An Extensive Method to detect the Image Digital Watermarking based on the Known Template

FENG Yang,[†] , *LUO Senlin*[††] , *PAN Limin*[†††]

Department of electric engineering, Beijing Institute of Technology, Beijing, China

Summary
There are many types of digital watermarking algorithms, but each type corresponds with a certain detecting method to detect the watermark. However, the embedding method is usually unknown, so that it is not possible to know whether the hidden information exists or not. An extensive digital watermarking detecting method based on the known template is proposed in this paper. This method extracts some feature parameters form the spatial, DCT and DWT domains of the image and template, and then use some detecting strategies on those parameters to detect the watermark. The experiment result shows that the correct detecting rate is more than 97%. Obviously, the extensive digital watermarking detection method can be realized, and the method is valuable in theory and practice.

Key words:
digital watermarking; extensive detection; correlative detection

1. Introduction

With the fast growing of network and media techniques, there has been growing interest in developing effective techniques to discourage the unauthorized duplication of digital data like audio, image and video. In traditional method, cryptology is often used to protect them, but when the cryptograph has been decoded, copying and republishing of the digital data would be out of control. The appearance of digital watermarking can change this status, digital watermarking is a new technique which protects the copyright in the circumstance of the open network, it also can attest the source and integrality of digital data [1] [2] [3]. Authors of digital media embed some information into their works by using an unappreciable method, and those information can not be found unless via a corresponsive detector.

Developing of digital watermarking techniques is in a high speed, there have been many types of digital watermarking methods. But each type is independent from each other, so the detection of each one should correspond with the method of embedding.

Generally, Methods of Images digital watermarking can be divided into two types, methods in spatial domain and methods in transform domain. And methods of transform domain can be divided into DCT domain methods and DWT domain (wavelet domain) methods. Cox. I. J, professor of Imperial College London, has proposed a frame of two steps watermarking detection [2] [4], as figure 1. The array of the watermarking image (the image which will be detected) in symbol spatial is extracted by the watermark extractor. And then, the watermarking information (hidden information) can be detected from the array by a simple detector. This simple detector could be a linear correlate detector, unitary correlate detector or correlate coefficient detector.

Fig. 1 Frame of the two steps watermarking detection

However, the method of embedding is usually unknown in the process of watermarking detection. There are more than one hundred methods of digital watermarking embedding, and because of the time consuming and the uncertainty detecting result, it is nearly impossible to use every corresponsive method to detect the watermarking information. In that way, does any extensive watermarking detection methods exist? By the analyzing of the digital watermarking embedding and detecting algorithms, an extensive images watermarking detection method is proposed in this paper, this method extract the feature parameters form the spatial, DCT and DWT domain (array in symbol space) of the image. These parameters would be taken for the inputs of a watermarking detector, and the result of the watermarking detector is the detecting value to judge the hidden information exists or not. The experimental result shows that the method of extensive digital watermarking detection can be realized, and it is very effective.

2. Method of extensive image digital watermarking detection

2.1 Theoretic analyze

Usually, two techniques are proposed for watermarking embedding [1] [2] [3] [5]:

$$v_i^{'} = v_i + \alpha w_i \quad (1)$$

$$v_i^{'} = v_i\left(1 + \alpha w_i\right) \quad (2)$$

Manuscript received March 25, 2006.
Manuscript revised March 30 , 2006.

In above equations, v_i is the feature parameter of the original image, and v_i' is the feature parameter of the watermarking image in spatial, DCT and DWT domains (the image which has been embedded some watermarking information); w_i is the feature parameter of the template; α is the embedding intensity. Equation (1) is the additive embedding method, and equation (2) is the multiplicative embedding method. Each of them could increase the correlation between the image and the template. Thus, the calculation of the correlation between the image and the template can be used for watermarking detection. The formula of unitary correlation is as follows [6]:

$$z_{nc}(V,W_r)=\sum_{i=0}^{n}\overline{V}[i]\overline{W_r}[i] \qquad (3)$$
$$\overline{V}[i]=\frac{V[i]}{|V|},\quad \overline{W_r}[i]=\frac{W_r[i]}{|W_r|}$$

In the equation (3), znc is the unitary correlate value between v and w_r. The unitary correlate value between two arrays means the cosine of their angle. That is:

$$\frac{V\cdot W_r}{|V||W_r|}>\tau_{nc}\Leftrightarrow\theta<\tau_\theta \qquad (4)$$
$$\tau_\theta=\cos^{-1}(\tau_{nc})$$

From the equation (3), the unitary correlate value z_{nc} between feature parameters of the image and the template can be gotten, and then compared with the threshold τ_{nc} (τ_{nc} is an experimental value), if $z_{nc}<\tau_{nc}$, the watermarking information should not exist, or else it exists.

From above analyzing, a group of results could be obtained by comparing the unitary correlate values, and then integrating the comparing results to get the final detecting result.

2.2 The framework of the extensive detection method

As the figure 2, is procedure of extensive images digital watermarking detection, the method has three steps: classifying images and templates; extracting and combining feature parameters of them; using some detecting strategies on those parameters to detect the watermark, and integrating the results.

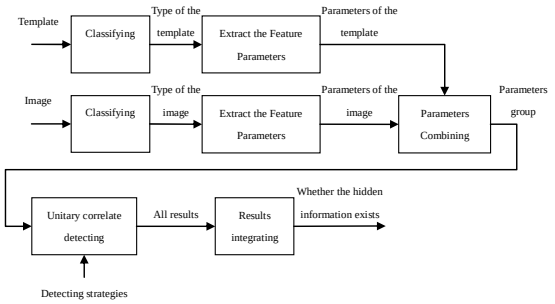

Fig. 2 Procedure of extensive images digital watermarking detection based on the known template

Images should be divided into two types: gray images and color images, and each type should be divided into three sub-types: non-compressed, compressed by JPEG and compressed by JPEG 2000. Templates should be divided into two types: smaller than image in size and in the same size of the image. After then, different feature parameters of images and templates can by extracted. The feature parameters of the images are listed in table 1, the sign of "Y" means that the feature parameter in the head of the column could be extracted from the images of the type in the head of the row.

Table 1: Feature parameters and watermarking images

Feature parameters of templates	Types of the images					
	Gray images			Color images		
	Non-pressed	Pressed by JPEG	Pressed by JPEG 2000	Non-pressed	Pressed by JPEG	Pressed by JPEG 2000
Coefficient in gray spatial	Y	–	–	–	–	–
Coefficient in RGB spatial	–	–	–	Y	–	–
DCT coefficient in gray spatial	Y	Y	–	–	–	–
8×8 DCT coefficient in gray spatial	Y	Y	–	–	–	–
DCT coefficient in YCbCr spatial	–	–	–	Y	Y	–
8×8 DCT coefficient in YCbCr spatial	–	–	–	Y	Y	–
DWT coefficient in M levels	Y	Y	Y	Y	Y	Y
8×8 DWT coefficient in M levels	Y	Y	Y	Y	Y	Y

Templates' feature parameters are listed in table 2:

Table 2: Feature parameters and templates

Feature of templates	Types of templates	
	Smaller than images	At the same size of images
Coefficient in gray spatial	Y	Y
8×8 blocks in gray spatial	–	Y
m×n blocks in gray spatial	Y	–

When the feature parameters of images and templates are extracted, they should be combined together, the parameters of image should be combined with parameters of template. Table 3 shows feature parameters of the image and its corresponsive parameters of the template.

Table 3: Feature parameters of watermarking images and templates

Feature parameters of images	Feature parameters of templates		
	Coefficient in gray spatial	8×8 blocks in gray spatial	m×n blocks in gray spatial
Coefficient in gray spatial	Y	–	–
Coefficient in RGB spatial	Y	–	–
DCT coefficient in gray spatial	Y	–	–
8×8 DCT coefficient in gray spatial	–	Y	Y
DCT coefficient in YCbCr spatial	Y	–	–
8×8 DCT coefficient in YCbCr spatial	–	Y	Y
DWT coefficient in M levels	Y	–	–
8×8 DWT coefficient in M levels	–	–	Y

Some detecting strategies should be use to calculate the unitary correlate values of the groups in table 3. Detection values $z_1, z_2, \ldots z_n$ from these strategies should be compared with their corresponsive thresholds $\tau_1, \tau_2, \ldots \tau_n$, and then the final detecting result is obtained by fusing the comparing results.

2.3 Detecting strategies

There are 10 groups of parameters in the table 3, they correspond with 6 different detecting strategies, and these strategies are showed in table 4.

Table 4: Detecting strategies

Detecting strategies	Parameters (image parameters + template parameters)
Strategy 1	Coefficient in gray spatial + Coefficient in gray spatial；
Strategy 2	Coefficient in RGB spatial + Coefficient in gray spatial；
Strategy 3	DCT coefficient in gray spatial + Coefficient in gray spatial； DCT coefficient in YCbCr spatial + Coefficient in gray spatial；
Strategy 4	8×8 DCT coefficient in gray spatial + 8×8 blocks in gray spatial; 8×8 DCT coefficient in YCbCr spatial + 8×8 blocks in gray spatial; 8×8 DCT coefficient in gray spatial + m×n blocks in gray spatial; 8×8 DCT coefficient in YCbCr spatial + m×n blocks in gray spatial;
Strategy 5	DWT coefficient in M levels + Coefficient in gray spatial；
Strategy 6	8×8 DWT coefficient in M levels + m×n blocks in gray spatial.

Strategy 1: v denotes the feature parameter of the image. w denotes the feature parameter of the template. In strategy 1, unitary correlate values between w and v should be calculated by scanning. The front data of v is used to calculate with w to get a detecting value z11, and then, v is shifted for an value and get detecting value z12 in the same way. This process should be repeated until the data of v had been used completed. From the whole process, some detecting values z11, z12, … z1n should be produced; the mean of them is the final detecting value of this strategy. The whole process is simulated in Matlab platform as follows:

```
len_v = length (v);
len_w = length (w);
% detected on scanning.
for offset = 0 : 1 : ( len_v – len_w )
      vw = v ((offset + 1) : (offset + len_w ) );
      % calculates the unitary correlate value
      % between vw and w.
      z( offset + 1 ) = UniCorrelate( vw, w );
end
% calculate the mean of all detecting values
z1 = mean( z );
```

Strategy 2: v has two-dimension matrix with three sub-vectors (RGB). Unitary correlate values between w and v should be calculated by scanning in these three sub-arrays, and there would produce three detecting values: z21, z22, z23, the mean of them is the final detecting value of strategy 2.

Strategy 3: v is transformed into V with Zigzag. V is an array in frequency domain. Elements of V are frequency parameters of the image. They are from low frequency to high frequency. The Unitary correlate value between w and V is the detecting value of strategy 3.

Strategy 4: v(i) is transformed into V(i) with Zigzag(i means the number of the block, and i from 1 to N). Elements of V(i) are frequency parameters of the image block i. They are from low frequency to high frequency. z5(i) is the unitary correlate value between w(i) and V(i), the mean of z5(i) is the detecting value of strategy 4.

Strategy 5: the unitary correlate values between w and low-frequency of v should be calculated by scanning. The result is the detecting value of strategy 5.

Strategy 6: the unitary correlate values z7(i) between w(i) and low frequency of v(i) should be calculated on scanning. The mean of z7(i) is the detecting value of strategy 6.

3. Experiments and results

In the experiments, 720 images which are 256×256 pixel in size are used, all the images were produced from 120 standard images by 6 different methods of digital watermarking embedding [2] [6] [7] [8] [9] [10]. Methods of embedding are listed in table 5. All standard images and templates are from Standard Image Database of Signal & Image Processing Institute, Electrical Engineering Department, School of Engineering, and University of Southern California (USC).

Table 5: Watermarking images in the experiment

No.	Count	Method of Embedding
1	120	Direct embed the information, which is modulated by template into gray-scale of gray-images.
2	120	Direct embed the information, which is modulated by template into color-scale of color-images.
3	120	Direct embed the information, which is modulated by template into DCT domain of images
4	120	Embed the information, which is modulated by template into 8×8 DCT domain of images.
5	120	Direct embed the information, which is modulated by template into DWT domain of images.
6	120	Embed the information, which is modulated by template into 8×8 DWT domain of images.

All produced images and their original images were used by the method of extensive images digital watermarking

detection, in total, there were 120 results of original images and 720 results of watermarking images. The Probability distribution of the detecting values is showed in figure 3. X-axis denotes the detecting values, Y-axis denotes the probability of detecting values, real line denotes the probability distribution of watermarking images' detecting values, broken line denotes the probability distribution of original images' detecting values.

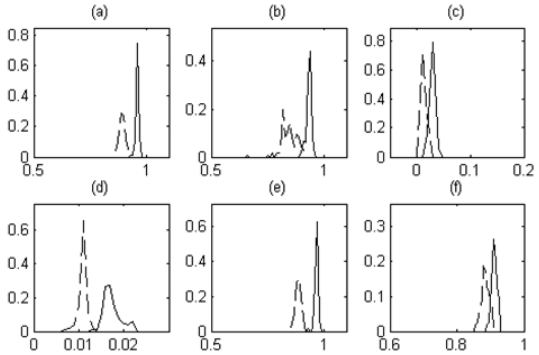

Fig. 3 Probability distribution of detecting values

(a) Strategy 1, (b) Strategy 2, (c) Strategy 3, (d) Strategy 4, (e) Strategy 5, (f) Strategy 6

Figure 3 shows that means of original images detecting values are smaller than that of watermarking images. Thus, watermarking images can be distinguished from original images by choosing appropriate thresholds. In this experiment, thresholds of 6 strategies are listed in table 6:

Table 6: Thresholds of detecting values

Detecting strategies	Thresholds	Detecting rate (%)	Error rate (%)
Strategy 1	0.917	100.00	0
Strategy 2	0.902	98.33	2.50
Strategy 3	0.014	100.00	2.56
Strategy 4	0.013	100.00	0.85
Strategy 5	0.910	100.00	0
Strategy 6	0.902	84.62	4.27
Mean	–	97.16	1.70

Table 6 shows that the correct rate of the detecting method proposed in this paper is 97.16%, and the error detecting rate is 1.70%. Obviously, the extensive watermarking detection method has achieved very good capability.

If lower thresholds were used, the correct detecting rate could reach a higher level, but the error detecting rate would be higher too. Oppositely, if higher thresholds were used, the error detecting rate could be lower, but the correct detecting rate would be lower too.

4. Conclusions

A new method of digital watermarking detection for images is proposed by this paper, this method is extensive in some extent. It's based on the known templates, the images and templates' feature parameters in spatial, DCT and DWT domains should be extracted, and than combined these parameters to obtain the detecting values by using the unitary correlative detection method; these detecting values show the correlation between images and their templates in different domains and different positions, so images can be divided into watermarking images or non-watermarking images by the comparing between these detecting values and thresholds.

The method in this paper suits the detection for some methods of digital watermarking based on templates which need templates to modulate the hidden information for embedding. For these embedding methods, the method of detection in this paper can detect whether hidden information exists in an image, without knowing the method of embedding. And the correct detecting rate can achieve a high level (about 97.16%) and the error rate is in a low level (about 1.70%). This paper proves that extensive detection of digital watermarking can be realized in some extent (for example, based on known templates). This extensive detecting method is very important and useful in application of information hidden and information security. The method of extensive digital watermarking detection based on unknown templates will be the next study.

References

[1] Frank Hartung. Multimedia Watermarking Techniques [D]. Proceedings of the IEEE. 1999, 7(87), 1079~1107.

[2] Cox I.J, Miller L.M, Bloom J.A. Digital Watermarking [M]. Beijing: Electronic Industries Press, 2003.

[3] WANG Baoyou, WANG Junjie, HU Yunfa.A Review of Copyright Protection by Digital Watermarking Techniques [J]. Computer Application and Software. 2004, 1(21): 30~87. (in Chinese)

[4] Cox I J, Kilian J, Leighton T, et al. Secure spread spectrum watermarking for multimedia [J]. IEEE Trans. on Image Processing, 1997,6 (12):1673-1687.

[5] ZHANG Jun, WANG Nengchao, SHI Baochang. Public Watermarking for Digital Images [J]. Journal of Computer-Aided Design & Computer Graphics. 2002, 4(14): 365~368. (in Chinese)

[6] SUN Shenghe, LU Zheming, NIU Xiamu. Digital Watermarking Techniques and Applications [M]. Beijing: Science Press, 2004. (in Chinese)

[7] HU Ming, PING Xijian, DING Yihong. A Blind Information Hiding Algorithm Based on DCT Domain of Image [J]. Computer Engineering and Applications. 2003,5:89~104. (in Chinese)

[8] LIU Jinghong, YAO Wei. A Watermarking Algorithm with Hight Definition [J] . Computer Engineering and Applications. 2004, 30: 76~115. (in Chinese)
[9] MA Miao, TIAN Hongpeng, ZHANG Huiqun. A Wavelet Energy Based Algorithm of Visible Watermark [J]. Journal of Xian University Sicence and Technology. 2002, 22(2):199~215. (in Chinese)
[10] ZHANG Xiaofeng, DUAN Huilong. Image Watermarking Based on Wavelet Transform [J]. Computer Engineering and Applications. 2004, 11: 64~204. (in Chinese)

FENG Yang received the B.S. and M.S. degrees in School of Information Science and Technique from Beijing Institute of Technology in 2003 and 2006. During 2004-2006, he stayed in Information Safe and Confrontment Laboratory (ISCL), Beijing Institute of Technology, China to study in Voice of IP (VoIP) and Information Hiding.