduction

With the rapid development of computer and network technology, the digitization of information media makes the accuracy of the information acquisition, information storage, and information transmission. People can easily spread information to all parts of the world by means of computers, scanners, printers and other electronic equipments. Compared with the traditional production, the digital production has more advantages. But, it is easy being copied and modified; so many copyright owners would not like to share their productions, which could prevent the cultural communication and development of technology. Under this background, digital watermarking [1] was born. The digital watermarking technique is to embed a message into the digital production in robust yet imperceptible way in order to product the copyright of digital production.

The characteristics of digital watermark are its quality of invisibility, robustness, certainty, and security. And the pre-processing of watermark information has a great help to the improvement of these characteristics. In this paper, we try to demonstrate how to use the error correction coding and chaotic maps as a watermark preprocessing method to improve it, with a watermarking algorithm to explain it.

## Image Watermarking System in DCT Domain

Digital image watermarking system can be divided into non-blind watermarking system and blind watermarking system according to the need of original image. Non-blind watermarking system significantly limits its practical application by requiring the original carrier [2]. The embedded and checkout models of blind watermarking system in DCT domain are shown in Fig. 1 and Fig. 2(Dotted box is not essential):
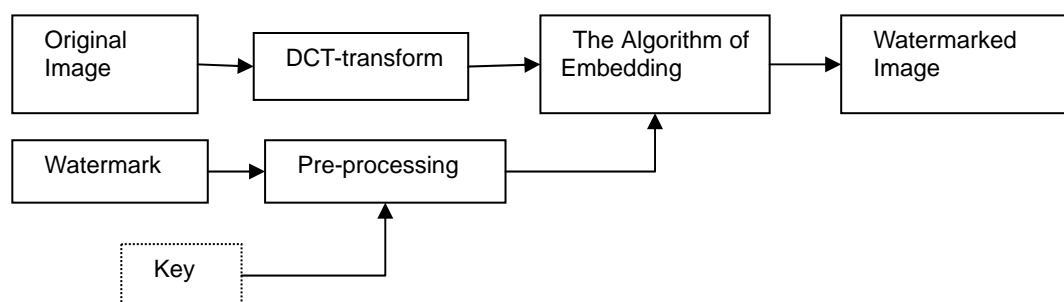


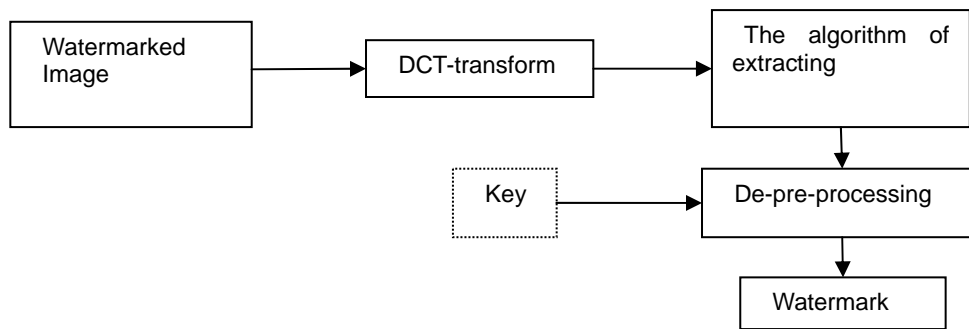Figure1.  Image Watermarking System of Embedded Model

Figure2.   Image Watermarking System of Detected Model

## The analysis of watermark pre-processing method

**The Introduction of Watermark Pre-processing**. The principle of watermark pre-processing is to make watermark mapped to a disordered sequence by watermark pre-processing method. The purpose is to break the correlation between the pixels in the original watermark, enhancing its invisibility and robustness. Many methods are used in watermark pre-processing, including the scrambling transformation, error correction coding, chaotic maps and spread spectrum, etc.

**Error Correction Coding.** The basic idea of error correction coding is to make the mutually independent, and unrelated information codes become the data sequence which has some relevance and some regularity by making some kind of transformation to the original sequence, According to this rule, the recipient of the information can make inspection and correct the errors of codes in the transmission channel. The principle of error correction [3] could be introduced to watermark algorithm to conduct error control, which can improve the robustness of the watermark.

Because of the consideration of real-time and computational complexity, the algorithm of this paper uses the most common (7, 4) Hamming code [4].We can detect errors of the message in transmission channel by (7, 4) Hamming code and the method is very quick and easy. Watermark technology requires the algorithm as simple as possible, so watermark pre-processing should be simple as well. (7, 4)Hamming code can ensure the efficiency of the watermark.

**Chaotic Map.** Chaos phenomenon is deterministic, which is similar to the random process that appears in a nonlinear dynamical system. This process is neither periodic nor convergent, and has extremely sensitive dependence on the initial value. With the maturity of the nonlinearity and chaos theory, the research for chaos is focused on application, especially on communication. The reason is that chaotic systems has sensitive dependence on the initial value, which can provide a large number of non-related, random but determined renewable signal.

A very simple but extensively studied dynamical system is the Logistic map; The definition is as follows [5]:

$$x_{k+1} = \mu x_k (1 - x_k) \tag{1}$$

Here $1 \le \mu \le 4$   $x_k \in (0,1)$ .   The results of chaotic system research show that: when $3.5699456 < \mu \le 4$, Logistic map is in a chaotic state.

In fact, Logistic map can also be defined in the (-1, 1) interval, its form is as follows:

$$x_{k+1} = 1 - \mu x_k^2 \tag{2}$$

Here $\mu \in [0,2]$.When $\mu \to \mu_\infty = 1.4115$, quickly reaches cycle $N \to \infty$, and then enters chaos state. The probability density function of chaotic sequence is:

$$\rho(x) = \frac{1}{\pi\sqrt{1-x^2}} \quad -1 < x < 1 \tag{3}$$

But in the first definition, when $\mu = 4$, probability density function can be rewritten as:

$$\rho(x) = \frac{1}{\pi\sqrt{\partial(1-x)}} \quad 0 < x < 1 \tag{4}$$

By means of $\rho(x)$ , we can easily get some meaningful statistical characteristics in chaotic sequence which is generated by Logistic map.

The advantages of Logistic map can be summarized as follows:

(1). The form is simple.

(2). Be sensitive to initial conditions.

(3). It has the statistical characteristics of white noise, and it can be used in a number of occasions which need white noise modulate.

We can choose the chaotic sequence to make watermark preprocessing because of these properties of the chaotic sequence.

**The Realization of the Algorithm of Watermarking System**

**The Pre-processing of Watermark.** The steps of the pre-processing of watermark are as follows.

1. The first step is to make chaotic sequence processing

(1). Convert the initial watermark to binary sequence and take it as the initial sequence $W$

(2). Set a key $x_0$ as the initial value of the chaotic sequence, select a $\mu$ between 3.5699456 and 4, then use Logistic map to produce a real value sequence.

(3). Convert real-valued sequence to binary chaotic sequence by threshold function, and make the binary chaotic sequence XOR with the original watermark sequence to modulate watermark information.

2. Transcode the generated sequence by 74 yards.

**The Embedded Algorithm of Watermark.** The steps of the embedded algorithm of watermark are as follows.

(1). 8 * 8 blocks DCT transform on the carrier image I, get a matrix $A$ .

(2). Select a group of adjacent coefficients in the zigzag arrangement in the matrix A in the low-frequency region. Embed watermark by modifying the relative size of the adjacent coefficients, we can get a new watermarked matrix $B$

The pseudo-code for the embedded watermark is:

Two coefficients are set as X, Y in the coefficient group. $msg$ represents the pre-processed watermark information, and $\alpha$ represents the embedding strength of watermark.

If $msg$ ==0

If X>Y

X=X-(X-Y)/2 - $\alpha$ ;

Y=Y+(X-Y)/2 + $\alpha$ ;

Else $msg$ ==1

If X<Y

X=X+(Y-X)/2 + $\alpha$ ;

Y=Y-(Y-X)/2 - $\alpha$ ;

(3). Make IDCT transformation to matrix $B$ , and then get watermarked image $I'$ .

**The Extraction Algorithm of Watermark.** The steps of the extraction algorithm of watermark are as follows.

(1). Make 8 * 8 block- DCT transformation on the image $I'$ , and then get a matrix $A_1$ .

(2). According to the Coefficients which are selected in step (2) in 4.2, we can extract watermark information by comparing the size of them.

The pseudo-code for the detection watermark is:

If X<Y msg=0

Else msg=1

**The De-pre-processing of Watermark.** The steps of the de-pre-processing of watermark are as follows.

(1). Through 74 yards of the inverse transform to extract the chaotic handled sequence.

(2). Set a key $x_0$ as the initial value of the chaotic sequence, and $\mu$ which is selected, we

can produce a real value sequence by logistic mapping.

(3). Convert real-valued sequence to binary chaotic sequence by threshold function, and make the binary chaotic sequence XOR with the original watermark sequence to decrypt watermark information, and get the watermark information.

## Experimental Results

To verify the algorithm, I selected two bmp images of Lena and the baboon of 512 gray levels to do a experiment. The experiment environment is MATLAB 7.0, coefficient pairs $(AC^{36}, AC^{63})$, $(AC^{41}, AC^{52})$ are selected to embed watermark, embedding strength $\alpha$=0.02, with $x_0 = 0.2$，$\mu = 3.9999$ in chaotic sequence. The types of attack used in the experiment are the down-sampling of halved sampling rate, the Gaussian low-pass filters of normalized cutoff frequency of 0.8, the Gaussian noise whose variance is 0.2 and the trans-coding of jpeg to bmp.

**Experimental Results when Embedded Position is（AC36 ， AC63）.**The PSNR of the attacked watermarked image and the NC value of the extracted watermark are showed in table1.

Table 1Experimental Results

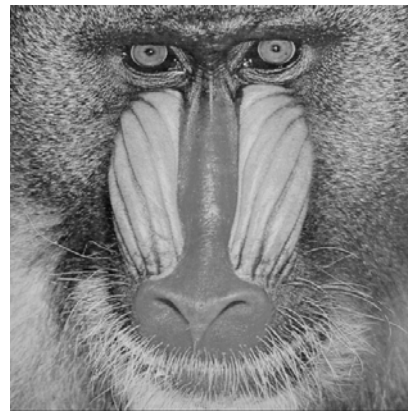| standard operation | PSNR （db） | | NC(%) | |
|---|---|---|---|---|
| | Lena | Baboon | Lena | Baboon |
| untreated | 50.90 | 49.05 | 100 | 100 |
| downscaling | 32.91 | 33.16 | 93.33 | 97.50 |
| GLPF | 22.63 | 26.98 | 95.00 | 97.50 |
| gaussian noise | 27.84 | 25.43 | 93.67 | 95.50 |
| transcoding | 37.61 | 31.27 | 100 | 100 |

Figure.3　Watermarked Lena　　Figure.4　Watermarked Baboon

（PSNR=50.90db）　　　　　　（PSNR=49.05db）

**Experimental Results when Embedded Position is（AC41 ,AC52）.**The PSNR of the attacked watermarked image and the NC value of the extracted watermark are shown in table2.

Table 2Experimental results

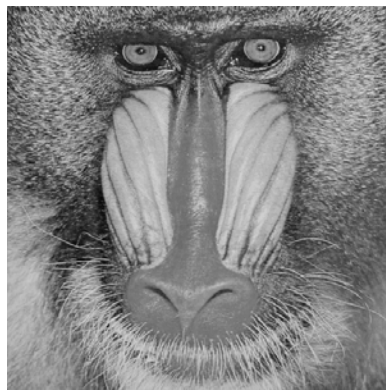| standard operation | PSNR （db） | | NC(%) | |
|---|---|---|---|---|
| | Lena | Baboon | Lena | Baboon |
| untreated | 37.61 | 44.00 | 100 | 100 |
| downscaling | 30.06 | 28.93 | 89.33 | 93.33 |
| GLPF | 31.72 | 28.13 | 93.50 | 96.67 |
| gaussian noise | 28.23 | 29.17 | 98.33 | 98.67 |
| transcoding | 37.44 | 31.11 | 100 | 100 |

Figure.5　Watermarked Lena （PSNR=50.90db）　　Figure.6　Watermarked Baboon （PSNR=49.05db）

It can be concluded from the experimental data, which the algorithm has good resistance characteristics to the above listed attacks. The PSNR of watermarked image is far greater than 30db requirements, in the watermarked image under attack, even if the PSNR is less than 30db; NC value of detected watermark is greater than required 75% [6].

## Conclusion

This paper presents a robust digital watermarking algorithm based on pre-processing. Firstly, in this algorithm watermark information is preprocessed, via encrypting and adding error correction code. Then the watermark information was embedded into the DCT coefficients of the image, which ensure the invisibility and good robustness of the watermarking system. The method can effectively resist the attacks, such as downscaling, noise adding, transcoding and filtering attacks. Finally the NC value can also be reached a very high standard. However, we find that this algorithm has some drawbacks. It is not good at resisting the attack of rotation and shear. In the future, the algorithm is improved in against the attack. And enlarging embedded watermark and enhancing adaptability are important tasks as well.

## Acknowledgements

## References:

[1] W.Yao, Y.G.DU: *Digital Watermark Pre-processing Method Research.* (2009)

[2] S.F.Sun, F.M.Dong and J.L.Wan: *A New General Binary Image Watermarking in DCT Domain.2008 International Seminar on Future Biomedical Information Engineering*, (2008),p.34-36.

[3] X.M.Wang, G.Z.Xiao: *Principles and Methods of Error Correcting Code[M]*. Xi′an: Xidian University Press. (2001)

[4] (7, 4) Hamming code code coding principle, DouDing library

[5] J.L.Luo: *Based on chaos digital watermarking technology and its application in military communication research[M]. Chongqing university master thesis.*(2007)

[6] C.M.Chu,H.C.Huang,J.S.Pan: *An Adaptive Implementation for DCT-Based Robust Watermarking with Genetic Algorithm.The 3rd International Conferrence on Innovative Computing Information.*(2008).