內嵌於分數傅立葉轉換域之 影像浮水印技術

葉敏宏

國立宜蘭技術學院電子系助理教授

摘 要

本篇論文提出一種利用分數傅立葉轉化作影像著作權保護之方法，本方法所加入的浮水印係一種在空間領域與頻率領域的結合。而所加入的影像中浮水印之強健性與統計效能亦將在文章中做一討論。

關鍵詞：浮水印、分數傅立葉轉換、影像加密

Image Watermark Embedded in the Fractional Fourier Transform Domain

Min-Hung Yeh

Assistant Professor, Department of Electronic Engineering, National Ilan Institute of Technology

Abstract

This paper proposes a method based on the fractional Fourier transform for image copyright protection. This approach use combination of the spacial and frequency domains for the watermark embedding. The watermark robustness and statistical performance are discussed in this paper。

Key Words：Watermark, Fractional Fourier Transform, Image Security

I. Introduction

In the past decade there has been an explosion in the use and distribution of digital multimedia data. And the copyright for digital multimedia data has become important, which brought about two complementary techniques: encryption and watermarking. Encryption techniques can be used to protect digital data during the transmission from the sender to the receiver. After the receiver has received and decrypted the data, however, the data is identical to the original data and no longer protected. Watermarking techniques can complement encryption by embedding a secret imperceptible signal, a watermark, directly into the original data in such a way that it always remains present. Such a watermark, for instance can be used for the following purposes: copyright protection, fingerprinting, broadcast monitoring, data authentication, indexing and data hiding [1][2][3].

In this paper, we will consider image watermarking in the fractional Fourier transform (FRFT) domain. This paper is organized as follows. The FRFT is described in Section 2. Watermark embedding in the FRFT domain is considered in Section 3. Numerical examples are given in Section 4

II. The Fractional Fourier Transform

The fractional Fourier transform (FRFT) indicates a rotation of signal in the time-frequency plane. And it is defined as[4]:

$$X_a(u) = \int_{-\infty}^{\infty} x(t) K_a(u,t)\,dt$$

where

$$K_a(u,t) = \begin{cases} \sqrt{\frac{1-j\cot a}{2p}}\, e^{\frac{1}{2}j(t^2+u^2)\cot a - jut\csc a} & \text{if } a \text{ is not multiple of } p \\ d(t-u) & \text{if } a \text{ is multiple of } 2p \\ d(t+u) & \text{if } a+p \text{ is multiple of } 2p \end{cases}$$

The inverse FRFT can be treated as a rotation for angle $-a$. The conventional Fourier transform is a special case of the FRFT for $a = \frac{p}{2}$

The numerical realization of the FRFT has been very intensively studied research topic. The discrete fractional Fourier transform presented in [5] is used in this paper for watermark embedding. The 2D discrete case extended from [5] can be found in [6]. The $M \times N$ point DFRFT of the 2D discrete signal x(m,n) is computed as:

$$: X_{a,b}(m,n) = \sum_{p=0}^{M-1} \sum_{q=0}^{N-1} x(p,q) R_{a,b}(p,q,m,n)$$

where

$$R_{a,b} = R_a \otimes R_b$$

R_a is the 2-D DFRFT with angle a

III. Watermark Embeding Algorithm

1. Embedding of a watermark

A. Image independent embedding method[2]

This method is the simples embedding method in the spectrum domain, which casts watermark data in to the selected region in the spectrum domain, i.e. middle band or low band. It has some disadvantage. It is hard to detect watermarks without original images, and perceptibility depends on the transform coefficients sensitivity, i. e. difference in scale. Even though this method has some deficient, it can be used to make watermarks robust in the respect that gain factor (k) can be increased, if watermark data are embedded in the low sensitivity region such as low band in the DCT or DFT domain.[2]

B. Image dependent embedding method[2][3]

This method also uses selected region like image independent embedding method. However, insertion watermark data based on this method is more robust against transform (DFRFT) coefficient in scale.

For an image $s(n_x, n_y)$ we find FRFT for angles (α_x, α_y), followed by transformation coefficients reordering in nonincreasing sequence $S = \{S_i \mid S_i \geq S_{i-1}\}$. The first L coefficients are omitted and the watermark is embedded in the next M transformation coefficients. If the watermark were embedded in the highest coefficients, it could produce significant image deformation, while if it were embedded in the lowest coefficients it could be cleaned by lossy image compression or lowpass filtering, without significant image visual degradation. Therefore, watermark is embedded as:

$$S_i^w = S_i + k_i' \mid \mathrm{Re}\{S_i\} \mid + j k_i'' \mid \mathrm{Im}\{S_i\} \mid \qquad i = L+1, L+2, \ldots, L+M$$

where (k_i', k_i''), $i = L+1, \ldots, L+M$ is a real-value water mark key. Figure 1 shows the block diagram for the watermark embedding.

2. Detection of the watermark

To detect a watermark in a possibly watermarked image, we calculate the correlation between the DFRFT coefficients of the watermarked image and the pseudo random noise pattern (watermark data). As mentioned before, the correlation value will be very high for the embedded watermark and would be very low otherwise. During the detection process, threshold T is set for detection

The method to detect a watermark without the original image is called blind detection. Now, we consider the method by, the second image dependent embedding method, The DFRFT coefficients of a possibly corrupted image are selected. Then, we calculate the correlation between potentially corrupted coefficients and the embedded watermark. This correlation is a measure of the watermark presence. Watermark detection must be reliable if the watermark key and possible of transmission coefficients are known. Let the watermark be a Gaussian white noise with variance σ^2. i. e. variances of k_i' and k_i'' are $\sigma^2/2$. A watermark detection check is performed comparing the detection value

$$d = \sum_{i=L+1}^{L+M} [k_i' - j k_i''] S_i^{(a)}$$

with a chosen threshold. Here, $S_i^{(a)}$ denotes the FRFT of the target image with a possible attack. The block diagram for the watermark detection is shown in Figure 2.

In order to determine the statistical performance of the proposed algorithm, we will first assume that the watermarked image is not changed by attacks (common image processing algorithms) or communication channel noise. Then, the value of *d* is equal to

$$d = \sum_{i=L+1}^{L+M} [k_i' - j k_i''][S_i + k_i' \mid \mathrm{Re}\{S_i\} \mid + j k_i'' \mid \mathrm{Im}\{S_i\} \mid]$$

Since the number of coefficients where the watermark is embedded (M) can be high. For a watermark key uncorrelated with image, the mean value of d is given as:

$$E\{d\} = \frac{\sigma^2}{2} \sum_{i=L+1}^{L+M} [\mid \mathrm{Re}\{S_i\} \mid + \mid \mathrm{Im}\{S_i\} \mid]$$

If there is no watermark (k_i', k_i'') in the image, $E\{d\} = 0$. Variance of *d* is the same in both cases:

$$\mathrm{var}\{d\} = \sigma^2 \sum_{i=L+1}^{L+M} \mid S_i \mid^2$$

Thus, the detection threshold should be chosen as $E\{d\}/2$, while the watermark key variance is chosen by a trade-off between watermark imperceptiveness and probability of false detection.

IV. Experimental Results

The experiment in this section is to test watermark scheme developed in the previous section. And we use the discrete fractional Fourier transform developed in [5]. The lena image with size 256×256, and the parameter L=1000, M=1000 were used in our experiment. The watermark noise a guassian noise is with zeros mean and variance $\sigma = 0.2$. The transform angles for the FRFT (α_1 and α_2) are both equal to $\frac{3}{8}\pi$. The original and watermarked images are shown in Figure 3(a) and (b), respectively. Detector response over different transform can make us know that to know the angles is necessary in watermark detection.

Besides the detection of watermark in the watermarked image, this watermarking approach is robust on some common attack. Watermarked image with white gaussian noise with variance 1 is shown in Fig.4(a). And the correlation of the detection is shown in Fig 4(b). The cropped watermarked image and the result of detection are shown in Fig 5(a) and (b), respectively. From Figure 4(b) and 5(b), we know that only the true watermark no. 500 is detected.

V. Conclusion

Base upon the proposed method, the FRFT transformation domain for image watermarking concept is proposed. It offers two more degrees or freedom, resulting in the possibility to generate more watermarks than in the conventional FT and DCT domains. This watermark is robust on some important attacks that could be performed by a pirate.

Reference

1. I. J. Cox, J. Kilian, F.T.Leighton, and T. Shamoon, (1997), "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Proc*., Vol. 6, No. 12 ,pp. 1673-1687.
2. Gerhard C. Langelaar, Iwan Setywan, and Reginald L. Lagendijk, (2000)," Watermarking digital image and video doata," *IEEE Signal Processing magazine*, pp. 1053-5888.
3. M. Barni, F. Bartolini, V. Cappelini and A. Piva, (1998), "A DCT-domain system for rubust image watermarking," *Signal Processing*, Vol. 66, pp. 357-372.
4. L. B. Almedia, (1994), "The fractional Fourier transform and time-frequency representation," *IEEE Trans. Signal Processing*, pp.2084-309.
5. S. C. Pei, M. H. Yeh and C. C. Tseng, (1999), "Discrete fractional Fourier transform based upon orthogonal projection," *IEEE Trans. Signal Processing*, pp. 1335-1348.
6. S. C. Pei and M. H. Yeh, (1998), "Two dimensional fractional Fourier transform," *Signal Processing*, Vol. 59, No.3, pp. 321-329.

91 年 09 月 16 日投稿
91 年 09 月 30 日接受

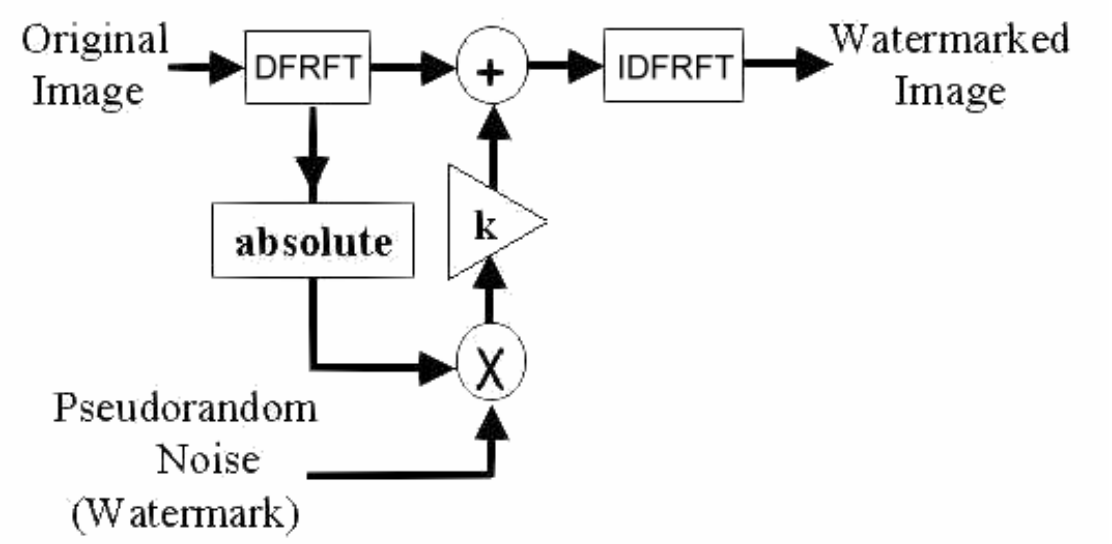


Fig 1　Image dependent watermark embedding.

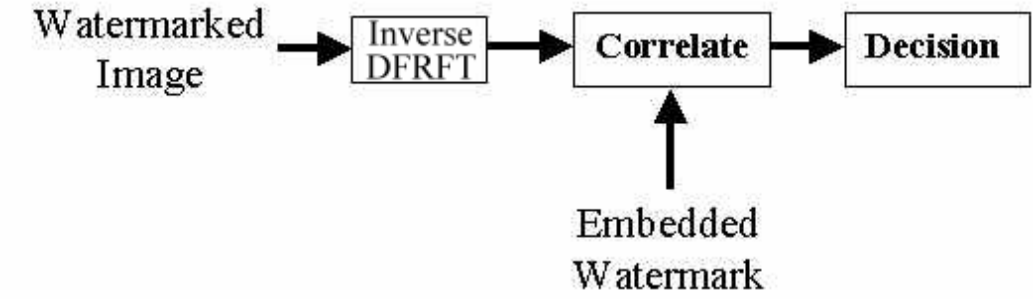
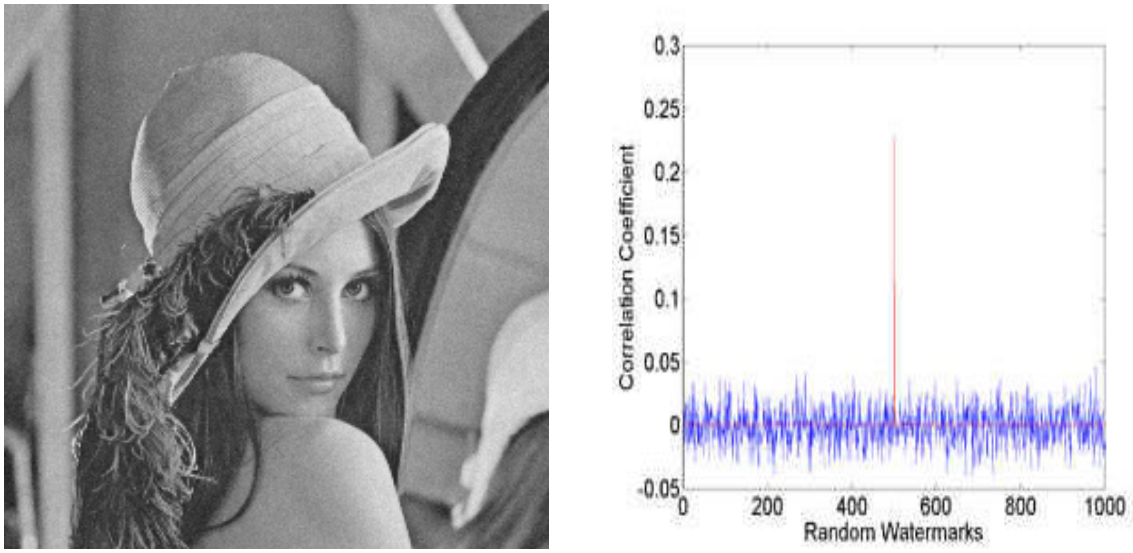


Fig 2 Block diagram for the blind detection in the fractional Fourier domain.

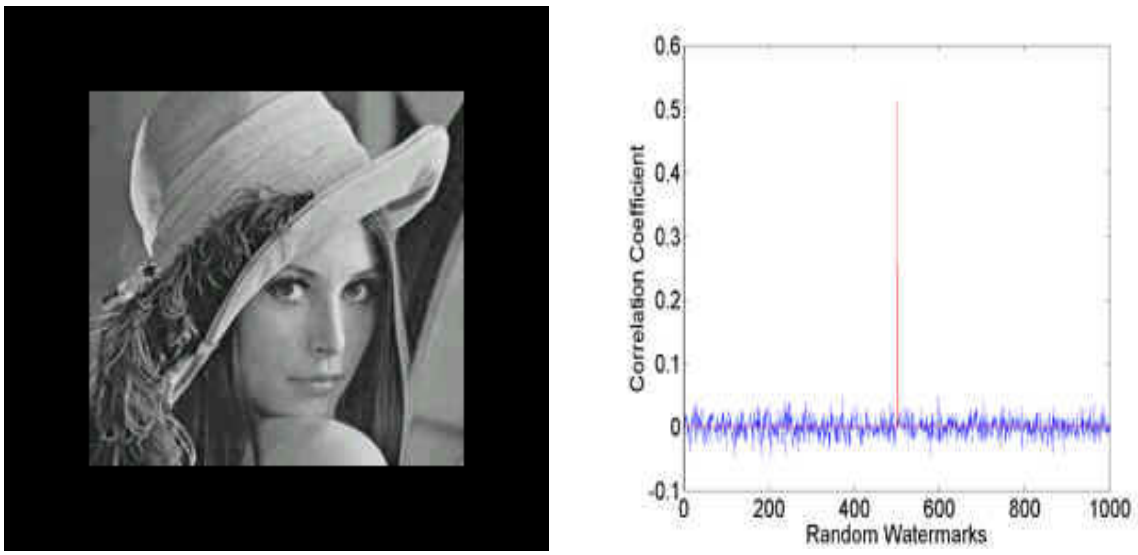
(a)　　(b)

Fig 3　(a)The original Lena image. (b) watermarked Lena image.



(a)　　(b)

Fig 4　(a)The cropped Lena image. (b) detection of watermark after embeding of noise.



(a)　　(b)

Fig 5　(a)cropped image ‘ Lena’. (b) detection of watermark after cropping.