

一种基于混沌和分数阶傅里叶变换 的数字水印算法*

邹露娟 汪波 冯久超†

(华南理工大学电子与信息学院, 广州 510641)

(2007 年 7 月 10 日收到, 2007 年 9 月 17 日收到修改稿)

基于混沌序列及离散分数阶傅里叶变换, 提出了一种基于混沌和分数阶傅里叶变换的数字水印算法, 并对算法及抗攻击性能进行了仿真分析. 结果表明, 该算法简单有效, 对 JPEG 压缩、噪声、滤波等攻击具有良好的鲁棒性.

关键词: 数字水印, 混沌, 分数阶傅里叶变换, 鲁棒性

PACC: 0545

1. 引言

随着多媒体技术与互连网技术的迅速发展, 基于数字水印技术的电子多媒体作品版权保护问题已成为信息科学领域的研究热点. 数字水印技术是信息隐藏技术的一个重要研究方向, 其基本方法是在被保护的数字产品(如静止图像、视频、音频等)中嵌入能够证明版权归属或跟踪侵权行为的水印信息, 并要求水印信息必须具有不可见性、鲁棒性和安全性^[1].

目前数字水印技术大体上可分为空域和变换域水印两大类^[2]. 空域数字水印是通过改变空域像素灰度值来嵌入水印信息, 如 LSB(least Significant bits)嵌入; 变换域数字水印则是将载体图像变换到变换域, 通过改变变换域系数来嵌入水印, 如 DCT(discrete cosine transform)域嵌入. 当嵌入的水印信息比较多时, 一般变换域水印要优于空域水印算法^[3].

近几年来, 一些学者开始对基于离散分数阶傅里叶变换(discrete fractional Fourier transform, DFRFT)域^[4]数字水印算法和基于混沌的数字水印算法进行了探讨. 分数阶傅里叶变换(fractional Fourier transform, FRFT)是一种在时频域内表示信号的新方法^[5], 它具有空域和频域的双域特性^[6]. 在 DFRFT 域水印方面, 刘正君等^[7]提出了一种分数阶傅里叶

域数字水印算法, 该算法分别对原始图像和水印图像进行不同阶次的分数阶傅里叶变换, 提取水印图像分数阶傅里叶谱的低频成分并直接叠加到原始图像的分数阶傅里叶谱的对角线元素上, 该算法简便可行、抗攻击性能较好; 而在基于混沌水印方面, 不少学者提出了基于混沌加密的水印算法. 郑融等^[8]提出基于混沌加密的 DCI(discrete cosine transform)域数字水印算法, 其基本思想是对混沌序列置乱处理后的二值图像进行调制, 再将其嵌入到 DCT 域低频系数中; 和红杰等^[9]提出基于混沌的自嵌入安全水印算法, 以混沌初值为密钥生成混沌序列, 根据混沌序列的索引有序序列随机生成图像块的水印嵌入位置.

本文综合混沌及 DFRFT 的特点, 提出一种基于混沌和分数阶傅里叶变换的数字水印算法, 该算法利用了混沌序列对初值的极端敏感性^[10], 控制水印图像置乱及分数阶变换的阶数, 并在分块 DFRFT 幅度谱上嵌入水印信号.

2. 分数阶傅里叶变换

一维连续函数 $x(t)$ 的分数阶傅里叶变换^[11]为

$$F_p(u) = \int_{-\infty}^{+\infty} K_p(u, t)x(t)dt, \quad (1)$$

其中 $K_p(u, t)$ 为变换核, 定义为

* 国家自然科学基金(批准号: 60572025)、教育部“新世纪优秀人才”基金(批准号: NCET-04-0813)、教育部重点项目基金(批准号: 105137)、广东省自然科学基金(批准号: 07006496, 04205783)资助的课题.

† 通信联系人, E-mail: fengjc@scut.edu.cn

$$K_p(u, t) = \begin{cases} \sqrt{\frac{1 - j \cot \alpha}{2\pi}} \exp\left(j \frac{u^2 + t^2}{2} \cot \alpha - \frac{jut}{\sin \alpha}\right), & \alpha \neq n\pi, \\ \delta(t - u), & \alpha = 2n\pi, \\ \delta(t + u), & \alpha = (2n \pm 1)\pi, \end{cases} \quad (2)$$

其中 $p(0 < |p| < 2)$ 为变换阶数, 对应的变换角度 $\alpha = \pi \times p/2$.

二维连续信号 $s(x, y)$ 的分数阶傅里叶变换为

$$F_{p_x, p_y}(u, v) = \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} s(x, y) K_{p_x, p_y}(x, y, u, v) dx dy, \quad (3)$$

其中 p_x, p_y 分别为横轴与纵轴方向的变换阶数, $K_{p_x, p_y}(x, y, u, v)$ 是二维 FRFT 的变换核.

二维离散信号 $s(p, q)$ 的分数阶傅里叶变换为^[12]

$$F(m, n) = \sum_{p=0}^{M-1} \sum_{q=0}^{N-1} s(p, q) K_{p_x, p_y}(p, q, m, n), \quad (4)$$

其中 $K_{p_x, p_y}(p, q, m, n)$ 是二维 DFRFT 的变换核.

3. 水印嵌入算法

3.1. 水印预处理

考虑将二值水印图像信号转换为一维的二值序列, 然后对其进行混沌置乱, 以提高水印的保密性. 本文用 Logistic 映射^[13-15]对序列进行混沌置乱, 它的动力学方程为

$$x_{n+1} = \mu x_n (1 - x_n), \quad (5)$$

其中 $\mu \in (0, 4]$ 称为分支参数; $x_n \in (0, 1)$. 当 $3.5699456 < \mu \leq 4$ 时, Logistic 映射工作于混沌状态. 该混沌序列具有形式简单、对初始条件极端敏感、具有“似噪声”等特性. 在不知道密钥 x_1 和 μ 的情况下, 即使破解了水印嵌入算法, 也无法正确恢复出水印信息.

置乱的具体算法如下: 用 Logistic 映射产生一个与水印序列等长的混沌序列 $X = \{x(k) | k = 1, 2, \dots, L\}$. 对此混沌序列排序, 从而得到一个新的序列 $X' = \{x'(k) | k = 1, 2, \dots, L\}$. 根据 X' 对水印序列进行随机换位, 其换位规则如下:

$$w'(d(k)) = w(k), \quad (6)$$

其中 $k = 1, 2, \dots, L$, w 和 w' 分别为置乱前后的水印信息.

3.2. 幅度谱水印嵌入

幅度谱水印嵌入及提取的流程如图 1 所示. 首先将原始图像分割为互不重叠的子块(如大小为 8×8)对每个子块进行 DFRFT 变换, 其阶数由混沌序列所控制, 然后在确定的幅度分量中加入水印信息, 并将其坐标位置保存做为水印提取的密钥, 得到嵌入水印的图像.

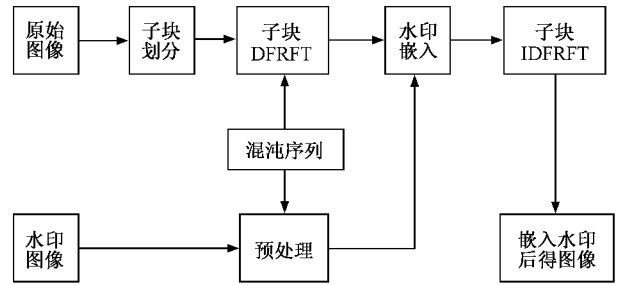


图1 算法流程图

幅度谱水印算法步骤如下:

1) 划分子块. 将原始图像分割成不重叠的图像子块(大小为 8×8), 子块数为 L .

2) 利用 Logistic 映射产生 p_x 与 p_y 两组混沌序列, 序列长度均为 L .

3) 对每个子块进行 DFRFT 变换得 F , 其横轴与纵轴方向的变换阶数分别由 p_x 与 p_y 混沌序列控制, 然后求出每一子块的平均频谱分量值

$$E = \frac{1}{64} \sum_{u=0}^7 \sum_{v=0}^7 |F(u, v)|^2. \quad (7)$$

4) 确定嵌入水印的坐标位置. 坐标 (m, n) 由以下式子确定:

$$\{(m, n) | E - |F(m, n)|^2 | \\ = \min(|E - |F(i, j)|^2 |)\}, \quad (8)$$

其中 $0 \leq i, j \leq 7$. 利用此低频系数对应的幅度分量嵌入水印信息来提高鲁棒性, 并生成提取水印信息的密钥, 即嵌入数字水印信息的坐标信息.

5) 嵌入水印信息并修改相应的幅度分量.

$$\begin{cases} |F(m, n)| \\ = \begin{cases} \sqrt{|E - |F(m, n)|^2 | + P}, & w'(k) = 1 \\ \sqrt{|E - |F(m, n)|^2 | - P}, & w'(k) = 0, \end{cases} \end{cases} \quad (9)$$

其中, P 为水印的嵌入强度. P 值越大, 水印的鲁棒性越强, 但保真性越差. 因此要选择适当的 P 来兼顾原始图像的保真性和水印图像的鲁棒性.

6) 对每一子块进行 IDFRFT 变换, 得到嵌入水印的数字图像.

3.3. 水印提取

把待提取的图像 I' 分割成互不重叠的子块(大小为 8×8), 其子块数为 L , 对每个子块进行 DFRFT 变换, 其横轴与纵轴方向的变换阶数分别由混沌序列 p_x 与 p_y 控制, 最后利用坐标密钥提取水印信息.

$$v(k) = \begin{cases} 1, & |F(m, n)| > \sqrt{E - |F(m, n)|^2}, \\ 0, & |F(m, n)| < \sqrt{E - |F(m, n)|^2}, \end{cases} \quad (10)$$

其中 $k = 1, 2, \dots, L$, L 为水印序列的长度. 对 v 作置乱反变换, 得水印序列 v' , 即

$$v'(k) = v(d(k)). \quad (11)$$

然后, 把 v' 按照原水印规格大小排列, 即可提取水印图像.

4. 仿真结果

仿真实验中采用原始 Lenna 图像(大小为 512×512 , 如图 2 所示)及二值水印图像(大小为 64×64)验证本文算法的鲁棒性.

4.1. 嵌入水印后的图像质量

一般用峰值信噪比(peak signal noise ratio, PSNR)来衡量嵌入水印后的图像的失真程度^[16],

$$\text{PSNR} = 10 \log_{10} \left(\frac{255^2}{\frac{1}{M^2} \sum_{i=0}^{M-1} \sum_{j=0}^{M-1} (I(i, j) - I'(i, j))^2} \right), \quad (12)$$

其中 I 为原图像灰度值, I' 为嵌入水印后的图像灰度值. PSNR 值越高, 原始图像失真程度越小, 则保真性能越好.

采用本文算法后, 嵌入水印后的图像 PSNR = 38.13 dB. 从图 2(b) 可以看出, 原图像嵌入水印后具有良好的保真性.

4.2. 抗攻击性能分析

数字图像在网络上被大量传输时, 它可能受到



理
华
工
南

(c)



图 2 原图像(a) 嵌入水印后的图像(b) 水印图像(c)

各种方式的攻击, 侵权者总是试图篡改或除去水印信息. 为了验证本文算法的鲁棒性, 本文分别对 JPEG 压缩、噪声干扰、滤波、图像旋转等几种典型的攻击进行了仿真分析.

提取的水印与原水印的失真程度通常用相关系数来度量, 归一化的相关系数(normalized correlation, NC)定义为

$$\text{NC} = \frac{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} u(i, j)v(i, j)}{\sqrt{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} [u(i, j)]^2}}, \quad (13)$$

其中 w 为原水印, v 为提取的水印, 水印的大小为

$M \times N$. 当 NC 大于一定值时, 则表明可以有效地提取水印信号. 图 3 与表 1 的实验结果表明, 对嵌入水印的图像进行 JPEG 压缩、噪声干扰、滤波、图像旋转等各种攻击, 本文算法都能有效地提取水印, 能抵抗各种图像攻击, 具有较强的鲁棒性.

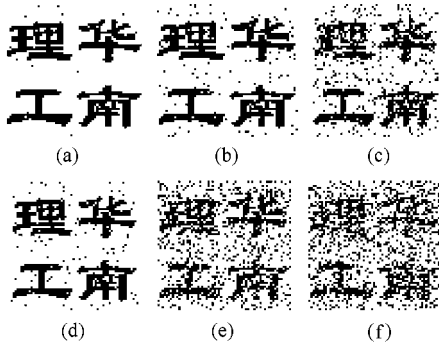


图 3 各种攻击下提取的水印图像 (a) JPEG 压缩因子 80 (b) 高斯噪声方差 0.002 (c) 椒盐噪声强度 0.015 (d) 高斯低通滤波 $\sigma=0.5$ (e) 均值滤波 (f) 图像旋转 0.1°

表 1 各种攻击下水印的鲁棒性测试结果

攻击类型	参数及对应攻击下所得 NC 值					
		90	80	70	60	50
JPEG 压缩	质量因子	0.998	0.996	0.989	0.991	0.991
	NC					
高斯噪声	标准差	0.001	0.002	0.003	0.004	0.005
	NC	0.987	0.966	0.945	0.920	0.895
椒盐噪声	噪声强度	0.010	0.015	0.020	0.025	0.030
	NC	0.934	0.905	0.883	0.859	0.830
高斯低通滤波	sigma	0.1	0.3	0.5	0.7	0.9
	NC	0.999	0.998	0.972	0.924	0.892
均值滤波	3×3			0.8986		
图像旋转	0.1°			0.7647		

5. 结 论

实验结果表明, 本文提出的基于混沌和分数阶傅里叶变换域的幅度谱数字水印算法, 不仅能很好地隐藏数字水印信息, 而且具有良好的鲁棒性, 能够很好地抵抗 JPEG 压缩、噪声、滤波等各种常见的图像攻击, 并能抵抗一定的旋转攻击. 同时该算法利用混沌序列控制水印图像置乱和分数阶傅里叶变换的阶数, 提高了水印图像的安全性.

- [1] Cheng Q, Huang T S 2003 *IEEE Trans. on Signal Proc.* **51** 906
- [2] Zhang F, Mu X M, Yang S Y 2005 *IEEE Int. Symp. Intelligent Signal Processing and Communication Systems (ISPCS)* **13** 141
- [3] Sun S H, Lu Z M 2000 *Acta Elec.* **8** 85 (in Chinese) [孙圣和、陆哲明 2000 电子学报 **8** 85]
- [4] Peis S C, Tseng C C, Yeh M H, Shyu J J 1998 *IEEE Trans. on Circuits and Systems. - II* **45** 665
- [5] Tao R, Qi L, Wang Y 2004 *Theory and Applications of the Fractional Fourier Transform* (Beijing : Tsinghua University Press) p1 (in Chinese) [陶 然、齐 林、王 越 2004 分数阶 Fourier 变换的原理与应用 (北京 清华大学出版社) 第 1 页]
- [6] He Q, Tian R Q, Wang Y M 2006 *Computer Engineering and Design.* **27** 4642 (in Chinese) [何 泉、田瑞卿、王彦敏 2006 计算机工程与设计 **27** 4642]
- [7] Liu Z J, Zhao H F, Zhu B H, Liu S T 2003 *Acta Photonica Sinica* **32** 332 (in Chinese) [刘正君、赵海发、朱邦和、刘树田 2003 光子学报 **32** 332]
- [8] Zhen R, Jin C, Wei W F, Li B 2005 *Journal of Computer Applications* **25** 2365 (in Chinese) [郑 融、金 聪、魏文芬、李 蓓 2005 计算机应用 **25** 2365]
- [9] He H J, Zhang J S 2007 *Acta Phys. Sin.* **56** 3092 (in Chinese) [和 红杰、张家树 2007 物理学报 **56** 3096]
- [10] Li Z H, Hou J J 2006 *Acta Elec.* **12** 2134 (in Chinese) [李赵红、侯建军 2006 电子学报 **12** 2134]
- [11] McBride A C, Kerr F H 1987 *IMA J Appl Math.* **39** 159
- [12] Pei S C, Yeh M H 1998 *Signal Processing.* **67** 99
- [13] Phatak S C, Rao S S 1995 *Physical Review E* **51** 3670
- [14] Feng J C, Xie S L 2005 *Proc. of Int. Conf. on Commu. Circuits and Systems* **2** 1173
- [15] Hou W, Feng G L, Dong W J 2005 *Acta Phys. Sin.* **54** 3940 (in Chinese) [侯 威、封国林、董文杰 2005 物理学报 **54** 3940]
- [16] Cai L M, Feng J C 2007 *Computer Science.* **34** 234 (in Chinese) [蔡丽敏、冯久超 2007 计算机科学 **34** 234]

A digital watermarking algorithm based on chaos and fractional Fourier transformation^{*}

Zou Lu-Juan Wang Bo Feng Jiu-Chao[†]

(School of Electronic and Information Engineering , South China University of Technology , Guangzhou 510641 , China)

(Received 10 July 2007 ; revised manuscript received 17 September 2007)

Abstract

Based on chaotic sequences and discrete fractional Fourier transform , a digital watermarking algorithm is proposed , and its resistance to attacks is simulated. The results show that the algorithm is easy to realize , and is robust to the attacks from JPEG compression , noise perturbation and filtering.

Keywords : digital watermarking , chaos , fractional Fourier transform , robustness

PACC : 0545

^{*} Project supported by the National Natural Science Foundation of China (Grant No. 60572025) , the Program for New Century Excellent Talents in China University (Grant No. NCET-04-0813) ; the Key Project Foundation of the Education Ministry of China (Grant No. 105137) and the Natural Science Foundation of Guangdong Province , China (Grant Nos. 07006496 , 04205783) .

[†] Correspondence author. E-mail : fengjc@scut.edu.cn