Research into Digital Watermark Algorithm Based on Wavelet Domain

Chen Guang-xue[a], Tang Bao-ling[b], Chen Qi-feng[c] , Tai Jing-lei

State Key Laboratory of Pulp and Paper Engineering, South China University of Technology, Guangzhou, China, 510641

[a]guangxuecn@yahoo.com.cn, [b]bltang@scut.edu.cn, [c]qfchen@scut.edu.cn

Keywords: Digital image; Digital Watermark; Wavelet Domain; Algorithm

Abstract. In this paper, the key research was focused on the algorithm based on wavelet domain after analyzing and comparing several watermark algorithms. Disperse Wave Transform(DWT) watermark and Disperse Cosine Transform(DCT) watermark are both belong to transform domain technology, and they have more robustness than spatial-temporal domain technology, and DWT is superior to DCT. DWT can use the spatial-frequency characteristics of Human Visual System, and Mosaic will not appear in reconstruct image. DWT also can use image fusion technology to disperse watermark into multiple scales of carrier data, and got more robustness. In this paper, watermark embedding based on wavelet domain in which raster data are carrier was performed, then extracting and detecting watermark were done. Experiment results show that digital watermark based on wavelet domain will get better invisibility and robustness, and can be used in following the data by digital fingerprint.

Introduction

Digital watermarking technology embed logo or copyright information into image data，such as serial number, text, images , etc. and then post them to the web. In future, the watermark tags embedded in digital images will be red and detected by the computer to protect copyright against piracy, infringement or random tampering delicts. Digital watermarking technology, as an important application of hiding information used in computer field, provides a new solution to protect the legitimate use of information.

As well as some other non-mainstream watermarking algorithms, such as NEC algorithm and visual model-based algorithm, there are two main kinds of methods to embed watermark in digital image, space domain method and transform domain method[1]. Spatial domain digital watermarking technology changes the image data directly, which was generally embedded in the brightness or chroma intensity values. LSB (least Significant bit) method, Patchwork method and texture mapping encoding method, etc. are major algorithms of spatial domain method, which has been widely used in simplicity, efficiency, but not emphasizing the security occasion. Transform domain method is similar to spread spectrum communication techniques. In this method, after image orthogonal transform, a subset of frequency coefficients is selected to change, and finally through inverse transform, images with watermark are abstained. DCT(Discrete Cosine Transform) domain algorithm, DFT(two-dimensional Fourier Transform) wavelet-based domain algorithm, DWT (Discrete Wavelet Transform) domain algorithm, and watermarking algorithm based on fractal coding and fractal-based coding belong to this method. The transform domain watermarking methods are employed in many digital watermarking schemes for its outstanding advantages in attacks e.g. lossy compression, filtering, etc.[2][3]. In this article, wavelet-based digital watermarking algorithm is researched and tested.

Algorithm theory of wavelet-based digital watermarking

Disperse wavelet transform(DWT) watermark and Disperse Cosine Transform(DCT) watermark are both belong to transform domain technology, and they have more robustness than spatial-temporal domain technology, and DWT is superior to DCT. DCT merely transforms data from spatial domain into the frequency domain purely, neglecting images space-frequency characteristics, which

coincide with some visual properties of human eyes. That is, we can achieve space-frequency characteristics of HVS (Human Visual System) by using the wavelet transform. Secondly, mosaic phenomenon will occur if apply the blocked DCT transform, but that will not in wavelet transform. Furthermore, DWT can distribute watermark into multiple scales of carrier data by image fusion in order to enhance the robustness of watermark [4].

Segment a static image with a certain wavelet function through 1-scale two-dimensional discrete wavelet transform, four coefficient matrixes are created: approximation wavelet coefficient matrix LL1, horizontal details coefficient matrix HL1, vertical detail coefficient matrix LH1, and the diagonal details coefficient matrix HH1. Four wavelet coefficient matrixes construct similar detail as original image, and describe the related image of original information. The processed image will be obtained by corresponding wavelet inverse transform, shown in Fig.1.
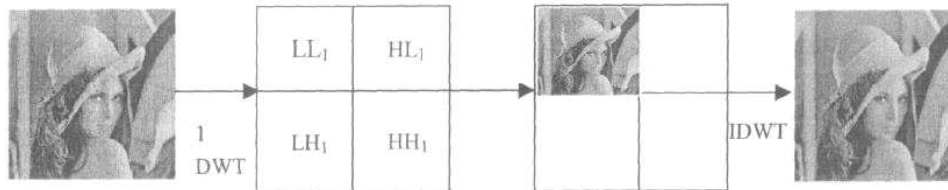

Fig.1 Schematic Diagram of 1-scale Wavelet Decomposition

Similarly, segment image with 2-scale wavelet, just like using wavelet transform on approximate image obtained in 1-scale wavelet transform, approximation coefficients and detail coefficients, LL2, LH2, HH2 and HL2 in second level are obtained. Processed image will be obtained by using accordingly 2-scale wavelet inverse transform to seven groups of coefficient, shown in Fig 2.
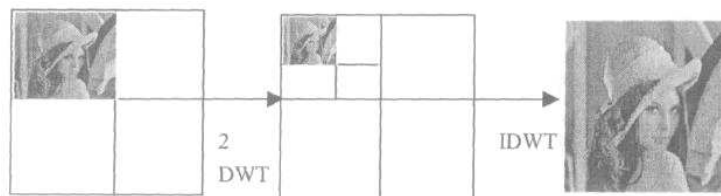

Fig.2 Schematic Diagram of 2-scale Wavelet Decomposition

Therefore, the basic process of watermarking in static image includes: make discrete wavelet transform to carrier image and watermark image simultaneously; embed three groups of detail coefficients and one group of approximation coefficients into every scale of carrier image respectively; and then the new image is obtained using 1-scale inverse wavelet transform on carrier coefficient blocks.

Watermark extraction is the reverse operation of watermarking, which can only be completed by the watermark designers themselves. Otherwise, it merely can distinguish the existence of watermark by any other detection methods.

Actualization of Wavelet Domain Digital Watermark Algorithm

Embedding Watermark.

(1) Segment carrier image of 512×512 using 3-scale DWT and we can get the approximation coefficient matrix, LL of 64×64 of the third layer and detail coefficient matrixes, HLi, LHi and HHi of the first layer, the second layer and the third layer respectively, in which i = 1, 2 and 3. When i is 1, the matrix is 256×256; when i is 2, the matrix is 128×128; when i is 3 the matrix is 64×64. Segment the image embedded watermark of 128×128 using 1-scale DWT and we could get the approximation coefficient matrix LL1 and detail coefficient matrixes, LH1, HL1 and HH1, in which each coefficient is 64×64.

(2)Partition the coefficient matrixes blocks of carrier image from step (1) according to the decomposition coefficient of watermark, 64×64. Then we could get a square that contains small matrixes of 8×8.

(3) In order to improve the robustness of watermark embedded into image, i.e., anti-interference performance, we should add high energy of watermark into frequency band with high energy and add low energy of watermark into frequency band with low energy. However, the imperceptibility of watermark restricts the energy of watermark. So we should make an optimal choice between robustness and perceptibility according to the property of human vision system, i.e. HVS.

We can get the contrast sensitivity of two specific spatial frequencies from human visual model proposed by Dooley as follows:

$$c(u,v) = 5.05e^{-0.178(u+v)}(e^{0.1(u+v)} - 1) \tag{1}$$

Compute the contrast sensitivity of blocks coefficients of carrier images and saliency of the image pixels (i.e.mathematical test about perceptivity according to HVS) to determine the embedding strength of watermark according to the properties of human vision. The computation process of saliency of image is as follows:

$$S_i = \sum\sum c(u,v)|F_i(u,v)|^2 \quad i = 1,2,3,\cdots,64 \tag{2}$$

Reconstruct the 64×64 coefficient blocks from step (2) to get the corresponding image blocks. Then 64×64 sub-image blocks, fi (m, n) (in which, I = 1, 2, …, 64) are generated. Transform each sub-image block using Fourier Transform two times and we can get image energy, $|F_i(u,v)|^2$ Contrast sensitivity matrix, c (m, n), of sub-image frequency spectrum can be computed according to contrast sensitivity equation. Then we could compute each saliency of sub-image as follows:

Compute the maximum saliencies of image blocks constructed by different detail coefficients of all layers, SH, SV and SD respectively. The process is as follows:

$$S_H = MAX(S_i)$$
$$S_V = MAX(S_j)$$
$$S_D = MAX(S_k) \tag{3}$$

Where, i denotes horizontal detail coefficient matrix block; j denotes vertical detail coefficient matrix block and k denotes diagonal coefficient matrix block [5].

Embed watermark adaptively according to the saliency of carrier image as follows:

$$LL'_3 = LL_3 + \alpha \cdot LL_1$$
$$LH'_i = LH_i + \frac{\alpha\sqrt{S_i}}{\sqrt{S_H}} \cdot LH_1$$
$$HL'_j = HL_i + \frac{\alpha\sqrt{S_j}}{\sqrt{S_V}} \cdot HL_1$$
$$HH'_k = LH_i + \frac{\alpha\sqrt{S_k}}{\sqrt{S_D}} \cdot HH_1 \tag{4}$$

in which, a is weighting coefficient which controls watermark strength. Typically, a is in the range [0, 0.02]. And in our experiment a is 0.01. i, j and k are defined as above and $i + j + k = 63$.

(4) Reconstruct the 64×64 coefficient blocks of carrier image embedded watermark from step (3), and we get LL3′, LH3′, HL3′, HH3′. Transform the four matrixes using 3-scale wavelet transform, we could obtain the expectant image.

Watermark Extraction. Watermark extraction algorithm is a simple and accurate inverse operation of embedding watermark and has good security. Its process is as follows:

(1)Transform Image I′ embedded watermark and original image I using 3-scale DWT.

(2) Partition according to the value of watermark wavelet coefficient blocks (i.e., 64×64).

(3)Subtract the coefficient blocks of I′ portioned from step (2) with the correspondent coefficient blocks of I. Then divide the result by appropriate embedded strength value of watermark coefficient. So that we could get the watermark coefficient blocks which were embedded into the image repeatedly. Average the watermark coefficient blocks extracted respectively then we could get LL′&LH′, HL′&HH′.

(4)Reconstruct the 64×64 coefficient blocks of carrier image embedded watermark from step (3), and we get LL3′, LH3′, HL3′, HH3′. Transform the four matrixes using 3-scale wavelet transform, we could obtain the expectant image.

Correlation Test. Correlation I could be denoted as follows:

$$I = \frac{\sum X \bullet X'}{\sqrt{\sum X^2}\sqrt{\sum X'^2}}$$

(5)

Where, X is original watermark; X' is watermark detected. We can use hypothesis test to test watermark. The method is as follows:

$$H_0 : E = f_w(x,y) - f(x,y) = N(no-watermark)$$
$$H_1 : E = f_w(x,y) - f(x,y) = W' + N(watermark)$$

(6)

Use λ test. When select signification level, α, the confidence interval r complies with the law as follows:

$$r > R_\alpha(n-2)$$

(7)

Where, Rα(n) can be obtained by lookup table and n is number of samples [6].

Results and Discussions

a. Original Image
b. Watermark
Approximate coefficient image
Level details image
Vertical detail image
Diagonal detail image
c. Image Sequence after Wavelet Transform
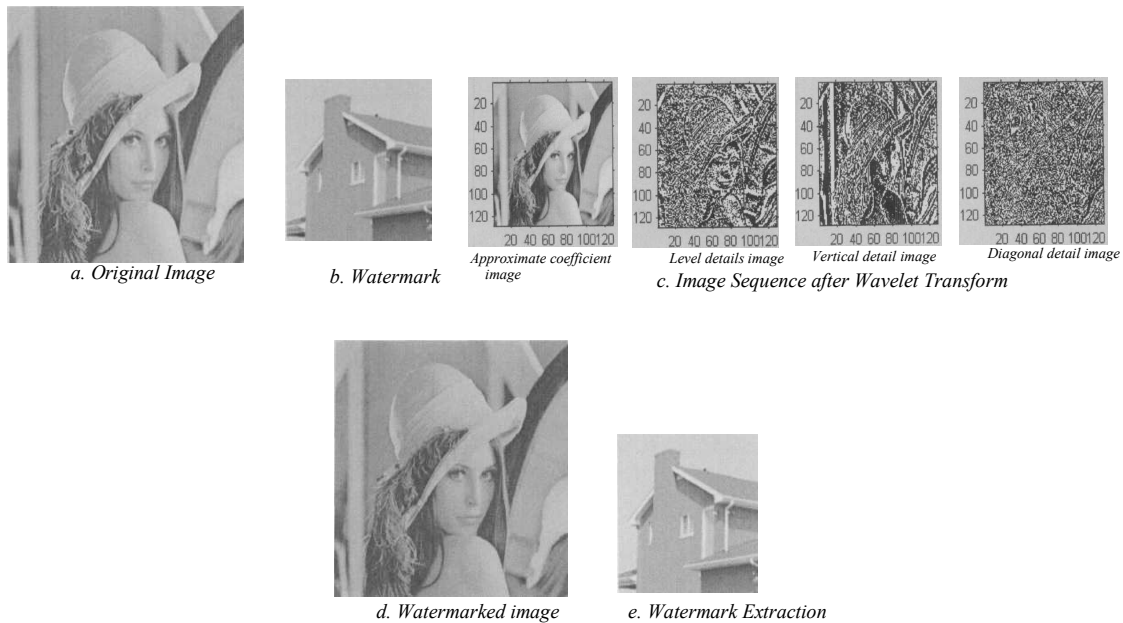

d. Watermarked image
e. Watermark Extraction

Fig.3 Experiments and Results

In experiment, Matlab was the software platform in which a lot of function library required in digital watermarking is well used. Matlab is scalable and has a programming interface with VC++ 6.0. The wavelet selected in this paper was DBL, and the carrier image is Lena with the size of 512x512. The watermark was embedded and extracted, and the experiment results are shown in Fig.3. The correlation coefficient of watermark is 0.9902.

Conclusions

In this paper, a digital watermarking algorithm based wavelet transform was studied. The digital watermark in which image is the carrier was embedded and extracted by DWT. Space-frequency characteristic (SFC) of image was used in DWT algorithm, so mosaic was not appeared in reconstructing image by Block transform. Watermark was embedded into Multi-scale of the carrier image using image fusion, and experiments show that the invisibilityand robustness of watermark are very strong which can meet the requirements of data trace by digital fingerprint.

Acknowledgments

Reference

[1] S. Katzenbeisser, F.A.P. Petiteolas. Information Hiding Techniques for Steganography and Digital Watermarking. Artech House. Boston, London, 1999.

[2] F. A. P. Petitcolas, R. J. Anderson. Attaeks on Copyright Marking Systems. Second workshop on information hiding. Portland, Oregon, USA, 1998.

[3] J.f. Jin. Wavelet Technology and Engineering Practice. Posts & Telecommunications Press. Beijing, 2003.

[4] A.L. Liu. Data Compression and Encryption Technology in Map Data Network Distribution. Master's thesis of Information Engineering University. Zhengzhou, 1998.

[5] J.M. Shapiro. Embedded image coding using zerotrees of wavelet coefficient. IEEE Trans on Signal Processing, 41(12). (1993)3445-3462

[6] W.J. Wang, Y.Y. Zhao. Digital Algorithm Based Wavelet Domain. J. Comp. Tech. and Dev., 19 (4). (2009) 122-124.