

基于 Tchebichef 矩和小波提升的数字水印算法

赵杰, 王暉, 何冰

(陕西师范大学物理学与信息技术学院, 西安 710062)

摘要: 提出一种基于 Tchebichef 矩和小波提升的抵抗几何攻击的内容认证水印算法, 对图像进行一次小波提升分解, 计算其低频成分的 Tchebichef 低阶矩不变量来构建水印系统。水印认证过程只须计算图像的几个低阶 Tchebichef 矩不变量。将该算法与基于几何矩不变量的算法进行比较。结果表明, 该算法简单、有效, 对旋转、缩放、剪切等几何攻击以及 JPEG 压缩等攻击具有较高的稳健性。

关键词: 数字水印; Tchebichef 矩; 小波提升

Digital Watermark Algorithm Based on Tchebichef Moments and Wavelet Lifting

ZHAO Jie, WANG Xuan, HE Bing

(School of Physics and Information Technology, Shaanxi Normal University, Xi'an 710062)

【Abstract】 The watermark based on Tchebichef moments and wavelet lifting is used in an authentication context. After the discrete lifting wavelet transform, the lower order Tchebichef invariant moments of the sub band coefficients are computed. The processing of the encoder and the decoder is simple, and a few low order moments need to be calculated. The algorithm is compared with the algorithm based on the geometrical moments. Results show that the scheme is simple, effective. It has high stabilities of geometrical attacks of rotation, scaling, shearing, and JPEG compression.

【Key words】 digital watermark; Tchebichef moments; wavelet lifting

1 概述

媒体的数字化方便了信息的存取和传播, 但同时也使盗版和非法篡改等行为难以认证, 水印技术是解决版权保护问题的一个有效途径。目前已提出许多数字水印的算法, 但现有的数字水印技术大多难以抵抗几何变换类攻击, 如旋转、平移和尺度变换等, 其中一个最主要的原因是: 几何变换虽然并未去除图像中的水印信息, 但却使水印的检测与嵌入之间失去同步, 从而导致水印检测的失效。因此, 同步问题被认为是抗几何攻击水印技术中有待解决的关键技术。常见抵抗几何攻击的水印算法有文献[1-2]提出的基于 Fourier-Mellin 变换的算法。

矩函数可以描述物体形状的全局特征, 并提供大量该物体特有的几何信息。矩函数的这种特性被广泛应用于图像编码压缩与重构、模式识别、目标状态与方位估计等方面, 数字水印技术是其应用领域之一。文献[3]提出基于 Zernike 矩的数字图像水印算法, 文献[4]提出基于几何矩不变量的数字水印算法。随着图像处理研究的深入, 引入了许多新的矩函数, 离散 Tchebichef 矩便是其中具有较好性能的一种^[5]。由于该矩本身是离散的, 因此其计算精度较高, 可直接应用于离散图像, 无须对定义域进行归一化处理, 并且 Tchebichef 多项式的计算具有递推关系和对称性, 可以加快运算。

本文提出一种基于小波提升和 Tchebichef 矩的水印算法, 并将其与几何矩的算法进行比较。

2 小波提升方案

由于传统小波变换的滤波器输出是浮点数, 而图像的像素值均为整数, 小波系数量化时存在舍入误差, 并且图像的

重构质量与变换时延拓边界的方式有关。文献[6]对小波的构造提出一种新的观点: 整数小波提升方案(lifting scheme), 也称为第 2 代小波变换。整数小波提升格式具有真正意义上的可逆性, 可不用考虑边界效应。提升方案基于传统小波变换的思想, 但效率更高。与传统小波变换相比, 提升方案主要有以下几个优点: (1)完全是基于空域的构造方法, 运算速度快, 节省存储空间。(2)不依赖于平移、伸缩的概念, 也不需要傅里叶变换进行频谱分析。(3)可直接将整数映射成为整数, 无须再进行量化。最低频子带包含了图像的基本信息, 占据了原始图像的大部分能量, 是鲁棒水印嵌入的合适位置。图像的小波分解过程如图 1 所示。

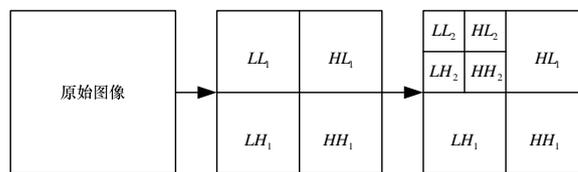


图 1 图像的小波分解

3 Tchebichef 矩

假设 $f(x, y)$ 表示大小为 $N \times N$ 的原始图像, 则离散 Tchebichef 多项式为 $t_n(x) = (1-N)_n \times_3 F_2(-n, -x, 1+n; 1-N; 1)$,

作者简介: 赵杰(1984—), 男, 硕士研究生, 主研方向: 图像处理, 数字水印; 王暉, 副教授; 何冰, 硕士研究生

收稿日期: 2008-10-06 **E-mail:** zhaojie261134@stu.snnu.edu.cn

其中, $n, x=0, 1, \dots, N-1$ 。

$${}_3F_2(a_1, a_2, a_3; b_1, b_2; z) = \sum_{k=0}^{\infty} \frac{(a_1)_k (a_2)_k (a_3)_k}{(b_1)_k (b_2)_k} \frac{z^k}{k!}$$

$$(a)_k = a(a+1)(a+2)\dots(a+k-1)$$

以 Tchebichef 多项式的乘积作为核函数引出 Tchebichef 矩为

$$T_{pq} = \frac{1}{\rho(p, N)\rho(q, N)} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} t_p(x)t_q(y)f(x, y)$$

其中, $p, q=0, 1, \dots, N-1$ 。

$$\rho(n, N) = \frac{N^2(N^2-1)(N^2-2^2)(N^2-3^2)\dots(N^2-n^2)}{2n+1} = (2n)!\binom{N+n}{2n+1}$$

其中, $n=0, 1, \dots, N-1$ 。

从上面 Tchebichef 矩的定义可知, 其定义域与离散图像的取值范围相吻合。但随着阶数 $p+q$ 的增大, Tchebichef 矩的取值范围过大, 不宜进行集中分析, 因此, 要对其值进行加权修正。加权的 Tchebichef 多项式为

$$\bar{t}_n(x) = \frac{t_n(x)}{\beta(n, N)} = \sum_{k=0}^n c_{k, n, N} N^k x^k$$

此时, $T_{pq} = \frac{1}{\bar{\rho}(p, N)\bar{\rho}(q, N)} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} (\sum_{i=0}^p c_{i, p, N} N^i x^i) (\sum_{j=0}^q c_{j, q, N} N^j y^j) f(x, y)$,

其中,

$$c_{k, n, N} = (-1)^{n-k} \frac{n!}{k!} \binom{N-1-k}{n-k} \binom{n+k}{n}$$

$$\bar{\rho}(n, N) = \frac{\rho(n, N)}{\beta(n, N)^2} = \frac{N(1-\frac{1}{N^2})(1-\frac{2^2}{N^2})\dots(1-\frac{n^2}{N^2})}{2n+1}$$

$$\beta(n, N) = N^n$$

上述过程也可利用几何矩来进行计算。

离散图像 $f(x, y)$ 的几何矩为

$$m_{pq} = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} x^p y^q f(x, y)$$

则 Tchebichef 矩可写为

$$T_{pq} = \frac{1}{\bar{\rho}(p, N)\bar{\rho}(q, N)} \sum_{i=0}^p \sum_{j=0}^q c_{i, p, N} c_{j, q, N} m_{ij}$$

可得一些低阶矩如 $T_{00} = \frac{m_{00}}{N^2}$, $T_{10} = \frac{6m_{10} + 3(1-N)m_{00}}{N(N^2-1)}$,

$T_{01} = \frac{6m_{01} + 3(1-N)m_{00}}{N(N^2-1)}$ 等。

4 Tchebichef 矩不变量

构造具有平移、缩放、旋转均不变的 Tchebichef 矩, 可分别通过对 $f(x, y)$ 进行平移、缩放和旋转处理得到。为保证平移不变性, 可将 $f(x, y)$ 图像转化为 $f(x+\bar{x}, y+\bar{y})$ 图像加以实现, 其中, (\bar{x}, \bar{y}) 为原图的质心, 且 $\bar{x} = \frac{m_{10}}{m_{00}}$, $\bar{y} = \frac{m_{01}}{m_{00}}$ 。

平移后的图像旋转 θ 度后得到 $f(\bar{x}+x\cos\theta - y\sin\theta, \bar{y}+y\cos\theta - x\sin\theta)$, $\theta = \frac{1}{2} \tan^{-1} \frac{2\mu_{11}}{\mu_{20} - \mu_{02}}$, 其中, μ_{nm} 为中心

距, 且有 $\mu_{nm} = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} (x-\bar{x})^n (y-\bar{y})^m f(x, y)$, 值域为 $[-45^\circ, 45^\circ]$,

$[0, 360^\circ]$ 的 θ 值可参考文献[7]。将图像缩放 α 倍得到规则化的图像 $g(x, y)$, 此时 $\alpha = (\frac{N}{2m_{00}})^{\frac{1}{2}}$ 。注意到 Tchebichef 矩的

中心为 $(\frac{N}{2}, \frac{N}{2})$, 将图像中心平移到 $(\frac{N}{2}, \frac{N}{2})$ 。转换后的新图像与原图像 $f(x, y)$ 的关系为

$$g(x+\frac{N}{2}, y+\frac{N}{2}) = f(\bar{x} + \frac{x\cos\theta - y\sin\theta}{\alpha}, \bar{y} + \frac{y\cos\theta - x\sin\theta}{\alpha})$$

根据图像 $g(x, y)$ 计算其几何矩, 得到新的几何不变矩, 其形式为

$$\bar{m}_{ij} = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} \alpha^2 f(x, y) \{ \alpha[(x-\bar{x})\cos\theta + (y-\bar{y})\sin\theta] + \frac{N}{2} \}^i \times \{ \alpha[(y-\bar{y})\cos\theta + (x-\bar{x})\sin\theta] + \frac{N}{2} \}^j$$

由此可得新的 $p+q$ 阶 Tchebichef 不变矩:

$$\bar{T}_{pq} = \frac{1}{\bar{\rho}(p, N)\bar{\rho}(q, N)} \sum_{i=0}^p \sum_{j=0}^q c_{i, p, N} c_{j, q, N} \bar{m}_{ij}$$

如果计算出的值较大, 可用 $|\lg \bar{T}_{pq}|$ 代替 \bar{T}_{pq} 。

5 水印系统

5.1 水印注册

将原始图像进行一次提升小波分解后, 计算其低频子图的 m 个低阶 Tchebichef 不变矩, 构成特征矢量 $F = (f_1, f_2, \dots, f_m)$, 其中, f_i 为第 i 个低阶 Tchebichef 不变矩。但 m 不宜取得过大, 否则计算量增加, 而且高阶矩的鲁棒性不如低阶矩。得到特征矢量后, 连同原始图像长宽信息以及密钥一并在可信第 3 方(如 IPR 注册中心)登记签名, 可信第 3 方对这些信息加盖时间戳后即宣布原始图像已经在水印技术保护之下, 水印注册过程如图 2 所示。

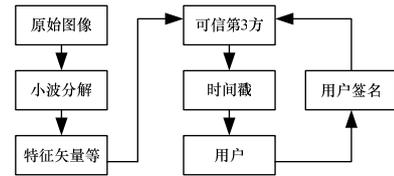


图 2 水印注册

5.2 水印检测

将待测图像进行一次提升小波分解后, 计算其低频子图的 m 个低阶 Tchebichef 不变矩, 构成特征矢量 $G = (g_1, g_2, \dots, g_m)$, 将其与 F 进行比较。这里, 定义参数 d 来衡量 G 和 F 的差距。

$$d = \frac{1}{m} \sum_{i=1}^m |f_i - g_i|$$

如果 $d \geq \varepsilon$ (ε 为事先设定的经验阈值) 则验证结束, 图片不含有水印, 否则认为水印存在。如很多人持有的检测图片都检测存在水印, 则检验其时间戳来确定谁是版权所有者, 水印认证过程如图 3 所示。

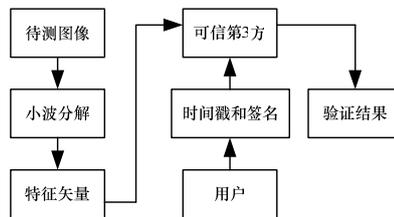


图 3 水印认证

6 实验分析

原始图像采用 256×256 的真彩色 lena 图片, 用 Matlab 7 进行仿真。分别计算原始图像 RGB 分量的低阶 Tchebichef 不变矩, 组成特征矢量 $F = (\bar{T}^R, \bar{T}^G, \bar{T}^B)$, 其中, $\bar{T}^R =$

$(\bar{T}_{00}^R, \bar{T}_{10}^R, \bar{T}_{01}^R, \bar{T}_{20}^R, \bar{T}_{02}^R, \bar{T}_{11}^R)$, \bar{T}^G, \bar{T}^B 与此类似。同理, 待测图像的特征矢量 G 也如上计算。为与几何矩方法作比较, 分别求出受攻击后的待测图像与原始图像 Tchebichef 不变矩特征矢量的差距 d_1 和几何不变矩特征矢量的差距 d_2 。几何不变矩特征矢量为 RGB 各分量的 7 个不变矩的组合^[8]。对原始图像进行攻击后作为待测图像进行测试, 用 PSNR 衡量攻击前后图像质量对比。

$$PSNR_R = 10 \lg \frac{N^2 f(x, y)_{\max}^2}{\sum_x \sum_y (f(x, y) - g(x, y))^2}$$

$PSNR_G$, $PSNR_B$ 类似, 则 $PSNR = (PSNR_R + PSNR_G + PSNR_B) / 3$ 。

原始图像见图 4, 遭受非几何攻击的测试结果见表 1, 遭受几何攻击的测试结果见表 2。

从实验结果可以看出, 本文方法对常见的噪声、滤波、JPEG 压缩、剪切、缩放、旋转攻击等有较强的鲁棒性。相对于几何矩不变量, Tchebichef 矩不变量更具有抗攻击的优势; 由于只利用了低阶的 Tchebichef 矩, 因此计算复杂度也没有明显增加。



图 4 原始图像

表 1 非几何攻击测试结果

攻击类型	PSNR/dB	d_1	d_2
高斯噪声	19.505	0.000 1	0.064
椒盐噪声	14.548	0.000 2	0.978
Speckle 噪声	18.538	0.000 3	0.029
中值滤波	29.511	0.000 1	0.038
均值滤波	31.718	0.000 1	0.009
高斯滤波	32.713	0.000 2	0.011
JPEG10	21.625	0.001 1	0.177
JPEG10+高斯噪声	17.158	0.000 6	0.112
JPEG10+均值滤波+椒盐噪声	13.496	0.001 8	0.961

表 2 几何攻击测试结果

攻击方式	d_1	d_2
剪切 15%	0.001 7	1.119
X 方向左平移 50 个像素	0.002 1	0.183
Y 方向上平移 20 个像素	0.001 1	0.025
放大 2 倍	0.000 5	0.051
旋转 45°	0.004 7	0.145
X 方向右平移 30 个像素	0.004 7	0.145
Y 方向下平移 45 个像素+缩小 2 倍	0.001 4	0.173
X 方向左平移 15 个像素	0.001 4	0.173
Y 方向上平移 55 个像素+放大 1.5 倍+旋转 300°	0.001 4	0.173

7 结束语

一般的水印信息为二值序列, 它的可信度较低。本文提出一种基于 Tchebichef 矩不变量和时间戳认证的抗几何攻击水印算法。该方案无须修改原始图像的任何信息, 不会引起图像质量的下降, 有很好的透明性, 可抵抗一些常见的攻击尤其是几何攻击。实验结果表明, 本算法有较强的鲁棒性, 并且能与其他嵌入水印方法结合, 形成多重水印认证算法, 这也是下一步的研究方向。

参考文献

- [1] Oruanaidh J K, Rotation P T. Scale and Translation Invariant Spread Spectrum Digital Image Watermarking[J]. Signal Processing, 1998, 66(3): 303-317.
- [2] Cai Lian, Du Sidan, Gao Duntang. Geometrically Invariant Watermarking Based on Radon Transformation[J]. Journal of Electronics, 2005, 22(5): 300-306.
- [3] Kim H S, Lee H K. Invariant Image Watermark Using Zernike Moments[J]. IEEE Trans. on Circuits and Systems for Video Technology, 2003, 13(8): 766-775.
- [4] Alghoniemy M, Tewfik H. Geometric Invariance in Image Watermarking[J]. IEEE Trans. on Image Processing, 2004, 13(2): 145-153.
- [5] Mukundan R, Ong S H, Lee P A. Image Analysis by Tchebichef Moments[J]. IEEE Trans. on Image Processing, 2001, 10(9): 1357-1364.
- [6] Sweldens W. The Lifting Scheme: A Custom Design Construction of Biorthogonal Wavelets[J]. Applied and Computational Harmonic Analysis, 1996, 3(2): 186-200.
- [7] Teague M R. Image Analysis via the General Theory of Moments[J]. Journal of Optical Society of American, 1980, 70(8): 920-930.
- [8] Hu Mingui. Visual Pattern Recognition by Moment Invariant[J]. IEEE Trans. on Information Theory, 1962, 8(2): 179-187.

编辑 金胡考

(上接第 103 页)

5 结束语

无线局域网的带宽和吞吐量稳定性是制约其应用与发展的重要因素, 本文研究活动节点数量、数据帧长度、退避时间等因素对吞吐量大小及稳定性的影响机制, 提出一种吞吐量优化算法, 通过仿真证明该算法的有效性, 下一步将在包优先级、时延和延迟抖动等性能方面进行深入研究。

参考文献

- [1] Romdhani L, Ni Qiang, Tuiletti T. Adaptive EDCF Enhanced Service Differentiation for IEEE 802.11 Wireless Ad Hoc Networks[C]//Proc. of WCNC'03. New Orleans, USA: IEEE Press,

2003: 1373-1378.

- [2] 虞莉娟, 朱容波, 熊惠民. 无线局域网持续时间自适应调度算法[J]. 武汉理工大学学报, 2008, 30(3): 408-411.
- [3] 范菁, 高飞, 王万升, 等. 无线自组织网络中的自适应竞争窗口退避算法[J]. 计算机工程, 2008, 34(9): 142-144.
- [4] 赵力强, 樊昌信. ADFC: IEEE 802.11 DCF 协议的自适应简便算法[J]. 电路与系统学报, 2003, 8(4): 100-103.
- [5] 张炜, 黄爱苹, 林正汉. 突发传输下 TCP 对无线局域网吞吐量的影响[J]. 浙江大学学报: 工学版, 2004, 38(12): 1660-1664.

编辑 金胡考