Research on Image Zero-watermark Algorithms based on DCT – domain

Tian Yu-min， Pan Rong，Wan Bo，Gong Yan；Research Institute of Peripherals ,Xidian University，Xi'an 710071。ymtian@mail.xidian.edu.cn,

Abstract

A kind of hybrid DCT-Logistic zero-watermark algorithm is proposed. The central idea of this method is to take the Logistic mapping sequences and several important coefficients of discrete cosine transform to form watermark. As many proposed image DCT zero-watermark techniques is sensitive to rotation, the geometric moments of original image are exploited to estimate the rotation. So that the corrupted watermarked image can be corrected and the watermark can be detected correctly. The obtained results show that the technique is robust to most attacks including JPEG compression, filter and geometric transform.

1. Introduction

Recent years, the explosive growth of digital multimedia techniques and digital network communication has created a pressing demand for techniques used for copyright protection and content authentication. Digital watermarking has been proposed as a way to meet these requirements. Digital watermarking is a technology that uses the redundant data and randomness which prevalently exist in digital works to embed copyright information in digital works to protect their copyright or integrity.

The watermark method must carry on the certain revision to the image information, which directly causes contradiction between the imperceptibility and the robustness. In view of this question, WEN Quan et al [1] proposed the concept of "zero watermark". The so-called "zero watermarks" is using the important characteristics of the image itself to construct watermark information, which does not make any revision to the image data. The zero-watermark technology has well balanced the contradiction among the robustness of digital watermark algorithm, the capacity of the information embedded and the robustness. Reference [1] used the DCT coefficients to construct zero-watermark, which well avoided the contradiction between the imperceptibility and the robustness and had a higher robustness to general image processing. But it was unable to resist the geometrical transformation like rotation and so on. Reference [2] used the spatial-domain image characteristic to carry on re-synchronization of the watermarked image which suffered the geometrical transformation. But the selection algorithm of the image feature points itself didn't resist to the geometrical transformation well, so the ability of this method in resisting geometric attack was not high, and because only DCT coefficients were used in constructing watermarking information, there existed certain insecurity. Reference [4] combined strange value decomposition（SVD）with DCT to obtain watermark information. It utilized geometric moment to carry on the parameter estimation and correction. But the geometric moment algorithm was time consuming and the calculation formula of scale transformation was complicated. It made against practical applications. In view of the shortcomings of references [2, 4], this paper combines DCT with chaotic theory to construct watermark information. A simple geometric moment algorithm is used in parameter estimation and correction of the watermarked image. Simulation results demonstrate the robustness against several attacks, such as filter, JPEG compression, scale transformation, rotation and cut operation.

2. Zero-watermark scheme based on DCT domain

Assume I is the original gray image with the size of N1×N2. Because the low-frequency and intermediate-frequency regions after DCT concentrate the most energy and characteristics of the original image, the intermediate-frequency coefficients are used to construct zero-watermark information. The algorithm steps are as follows:

1. Do block-DCT to original image, convert spatial-domain pixel matrix to DCT coefficient matrix;
2. Select intermediate-frequency coefficients after block-DCT to constitute one-dimension sequence$A$;
3. Construct bianry sequence B according to formula (1):

$$B_i = \begin{cases} 0 & A_i \le 0 \\ 1 & A_i > 0 \end{cases} \qquad i = 1 \cdots 1024 \qquad (1)$$

4. Encrypt the sequence B using Logistic mapping [5] to produce the binary watermark sequence W .

Encrypting binary sequence B and changing it into a watermark sequence, which can improve the security of the watermark and difficulty of analyzing and explaining of the algorithm. The Logistic mapping in Chaos is used here, which comes from the worm model of chaotic dynamics, and it is defined as formula (2):

$$x_{i+1} = \mu x_i \left(1 - x_i\right) \qquad (2)$$

When $3.5699456\cdots < \mu \le 4$, Logistic mapping works at the chaotic state, $x_i \in (0,1)$.Bring the real-value sequence $\{x_i\}$ produced by Logistic mapping into formula (3) to carry on binarization.

$$\Gamma(x) = \begin{cases} 0 & 0 \le x < 1/2 \\ 1 & 1/2 \le x < 1 \end{cases} \qquad (3)$$

The chaotic binary sequence is got in this way, recorded as: $S = \{k_i \,|\, k_i = \Gamma(x), i = 1, 2, 3\cdots\}$ .The chaotic binary sequence retains the excellent characteristics of chaotic sequence such as easy generation, very large quantity and sensitive initial conditions.

The finally watermark signal is formed by taking the bitwise exclusive OR operation between the chaotic sequence and the binary sequence B. Where the initial values x_0 and μ of Logistic mapping can be used as two keys k_1 and k_2 for watermark algorithm. Finally, add W into Intellectual Property Right (IPR) watermark database and register it, the image copyright can be considered under the protection of watermark technology.

3. Watermark synchronous detection Scheme

3.1 Estimation of the rotational angle of watermark image

Because the zero-watermark algorithm based on DCT domain has the weaker ability to resist the rotational attack, so we use image geometric moment which was proposed in reference [6] to estimate the rotational angle of image and correct it. Although this method is a non-blind watermark algorithm, it uses only a few low order geometric moment of original image which with little estimate error and simple calculation.

Assume that the image is a real function $f(i,j)$ which is defined on the Cartesian coordinate system, where $1 \le i \le M$, $1 \le j \le N$. Then the geometric moment m_{pq} with order of $p+q$ of image is defined as:

$$m_{pq} = \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} i^p j^q f(i,j) \qquad (4)$$

Assume that the original image is represented as $f(x,y)$, and $f(x',y')$ is the image that is rotated with angle of θ, where θ is negative when the image is clockwise rotated and is positive when it is anticlockwise rotated. According to a certain angle the image rotated, the rotated angle θ can be calculated as:

$$\theta = \arcsin \frac{m'_{01} m_{10} - m'_{10} m_{01}}{m_{10}^2 + m_{01}^2} \qquad (5)$$

Where m_{01} and m_{10} , m'_{01} and m'_{10} are the one-order geometry moments of original image and rotated image respectively.

3.2 Quadric-detecting scheme for zero-watermark

The steps of quadric-detecting scheme for zero-watermark are as follows:

1. Adopt normal detection algorithm to detect the zero-watermark. Image I' which is to be tested is transferred by block-DCT, and the keys of k_1 and k_2 is inputted to generate Logistic mapping sequence. Then the bitwise exclusive OR operation is used between the sequence and the coefficients after DCT to form watermark. Finally, $sim(W,W') = W \times W' \Big/ \sqrt{W'^2}$ is used to carry on the relevant examination.
2. If the pertinence meets the pre-set targets, the watermark is considered existent and the detection is finished. Otherwise, the above geometric transformation parameter estimation methods is used to correct image rotational angle, and re-synchronize the images. Based on this, the watermark image is quadric-detected.
3. Do zero-watermark quadric-detecting for the watermarked image after corrected, if the similarity is greater than the threshold which is provided before, the watermark is thought to be existent and the image copyright should belongs to the author, otherwise there is no watermark and the image copyright has nothing to do with the author, and watermark detection is finished.

From the above detection steps, it can be seen that, as adopting a quadric-detecting method, rotation transform geometric attacks can be resisted effectively, and only when conventional detection algorithm is failed, the secondary detection is used, so the actual application will not reduce the efficiency of the watermark algorithm.

4. Experimental results

Adopting 256 level gray Lena with size of 256×256 as the original image, watermark information is constructed and detected by the above method, and the watermark is recovered from the image without any watermark attacks, as shown in figure 1 and figure 2 (As no data is embedded, Figure 1 and 3 are similar without any distinction).

To test the anti-attack capability for the algorithm, we have carried on various distortion operations to watermarked image. Test results show that the defensive ability of the algorithm for the JPEG compression is outstanding, even at compression rate of 5%, it can get high detection results. The algorithm also has strong defensive ability for geometric transformation, such as filter, scale transformation and cut operation. But for the rotation, it has less ability to resist. The test results are shown in Table 1.

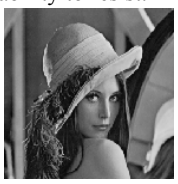

Fig1 Original Image

Fig2 Zero-watermark

Fig3 Watermarked Image

Table1 The Detection Results of Several Processes and Geometric Transformations of the Watermarking-image

Mean filter sim	3×3	5×5	7×7	
	0.8184	0.7910	0.7622	
Compression radio sim	75%	50%	25%	5%
	1	1	1	1
Rotated angle sim	−5	3	5	30
	0.5332	0.5400	0.5420	0.5273
Transfer factor sim	0.5	1.5	2.0	3.0
	0.9004	0.9600	0.9541	0.9502
Cut intensity sim	12%	25%	40%	50%
	0.9404	0.8711	0.8018	0.7520

This algorithm has weaker capability to resist attack of rotation transformation, but after parameter estimating and correcting using geometric moments, then the quadric-detecting is done. The results show that the watermark has high robustness to rotation . After correcting using geometric moments, the test results are shown in table 2.

Table2 The Results of Rotating The Watermarking-image after Geometric Correction

Rotated angle	－5	3	5	30
sim	0.9146	0.9360	0.9482	0.9217

5. Conclusion

A zero-watermark algorithm which combines DCT with Logistic mapping is proposed in this paper. This algorithm solves the contradiction between imperceptibility and robustness, enhances the security and the robustness effectively. It not only meets the demand of copyright authentication of image, but also can realize the data hiding. Finally the geometric moment is used to parameterized estimate and correct the geometric transform which the watermarked image suffered, which solves the problem of anti-rotation geometric attack. Experiments indicate that the method has better robustness to attacks such as compression, filtering, geometric transformation etc.

References:

[1] WEN Quan, SUN Tan-Feng, WANG Shu-Xun.Based zero-watermark digital watermarking technology [A]. China International Information Hiding Workshops (CIHW'2001)[C]. Xi'an: Publish house of Xidian University, 2001.

[2] JI Cheng-Li,YANG Xiao-Yuan, ZHANG Chong et al. A Transform-domain Zero-Watermark Quadric-detecting Schema Combined with Spatial-domain Invariants [J].Computer Engineering, 2004,30(14):105-115.

[3] Cordelia Schmid,Roger Mohr,Christian Bauckhage.Evaluation of Interest Point Detectors[J].International Journal of Computer Vision,2000,(2):151-172.

[4] ZHOU Ling-Yu,ZHANG Hua-Rong,ZHANG Ming.A Hybrid SVD-DCT Zero-Watermark Algorithm [J]. Journal of Jinling Institute of Technology, 2004, 20(4):3-6.

[5] Tohr Kohda,Akio Tsueda.Statistics of Chaotic Binary Sequences.IEEE Trans Information Theory,1997,6(43):104～112.

[6] GAO Zhen,TAI Li-Chun, ZHANG Zhi-Hao. Research on Methods Against Geometrical Attacks of Digital Watermarking [J].Computer Engineering, 2006, 32(5):135-137.

Author Biography

Tian yumin received his BS and MS in Computer Application from the Xidian University at 1984 and 1987 respectively . Her work has focused on content-based Multimedia retrieval, Digital watermarking and information hiding.