

基于混沌和傅里叶变换的数字水印算法

赵梅, 姜梅, 甘信丹

(青岛理工大学计算机工程学院, 山东 青岛 266033)

摘要:提出一种基于混沌映射和分数阶傅里叶变换的数字水印算法。采用有版权信息的二值图像作为水印, 利用混沌映射在密钥的控制下对水印进行加密置乱。利用由密钥生成的混沌序列对数字图像进行分数傅里叶变换, 并将已经混沌置乱的水印信息嵌入到原始图像的中频幅度谱系数对应的相位谱系数中, 最后进行分数傅里叶逆变换可以得到嵌入水印的图像。通过仿真实验可以证明该算法简便易行, 且具有良好的不可见性, 对图像的剪切、压缩、添加噪声和旋转一系列的图像攻击操作具有良好的鲁棒性。

关键词:数字水印; 分数傅里叶变换; 混沌; 鲁棒性

中图分类号:TP309

文献标识码:A

文章编号:1673-629X(2011)02-0189-04

Digital Watermarking Algorithm Based on Chaos and Fourier Transform

ZHAO Mei, JIANG Mei, GAN Xin-dan

(School of Computer Engineering, Qingdao Technological University, Qingdao 266033, China)

Abstract: A digital watermarking algorithm is proposed based on chaotic map and fractional Fourier transform. Design a binary image as a watermark, and encrypt it by a chaotic map under the control of the secret key. The original digital image is fractional Fourier transformed with the chaotic sequences generated by the key, and the watermark is embedded in the phase spectrum coefficient. Finally the watermarked image can be obtained by inversely fractional Fourier transformation. The experimental results show that the algorithm is simple, invisible, and robust against crop, compression, added noise and rotation.

Key words: digital watermarking; fractional Fourier transform; chaos; robustness

0 引言

随着多媒体技术与网络信息技术的迅速发展, 各种数字化信息被广泛的生成、存储、交换和使用, 与此同时, 对多媒体数字产品的版权保护也随即成为需要迫切解决的问题, 而基于数字水印技术的数字信息版权保护被认为是一种保证网络资源安全的有效技术。

所谓数字水印可以视为是在原始信号强背景下叠加的一个弱信号, 只要叠加的水印信号强度低于人的视觉系统(HVS)或听觉系统(HAS)的感知门限, 人就无法感知到水印信号的存在。由于分数傅里叶变换同时包括时域和频域信息, 可以把水印信息隐藏在被保护信息的中频分数傅里叶谱部分的系数上, 从而起到保护数字作品版权或完整性的作用^[1]。

近年来, 数字水印技术的研究取得了很大进展和突破, 陆续提出了空域、变换域、压缩域等多种数字水

印算法。其中, 基于离散傅里叶变换(DFT)域的水印算法原理比较简单, 有着其他频率域算法不可替代的优点。其研究方向主要分为两大类: 一类是基于DFT域的平移、缩放和旋转的几何不变性, 将载体图像进行傅里叶梅林(Fourier-Millin)变换实现水印的嵌入来抵抗几何攻击。但是水印嵌入后会引入较大的失真, 并且算法的复杂度高, 实现起来难度比较大; 还有一类DFT域水印算法是把水印信息嵌入到变换域的频谱中。而且, Cox和Ruanaidh等人还认为图像水印应嵌在最重要的分量上以获得较好的鲁棒性, M. H. Hayes通过研究分析得出DFT相位成分和幅度成分的相关重要性, 并证明了图像DFT系数中相位分量比幅度分量更重要^[2]。目前已有的大部分变换域算法都是将水印嵌入到变换系数的幅值中。

文中综合混沌序列及分数傅里叶变换的特点, 提出一种基于混沌序列和离散分数阶傅里叶变换的相位谱数字水印算法, 设计了一种包含版权信息的二值图像作为待嵌入的水印, 利用Logistic混沌序列对其加密置乱, 然后将水印图像间接嵌入到原始图像的分数

收稿日期: 2010-06-10; 修回日期: 2010-09-03

作者简介: 赵梅(1986-), 女, 山东德州人, 硕士研究生, 研究方向为信息安全、数字水印; 姜梅, 副教授, 博士, 研究方向为计算机网络及其安全。

阶傅里叶变换域中的相位成分中,以此来实现水印的安全隐藏。通过实验证明:该算法简便易行,且具有良好的不可见性和鲁棒性。

1 离散分数阶傅里叶变换

离散傅里叶变换(DFT)是线性系统分析的得力工具^[3]。由于DFT是复数变换,其变换的实部和虚部分别表示信号的幅度和相位信息,在幅度和相位满足一定的条件时,数字水印信息即可以嵌入到宿主信号的幅度上,也可以隐藏在相位中。

离散分数阶傅里叶变换(DFRFT)^[4]是经典的离散傅里叶变换的分数级推广,是一种介于函数与其傅里叶变换之间的信号双域描述,基于此的水印嵌入能兼顾空间域和变换域水印处理技术的优点。

下面介绍DFRFT。

一维连续函数 $x(t)$ 的分数阶傅里叶变换为^[5]:

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

其中 $K_p(u, t)$ 为变换核,定义为:

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

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

二维连续信号 $s(x, y)$ 的分数阶傅里叶变换为:

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

其中 px, py 分别为横轴与纵轴方向上的变换阶数,对应的变换角度为 $\alpha = \pi * p/2$ 。

二维离散信号 $s(m, n)$ 的分数阶傅里叶变换为:

$$F(p, q) = \sum_{m=0}^{p-1} \sum_{n=0}^{q-1} s(m, n) K_{px, py}(m, n, p, q) \quad (4)$$

其中 $K_{px, py}(m, n, p, q)$ 是二维DFRFT的变换核。

2 二值数字图像的混沌加密

数字水印的生成过程就是在密钥 K 的控制下由原始版权信息或其他相关信息 m 生成适合嵌入到宿主信息 x 中的待嵌入水印信号 w 的过程。文中采用带有可识别的版权信息的二值数字图像作为水印信号,嵌入后经过可逆变换其水印信息可以被提取出来。通常情况下,使用的原始水印信息是具有特定意义的,其向邻近的像素或采样点之间有很强的相关性,一旦提取算法泄漏被人知道,攻击者很容易获取水印信息,这样不

利于实现版权保护。而混沌序列^[6]对初值的极端敏感性高,形式简单,比普通的伪随机序列有更好的低通特性,可很好地应用于数字水印信息的加密置乱,有利于提高水印技术的安全性。

文中采用Logistic映射来产生混沌序列,它是一类非常简单却被广泛研究的动力系统,其定义如下:

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

当 $3.5699456 < \mu \leq 4$ 时,Logistic映射处于混沌状态。此时,由初值密钥 x_0 在Logistic映射的作用下产生的序列 $\{x_k; k=0, 1, 2, \dots\}$ 是非周期的、不收敛的,并且对初值极其敏感。下面具体介绍混沌序列的工作流程,首先将二值水印图像转换为一维的二值序列,然后对其混沌置乱,如图1所示。

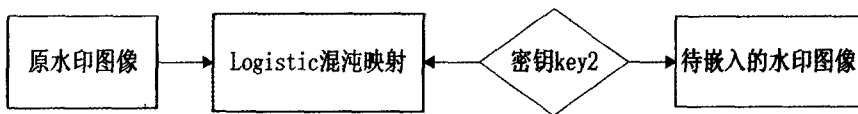


图1 混沌加密流程

设原始水印图像为 W ,大小为 $m * n$,把水印图像信号转换为一维的二值序列,然后用混沌序列对其置乱操作,以提高水印的安全性。

给定密钥 $key2$,令 $x_0 = key2$,由式(1),用Logistic映射产生一个与水印序列等长的混沌序列 $X = \{x_k; k=0, 1, 2, \dots\}$ 。对此混沌序列 X 进行排序得 X' ,根据 X' 在 X 中的位置对水印序列进行随机换位,这样可得到置乱后的水印序列。置乱水印的解密过程即为上述加密过程的逆。

在不知道初值密钥 $key2$ 和分支参数 μ 的情况下,即使破解了水印嵌入算法获得了水印信号的数字矩阵,也无法恢复出可识别的水印图像,从而可以提高水印系统的安全性^[7]。

3 水印嵌入算法

3.1 相位谱水印嵌入流程

相位谱水印嵌入的流程如图2所示。由于分数傅里叶谱的低频部分集中了图像的大部分能量,修改这部分系数容易引起图像失真。若嵌入到高频系数中,则有损压缩和低通滤波操作很容易把水印去除,水印系统的鲁棒性会很弱。文中兼顾考虑到嵌入水印保证原始图片的视觉真实性和水印系统的鲁棒性,将水印信息嵌入到分数傅里叶谱中频系数中^[8]。通过幅度谱确定要嵌入水印的分数傅里叶谱系数,将水印嵌入到其对应的相位谱中,这样可以在幅度不改变的情况下,既提高了鲁棒性和安全性,又能根据密钥确定水印信息所在的与幅度相对应的相位谱,从而可以最大程度地提取出水印信息。

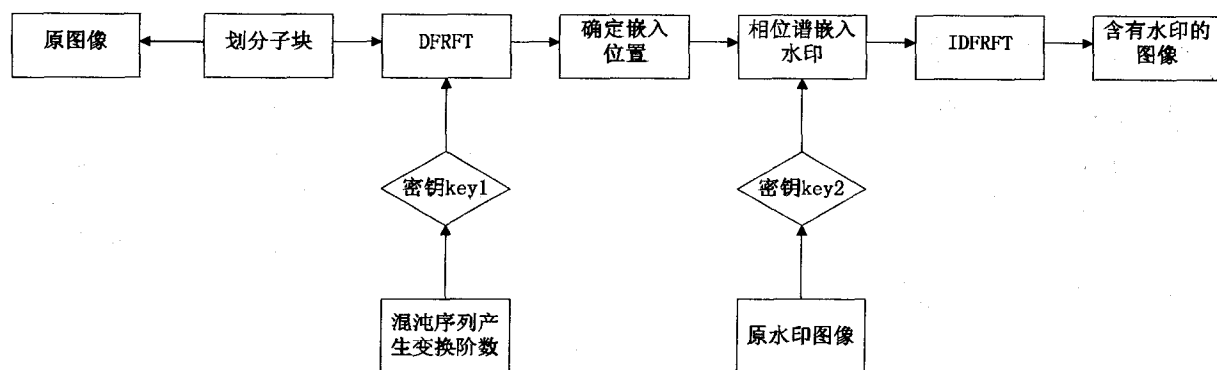


图2 水印算法流程

(1) 将原始图像分成互不重叠的子块^[9](文中取每块大小为 8×8), 总共的子块数为 L , 则:

$$f(u, v) = \bigcup_{k=0}^{L-1} f_k(m', n'), 0 \leq m', n' < 8 \quad (6)$$

(2) 使用相关密钥 key1, 根据 Logistic 混沌映射产生两组相关性很小的混沌序列 k_1, k_2 , 长度均为 L , 用于控制各个子块的 DFRFT 在 x, y 方向上的变换阶数。

(3) 对每一个子块进行二维 DFRFT 变换。

$$F_k(u', v') = \text{DFRFT}\{f_k(m', n'), 0 \leq m', n' < 8\}, 0 \leq u', v' < 8 \quad (7)$$

将变换后得到的系数矩阵 F 分解为幅度谱矩阵 A 和相位谱矩阵 P , 然后根据幅度谱矩阵 A 求出每个子块的平均谱度分量值:

$$E = \frac{1}{8 \times 8} \sum_{u=0}^7 \sum_{v=0}^7 |A(u', v')|^2 \quad (8)$$

(4) 确定中频系数所对应的相位谱分量为待嵌入水印的位置。首先确定幅度谱矩阵的中频系数, 其坐标位置 (m', n') 由下式确定:

$$|E - |A(m', n')|^2| = \min |E - |A(i', j')|^2| \quad (9)$$

如此亦生成了提取水印信息的坐标密钥, 然后根据所确定的位置对应同样位置中的相位谱矩阵 P 中的相位值来嵌入水印信息, 提高水印的安全性。这样通过不改变的幅度谱来确定嵌入水印的相位谱, 亦能通过不改变的幅度谱确定已经嵌入了水印信息的相位谱, 如此, 可以更有效地提取水印信息。而且, 水印信息是嵌入在相位谱中, 文献[2]已经证明 DFT 系数中相位分量比幅度分量更重要, 如此水印处理技术有更可观的鲁棒性。

(5) 修改相位谱分量。设水印位 $\omega_i \in \{0, 1\}$, 文中采用一种非常经典的相位调制方法^[6], 实现水印盲提取。由于 DFT 域的相位变化是负对称的, 应同时确保水印嵌入后仍保持这种性质不改变^[10], 水印嵌入方法如下:

$$P^w(m, n) = \begin{cases} \theta_1, \omega_i = 0 \\ \theta_2, \omega_i = 1 \end{cases} \quad (10)$$

$$P^w(7-m, 7-n) = \begin{cases} -\theta_1, \omega_i = 0 \\ -\theta_2, \omega_i = 1 \end{cases} \quad (11)$$

(6) 对每一个子块进行 IDFRFT 变换, 得到嵌入水印的数字图像。

3.2 提取/检测水印

水印的提取是水印嵌入过程的逆过程。把待提取的图像 F 划分成互不重叠的子块(大小为 8×8), 子块数为 L , 对每个子块进行 DFRFT 变换, 变换阶数由混沌序列 k_1, k_2 控制, 最后由坐标密钥确定嵌入水印信息的坐标, 从对应的相位中提取出水印信息。

$$\omega_i = \begin{cases} 0, |P^w(m, n)| = \theta_1 \\ 1, |P^w(m, n)| = \theta_2 \end{cases} \quad (12)$$

这里 $i=0, 1, 2, \dots, L$, L 为水印序列的长度。然后对 ω 做置乱反变换, 得到水印序列 ω' , 把 ω' 按照原水印规格排序即可提取到最终的水印图像。

4 仿真实验

在 MATLAB7.0 环境下实施相关实验。原始版权水印图像为 64×64 具有 logo 的二值图像, 宿主图像为 512×512 的标准 lena 图像, 如图 3 所示。



正

图3 原始图像和水印图像

通过本实验, 其嵌入和提取的结果如图 4 所示, 嵌入水印的图像有良好的保真性, 嵌入的水印有良好的伪装性, 提取出的水印清晰可见。文中根据提取出的水印信号与原始水印信号的相似度(SIM)^[11,12]来作为水印评价的指标。定义它为:



图 4 嵌入水印的图像、乱水印,提取水印

$$SIM(w, w') = \frac{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} w(i, j) w'(i, j)}{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} [w(i, j)]^2} \quad (13)$$

其中, w 为原始水印信号, w' 为提取出的水印信号。显而易见, SIM 的值越接近 1, 表示嵌入和提取的水印图像的相似程度越高; SIM 值越接近 0, 则表示嵌入和提取出的水印相似程度越低。

4.1 水印鲁棒性实验结果及分析

鲁棒性是指水印产品在经过常规信号处理操作后仍能检测出水印的能力。由于多种方式的攻击, 侵权者会试图从水印图像中检测并去除水印。一个良好的水印算法必须经过实验测试才能对之做出客观的评价。本实验对嵌入了水印的图像进行一定的剪切、压缩、添加噪声和旋转一系列的图像攻击操作, 然后再通过算法提取出水印。表 1 给出了相应的图像处理操作的实验结果。

表 1 不同攻击下的实验结果

攻击类型	不同的攻击下鲁棒性实验结果			
剪切	(右下剪切 1/4, SIM=0.9231)	(中心剪切 1/4, SIM=0.7832)	(右剪切 1/2, SIM=0.8991)	(随机剪切, SIM=0.8021)
压缩	(90% 压缩率, SIM=0.9810)	(80% 压缩率, SIM=0.9725)	(75% 压缩率, SIM=0.9122)	(70% 压缩率, SIM=0.8857)
噪声	(椒盐噪声 $d=0.02$, SIM=0.7526)	(椒盐噪声 $d=0.002$, SIM=0.8950)	(高斯噪声 $\varepsilon=0.5$, SIM=0.9627)	(高斯噪声 $\varepsilon=0.7$, SIM=0.9146)
旋转	(45°, SIM=0.8899)			

实验结果数据表明, 对嵌入水印的图像进行一定的剪切、压缩、添加噪声和旋转一系列的图像攻击操作, 都能有效地提取到水印, 如图 5 所示。

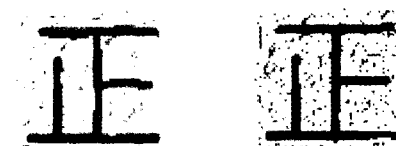
4.2 水印安全性验证实验结果及分析

水印的安全性是指任何非授权的用户既不能检测到图像中的水印存在, 也不能解码水印。文中水印算法使用了两个密钥, 分别为: $key1$ 分数阶傅里叶变换的阶数 (px, py) , $key2$ 将二值图像水印加密置乱的密钥。图 6 给出了有一个密钥不正确时读取的水印和相应的相似度。可见当有一个密钥不正确时, 提取出的

水印图像与原始水印图像的相似度很低, 从视觉上很难辨认。通过多次实验证实任何不知道两个密钥的用户都很难提取出水印, 保证了水印的安全性。



(1) 剪切右下 1/4 (2) 压缩 50% (3) 椒盐噪声 $d=0.002$



(4) 高斯噪声 $\varepsilon=0.7$ (5) 选择 45°

图 5 水印攻击的实验效果



(A) Key1 不正确 (B) Key2 不正确

图 6 安全性实验结果

5 结束语

文中提出的基于混沌映射和分数阶傅里叶变换的相位谱数字水印算法, 提取水印时不需要原始载体图像, 实现了盲提取; 不仅能很好地隐藏数字水印信息, 而且经过实验证明有良好的鲁棒性。

参考文献:

- [1] 孙圣和, 陆哲明, 牛夏牧, 等. 数字水印技术及应用[M]. 北京: 科学出版社, 2004: 32-37.
- [2] Hayes M H. The Reconstruction of a Multidimensional Sequence from the Phase or Magnitude of the FFT[J]. IEEE Transactions on Acoustics, Speech and Signal Processing, 1992(4): 140-145.
- [3] Mendlovic D, Zalevsky Z, Dorsch R G, et al. New signal representation based on the fractional Fourier transform[J]. J. Opt. Soc. Am., 1995, 10(12): 2424-2521.
- [4] Ozaktas H M, Mendlovic D. Fractional Fourier optics[J]. J. Opt. Soc. Am., 1995, 10(12): 2522-2548.
- [5] 邹露娟, 汪波, 冯久超. 一种基于混沌和分数阶傅里叶变换的数字水印算法[J]. 物理学报, 2008(5): 2750-2753.
- [6] May R M. Simple mathematical model with very complicated

从以上检测数据和检测图像中可以看出,该算法在进行各种常见攻击(如压缩、滤波等)和几何攻击(如旋转、缩放、平移等)后,都可以正确检测出水印,有些区域相关性为1,可以完全检测出水印,充分验证了该算法的可靠性。

同时,有部分区域不能正确检测出水印,这是由于待检测图像与其原图像的特征点相比较发生了漂移,从而导致提取区域与原图像发生了改变,影响了此区域水印的正确检测。但是,这并不影响本算法检测水印的相关性,因为只要有一个检测正确就可以判定水印存在。

5 结束语

以数字图像为研究对象,利用第二代水印的框架来解决鲁棒盲水印中的抗几何攻击的难题,并提出了一套基于Harris算子的鲁棒水印算法,对这些算法进行了实验验证。结果表明该算法不仅能抵抗压缩、滤波等常见的攻击,而且对几何攻击,如旋转、缩放等都有较好的鲁棒性。

此外,在水印不被察觉的基础上如何增大嵌入信息量的问题是有待进一步研究和改进的。

参考文献:

- [1] 孙圣和,陆哲明,牛夏牧. 数字水印技术及应用[M]. 北京:科学出版社,2004:67-98.
 - [2] 钮心沂. 信息隐藏与数字水印[M]. 北京:北京邮电大学出版社,2004:51-63.
 - [3] 俞龙江,牛夏牧,孙圣和. 一种旋转尺度变换和平移鲁棒水印算法[J]. 电子学报,2003,31(12A):2071-2073.
 - [4] Pereir S, Pun T. Robust template matching for affine resistant image watermarks[J]. IEEE Trans. Image Process, 2000, 9: 1123-1129.
 - [5] Bas P, Chassery J M, Macq B. Geometrically invariant watermarking sing feature points[J]. IEEE Trans. Image Processing, 2002, 11(9):1014-1028.
 - [6] 石磊,钟铭,洪帆. 抵抗几何变换的基于量化的水印技术[J]. 计算机辅助设计与图形学学报, 2004, 16(6):850-855.
 - [7] Simitopoulos D, Koutsonanos D E, Strintzis M G. Robust image water-marking based on generalized radon transformations[J]. IEEE Trans. Circuits Systems Video Technol, 2003, 13(8):732-745.
 - [8] Schmid C, Mohr R, Bauckhage C. Evaluation of interest point detectors[J]. International Journal of Computer Vision, 2000, 37(2):151-172.
 - [9] 李建. 抗几何攻击的数字图像水印技术的研究[D]. 南京:南京理工大学,2010.
 - [11] Lin Wei-Hung, Horng Shi-Jinn, Kao Tzong-Wann, et al. An Efficient Watermarking Method Based on Significant Difference of Wavelet Coefficient Quantization[J]. IEEE Trans. on Multimedia, 2008, 10(5):749-757.
 - [10] 李水乡,陈斌,赵亮,等. 快速Delaunay逐点插入网格生成算法[J]. 北京大学学报(自然科学版),2006(3):1-5.
 - [12] 于帅珍,冯丽平. 数字水印的关键技术[J]. 计算机技术与发展,2010,20(2):148-151.
-
- (上接第188页)
- 1.]:[s. n.],2000:752-757.
 - [10] 简清明. WebDAV及其在Web群件系统中的应用[J]. 安庆师范学院学报,2004(4):112-117.
 - [11] 江雨燕. Web环境下的在线协同编辑系统设计与实现[J]. 电子科技大学学报,2002,31(6):630-635.
 - [12] 张选平,谭小鹏,朱永虎. 面向Internet的文档管理系统的设计与实现[J]. 计算机工程与设计, 2004, 25(1):135-138.
-
- (上接第192页)
- dynamics[J]. Nature,1976,261:459-481.
 - [7] 王银花,柴晓东,周成鹏,等. 基于混沌序列和分数傅立叶变换的图像加密技术[J]. 计算机技术与发展,2006,16(9):213-215.
 - [8] 王银花,柴晓东,周成鹏,等. 基于分数傅立叶变换的盲数字水印算法[J]. 计算机技术与发展,2008,18(1):168-171.
 - [9] 杨倬,冯久超,方勇. 一种基于混沌和分数阶傅立叶变换的图像加密算法[J]. 计算机科学,2008(9):239-274.
 - [10] 曹荣,王颖,李象霖. 一种基于离散傅立叶变换域相位和幅度的数字水印算法[J]. 计算机应用,2005(11):2536-2543.
 - [11] 王炳锡,陈琦,邓峰森. 数字水印技术[M]. 西安:西安电子科技大学出版社,2003.
 - [12] 王远干,喻洪麟,黄良明. 基于M周期离散分数傅立叶变换的数字水印算法[J]. 计算机应用研究,2005(2):229-231.