第 34 卷 第 8 期 计 算 机 工 程 2008 年 4 月
Vol.34 No.8 Computer Engineering April 2008
·博士论文· 文章编号：1000—3428(2008)08—0015—04 文献标识码：A 中图分类号：TP391.41

基于小波与分数傅里叶变换的图像水印算法

李东明，王典洪，严 军，陈分雄
(中国地质大学机电学院，武汉 430074)

摘 要：载体图像的空域隐藏 Chirp 信号可以通过分数傅里叶变换在变换域中进行盲检测。为了提高该算法的鲁棒性能，该文研究直接离散化方法，合理选取分数傅里叶变换的算子阶数，将 Chirp 信号隐藏在图像信号的低频小波域中。仿真实验表明，改进后的水印算法提高了直接在空域进行信息隐藏的鲁棒性。

关键词：小波变换；分数傅里叶变换；数字图像水印；Chirp 信号

Image Watermarking Algorithm Based on Wavelet and Fractional Fourier Transform

LI Dong-ming, WANG Dian-hong, YAN Jun, CHEN Fen-xiong
(Electromechanical Institute, China University of Geosciences, Wuhan 430074)

【Abstract】 Chirp signal used as watermarking can be hidden in the spatial domain of the host image, and the watermarking is detected blindly through the fractional Fourier transform in the transform domain. To enhance the robust performance of the algorithm, this paper analyzes the reasonable order of fractional operator for direct discrete Fourier transform method, and hides a Chirp signal into low frequency wavelet-domain. Experiments show that the improved blind watermarking detection algorithm is robuster than the algorithm which embedded watermarking into the special domain of the host image, and can detect the Chirp watermarking rapidly.

【Key words】 wavelet transform; fractional Fourier transform; digital image watermarking; Chirp signal

1 概述

数字水印是一种可以在开放的网络环境下保护版权和认证来源及完整性的新技术。常用的数字水印嵌入算法是空域和变换域的数字水印嵌入算法。水印的空域算法是将水印信息直接嵌入到数字媒体的空间域中，算法运算量小，嵌入方法简单，缺点是对图像处理的鲁棒性较差。变换域水印算法在变换域中实现信息的隐藏，由于其稳健性使得目前的研究主要集中在变换域。变换域算法最常用的变换是DCT和DWT变换，算法具有鲁棒性好，而且可以和国际编码标准很好地结合。近几年提出的Chirp类水印信号，在FRFT(分数傅里叶变换)域，Chirp信号具有良好的聚焦特性[1-4]。文献[5]提出在图像空域嵌入二维Chirp信号作为水印，检测时对嵌入水印后的图像进行Radon-Wigner变换，变换域的峰值大于某一阈值时，意味着水印的存在，但是多分量Chirp信号由于变换的非线性，会出现交叉项的干扰。文献[6]将水印信号嵌入在FRFT域内，然后直接通过FRFT的逆变换还原得到含有水印的图像。但目前的FRFT离散数值计算都存在误差，在分数傅里叶变换域嵌入水印会降低逆变换的还原精度，从而降低了所嵌入水印的透明度。文献[7]分析了图像在分数阶傅里叶域能量分布，在空域嵌入二维多分量Chirp信号，检测时采用对含有Chirp水印的图像在特定的阶数附近以一定的分辨率进行FRFT域模幅度峰值扫描。通过扫描不同分数阶域的FRFT幅度模峰值来完成Chirp 水印信号的盲提取。但在空域直接进行数据的嵌入存在以下的问题：嵌入的Chirp水印数据幅度不能过大，否则会影响载体的透明度；嵌入Chirp水印数据幅度不能过小，否则会增大检测器检测正确检测的难度，同时空域嵌入水印对抗旋转、剪切、压缩等攻击鲁棒性差。

为了提高水印抵抗攻击的能力，本文分析了直接离散化计算 FRFT 的算子阶数的合理选取，然后在载体图像的低频小波域内嵌入 Chirp 水印数据，水印的检测则在分数傅里叶变换域进行，仿真实验表明，算法有效地提高了水印抗攻击的能力，对高斯白噪声干扰、旋转、压缩、裁剪等图像处理过程具有鲁棒性。

2 分数傅里叶变换的数值计算及误差分析

FRFT 也称为角度傅里叶变换(AFT)或者旋转傅里叶变换(RFT)，其定义式为

$$X_p(u)=\int_{-\infty}^{+\infty}x(t)K_p(t,u)\mathrm{d}t \tag{1}$$

其中，变换核为

$$K_p(t,u)=\begin{cases}\sqrt{\dfrac{1-j\cot\alpha}{2\pi}}\mathrm{e}^{(\mathrm{j}\frac{t^2+u^2}{2}\cot\alpha-tu\csc\alpha)}, & \alpha\neq n\pi\\ \delta(t-u), & \alpha=2n\pi\\ \delta(t+u), & \alpha=\alpha=(2n+1)\pi\end{cases}=$$

$$\sum_0^{\infty}\mathrm{e}^{\mathrm{j}n\alpha}H_n(t)H_n(u)$$

其中，p 为 FRFT 的阶，可以为任意实数；$\alpha=p\pi/2$；n 为整数；变换核对阶次(角度)α是完全连续的；$H_n(t)$是方差为 1 的 n 阶归一化 Hermite 函数：

基金项目：湖北省自然科学基金资助项目(2004ABA068)
作者简介：李东明(1982－)，男，博士研究生，主研方向：计算机图像处理，模式识别；王典洪，教授、博士生导师；严 军，副教授；陈分雄，讲师
收稿日期：2007-04-30 **E-mail：**universeli@163.com

$$H_n(t)=\frac{1}{\sqrt{2^n n!\sqrt{\pi}}}h_n(t)\mathrm{e}^{-\frac{t^2}{2}}$$

其中，$h_n(t)$ 为 n 阶 Hermite 多项式：$h_n(t)=(-1)^n\mathrm{e}^{t^2}\dfrac{\mathrm{d}^n}{\mathrm{d}t^n}(\mathrm{e}^{-t^2})$。

变换域数字水印技术的一个关键部分是可逆变换，然而目前的 FRFT 数值计算方法均有误差，如果是在分数傅里叶变换域嵌入水印，那么将碰到逆变换还原的精度问题。为避开该问题，本文采取在小波变换系数中嵌入 Chirp 水印，而在水印检测时，则在小波变换域使用 FRFT 搜索 Chirp 信号水印。

本文采用直接离散化方法计算 FRFT，根据文献[4]所提出的直接离散化方法计算分数阶傅里叶变换，由式(1)得

$$X_p(u)=\int_{-\infty}^{+\infty}x(t)K_p(t,u)\mathrm{d}t=\sum_{n=0}^{+\infty}H_n(u)(\mathrm{e}^{\mathrm{j}n\alpha}\int_{-\infty}^{\infty}x(t)H_n(t)\mathrm{d}t)\quad(2)$$

对信号 $x(t)$ 进行 N(N 为奇数)点取样，取样间隔为

$$T_s=\sqrt{\frac{2\pi}{N}},\ U_s=\sqrt{\frac{2\pi}{N}}$$

取样区间为

$$[-\sqrt{\frac{N\pi}{2}},\sqrt{\frac{N\pi}{2}}]\times[-\sqrt{\frac{N\pi}{2}},\sqrt{\frac{N\pi}{2}}]$$

从而可以得到

$$X_p(u)=\sum_{n=0}^{+\infty}H_n(u)(\mathrm{e}^{\mathrm{j}n\alpha}\int_{-\infty}^{\infty}x(t)H_n(t)\mathrm{d}t)=$$
$$\sum_{n=0}^{N-1}\mathrm{e}^{\mathrm{j}n\alpha}H_n(u)T_s\boldsymbol{H}_n^{\mathrm{T}}\boldsymbol{X}_N+\sum_{n=N}^{\infty}\mathrm{e}^{\mathrm{j}n\alpha}H_n(u)T_s\boldsymbol{H}_n^{\mathrm{T}}\boldsymbol{X}_N$$

文献[4]指出，当 $N\to\infty$ 时，$\sum_{n=N}^{\infty}\mathrm{e}^{\mathrm{j}n\alpha}H_n(u)T_s\boldsymbol{H}_n^{\mathrm{T}}\boldsymbol{X}_N\to 0$，于是分数阶傅里叶变换可以用以下算子表示：

$$X_p(u)=T_s(\sum_{n=0}^{N-1}\mathrm{e}^{\mathrm{j}n\alpha}\boldsymbol{H}_n\boldsymbol{H}_n^{\mathrm{T}})\boldsymbol{X}_N=T_s\cdot\boldsymbol{H}_N\boldsymbol{D}^p\boldsymbol{H}_N^{\mathrm{T}}\cdot\boldsymbol{X}_N=\boldsymbol{F}_p(\boldsymbol{X}_N)\ (3)$$

其中，

$$\boldsymbol{D}^p=\mathrm{diag}(\mathrm{e}^{-\mathrm{j}0},\mathrm{e}^{-\mathrm{j}\alpha},\mathrm{e}^{-\mathrm{j}2\alpha},\cdots,\mathrm{e}^{-\mathrm{j}(N-1)\alpha})$$
$$\boldsymbol{H}_n=[\boldsymbol{H}_{n,-\frac{N-1}{2}},\boldsymbol{H}_{n,-\frac{N-1}{2}+1},\cdots,\boldsymbol{H}_{n,\frac{N-1}{2}}]^{\mathrm{T}},n=0,1,2,\cdots,N-1$$

是 n 阶 Hermite 函数的 N 点取样列向量；$\boldsymbol{H}_N$ 是取样长度为 N 时 Hermite 函数的离散化矩；$\boldsymbol{X}_N=[x_{-\frac{N-1}{2}},x_{-\frac{N-1}{2}+1},\cdots,x_{\frac{N-1}{2}}]^{\mathrm{T}}$ 是信号的 N 点列向量。一旦阶数 N 确定，则分数傅里叶变换的算子矩阵 $\boldsymbol{F}_p$ 也相应确定，下文将对算子矩阵的特性进行分析。对于二维图像信号 $I(x,y)$，其采用可分离的分数傅里叶变换表示为

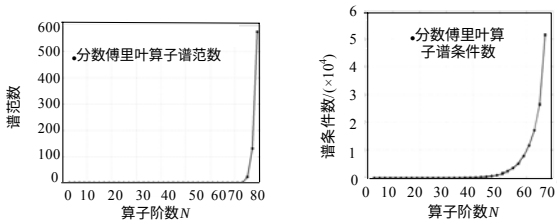
$$S_{p_1,p_2}(u,v)=F_{p_1}\{F_{p_2}(I(x,y)\}=F(I(x,y))\quad(4)$$

但是阶数 N 较大时，式(3)存在严重的计算误差。分数傅里叶变换是线性有界变换，所以，算子 $\boldsymbol{F}_p$ 同样应该满足有界的要求。分数傅里叶算子 $\boldsymbol{F}_p=T_s\cdot\boldsymbol{H}_N\boldsymbol{D}^p\boldsymbol{H}_N^T$ 的谱范数为

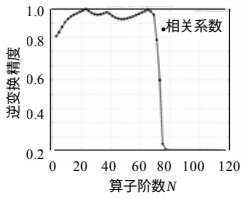
$$\|\boldsymbol{F}_p\|=\sqrt{\lambda_{\max}(\boldsymbol{F}_pF^H)}$$

对于不同的阶数 N，算子的谱范数和条件数有不同的表现，且不同的阶数选择则有不同的分数傅里叶逆变换还原精度，如图 1 所示。

由图 1(a)可以看出，当阶数超过 75 时会使得算子变得无界，此时由图 1(b)看出算子矩阵是一个严重病态的矩阵；选用阶数过高的算子矩阵会使得还原误差过高，还原精度采用原始图像和变换后经逆变换还原的图像信号之间的相关系数进行衡量，图 1(c)表明阶数过高时逆变换几乎无法还原图像信号。



(a)算子F_p谱范数随阶数变化　(b)算子F_p谱条件数随阶数变化



(c)算子F_p逆变换精度随阶数变化

图 1　算子F_p选择阶数N较大时趋于无界、病态、不可逆

因此，本文选用 N=65 阶的 Hermite 矩阵，此时的算子谱范数为 1.055 3，逆变换还原精度为 0.996 9。水印检测算法的关键在于 FRFT 的数值计算，此处重写直接离散化计算 FRFT 的计算式(3)：

$$X_p(u)=T_s\cdot\boldsymbol{H}_N\boldsymbol{D}^pH_N^{\mathrm{T}}\cdot\boldsymbol{X}_N=\boldsymbol{F}_p(\boldsymbol{X}_N)$$

其中，$T_s=\sqrt{\dfrac{2\pi}{N}}$；$\boldsymbol{D}^p=\mathrm{diag}(\mathrm{e}^{-\mathrm{j}0},\mathrm{e}^{-\mathrm{j}\alpha},\mathrm{e}^{-\mathrm{j}2\alpha},\cdots,\mathrm{e}^{-\mathrm{j}(N-1)\alpha})$；$\boldsymbol{H}_N$ 是取样长度为 N 时 Hermite 函数的离散化矩阵，将上式展开得

$$\boldsymbol{X}_p(u)=\begin{pmatrix}F_{p,-\frac{N-1}{2},-\frac{N-1}{2}} & F_{p,-\frac{N-1}{2},-\frac{N-1}{2}+1} & \cdots & F_{p,-\frac{N-1}{2},\frac{N-1}{2}}\\ F_{p,-\frac{N-1}{2}+1,-\frac{N-1}{2}} & F_{p,-\frac{N-1}{2}+1,-\frac{N-1}{2}+1} & \cdots & F_{p,-\frac{N-1}{2}+1,\frac{N-1}{2}}\\ \vdots & \vdots & & \vdots\\ F_{p,\frac{N-1}{2},-\frac{N-1}{2}} & F_{p,\frac{N-1}{2},-\frac{N-1}{2}+1} & \cdots & F_{P,\frac{N-1}{2},\frac{N-1}{2}}\end{pmatrix}\begin{pmatrix}x_{-\frac{N-1}{2}}\\ x_{-\frac{N-1}{2}+1}\\ \vdots\\ x_{\frac{N-1}{2}}\end{pmatrix}\quad(5)$$

当取得合适的 $p=2\alpha/\pi$ 使得 Chirp 信号 $x=\mathrm{e}^{\mathrm{j}\frac{c}{2}t^2}$ 在 $u=0$ 处聚焦，即 $X_p(u)$ 在 $u=0$ 处得到最大值 $X_p(0)$：

$$|X_p(0)|=\left|\sum_{i=-\frac{N-1}{2}}^{\frac{N-1}{2}}F_{0,i}\cdot x_i\right|\le\sum_{i=-\frac{N-1}{2}}^{\frac{N-1}{2}}|F_{0,i}|\cdot|x_i|=$$
$$\sum_{i=-\frac{N-1}{2}}^{\frac{N-1}{2}}|F_{0,i}|=8.033\,|_{N=65}\quad(6)$$

因此，当可分离二维分数傅里叶变换在适当的阶数下出现二维 Chirp 信号聚焦时，聚焦幅度为

$$S_{p_1,p_2}(0,0)=F_{p_1}\{F_{p_2}(I(x,y)\}=F(I(x,y))=64.52\quad(7)$$

载体的小波变换后的低频系数在阶数远离 1 时($p=1.6$)的分数傅里叶变换幅度 $S_{p_1,p_2}(0,0)<3$，所以，理论上二维 Chirp 信号聚焦的幅度超过载体低频小波系数的 FRFT 值 20 倍，然而在计算机实际搜索峰值的过程中由于计算误差，这个倍数略小于 20。当嵌入强度 $\alpha=0.1$ 时，Chirp 信号在合适阶数的 FRFT 聚焦时的峰值超过载体的 FRFT 2 倍左右，且满足水印透明性的要求。

3　基于小波和分数傅里叶变换的水印嵌入与检测

为了提高水印的鲁棒性能，本文采取在载体图像的低频小波系数中嵌入 2 分量二维 Chirp 信号。

3.1　小波变换域中 Chirp 水印信号的嵌入

水印嵌入过程如图 2 所示。

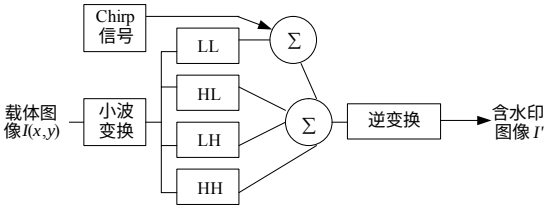


图 2　水印嵌入

首先将载体图像 I 进行小波变换，提取低频小波系数 $C(x,y)$。然后将给定的离散 Chirp 信号 $S(x,y)$ 嵌入到 $C(x,y)$ 中，嵌入公式为 $W(x,y)=C(x,y)+\alpha S(x,y)$，其中，$\alpha$ 为嵌入强度。最后逆变换得到含有水印的图像。本文采用 2 分量的二维离散 Chirp 信号作为水印，初始频率和初始相位设为 0，此时，水印信号表示为 $S(t_1,t_2)=\sum_{i=1}^{2}A_i\mathrm{e}^{\mathrm{j}(\pi\mu_{i1}t_1^2+\pi\mu_{i2}t_2^2)}$，经过采样率为 f_1,f_2 的采样并取实部获得离散 Chirp 信号：

$$S(x,y)=\sum_{i=1}^{2}A_i\cos(\pi\mu_{i1}\frac{1}{f_1^2}t_1^2+\pi\mu_{i2}\frac{1}{f_2^2}t_2^2)=\sum_{i=1}^{2}A_i\cos(a_ix^2+b_iy^2) \tag{8}$$

本文选取 $a_i=b_i=\pi\mu_{i1}=\pi\mu_{i2}=-\pi\cot(\frac{p_i\pi}{2}),\ i=1,2$。式(8)中各个水印信号的幅度$A_i$可以取得很小。水印的参数 (a_i,b_i) 作为密钥通过公共安全密钥机制传给接收方，也可以把与参数 (a_i,b_i) 匹配的FRFT阶数 p_i 作为密钥传给接收方。

3.2　水印信号检测

水印的检测采用和单分量一样的检测算法：在各个不同的与密钥参数 (a_i,b_i) 匹配的阶数 p_i 附近以一定的分辨率做DFRFT，然后做出各个不同变换阶数下峰值 $\max\left|X_{p_1,p_2}(u,v)\right|$ 随阶数变化的曲线，若曲线的变化中有尖峰，则认为有水印，如果变化平缓，则认为不存在水印。Chirp 水印检测的过程如图 3 所示。

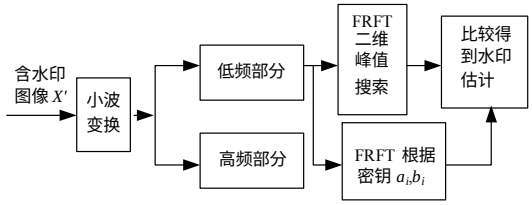


图 3　Chirp 水印检测

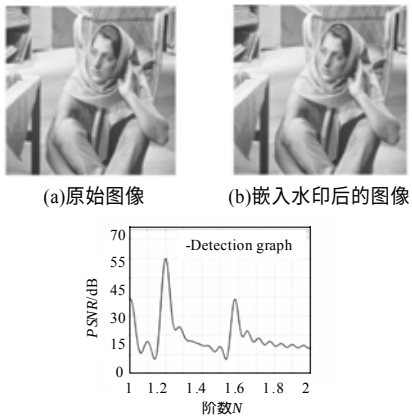
考虑到载体在 P=1 附近的能量集中特性，应该将需要嵌入的 Chirp 信号调频率提高，使得 Chirp 信号聚焦的分数傅里叶变换的阶数远离 1 而接近 2。

4　仿真实验与抗攻击测试

4.1　仿真实验

仿真试验采用原始图像为 256×256 的灰度级 Wbarb 图像。

Chirp水印信号调频率为a_1=b_1=1.08，a_2=b_2=4.05，其能量聚集的变换阶数分别为 $p_1=p_2=1.21$ 和 $p_1=p_2=1.58$；使用 10 dB小波，嵌入的幅度分别为 $A_1=A_2=1$，嵌入强度为 α=0.05，其峰值信噪比 $PSNR=48.8173$。扫描步长为 0.005。为简化运算，检测时仅对嵌入水印的图像在与调频率匹配的阶数附近做DFRFT。图 4(a)、图 4 (b)是原始图像和加入水印后的图像。图 4(c)给出了检测器在阶数$p1$=$p2$=1.21 和p_1=p_2=1.58 附近进行DFRFT的扫描峰值曲线。嵌入的Chirp 信号分别在阶数p_1=p_2=1.21 和p_1=p_2=1.58 下有很好的能量聚集，并被检测器检测出来。



(a)原始图像　(b)嵌入水印后的图像

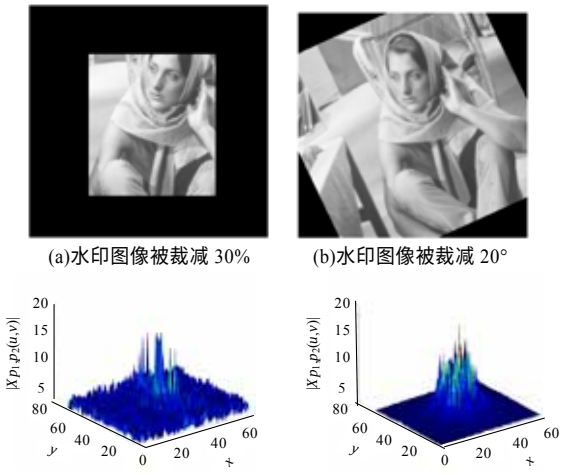
(c)检测器在不同 FRFT 阶数上的响应

图 4　原始图像、嵌入 Chirp 水印的图像以及水印检测器的响应

实验表明，载体图像剪切不超过 30%时漏检率为 0，因剪切引起的 p 的检测偏差不超过 0.01，此时提高嵌入强度，p 的检测偏差可以降为 0；在小波域内嵌入水印信息，压缩比不超过 64 时漏检率为 0，转角不超过 45°的旋转攻击下的漏检率为 0，这 2 种情况下 p 的检测偏差均为 0。当图像不含有水印时，检测器不能在变换域产生聚焦，误检率为 0。在阶数扫描时算子矩阵 $\boldsymbol{H}_N$ 不需要重新计算，只需要改变角度，即可得到新的阶数下的算子矩阵，因此，缩短了计算时间，提高了检测精度。

4.2　算法的抗攻击性能测试

图 5(a)、图 5 (b)分别为载体图像被裁减 30%，旋转 20°；图 5(c)、图 5(d)分别为 2 种攻击下水印检测器在 $p_1=p_2=1.21$ 的响应。一般剪切是水印较难抵抗的攻击， 但是试验显示如果裁减的图像为原始图像的 30%以上时，该系统仍然能够检测出水印的存在。由于嵌入的是多分量水印，因此对于旋转，该系统具有一定的鲁棒性。



(a)水印图像被裁减 30%　(b)水印图像被裁减 20°

(c)图(a)的监测器响应　(d)图(b)的监测器响应

图 5　性能测试

p_1,p_2 是在空域嵌入水印时检测到的阶数，p'_1,p'_2 是在小波域嵌入水印时检测到的阶数，p_1,p_2/p'_1,p'_2见表 1。本文主要比较在各种信号处理的攻击下，算法检测到的使得Chirp水印信号聚焦的阶数，由于本文使用 2 分量的Chirp水印，因此检测的FRFT有两个聚焦阶。“ - ”表示未能检测出使得FRFT聚焦的阶数。数据表明，本文在小波域嵌入水印较在空域嵌入水印提高了水印的鲁棒性能。

表 1　水印直接嵌入空域/水印嵌入低频小波系数抗攻击性能比较

嵌入强度 a	含水印图像无攻击 $(p_1,p_2/p'_1,p'_2)$	叠加加性高斯噪声 $(p_1,p_2/p'_1,p'_2)$	JPEG2000 压缩 (32:1) $(p_1,p_2/p'_1,p'_2)$	含水印图像旋转 45° $(p_1,p_2/p'_1,p'_2)$	含水印图像旋转 25° $(p_1,p_2/p'_1,p'_2)$	剪切 30% $(p_1,p_2/p'_1,p'_2)$
0.05	1.00, —/1.21, 1.58	1.00, —/1.20,1.55	1.00, —/1.20,1.57	1.00, —/1.20,1.56	1.00, —/1.20,1.56	1.00, —/1.20,1.54
0.06	1.15, —/1.21, 1.58	1.00, —/1.20,1.56	1.05,1.48/1.21,1.58	1.00, —/1.20,1.57	1.00, —/1.21,1.56	1.00, —/1.20,1.56
0.07	1.17,1.54/1.21, 1.58	1.10,1.48/1.21,1.56	1.08,1.50/1.21,1.58	1.00, —/1.21,1.57	1.00, —/1.21,1.57	1.00, —/1.20,1.56
0.08	1.18,1.55/1.21,1.58	1.10,1.48/1.21,1.57	1.11,1.52/1.21,1.58	1.10,1.44/1.21,1.58	1.07,1.44/1.21,1.57	1.06, —/1.21,1.56
0.09	1.20,1.55/1.21,1.58	1.13,1.50/1.21,1.58	1.14,1.51/1.21,1.58	1.12,1.40/1.21,1.58	1.10,1.43/1.21,1.58	1.05, —/1.21,1.57
0.10	1.21,1.57/1.21,1.58	1.15,1.50/1.21,1.58	1.17,1.50/1.21,1.58	1.15,1.42/1.21,1.58	1.10,1.44/1.21,1.58	1.05,1.40/1.21,1.58

根据文献[7]，将水印直接嵌入空域和本文将水印信号嵌入载体的低频小波域进行比较：*PSNR*1, *PSNR*2 分别是根据文献[7]的空域水印算法和根据本文的小波域水印算法得到的含水印图和原始图像之间的峰值信噪比。如图 6 所示，在小波域嵌入水印有较高的峰值信噪比。

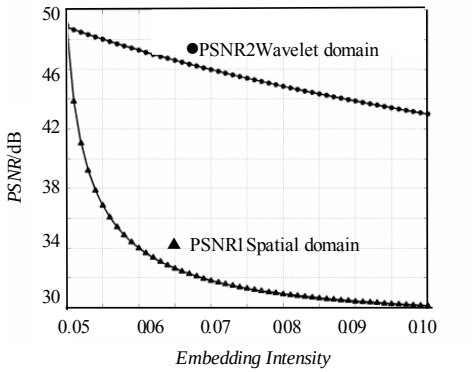


图 6　Chirp 信号嵌入图像空域和小波域的比较

5　结束语

本文提出了一种将多分量 Chirp 信号作为数字水印嵌入到原始图像低频小波系数中的方法，研究了直接离散化方法计算分数傅里叶变换的合理阶数的选取。水印检测算法利用分数阶傅里叶变换有效地将水印信号提取出来。仿真实验表明本文提出的算法对于一些常见图像处理操作和有损压缩具有鲁棒性。未来的工作可以在本文的基础上，进一步提高 FRFT 的计算精度，从而利用 FRFT 对 Chirp 信号特有的能量聚集性进行有意义的水印算法研究。

参考文献

[1] Santhanam B, McClellan J H. The Discrete Rotational Fourier Transform[J]. IEEE Transactions on Signal Processing, 1996, 42(4): 994-998.

[2] Ozaktas H M, Arikan M O. Alper Kutay and Gozde Bozdag2i. Digital Computation of the Fractional Fourier Transform[J]. IEEE Transactions on Signal Processing, 1996, 44(9): 2141-2150.

[3] Chang Pei Soo, Hung Yeh Min, Cheng Tseng Chien. Discrete Fractional Fourier Transform Based on Orthogonal Projections[J]. IEEE Transactions on Signal Processing, 1999, 47(5): 1335-1347.

[4] 平先军, 陶　然, 周思永, 等. 一种新的分数阶傅里叶变换快速算法[J]. 电子学报, 2001, 29(3): 406-408.

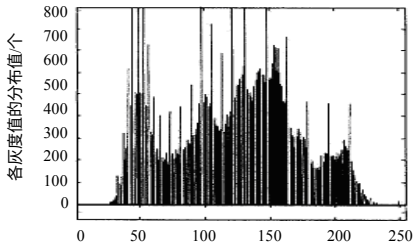
[5] Stankovic S, Djurovic I, Pitas I. Watermarking in the Space/Spatial-frequency Domain Using Two-dimensional Radon-wigner Distribution[J]. IEEE Trans. on Image Processing, 2001, 10(4): 650-658.

[6] 刘正君, 赵海发, 朱邦和, 等. 分数傅里叶域数字水印算法[J]. 光子学报, 2002, 32(3): 332-335.

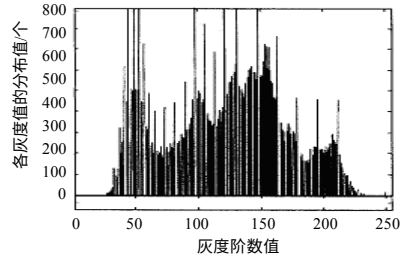
[7] 朱春华, 穆晓敏, 张　峰. 基于修正 Chirp-fourier 变换的数字水印算法[J]. 计算机工程, 2006. 32(17): 213-215.

(上接第 14 页)

图 4 为原始图像和密文图像的灰度直方图。



(a)原始图像灰度直方图



(b)密文图像灰度直方图

图 4　加密前后图像的灰度直方图

利用算法 1 得到 x_0, x_1, x_2, x_3, x_4 平均有 7 个候选值，混沌序列 $x_0, x_1, \cdots, x_{M+N-1}$ 其余 1 019 个值只有 1 个候选值，利用这些 $x_0, x_1, \cdots, x_{M+N-1}$ 对密文图像进行解密并与原始图像对照，得到正确的混沌序列。再利用算法最终得到密钥 a 和 n 的值。在约 70 s 内求出了密钥参数 x_0 , a 和 n，所使用计算机的参数为主频 2.5 GHz 的 Pentium4 PC。根据图 3 可以看出，原始图像和密文图像的灰度直方图完全相同。

4　结束语

本文分析了基于混沌序列的图像加密算法，发现该加密算法本质上是利用密钥产生一个移位密码，理论分析和实验结果都证明该加密算法是不安全的。因此，要设计一个性能良好的数字化混沌密码，必须对所使用的变换环节深入研究，以避免各种安全隐患[4]。

参考文献

[1] 陈永红, 黄席樾. 基于混沌序列的图像加密解密算法[J]. 计算机工程, 2004, 30(21): 104-106.

[2] Masud N, Aihara K. Cryptosystems with Discretized Chaotic Maps[J]. IEEE Trans. on Circuit and Systems, 2002, 49(1): 28-40.

[3] 金晨辉, 高海英. 对两个基于混沌的序列密码算法的分析[J]. 电子学报, 2004, 34(7): 1066-1070.

[4] 李树钧. 数字化混沌密码的分析与设计[D]. 西安: 西安交通大学, 2003.