Journal of Theoretical and Applied Information Technology
15th November 2012. Vol. 45 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AN IMPROVED BLIND WATERMARKING ALGORITHM FOR IMAGE BASED ON DWT DOMAIN

YINGLAN FANG, LIN TIAN

Department of Computer, North China University of Technology, Beijing, 100144, China

ABSTRACT

This paper has brought forward an improved blind watermarking algorithm based on two-dimensional discrete wavelet transform. Watermarking applied binary image which had direct testing result and special meaning as watermark. Before embedded watermark, the watermarking image is pretreated by using Arnold scrambling to improve its security. According to the human eyes visual characteristic, it selected the watermark embedded position and improved its concealment. The specific means handled the original image two-level DWT and blocks DA sub-graph. Then it used scrambling watermarking values 0 and 1 as control signal to deal with coefficients in each block. It has achieved the watermarking information embedding. As the algorithm extracted watermark, it only needed use the relevant key without the original image and it had more practical value. Experimental results have showed that this algorithm had better concealment and improved the robustness and efficiency.

Keywords: *DWT, Blind Watermarking, Concealment, Robustness*

1. INTRODUCTION

In recent years, with the rapid development of computer and network, the copyright protection problem of digital media has become increasingly serious, which greatly damaged the commercial benefit of the product owner. Digital watermarking technology as a means of an effective complement to traditional encryption technology, it has provided effective way to solve the copyright protection problem of digital media. It can protect the digital product copyright, certified sources, and certified integrity of digital products under open network environment.

Digital watermarking technology has formally proposed since 1994. Many digital watermarking algorithms and implementations are also appeared. Many universities, companies and research institutes dedicated to the study of this technology, and achieved certain results. Some companies have launched some digital watermarking software products. Along with international extensive exchange, reaction of the domestic academic digital watermarking technology is also reacts very fast. It has a considerable number of the scientific research institutions into research in this domain. But research is mostly limited to the initial stage, it has not yet formed a complete system of theoretical knowledge, Currently digital watermarking has many mature algorithms: least t bit algorithm, Patchwork algorithm and adaptive methods [5-6] based on the spatial domain; discrete wavelet transform (DWT) based on transform domain, the discrete cosine transform (DCT) and discrete Fourier transform (DFT) method and so on.

On the basis of the above references, this paper has improved a digital watermarking algorithm. The watermark was pretreated by Arnold scrambling in order to enhance the security of watermark information. The improved algorithm selected embedding position of the watermark according to the human visual characteristic. It used the scrambling watermark information as a control signal for processing the part coefficients to the original image 2 DWT and implemented blind watermarking.

2. DIGITAL WATERMARKING BASIC PRINCIPLE

Any multimedia information will produce the physical random noise in the process of digitalization and the human visual system is not sensitive to the random noise [6]. By the philosophy, we can use some digital information replace the multimedia random noise and it couldn’t affect the original data visual effect.

3. RELATED TECHNOLOGY

3.1 Discrete Wavelet Transform

Digital image can be seen as a two-dimensional signal, so the basic idea of using DWT [8] processing image is put image to multi-resolution

Journal of Theoretical and Applied Information Technology
15th November 2012. Vol. 45 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

decomposition. Decompose the original image into four quarter-size sub-graphs by one-level DWT. They are low frequency sub-graph and high frequency sub-graph in horizontal direction, vertical direction and diagonal direction. After discrete wavelet transform, the image energy is mainly concentrated in the low frequency sub-graph, which represents an overview of the image, and the high frequency sub-graphs contains a small amount of energy, which represents the edges information of the image. Then the low frequency sub-graph can be wavelet transformed by the same method and get smaller resolution sub-graphs. Two-level DWT decomposition of an image is shown in Fig. 1.

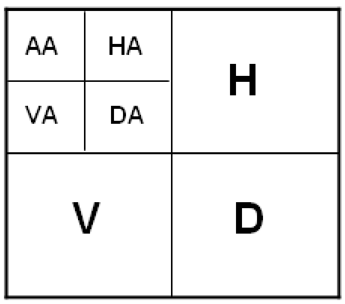


Figure 1: Two-level DWT Structure Diagram

3.2 Watermark Image Scrambling Encryption Technology

Image scrambling refers to some kind of transform, which makes the spatial location of the pixel becomes chaos and lost their original features and meaning. But the total number of pixels and histogram has not unchanged so as to achieve the purpose of encryption. As well as the scrambling must be one kind reversible transform, otherwise it will not have any significance in the practical application. If you do not know the rules and keys of the transform, it is impossible to recover the original image. And in the process of scrambling, the loss of the watermark information is dispersed into the whole watermark data. Thereby it minimizes the loss of meaningful information in order to reach purpose of improving robustness. Therefore image scrambling technology has been widely applied in the digital watermarking field.

The paper algorithm has encrypted and pretreated to watermarking image by Arnold Transform, which is a kind of transformation proposed by Arnold V J in the traversal theory study, also known as Cat Transform. Assuming the watermarking image's pixel point coordinates is x, y $\in [0, 1, \ldots, N]$, then the Arnold Transform is:

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

Where, the[x', y']T is pixel point coordinates of watermarking image after Arnold transform and N is the order number of image matrix.

The watermarking image has been made repeatedly iteration by using formula (1), until it get a "chaotic" watermark image. Suppose the watermarking image has iterated for k times we got the "chaotic" watermarking image, so k can be saved as a key. However it needed to point that Arnold transform has periodicity because of the images represented by N×N pixels is limited. If it continuous uses Arnold transform to scramble image, it will recover original watermarking image in certain step.

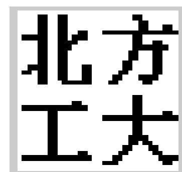


Figure2: Original Watermark Image

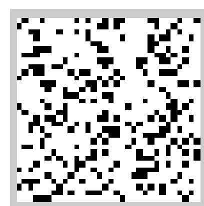


Figure 3: Watermark Image after 20 times Arnold

3.3 Human Visual System (Hvs)

HVS (Human Visual System) [3] combines the elements of visual physiologic, psychology and derive from a variety of visual masking characteristics, including frequency sensitive characteristics, texture masking characteristics and directivity characteristics. Frequency sensitive characteristics referred human eye is more sensitive to low-frequency domain and not very sensitive to the high-frequency domain. Texture masking characteristics referred the human eye is not sensitive to the complex texture domain. The background texture is more complex, the human visual system cannot feel the presence of sign. Directivity characteristics referred human eye sensitivity to oblique direction is less sensitive than horizontal and vertical direction, and the least sensitive is 45° or 135° direction. According to these characteristics it selects the embedded watermark position in order to obtain and improve its concealment.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3.4 Performance Analysis

Digital watermarking evaluation criterion [6] mainly includes two sides: concealment and robustness. These two sides are influenced by the watermarking embed quantity and embed strength. Usually, the watermarking quantity is more, the watermarking strength is greater, the robustness is better, but the concealment is less. As a result, we should consider both tradeoffs when the watermarking algorithm is designed.

Concealment [4-6] referred that watermarked image and the original image is indistinguishable in human visual system. Its objective evaluation standard is PSNR (Peak Signal to Noise Ratio), which represents that it get to the vertex signal of noise ratio. So when PSNR value is larger, it represents that the image distortion is less and the watermarked concealment is better. Assume that *I* represent the original image and *I'* represents the watermarked image, the PSNR formula is:

$$MSWE = \frac{1}{MN}\sum_{i=1}^{i=M}\sum_{j=1}^{j=N}(I(i,j) - I^{\sim}(i,j))^2 \qquad (2)$$

$$PSNR = 10 \times \lg(\frac{255^2}{MSE}) \qquad (3)$$

Where, MSE is the mean square error.

Robustness [4-6] refers that ability to extract the watermark after the carrier which contain watermarked is intentionally or unintentionally attacked. Its objective evaluation standard is NC (Normalized Correlation). NC can quantitatively analyze the extracted watermark and the degree of similarity of original watermark. NC value is larger, the extracted watermark and original watermark is more similar. Assume that *W* represents the original watermark and W' represents the extracted watermark, the NC formula is:

$$NC = \frac{\sum_{i=1}^{i=M}\sum_{j=1}^{j=M} W(i,j)W'(i,j)}{\sum_{i=i}^{i=M}\sum_{j=1}^{j=M} W(i,j)^2} \qquad (4)$$

4. IMPROVED ALGORITHM FORM

4.1 Improved Algorithm Design

In References [6], the original image is carved into blocks, and then each block is decomposed by one-level DWT, and finally watermarking is embedded. Although that algorithm has realized a blind watermarking, its efficiency is lower, because of it need multiple DWT.

This paper algorithm has improved that algorithm based on References [6]. First, the original image is decomposed by two-level DWT and get DA sub-graph and make it block. Second, it uses Arnold "chaotic" technology to pretreatment watermark image and makes the scrambled watermark image as control signal. It deals with part DWT coefficients in DA sub-graph after blocked according to certain rules so as to achieve the embedding of the watermarking information.

4.2 Wavelet Base Choice

On the one hand, wavelet is a unique discontinuous and unique strictly orthogonal wavelet in Dubieties wavelet system. On the other hand, it can effectively overcome the rounding error problem which is common in algorithms based on wavelet domain. Therefore, we adopt wavelet to decompose original image.

4.3 Watermark Embedding Process

Assume that the original images is grayscale image I with size M×M, watermark image is the binary and meaningful image W with size N×N. So the specific steps are as follows.

1: To determine whether the watermark is too big by proportion of original image I and original watermark image. When the size of watermark is consistent with the standard, N can be saved as a key, denoted by *k0*.

2: The watermark image has been encrypted and pretreated by Arnold scrambling. The scrambling number can be saved as a key, denoted by *k1*

3: Take the pretreated watermark image transform into a one-dimensional matrix and denoted by $WLine = \{w_i \mid i = 1, 2 ... N \times N\}$.

4: Decompose the original image *I* into seven sub-graphs by two-level DWT (shown as Fig.1).

5: Carve two-level diagonal sub-graph *DA* to block, denoted by *BLOCK* and its size is *M/4/N.*

6: Watermark information is embedded to each block in turn. The specific process is as follows.

a) When $w_i = 0$, if *BLOCK(1,2)>BLOCK(2,1)*, it exchange the two coefficient position;

b) When $w_i = 1$, if *BLOCK(1,2)≤BLOCK(2,1)*, it exchange the two coefficient position;

c) When *BLOCK(1,2)>BLOCK(2,1)*, it judge whether *BLOCK(1,2)-BLOCK(2,1)<K*,(*K* is the embedded watermark strength, here it set *K=20*) if the answer is true

$$\begin{cases} BLOCK(1,2) = BLOCK(1,2) + \frac{K}{2} \\ BLOCK(2,1) = BLOCK(2,1) - \frac{K}{2} \end{cases}$$

d) When BLOCK(2,1)>BLOCK(1,2) it judge whether BLOCK(2,1)-BLOCK(1,2)<K, if the answer is true;

Journal of Theoretical and Applied Information Technology
15th November 2012. Vol. 45 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$$\begin{cases} BLOCK(2,1) = BLOCK(2,1) + \dfrac{K}{2} \\ BLOCK(1,2) = BLOCK(1,2) - \dfrac{K}{2} \end{cases};$$

7: Take each watermarked block regroup into two-level diagonal sub-graph *DA'* and compose *DA'* and six sub-graphs by two-level IDWT. Then we get the watermarked image $I^{\sim}$.

4.4 Watermark Extracting Process

When this algorithm extracts watermark, it need not use the original image. So this algorithm is a blind watermarking algorithm. But it only needs relevant k0 and *k1*, which respectively represents the size of watermarking and the number of Arnold scrambling to watermarking. Generally speaking, the extracting process is the inverse embedding process. Specific steps are as follows.

1: The watermarked image *I'* is read and made two-level DWT to obtain two-level sub-graphs DA'.

2: Using key k0 to sub-graph DA get sub block BLOCK', its size is M/4/k0

3: Watermark scrambling information is extracted in each block BLOCK' in turn. The specific process is as follows.

$$a)\ when\ BLOCK^{'}(1,2) < BLOCK^{'}(2,1),\ \ w_i = 0, i = 1,2,...,k_0 \times k_0$$

$$b)\ when\ BLOCK^{'}(1,2) > BLOCK^{'}(2,1),\ \ w_i = 1, i = 1,2,...,k_0 \times k_0$$

4: Get "chaotic" watermark image by compose $w_i^{'}(i = 1,2,...,k_0 \times k_0)$ into a k*0*×k*0* matrix in turn, the GW is scrambling watermark. .

5: To decrypt GW by inverse Arnold scrambling and key k_1 (k_1 the scrambling number). Then we get extracted watermark image W'.

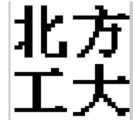
5. EXPERIMENT RESULTS

Using MATLAB programming to achieve the above algorithm .In the experiment, gray-level image with size 512×512 are used as the original image, called Lena A university logo with size of 32 by 32 is used as the watermark.

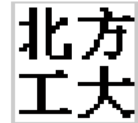
5.1 Non-Attack Environment

(a) The original image

(c) The watermarked image



(b) The watermark image



(d) extracted watermark image

Figure 4: Experiment in non-attack environmental result

The experiments show that, the original image and the watermarked image is basically no difference whether the overall effect or the local details contrast of images from subjective view. In other words, the watermarked image is able to maintain a better visual effect. PSNR of watermarked image and original image is equal to 44.9927 and NC of the extracted watermark and the watermark image is equal to 1 from objective view. These show that the algorithm has good imperceptibility.

5.2 Attack Environment

In order to detect robustness of the algorithm, we extract watermark from watermarked image which attacked by various attack (Gaussian Noise, Salt and Pepper Noise, Filtering, Resizing, Rotation, JPEG Compression.)

(1) Noise Attack

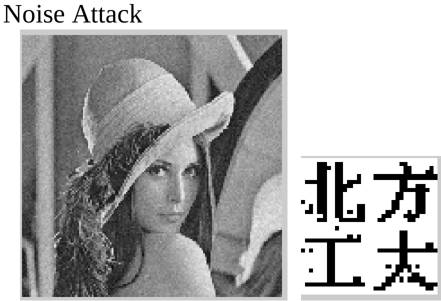


Figure 5: Gaussian Noise (aver=0, ver=0.001NC =0.9805

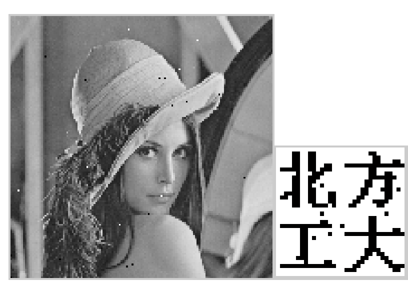


Figure 6: Salt and Pepper Noise (density=0.001 NC = 0.9883)

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

(2) Filtering Attack

Figure 7: Median Filtering Image NC=0.9662

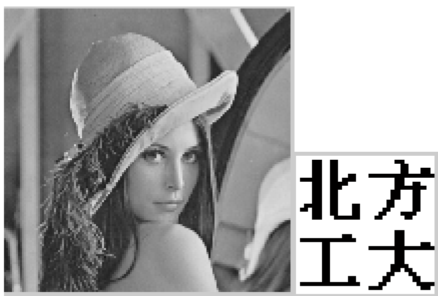


Figure 8: Gaussian Low-pass Filtering Image NC=1

(3) Geometric Attack

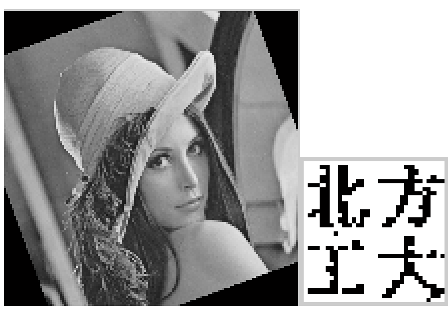


Figure 9: 20° Counterclockwise Rotation NC=0.9896

Figure 10: 30° Clockwise Rotation NC=0.9870

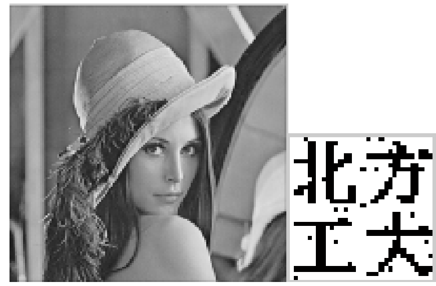


Figure 11: Narrow 0.5 Times NC=0.9701

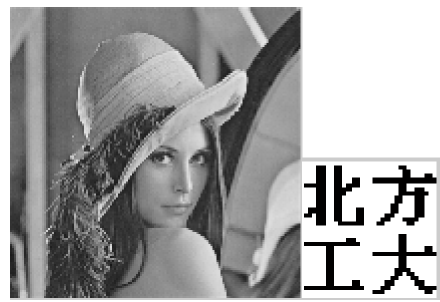


Figure 12: Expand 2 Times NC=1

(4) JPEG Compression Attack

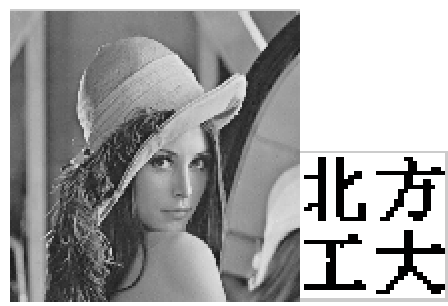


Figure 13:.JPEG Compression (Quality=70% NC=0.9987)

Figure 14: JPEG Compression (Quality=50% NC=0.8948)

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

(5) Robustness Contrast among Algorithms

In order to contrast robustness, it analysis and compare extracted watermark which obtained by the different algorithms but the watermarked images were attacked by same attack (Noise, Filtering, Resizing, Rotation, JPEG Compression). In order to make algorithms have comparability, requirements different watermarked image has the similar PSNR（$PSNR \approx 45$）. Table 1 shows the comparative data of improved algorithm, Cox algorithm and that algorithm of References [6].

Table I: Nc Of Extracted Watermark By Different Attack

Attack Name	Cox Algorithm	References Algorithm	Improved Algorithm
Gaussian Noise	0.9961	0.9714	0.9805
Salt and Pepper Noise	0.9987	0.9974	0.9870
Median Filtering	0.1299	0.4000	0.9662
Gaussian Low-pass Filtering	1	0.9779	1
Resizing（50%）	0.5013	0.6818	0.9701
Resizing（200%）	0.9961	0.9779	1
20° Clockwise Rotation	0.9455	0.9792	0.9896
90% JPEG Compression	1	0.9714	1
70% JPEG Compression	0.8714	0.7273	0.9987

Experiments show that the similarity of original watermark and extracted watermark obtained from watermarked image which attacked by various attack (Noise, Filtering, Resizing, Rotation, JPEG Compression) with the improved algorithm better than with the other two algorithms. So the improved algorithm is not only to meet the requirements of robustness but also better than other algorithms.

6. CONCLUSION

The proposed algorithm is an improved algorithm based on the wavelet domain in the digital image watermark technology. The extracting process only need relevant key without the original image, so it has more practical value. In order to encrypt watermark, the algorithm preprocess the watermark with Arnold Transform. It can meet the requirements of concealment because the watermarked image is able to maintain a better visual effect. At the same time, it shows a strong robustness when watermarked image attacked by a variety of common watermark attacks. The algorithm is applicable not only to a grayscale images, but also applicable to the color image. We have used it in the RGB space through decompose the G component by DWT and embedded the watermark by the improved algorithm. The results show concealment and robustness can meet the requirements.

REFRENCES:

[1] Cox I J, Kilian J, Leighton T , etal., “Secure spread spectrum watermarking for images”, In Proceedings of ICIP, Switzerland, 1996, No.3, 243-246.

[2] Cox I J, Kilian J, Leighton T, et al., “Secure Spread Spectrum Watermarking for Multimedia”, IEEE Trans on Image Processing, Vol. 6, No. 12, 1997, pp.1673-1687.

[3] Jung, Yong J, Kang, Ho K. Ro, Yong M. “Novel watermark embedding technique based on human visual system”, Proc.SP1E, 2001.

[4] Liu Xing, “Information hideaway and digital watermark”, Beijing: Beijing University of Posts and Telecommunications Press, 2004.

[5] Wang Ying, Xiao Jun, Wang Hong, “Digital Watermarking Principles and Techniques”, Beijing, Science Press, 2007

[6] Ren Pengkuan, “Research on image blind watermarking algorithms in DCT and DWT Domain”, Xi an: Xian university of science and technology, 2008.

[7] Rafael C. Gonzalez, Richard E. Woods, Steven L. “Digital image processing using MATLAB”, Singapore: McGraw-Hill, 2011.

[8] Leung H Y, Cheng LM., “A Robust Watermarking Scheme Using Selective Curvet Coefficients on A HVS Model”, International Journal of Wavelets, Multisolution and Information Processing, Vol. 8, No. 6, 2010, pp.941-959.

[9] Yong Fu, “Novel self-Reference Based Image Watermarking Scheme”, Journal of Circuits, Systems, and Computers, Vol. 19, No. 2, 2010, pp. 491-502.

[10] Gaurav Bhatnagar, Balasu bramaniag Raman, “Distributed Multi resolution Discrete Transform and its Application to Watermarking”, International Journal of Wavelets, Multiresolution and Information Processing, Vol. 8, No. 2, 2010, pp. 225-241.