一种基于分数阶微积分的分数阶伪随机数字水印新算法

邓 英

(西华大学网络管理中心 成都 610039)

摘 要 本文研究和实现了一种基于分数阶微积分的分数阶伪随机数字水印算法。首先,提出并论述用正弦型信号的分数阶微分的采样差构造分数阶微分伪随机数字序列,该分数阶微分伪随机数字序列对分数阶微分阶次和正弦型信号相位的初始值敏感,当分数阶微分阶次和正弦型信号的初始相位未知时,无法恢复出该伪随机数字序列。其次,在此基础上,提出并论述一种基于分数阶微分的分数阶伪随机数字水印算法,其算法的保密性取决于分数阶微分阶次和正弦型信号的初始相位的不可知性。最后,仿真实验表明本分数阶微积分水印算法的不可感知性和顽健性好。

关键词 分数阶微积分,数字水印,分数阶伪随机序列,分数阶微分阶次,归一化互相关函数

A Novel Fractional Order Pseudo-random Digital Watermark Algorithm Based on Fractional Calculus

DENG Ying

(Center of Network Management, Xihua University, Chengdu 610039, China)

Abstract The paper mainly concerns and studies the application and implementation of fractional calculus to digital watermark algorithm. In the first, it discusses how to implement fractional calculus pseudo-random sequence by the sampling deviation of fractional calculus sinusoidal signal. In addition, it puts forward a fractional calculus based digital watermark algorithm, the security of which depends on the unknown of fractional orders and initial phrases. At last, it proves the imperceptibility and robustness of this algorithm by simulation experiment, and shows that whether the embedded digital watermark sequence is extracted completely depends on the awareness of fractional order and initial phrase.

Keywords Fractional calculus, Digital watermark, Fractional order pseudo-random sequence, Order of fractional differential, Normalized cross correlation function

1 问题的提出

近年来,随着世界各国对知识版权保护需求的迅速增加,数字水印技术已成为信息安全研究领域的热点课题之一[1,2]。数字水印(Digital Watermark)将水印信息嵌入到音频、图像、视频等各种数字载体中,利用数字载体中存在的冗余信息或其它特性,在载体中隐藏嵌入的水印信息,成为可见或不可见的标志。由于基于分数阶微积分、分数阶傅立叶变换等分数阶演算对于处理以及时-频分析非线性、非平稳、非高斯信号有独到优势,因此研究构造出分数阶的数字水印算法是目前数字水印算法研究的一个热点分支。

近三百多年来,分数阶微积分已经成为数学分析的一个重要分支,但对于工程技术界学者而言它还鲜为人知[3]。如何运用分数阶微积分来实现数字水印,在国际上是一个崭新的研究方向[2-6]。本文将分数阶微分的阶次作为水印的密钥,对正弦型信号进行分数阶微分,求两分数阶微分阶次相差很小的抽样序列的差值序列,产生分数阶微分伪随机离散序列,然后将该伪随机序列在原始图像中进行加密置乱,得到嵌入数字水印序列后的嵌入图像。仿真实验表明,当分数阶微分阶次和正弦型信号的初始相位未知时,无法提取出嵌入的数字水印序列;当分数阶微分阶次已知时,可以恢复出相应的水印信息。

2 提出并论述基于分数阶微分的分数阶伪随机数字水印嵌入算法

2.1 提出并构造分数阶伪随机数字序列

分数阶微积分的 Grümwald-Letnikov 定义是从研究连续函数整数阶导数的经典定义出发,将微积分的阶数与因次由整数扩大到分数推衍而来的[3,4]。$\forall v\in \boldsymbol{R}$ 时(包括分数),令其整数部分为$[v]$,若信号 $s(t)\in[a,t](a<t,a\in\boldsymbol{R},t\in\boldsymbol{R})$存在 $m+1(m\in\boldsymbol{Z}$ 时,$\boldsymbol{Z}$ 表示整数)阶连续导数;当 $v>0$ 时,m 至少取$[v]$,定义 v 阶导数为:

$$ {}_a^G D_t^v = s(t) \triangleq \lim_{h\to 0} s_h^{(v)}(t) \triangleq \lim_{h\to 0} h^{-v} \sum_{r=0}^{n} \begin{bmatrix} -v \\ r \end{bmatrix} s(t-rh) \qquad (1) $$

其中,$\begin{bmatrix} -v \\ r \end{bmatrix} = \dfrac{(-v)(-v+1)\cdots(-v+r-1)}{r!}$。若将组合数 $\binom{g}{r} = \dfrac{(g)(g-1)\cdots(g+r-1)}{r!}$ 中 g 扩展为任意实数(包括分数),则 $\binom{-g}{r} = (-1)^r \begin{bmatrix} g \\ r \end{bmatrix}$。为使 $s_h^{(-v)}(t)$ 达到非零极限,须当 $h\to 0$ 时 $n\to\infty$,故令 $h=\dfrac{t-a}{n}$,于是 $n=\left[\dfrac{t-a}{h}\right]$。对式(1)先数学归纳,再分部积分可得:

$$ {}_a^G D_t^v = \sum_{k=0}^{m} \frac{s(k)(a)(t-a)-v+k}{\Gamma(-v+k+1)} + \frac{1}{\Gamma(-v+m+1)} \int_a^t (t-\tau)^{-v+m} s^{(m+1)}(\tau)\,\mathrm{d}\tau \qquad (2) $$

其中,Gamma 函数 $\Gamma(\alpha) = \int_0^\infty e^{-x}x^{\alpha-1}\,\mathrm{d}x = (\alpha-1)!$。

任意平方可积的能量型信号 $s(t)\in L^2(\boldsymbol{R})$ 的一阶导数 $s'(t)$ 的 Fourier 变换为 $\boldsymbol{D}s(t) \overset{FT}{\Leftrightarrow} (\hat{\boldsymbol{D}}s)(\omega) = (i\omega)\cdot\hat{s}(\omega) = d(\hat{\omega})\,s(\hat{\omega})$。同理可得,其 v 阶分数阶微分的 Fourier 变换为:

邓 英 讲师,工学硕士,主要研究方向为信息安全、网络管理。

$$D^v s(t)=D_v s(t)=\frac{d^v s(t)}{dt^v}\overset{FT}{\Leftrightarrow}(\hat{\boldsymbol{D}}_v s)(\omega)=(i\omega)^v\cdot\hat{s}(\omega)=$$

$$d_v(\hat{\omega})s(\hat{\omega})v\in\boldsymbol{R}^+ \tag{3}$$

其中，v 阶微分算子 $D_v=D^v$ 是 v 阶微分乘子函数 $\hat{d}(\omega)=(i\omega)^v$ 的乘性算子，其复指数形式和时域形式分别为：

$$\begin{cases}\hat{d}(\omega)=(i\omega)^v=\hat{a}_v(\omega)\cdot\exp(i\theta_v(\omega))=\hat{a}(\omega)\cdot\hat{p}_v(\omega)\\ \hat{a}_v(\omega)=|\omega|^v,\hat{\theta}_v(\omega)=\frac{v\pi}{2}\operatorname{sgn}(\omega)\end{cases} \tag{4}$$

$$d_v(t)=a_v(t)*p_v(t)=\frac{1}{2\pi}\int_{-\infty}^{+\infty}(i\omega)^v\cdot e^{i\omega t}\,d\omega \tag{5}$$

$$a_v(t)=\int_{-\infty}^{+\infty}\hat{a}(\omega)\cdot e^{i\omega t}\,d\omega=\frac{1}{\pi}\int_0^{+\infty}|\omega|^v\cdot\cos(i\omega t)\,d\omega \tag{6}$$

$$p_v(t)=\frac{1}{2\pi}\int_{-\infty}^{+\infty}\hat{p}_v(\omega)\cdot e^{i\omega t}\,d\omega=\cos\frac{v\pi}{2}\cdot\delta(t)-$$

$$\sin\frac{v\pi}{2}\cdot\frac{1}{\pi t} \tag{7}$$

由式(4)知，从通信调制角度看，信号分数阶微积分的物理意义可以理解为广义的调幅调相，其振幅随频率呈分数阶幂指数变化，其相位是频率的广义 Hilbert 变换[5]。由式(5)-(7)知，分数阶微分滤波器的滤波函数为 $\hat{d}_v(\omega)=(i\omega)^v=|\omega|^v\cdot\exp(i\theta_v(\omega))$，其振幅特性是偶函数，相位特性是奇函数，故仅需研究当 $\omega>0$ 时 $d_v(t)$ 的滤波特性即可。

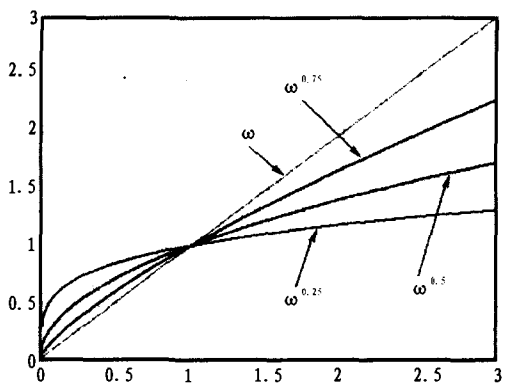


图 1　分数阶微分滤波函数

由图 1 知，从信号处理角度看，v 阶微分运算是对信号进行线性时不变滤波。在时域中信号 $s(t)$ 分数阶微积分的卷积形式为：

$$D_v s(t)=d_v(t)*s(t)=a_v(t)*p_v(t)*s(t)=\left[\cos\frac{v\pi}{2}\cdot\right.$$

$$\left.\delta(t)-\sin\frac{v\pi}{2}\cdot\frac{1}{\pi t}\right]*\int_{-\infty}^{+\infty}a_v(t-\tau)s(\tau)\,d\tau \tag{8}$$

可见，当 $v=0$ 时，它是全通滤波器，$\hat{d}_v(\omega)\equiv1\Leftrightarrow d_v(t)=\delta(t)$；当 $v<0$ 时，它是积分器，$\hat{d}_v(\omega)$ 是奇异低通滤波；当 $v>0$ 时，是对信号作微分运算，$\lim_{|\omega|\to\infty}|\hat{d}_v(\omega)|\to\infty$，$\hat{d}_v(\omega)$ 是奇异高通滤波器。v 越大，通频带越窄，高通特性越明显，相应加强信号 $s(t)$ 的高频成份，相对压制其低频成份，这有利于突出信号的细节，但抗高频干扰成份性能就越差。

令幅度值为 A，频率为 ω_0，初始相位值为 φ 的正弦信号可以表示为：

$$x(t)=A\sin(\omega_0 t+\varphi) \tag{9}$$

显然，该正弦信号的周期为 $T=2\pi/\omega_0$，其最高频率为 $\omega_0=2\pi f_0$。对于 $x(t)=A\sin(\omega_0 t+\varphi)$ 形式的正弦信号，若以 $f_s=2f_0$ 对 $x(t)$ 进行抽样，抽样后的离散信号为 $x(n)$。当正弦信号的初始相位 $\varphi\in(0,\pi/2)$ 时，由 $x(n)$ 重建出的信号将是初相位为 0、振幅为 $A\sin(\varphi)$ 的同频率余弦信号；如果初相 φ 已知，则可以由重建信号恢复出原始信号 $x(t)$；如果初相 φ 未知，则无法恢复出原始信号 $x(t)$。对于正弦信号抽样时，若 φ 为未知，其最小的抽样频率应该取正弦信号频率的三倍。所以，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[7]。

对正弦信号进行 v 阶 $v\in(0,1)$ 分数阶微分得到的结果为[2-6]：

$$D^v\sin(\omega_0 t)=[\sin(\omega_0 t)]^{(v)}=\omega_0^v\sin(\omega_0 t+\frac{v\pi}{2}) \tag{10}$$

正弦信号的分数阶微分是其幅度以 ω_0^v 因子进行广义调幅，其相位以 $v\pi/2$ 进行广义希尔伯特变换[5]。

为了离散化式(2)，以便计算机数值实现，对分数阶微积分运算后得到的正弦信号进行等间隔周期采样，转化为离散信号。令抽样频率为 $f_s=(2+v)\cdot f_0$。由于分数阶微分的阶次 $v\in(0,1)$，故抽样频率 $2f_0<f_s<3f_0$。由于抽样倍数是分数 $(2+v)$，抽样结果将会产生伪调制现象。将 $t=\frac{n}{f_s}=\frac{n}{(2+v)f_0}$ 带入正弦信号表达式中可得：

$$x(n)=A\sin(\frac{2n\pi}{2+v}+\varphi) \tag{11}$$

令 N 为自然数，故有 $x(n+N)=A\sin(\frac{2N\pi}{2+v}+\frac{2n\pi}{2+v}+\varphi)$。若 $\frac{2N\pi}{2+v}=2k\pi$，k 为自然数，则有 $x(n+N)=x(n)$，此时采样得到的序列 $x(n)$ 具有周期性质。若采样倍数 $(2+v)$ 为有理数，设为 $2+v=\frac{p}{q}$，其中 p,q 互质，当 $k=q$ 时，满足 $N=p$，此时采样结果序列 $x(n)$ 满足周期性质，$x(n)$ 的周期为 $T=2k\pi=2q\pi$，一个周期内有采样点数为 p 点。由于计算机存储与计算字长有限，故本文不考虑采样倍数 $(2+v)$ 为无理数的情况。

2.2　提出并构造分数阶伪随机水印嵌入算法

本文提出的分数阶伪随机数字水印嵌入算法如 2 图所示。

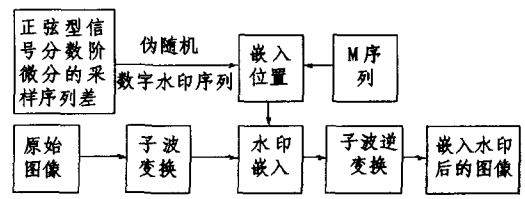


图 2　分数阶伪随机数字水印嵌入算法

设原始载体图像 $S(x,y)$ 大小为 $M\times M$，其中，$x,y=1,2,\cdots,M$，$M=2^m$，m 为整数。水印图像 $D(x,y)$ 大小为 $N\times N$。对原始图像 $S(x,y)$ 做离散小波变换 DWT，每一级二维小波变换将产生水平方向与垂直方向的低频分量图像 LL，以及三个高频分量图像 LH，HL 和 HH。选择第 k 级小波变换产生的低频近似子图像 LL_k 做水印信息的嵌入。

然后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 F，将其作为数字水印序列。同

时利用 M 伪随机序列对高阶小波变换得到的低频分量系数进行嵌入位置选择，将伪随机数字水印序列 F 与原始图像以嵌入强度系数 δ 进行水印叠加。

$$\widetilde{LL}_k = LL_k + \delta \cdot F \tag{12}$$

叠加数字水印序列后，对低频子图像 $\widetilde{LL}_k$ 进行小波逆变换 IDWT，得到嵌入后的图像 $S(\tilde{x}, y)$，从而完成水印嵌入过程。

2.3 提出并构造分数阶伪随机水印提取算法

水印提取算法即水印检测算法，与水印嵌入算法互逆。本文提出的分数阶伪随机数字水印提取算法如图 3 所示。

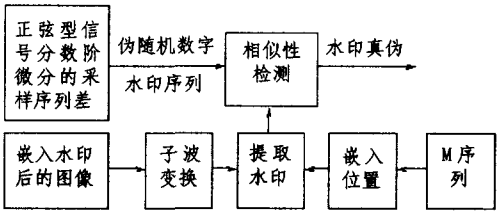


图 3 分数阶伪随机数字水印提取算法

首先，对存在待检测的嵌入数字水印的图像 $S(\hat{x}, y)$ 进行高阶小波变换，离散小波变换得到低频分量图像 $\hat{LL}_k$。利用 M 序列选择原始水印嵌入位置，提取叠加的伪随机数字序列 $\tilde{F}$。最后将 $\tilde{F}$ 与正弦型信号分数阶微分采样序列差产生的伪随机序列 F 进行相似性检测，以判断水印信息的真伪。本文采用归一化互相关函数 NC(Normalized Cross-Correlation) 来度量提取出的数字水印序列 $\tilde{F}$ 与原始数字水印序列 F 的相似性程度。

$$NC = \frac{\sum \tilde{F} \sum F}{\sum \sum F^2} \tag{13}$$

设定门限值 T，如果相似度 $NC > T$，则可认为数字水印信息为真；否则认为数字水印信息为假。显然，在本文提出的水印检测过程未使用到原始数字水印序列，因此为共有水印系统。如上所述，若不知道分数阶微分阶次和正弦型信号的初始相位，将无法生成相应的伪随机序列，保证了本算法的顽健性。

3 实验仿真及分析

不失一般性，本文以初相为零的正弦信号进行 v，($0 < v < 1$) 阶分数阶微分。

$$D^v \sin(\omega_0 t) = [\sin(\omega_0 t)]^{(v)} = \omega_0^v \sin\left(\omega_0 t + \frac{v\pi}{2}\right) \tag{14}$$

令相位 $\varphi = v\pi/2$，显然 $\varphi \in (0, \pi/2)$。若 v 未知，则 φ 也未知。对式(6)进行离散化抽取，采样频率 f_s 与正弦信号频率 f_0 满足关系式：$f_s = (2+v) f_0$，由此得到的正弦信号离散序列记为 $v(n)$。因此，在相位 φ 未知的情况下，无法从采样得到的序列 $v(n)$ 恢复出原始正弦信号来。

同时，对于两个差值非常小的微分阶次 v_1 和 v_2，对正弦信号微分处理后得到的离散序列为 $v_1(n)$ 和 $v_2(n)$，两序列的差值随着 n 的取值变化而变化。序列 $v_1(n)$ 和 $v_2(n)$ 的差值(取值的偏离程度)与 n 值的变化在一定范围内成正比。在取 n 值特定的区间内，$v_1(n)$ 与 $v_2(n)$ 两者的差值能够布满整个域值空间。本实验中两分数阶微分阶次分别取为 $v_1 = 0.5135$，$v_1 = 0.5136$，采样点为 $n \in [1\times10^6, 1\times10^7]$。利用 MATLAB7.0 进行的仿真结果如图 4 所示。

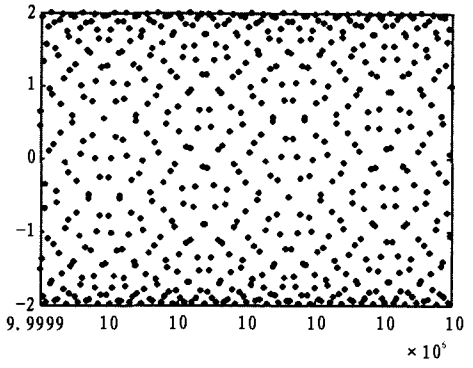
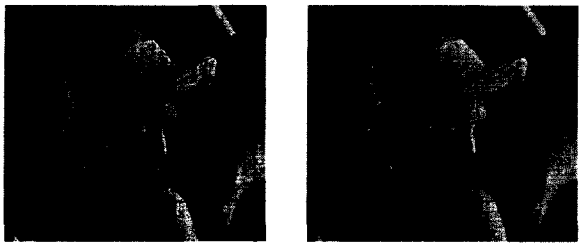


图 4 正弦型信号分数阶微分的差值伪随机序列

实验表明，对于无论差值多么小的两个微分运算阶次 v_1 和 v_2，只要选择合理的 n 值区间，序列 $v_1(n)$ 和 $v_2(n)$ 的数值差异将很大。将该差值数字序列作为数字水印序列嵌入 256×256 的 256 灰度值的 Lena 图像中。



A 原始图像 (Lena)　　B 嵌入数字水印序列后的图像

图 5 原始图像和嵌入水印后的图像对比

由于人类视觉对相位失真比较敏感，因此选择具有线性相位的双正交小波滤波器组进行离散小波变换 DWT，选取的小波为 bior3.7 小波，分解的级数为 3 级分解。二维离散小波变换存在边界效应，因此只选择子图像 LL 部分居中的参数进行水印信息的嵌入。在无恶意攻击时，提取出的数字水印序列如图 6 所示。

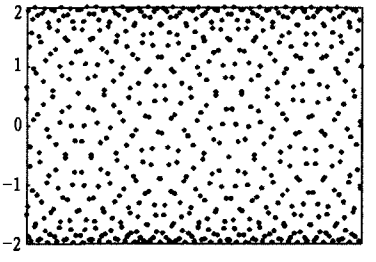


图 6 提取的数字水印序列

实验表明当无任何恶意攻击时，提取出的图像与原始水印图像相关系数为 $NC = 1.00$，即能完全地被恢复出原数字水印序列。将嵌入水印后的图像左上角 1/4 图像进行剪切的恶意攻击，用本算法提取出的数字水印序列如图 7 所示。

此时提取出的数字水印序列和原始数字水印序列的相似度为 $NC = 0.86421$。水印信息能较好地恢复。由上图还可知，本水印算法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。如果运算阶次的差值 $v_1 - v_2$ 进一步

(下转第 252 页)

的影响，而对于整个宏块而言，这种影响则很小或可以忽略，因一个宏块包含 64 个像素；(2)当在一个宏块内的像素被损伤或干扰时，由于 DCT 变换的性质使其可以进行相互补偿，并且一个宏的块边缘模式是由 4 个 16 个像素组成的子块决定的，也就是说，个别像素值的变化，不会导致提取的块边缘模式发生改变。

结束语 本文提出一种有效的 JPEG 图像和 MPEG 视频的内容描述符。与现行的算法比较，我们提出的算法具有如下优势：(1)对于传输、处理、编辑和存储过程中常常出现的图像方位变化和噪声干扰具有较好的稳健性；(2)RLEBH 是基于压缩域的算法，因此适合处理大量的压缩图像或视频；(3)极低的运算复杂度，便于实时实现和快速图像或视频内容管理应用。大量的实验证明，本文提出的算法与目前文献报导的类似算法相比，在平均查准率和查全率两方面都有所提高。

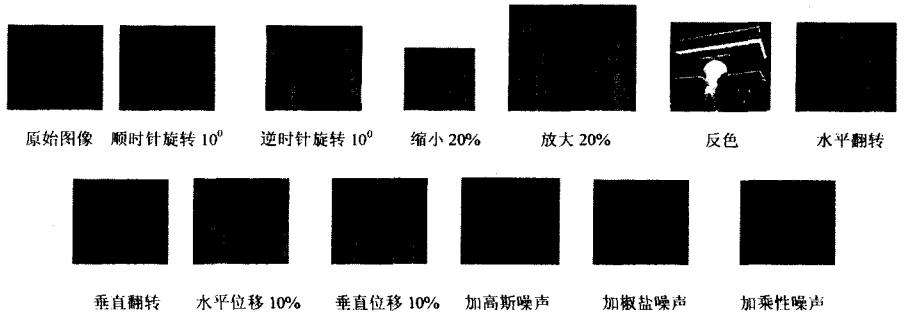


图 2 图像的各种变换实例

参 考 文 献

[1] Chang S F. Compressed domain techniques for image/video indexing and manipulation// IEEE International Conference on Image Processing. 1995:314-317

[2] Ngo C W, Pong T C. Exploiting image indexing techniques in DCT domain. Pattern Recongnition, 2001, 34:1841-1851

[3] Feng G Can, Jiang J M. JPEG compressed image retrieval via statistical features. Pattern Recognition, 2003, 36:977-985

[4] Sim D G, Kim H K, Park R H. Fast texture description and retrieval of DCT-based compressed image. Electronic Letters, 2001, 37(1):18-19

[5] Liu J H, H M Gu. Image retrieval in various domains. Computers & Graphics, 2003, 27:807-812

[6] Zhong D, Defee I. DCT histogrom optimization for image database retrieval. Pattern Recongnition Letters, 2005

[7] Soltane S, Kerkeni N, Angue J C. The use of two dimensional discrete cosine transform for an adaptive approach to image segmentation// Proceedings of the SPIE Image and Video Processing IV. 1996:242-251

[8] Han J W, Guo L. A shape-based image retrieval method using salient edges. Signal processing: Image communication, 2003, 18:141-156

[9] Banerjee M K, Kundu M. Edge based features for content based image retrieval. Pattern Recognition, 2003, 36: 2649-2661

[10] Kim D S, Lee S U. Image vector quantizer based on a classification in the DCT domain. // IEEE Trans. Commun, 1991, 39(4):549-556

[11] Shen B, Sethi I K. Direct feature extraction from compressed images// Proc. SPIE: Storage and Retrieval for Still Image and Video Databases IV. 1996, 2670: 404-414

[12] Chang H S, Kang K. A compressed domain scheme for classifying block edge patterns. IEEE Transactions on image processing, 2005, 14(2):145-151

[13] Li H, Liu G, Li Y. An effective approach to edge classification from DCT domain// Proc. IEEE Int. Conf. Image Processing. 2002:940-943

[14] Jiang J. A low cost content adaptive and rate controllable near lossless image codec in DPCM domain. IEEE Trans. on Image Processing, 9(4):543-554

[15] Theo G, Arnold W M. PicToSeek: combining color and shape invariant features for image retrieval. IEEE Transactions on Image Processing, 2000, 9(1):102-119

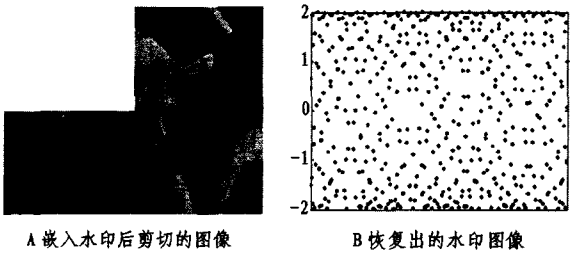
[16] Bartsch H J. Handbook of mathematical formulas. Academic press, 1974

[17] Popovici I, Withers W D. Custom-built moments for edge location. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2006, 28(4):637-642

[18] Shneier M, Mottaleb M A. Exploiting the JPEG compression scheme for image retrieval. IEEE Trans. Pattern Anal. Mach. Intell, 18(8):849-853

(上接第 248 页)

地减小，增大 n 值取值范围，使产生的两个伪随机序列差值尽可能大，以保证水印提取端无法恢复水印信息。



A 嵌入水印后剪切的图像　　B 恢复出的水印图像

图 7 嵌入水印后剪切的图像与恢复出的水印图像

结束语 本文提出了基于分数阶微积分的分数阶伪随机序列数字水印算法。首先对正弦型信号进行分数阶微积分，再通过与其分数阶微分阶次相关的抽样，然后求得其差值伪随机序列 $v(n)$，$v(n)$对于分数阶微分的阶次 v 的初始值敏感性，保证了本分数阶伪随机数字水印的顽健性。

分数阶微积分在数字水印中应用的研究目前是一个新兴的研究领域，本文做的工作只是在这一领域的一些初步的尝试，还有许多问题需要进一步研究，如：如何设计顽健性能更好的水印嵌入-提取算法。

参 考 文 献

[1] 李忠源，郭全成，任亚萍. 图像中的信息隐含及水印技术[J]. 电子学报，2000，28(4)：61-63

[2] Castleman K R. Digital Image Processing. Prentice-Hall, Inc, 1996

[3] Oldham K B, Spanier J. The Fractional Calculus. New York and London: Academic Press, 1974

[4] Yuan Xiao, Chen Xiangdong, LI Qiliang, et al. Differential operator and the construction of wavelet. Acta Electronica Sinica, 2002, 30(5):769-773

[5] Pu Yi-fei, Yuan Xiao, Liao Ke, et al. Five Numerical Algorithms of Fractional Calculus Applied in Modern Signal Analyzing and Processing [J]. Journal of Sichuan University (Engineering Science Edition), 2005, 37(5):118-124

[6] Trencevski K, Tomovski Z. On some fractional derivatives of functions of exponential type[J]. Univ. Beograd. Publ. Elektrotehn. Fak. Ser. Mat. , 2002, 13:77-84

[7] 胡广书. 数字信号处理：理论、算法与实现[M]. 北京：清华大学出版社，1997