

分数阶微积分在数字水印中的应用研究

万晶晶, 于盛林

(南京航空航天大学 自动化学院, 江苏 南京 210016)

摘要:提出并实现了基于分数阶微积分运算的数字水印系统模型。将分数阶微积分运算阶次 v 作为水印嵌入与提取的密钥, 嵌入的水印能够获得好的不可感知性。在信息提取端, 如果不知道确切的分数阶微积分运算阶次, 将无法完成水印信息的提取, 从而保证了发送者与合法接收者之间通信的有效保密性。利用 Matlab 进行计算机仿真实验证实了基于分数阶微积分运算的数字水印系统的有效性与可行性。

关键词:数字水印; 分数阶微积分; 数字图像; Matlab

中图分类号: TP393.08

文献标识码: A

文章编号: 1673-629X(2008)10-0139-04

Application of Fractional Calculus in Digital Watermarking

WAN Jing-jing, YU Sheng-lin

(College of Automation Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China)

Abstract: A fractional calculus-based digital watermarking system model is proposed and realized. Using the fractional calculus operations order v as the key of watermarking embedding and extraction, and the embedded watermarking is good at invisible. About the information extraction side, if we do not know the exact fractional calculus computing order, it will be impossible to complete watermarking extraction, thus ensuring the effective and confidential communication between the sender and the legitimate receiver. Using Matlab to execute computer simulation confirmed that the fractional calculus-based digital watermarking system is effective and feasible.

Key words: digital watermarking; fractional calculus; digital images; Matlab

0 引言

随着多媒体技术和网络技术的迅速发展及广泛应用, 对多媒体数字产品的版权保护已成为迫切需要解决的问题。传统的加密技术已经不足以解决问题, 而数字水印技术在这方面显示出了巨大的潜力。数字水印算法将一个版权识别代码序列(水印信号)嵌入到图像(空域或变换域)中, 利用它可以跟踪数字产品拷贝的非法销售和使用。

根据实现的过程, 图像水印算法可分为空域和变换域两类方法。

空域算法通过直接改变原始图像的像素值嵌入水印, 其中最典型的是最低有效位(least significant bit LSB)方法^[1], 该算法是将水印序列嵌入原始图像的每个像素值的最低有效位中。LSB算法的稳健性和安全性较弱, 这是由于图像的低位数据是极易改变的, 简单的数字图像处理或图像变换就会导致低位数据的变

化, 因此攻击者只需简单地删除图像低位数据或者对数字图像进行某种变换就可将水印信息移除或破坏掉。尽管如此, LSB算法具有实现简单, 隐藏数据量较大这两项突出优点。另有一种技术称为 Patchwork 算法^[2], 它是将原始图像分为 A, B 两个子集, 对两个子集中的像素值分别增加和减少一个相同的调整量, 在水印的检测过程中通过比较两个子集的均值即可判断水印的有无。该算法在检测过程中不使用原始图像, 同时隐蔽性较好, 对 JPEG 有损压缩, 滤波等操作具有较好的抵抗能力。还有一种算法称为纹理块映射编码算法^[2], 该算法是通过将一个图像纹理块拷贝到同一幅图中具有相似纹理的另一区域来嵌入水印, 然后计算自相关性检测水印。该算法具有很高的稳健性, 但仅适用于具有大量相似纹理的图像, 而且需要人工干预。

变换域算法是在某些变换系数中嵌入水印。这类技术一般是基于常用的局部或全局的图像变换, 如离散余弦变换(Discrete Cosine Transform, DCT)、离散小波变换(Discrete Wavelet Transform, DWT)、Fourier 变换、压缩域算法等。由于静止图像压缩标准 JPEG 和

收稿日期: 2008-01-06

作者简介: 万晶晶(1983-), 男, 安徽芜湖人, 硕士研究生, 研究领域为信号处理、分数阶微积分; 于盛林, 教授, 博士生导师, 研究领域为信号处理、混沌分形理论及应用。

视频编码标准 MPEG、ITU H. 26x 都采用了块 DCT, 所以块 DCT 变换是最常用的变换之一。小波变换是傅里叶变换和窗口傅里叶变换的一个重大突破, 为信号处理、图像处理及其它非线性科学的研究领域带来革命性的影响, 在一些应用中, 基于小波变换的数字水印方案比基于 DCT 变换的水印方案更具优势, 因此基于离散小波变换的数字水印算法已成为当前研究的热点。DFT 变换是复数变换, 在幅度和相位满足特定的条件下, 数字水印信息既可以嵌入到媒体信号的幅度上, 也可以隐藏在它的相位中, DFT 变换的优点在于可以把信号分解为相位信息和幅值信息, 在数字水印处理技术中受到了高度重视。但相对于 DCT 和 DWT 变换, 目前基于 DFT 的水印算法相对较少。压缩域方法是指把水印嵌入到压缩位流中的嵌入方法, 其特点是嵌入过程不需要解码和重新编码, 速度快。

由此可见, 对于水印的各种嵌入与提取算法, 都已经有了比较完整的体系与研究方法, 而密钥作为水印算法设计的一部分, 起着相当重要的作用。在水印的嵌入端, 如果将原始水印进行严格加密预处理, 对初始水印信号置乱, 并且该加密系数对于水印图形具有相当大的敏感性, 那么, 在水印提取端, 即使已经提取出置乱的水印信号, 也无法恢复出原始水印信息, 这将给非法水印提取者带来非常大的困难。在研究中发现, 分数阶微积分对于某些函数的处理中, 微积分运算阶次 v 对于运算结果具有相当大的敏感性, 而近年来对于分数阶微积分的研究也逐渐成熟, 若将分数阶微积分运算阶次 v 作为水印嵌入与提取的密钥, 嵌入的置乱水印具有非常高的保密性, 在信息提取端, 如果不知道确切的分数阶微积分运算阶次, 将无法完成水印信息的提取, 从而保证了发送者与合法接收者之间通信的有效保密性。

1 分数阶微积分的概念

分数阶微积分运算虽然已经提出了三百多年, 但其间大多数时间一直是数学工作者的珍玩, 并没有被广大工程研究人员所认识。

分数阶微积分运算应用在工程实践中, 是近几十年来新兴的研究方向。随着计算技术的发展和分数阶微积分运算应用研究探索的深入, 分数阶微积分运算在多个领域中起到了越来越重要的作用, 其中包括机械力学、电子学、化学、生物学、经济学、控制理论、机器人、材料科学、岩石力学、分形理论、电磁场理论、图像与信息处理等方面。特别是在信息科学领域中, 一些新颖的应用被相继地实现, 如系统建模、曲线拟合、信号滤波、模式识别、图像边界提取、系统辨识、系统稳

定性分析等等。

1.1 正弦信号的分数阶微积分运算

正弦信号是在理论上和工程实际中应用广泛的一类信号, 其表达式为:

$$x(t) = A \sin(\omega_0 t + \varphi) \quad (1)$$

式中 A 为正弦信号的幅度值, ω_0 为正弦信号的频率, φ 为初始相位值。

根据分数阶微积分公式, 对正弦信号进行分数阶 v 阶微分 $v \in (0, 1)$ 得到的结果为^[3]:

$$D^v \sin(\omega_0 t) = [\sin(\omega_0 t)]^{(v)} = \omega_0^v \sin(\omega_0 t + \frac{v\pi}{2}) \quad (2)$$

可见, 对正弦信号进行分数阶微分运算后, 其幅度以 ω_0 因子进行缩放, 其相位以 $v\pi/2$ 进行改变。

式(2) 是正弦信号连续时间变量表示式, 为了将该表达式进行离散化, 对分数阶微积分运算后的正弦信号进行等间隔周期采样, 转化为离散信号。由于正弦信号的特殊性质, 对正弦信号的抽样特性有以下结论: 对于正弦信号的抽样, 在抽样频率 f_s 位于区间 $2f_0 < f_s < 3f_0$ 内时, 如果初相 φ 已知, 则可以完全地恢复出原始正弦信号来; 如果初相 φ 值未知, 则不能恢复出原始正弦信号^[4]。

因此, 可以利用分数阶微积分运算算子 $v \in (0, 1)$ 的特性, 构造出抽样频率为 $f_s = (2 + v)f_0$, 则抽样频率 $2f_0 < f_s < 3f_0$ 。对于式(1), 这里的 $\varphi = v\pi/2$, 也就是说, 在不知道分数阶微积分参数 v 的情况下, 是无法对取样前的信号进行恢复的, 从而保证了数据的严密性。

1.2 不同微分阶次的正弦信号差值分析

对于 $D^v \sin(\omega_0 t) = [\sin(\omega_0 t)]^{(v)} = \omega_0^v \sin(\omega_0 t + \frac{v\pi}{2})$, 取 $\omega_0 = 2\pi \times 50$, 对于分数阶微积分阶次, 取两个差值非常小的微分阶次 $v_1 = 0.681\ 53$ 和 $v_2 = 0.681\ 52$, 进行分数阶微积分运算, 再离散化后得到的序列为 $x_1(n)$ 和 $x_2(n)$, 两序列的差值随着 n 的取值变化而变化, 在 n 取值特定的区间内, $x_1(n)$ 与 $x_2(n)$ 两者的差值能够布满整个域值空间。

2 数字水印系统的实现

2.1 水印的嵌入

文中实现的水印嵌入算法如下:

首先对正弦信号进行分数阶微分运算及抽样离散化, 产生任意长周期的伪随机序列, 利用该伪随机序列与待嵌入的水印图片信息进行叠加置乱操作, 该过程相当于对水印信息进行加密, 得到待嵌入的加密后水

印信息,接着对原始图像进行嵌入位置选择,选择特定的嵌入位置进行水印信息的叠加。叠加后对于数据进行整合,就得到了嵌入水印后的图像。

2.2 水印的提取

水印的提取为水印嵌入的逆过程,其提取过程如下:

接收到嵌入水印后的图像后,利用合法给定的分数阶微积分参数对正弦信号进行处理,再离散化得到伪随机序列,然后选择图像的嵌入位置的数据,并与原始图像进行比较,用比较结果数据除去伪随机序列,即可以得到重建后的水印图像。在没有得知确切的分数阶微积分参数的时候,是无法得出正确的水印信息的,很好地保证了信息的安全性。

3 水印系统仿真

仿真试验^[5]中,选取正弦信号为 $y = \sin(2\pi \times 50t)$,选取原始正弦信号为分数阶微积分运算阶次为 $v_1 = 0.681\ 53$,得到的分数阶微积分运算公式^[6]为:

$$D^v(y) = D^v \sin(\omega_0 t) = \omega_0^v \sin(\omega_0 t + \frac{v\pi}{2}) = (2\pi \times 50)^{0.68153} \sin(2\pi \times 50t + \frac{0.68153\pi}{2})$$

取大小为 $40 \times 40 = 1600$ 点的二值图像作为嵌入的水印信息图像;选择大小为 512×512 的 256 灰度值的 Lena 图像作待嵌入水印的载体图像。水印图像与载体图像如图 1 所示,其中(a)图为水印图像,(b)图为待嵌入水印的载体图像。

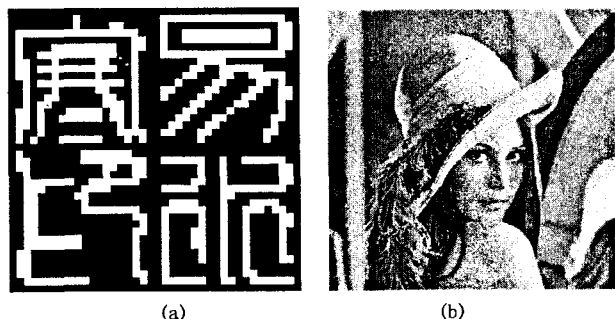


图 1 水印图像与原始载体图像

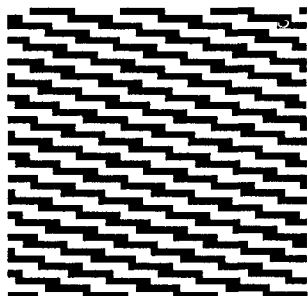


图 2 加密后的置乱图像

选择 $n = 20\ 000$ 点开始后的 1 600 点 $x(n)$ 数据

作为伪随机序列 R ,与原始水印图像进行叠加加密处理。经过分数阶微分运算后的正弦信号加密处理的水印图像如图 2 所示。

加入水印后的载体图像和提取出的水印图像如图 3 所示。

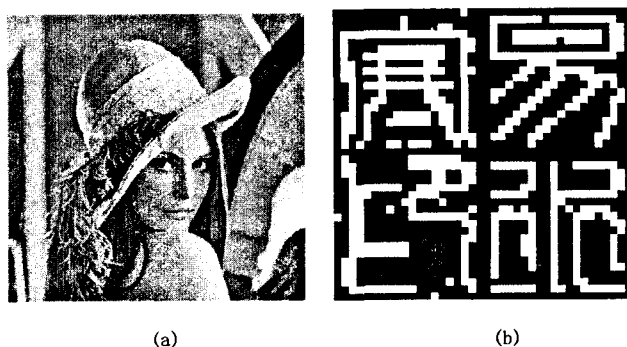


图 3 加入水印的图像和提取出的水印信号

其中(a)图为嵌入了水印后的载体图像,和原始图像几乎无任何差别,保持了良好的水印隐蔽性。(b)图是从(a)图中提取出来的水印信号,可见,进行分数阶微积分叠加置乱处理后的水印信号,在重新提取后,虽然由于数据整合过程中的精度失调问题造成了一些点的错乱,但是还是保持了相当良好的可读性,这也在误差容许范围之内,因此可以应用于常用的图像版权保护。

4 对分数阶微积分运算阶次的敏感性分析

在水印提取端,如果不知道确切的分数阶微积分运算阶次 v ,将无法恢复出嵌入的水印信息。即使水印提取过程中选取与水印嵌入时使用的分数阶微积分运算阶次很接近的数值,仍然无法提取出水印信息,以下就水印系统的微分阶次敏感性进行分析。

设水印嵌入过程中,使用的分数阶微积分运算阶次 $v = 0.681\ 53$;而在水印的提取端,使用的分数阶微积分运算阶次为 $v = 0.681\ 52$,使用的伪随机序列都为 $n = 20\ 000$ 开始的一段数据。仿真得到改变阶次后提取的水印图像如图 4 所示。

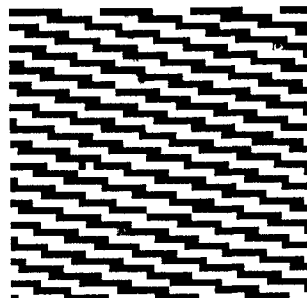


图 4 改变阶次后提取的水印图像

由图 4 可见,该水印系统对于分数阶微积分运算

阶次具有很高的敏感性,在不知道确切的分数阶微积分运算阶次的情况下,无法提取出嵌入的水印信息。

该仿真实例中,水印提取端与水印嵌入端使用的分数阶微积分运算阶次差值仅为 $v_1 - v_2 = 0.000\ 01$ 。如果运算阶次的差值 $v_1 - v_2$ 进一步地减小,那么在水印嵌入过程中,应该选择伪随机序列 $x(n)$ 的起始 n 值更大的一段取值范围,以保证水印提取端无法恢复水印信息。理论上对于这种敏感性的精度为无限小,因为无论 $(v_1 - v_2)$ 多么小,总可以找到足够大的一段 n 值范围,使其满足两组序列的差值足够大,从而无法提取出水印。

5 结束语

提出了基于分数阶微积分运算数字水印系统,该种水印系统为不可见、私有水印实现方案。并采用计算机进行数值仿真实验,证明了水印系统是可行的,而且是有效的。

分数阶微积分运算对于正弦信号进行处理,通过离散化操作,得到离散伪随机序列 $x(n)$,该伪随机序列对于分数阶微积分运算的阶次具有初始值敏感性。表现在水印系统中,对于两个非常接近的分数阶微积分运算阶次,可以找到合适的一段 n 值取值范围,使产生的两个伪随机序列差值尽可能大,从而在接收端无法恢复出原始水印信息。因此,通信双方可以利用分数阶微积分运算阶次作为保密密钥,进行保密通信。仿真结果表明,在分数阶微积分运算阶次未知的情况下,将导致接收端无法正确恢复原始信号,不能重建水

印图像,从而达到了信息掩盖的目的。

而在传统的水印嵌入与提取算法中,大部分用到的伪随机序列是 $(0,1)$ 随机数,该算法虽然也有一定的初始值敏感性,但很难达到 10^{-5} 以上的精确度,而如果利用文中所说的分数阶微积分的方法,只要适当选取伪随机序列的取值范围,理论上该精确度可以达到无限小,几乎没有非法破解的可能性。

如何进一步地对基于分数阶微积分运算的水印系统进行完善,以及设计鲁棒性能更好的水印嵌入与提取算法,将是下一步需要研究的课题。

参考文献:

- [1] van Schyndel R G, IT'rkcl A Z, Osborne C F. A digital watermark[C]//Proc of IEEE International Conference on Image Processing. Austin: IEEE Press, 1994: 86 - 90.
- [2] Bender W, Gruhl D, Morimoto N. Techniques for data hiding [C]//Proc of the SPIE Conference on storage and retrieval for image and video database. San Jose: SPIE Press, 1995: 164 - 173.
- [3] Kleinz M, Osler T J. A child's garden of fractional derivatives [J]. The College Mathematics Journal, 2000(31): 82 - 88.
- [4] 赵元英,袁晓,滕旭东,等. 常用周期信号的分数阶微积分[J]. 四川大学学报: 工程科学版, 2004(36): 94 - 97.
- [5] 王剑,林福宗. MATLAB 在数字水印技术研究中的应用[J]. 计算机工程与应用, 2003(11): 156 - 158.
- [6] Trancevski K, Tomovski Z. On some fractional derivatives of functions of exponential type[J]. Univ. Beograd. Publ. Elektrotehn. Fak. Ser. Mat., 2002(13): 77 - 84.

(上接第 138 页)

需要改变 aspect 相关代码,而不必改动核心关注模块代码;这种独立的访问控制策略,使软件具有更好的复用性。另外,由于访问控制模块与主功能模块代码完全分离,使软件具有更好的可读性,提高了软件的质量。

3 结束语

面向方面编程思想的提出,是为了降低软件的复杂性,更好地分离核心关注模块和横切关注模块,可以说,软件系统的访问控制模块是一个相当理想的面向方面编程的实例。文中基于 AsepectJ 构建了一个 Web 信息系统的角色访问控制模块,该模块已经应用于实践,取得了较好的效果。相信随着 AOP 技术的不断发展,会有越来越多的软件系统利用面向方面的编程思

想来进行开发、测试,以构建更好的松散耦合的软件系统。

参考文献:

- [1] 叶锡君,许勇,吴国新. 基于角色的访问控制在 Web 中的实现技术[J]. 计算机工程, 2002, 28(1): 167 - 169.
- [2] 邓阿群,厉小军,俞欢军,等. 一种新型软件设计方法 AOP 的研究[J]. 系统工程与电子技术, 2004, 26(7): 970 - 975.
- [3] 李志纯,张南平. 面向 Aspect 编程的应用研究[J]. 计算机技术与发展, 2006, 16(5): 217 - 222.
- [4] Kiczales G, Hilsdale E, Hugunin J, et al. An Overview of AspectJ[C]// In Proceedings of the European Conference on Object - Oriented Programming. Hungary: Springer - Verlag, 2001.
- [5] Miles R. AspectJ cookbook 中文版[M]. 北京:清华大学出版社, 2006.