

基于 Krawtchouk 不变矩和 SVD-LWT 的双重水印研究

郭丹, 王冰

(西北大学信息科学与技术学院, 西安 710127)

摘要: 为提高数字图像水印的鲁棒性和透明性, 提出了一种基于 Krawtchouk 不变矩、奇异值分解(SVD)和提升小波变换(LWT)的彩色图像双水印算法。该算法首先从载体 RGB 图像中提取绿色分量进行两级提升小波变换, 利用 Krawtchouk 不变矩对平移、旋转和缩放的不变性以及 Krawtchouk 矩良好的局部特性和重构性, 计算其低频分量的 Krawtchouk 低阶矩不变量构造水印系统; 然后对其变换后的中频分量奇异值进行分解, 嵌入混沌置乱后的水印图像的奇异值作为另一水印系统。仿真实验结果表明, 该算法不仅有良好的不可见性, 而且对常见攻击和几何攻击都具有很好的鲁棒性, 并具有一定的应用价值。

关键词: Krawtchouk 不变矩; 奇异值分解; 提升小波变换; 双重水印; 混沌置乱; 几何攻击

中图分类号: TP391 **文献标志码:** A **文章编号:** 1001-3695(2012)12-4615-03

doi:10.3969/j.issn.1001-3695.2012.12.054

Double watermarking examination based on Krawtchouk moment invariants and SVD and LWT

GUO Dan, WANG Bing

(School of Computer Science & Technology, Northwest University, Xi'an 710127, China)

Abstract: In order to improve the robustness and transparency of the digital image watermarking, this paper proposed a color image double watermarking algorithm based on Krawtchouk moment invariants, singular value decomposition (SVD) and the lifting wavelet transform (LWT). Firstly, the algorithm extracted green component from the RGB image for two level ascension wavelet transform. The invariance of Krawtchouk moment invariant to translation, rotation and scaling, and more, good local characteristics and reconstruction of Krawtchouk, which could calculate Krawtchouk moment invariants of the low frequency components to structure one watermarking system. And then, the transformation of the intermediate frequency component singular value decomposition, embedded chaos after scrambling watermark image of the singular value as another watermarking system. Simulation results show that this algorithm not only has good invisibility, but also has very good robustness to the common attack and geometric attacks, and it has application value.

Key words: Krawtchouk moment invariants; singular value decomposition; lift wavelet transformation; double watermarking; chaotic scrambling; geometric attacks

0 引言

随着计算机和网络技术的迅猛发展, 给人们的日常生活带来了很大程度的方便, 人们可以对传播中的数据进行复制、修改、删除、利用, 但其也伴随着信息安全和版权保护问题的涌现, 数字水印技术已成为实现信息安全和版权保护的有效途径之一。近年来已经有大量的研究机构投入到数字水印的研究中, 并取得了众多成果。Zhou 等人^[1]从理论上证明, 图像的奇异值对几何失真(转置、镜像、旋转、放大、平移)具有稳定性, 可以用来嵌入水印。王丽娜等人^[2]、刘瑞祯等人^[3]提出了基于小波域、混沌序列和奇异值分解的数字水印算法, 他们对水印图像作奇异值分解, 并修改宿主图像的离散小波变换系数和水印图像的奇异值。其算法不仅具有良好的不可见性, 而且对诸如滤波、几何攻击、JPEG 压缩和旋转等常见的图像攻击具有很强的鲁棒性, 验证了 Zhou 等人^[1]的理论。其后, 数字水印逐

步发展到彩色图像方面, 刘连山等人^[4]提出了一种在彩色图像绿色分量的离散余弦变换(DCT)域嵌入水印的方案, 该算法实现简单, 但鲁棒性差。Sweldens^[5]提出了一种新的小波构造方法—提升方案(lifting scheme), 也叫做第二代小波变换或整数小波变换^[6]。徐国荣等人^[7]和赵玉霞等人^[8]都采用提升小波对原始图像进行多级变换, 用一定的算法将水印信息置乱后合理地嵌入到原始图像中去, 但其嵌入信息量少, 并且提出的水印质量差。张力等人^[9]、吴一全等人^[10]、王春桃等人^[11]、夏嵬等人^[12]都证实了 Krawtchouk 矩不变量是一种不随图像的平移、旋转、尺度变换而变化的矩特征量, 可以利用这些不变量构造水印。

本文提出了一种基于 Krawtchouk 不变矩、奇异值分解和提升小波变换的彩色图像双水印算法。提取 RGB 图像的绿色分量进行两级提升小波变换, 计算其低频分量的七个 Krawtchouk 矩不变量构造一个水印; 然后对中频系数进行奇异值分

收稿日期: 2012-05-17; 修回日期: 2012-06-28

作者简介: 郭丹(1987-), 女, 陕西渭南人, 硕士研究生, 主要研究方向为图像处理、信息隐藏、数字水印(guod123@126.com); 王冰(1954-), 男, 陕西西安人, 教授, 硕导, 主要研究方向为图像处理、信息隐藏、数字水印。

解,对水印图像进行 Logistic 混沌置乱后作奇异值分解;最后选择合适的嵌入强度将水印图像的奇异值嵌入到中频分量的奇异值中,双重水印保证了整体的鲁棒性。实验表明,与文献 [7,8]相比,该算法具有更好的鲁棒性,并且提取出的水印质量较好。

1 提升小波变换

由于一般的小波滤波器的输出结果是浮点数,因而在对变换后的数据进行压缩时,要先进行量化,以得到相应的整数,这必然会引入误差,不适合于图像的无损压缩,并且图像的重构质量与变换时延拓边界的方式有关。与传统的小波变换相比,提升小波具有以下优点:a)效率高,利用复合赋值,减少了浮点运算量;b)本位操作,对内存的需求量小,便于 DSP 芯片实现;c)并行性,一个提升步骤中的操作是并行的,而多个提升步骤之间是串行;d)非线性,易于构造非线性小波变换;e)通用性,变换过程不依赖 Fourier 分析,容易推广到一般性应用领域;f)逆变换,逆变换只需改变代码执行顺序,具有与正变换相同计算复杂度;g)自适应性,支持自适应小波变换,函数由粗到细逐步进行分析,细化过程可针对关注区域。

提升小波变换主要包括三个步骤。

1)分裂 分裂(split)是将原信号 $S_j = \{S_{j,k}\}$ 分为偶数序列 e_{j-1} 和奇数序列 o_{j-1} ,即

$$\text{split}(S_j) = (e_{j-1}, o_{j-1}) \quad (1)$$

2)预测及预测算子 预测(predict)是利用奇偶序列之间的相关性,由其中一个序列(一般是偶序列 e_{j-1})来预测另一个序列(一般是奇序列 o_{j-1})。实际值 o_{j-1} 与预测值 $P(e_{j-1})$ 的差值 d_{j-1} 称做小波系数,它是原信号 S_j 的高频部分,反映了两个序列的逼近程度。预测过程如下:

$$d_{j-1} = o_{j-1} - P(e_{j-1}) \quad (2)$$

其中:预测算子 P 可用预测函数 P_k 来表示,而预测函数 P_k 可取为 e_{j-1} 数据本身:

$$P_k(e_{j-1,k}) = e_{j-1,k} = s_{j,2k} \quad (3)$$

3)更新及更新算子 经过分裂产生的子集 s_{j-1} 的某些整体特征(如均值)可能与原始数据 S_j 并不一致,为了继续保持原始数据的某些全局特性,需要一个更新的(update)过程。其过程如下:

$$s_{j-1} = e_{j-1} + U(d_{j-1}) \quad (4)$$

其中: s_{j-1} 为原信号 S_j 的低频部分,更新算子 U_k 为

$$U_k(d_{j-1,k}) = \frac{d_{j-1,k}}{2} \quad (5)$$

小波提升是一个完全可逆的过程。重构时,首先逆更新恢复出偶数序列,然后逆预测恢复出奇数序列,最后将奇数序列和偶数序列交叉放置,重构出原始信号。

本文算法采用 512×512 的 Lena 彩色图像作为载体图像,图 1 为对载体图像的绿色分量进行二级提升小波变换的分解过程。

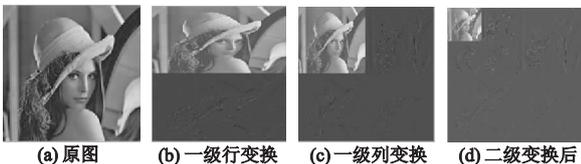


图1 二级提升小波变换分解过程

2 Krawtchouk 矩不变量

Krawtchouk 矩是基于离散 Krawtchouk 多项式提出的一组新的正交矩。利用图像的 Krawtchouk 矩可以很好地恢复出原始图像。

Krawtchouk 矩的核函数是由一系列的 Krawtchouk 多项式组成的。 n 阶 Krawtchouk 多项式定义为

$$K_n(x;p,N) = \sum_{k=0}^n a_{k,n,p} x^k = {}_2F_1(-n, -x; -N; 1/p) \quad (6)$$

$${}_2F_1(a,b;c;z) = \sum_{k=0}^n \frac{(a)_k (b)_k}{(c)_k} \frac{z^k}{k!} \quad (7)$$

其中: ${}_2F_1(a,b;c;z)$ 是超几何函数; $x=0,1,\dots,N,N>0,p \in (0,1), (a)_k = a(a+1)\dots(a+k-1)$ 。

对于大小为 $M \times N$ 的图像 $f(x,y)$,其 $m \times n$ 阶 Krawtchouk 矩定义为

$$Q_{mn} = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y) \bar{K}_m(x) \bar{K}_n(y)$$

$$\bar{K}_m(x) = \bar{K}_m(x;p_1, M-1) = K_m(x;p_1, M-1) \sqrt{\frac{\omega(x;p_1, M-1)}{\rho(x;p_1, M-1)}}$$

$$\bar{K}_n(x) = \bar{K}_n(x;p_2, N-1) = K_n(x;p_2, N-1) \sqrt{\frac{\omega(x;p_2, N-1)}{\rho(x;p_2, N-1)}}$$

$$\sum_{x=0}^{N'-1} \bar{K}_m(x;p, N'-1) \bar{K}_n(x;p, N'-1) = \delta_{nm}, N' = \min(M, N) \quad (8)$$

Krawtchouk 矩不变量是一种不随图像的平移、旋转、尺度变换而变化的矩特征量,其定义为

$$\bar{Q}_{nm} = [\rho(n)\rho(m)]^{-\frac{1}{2}} \sum_{i=0}^n \sum_{j=0}^m a_{i,n,p_1} a_{j,m,p_2} \tilde{v}_{ij} \quad (9)$$

$$\tilde{v}_{nm} = \sum_{p=0}^n \sum_{q=0}^m \begin{bmatrix} n \\ p \end{bmatrix} \begin{bmatrix} m \\ q \end{bmatrix} \begin{bmatrix} N'^2 \\ 2 \end{bmatrix}^{(p+q)/2+1} \begin{bmatrix} N' \\ 2 \end{bmatrix}^{n+m-p-q} v_{pq} \quad (10)$$

其中: v_{pq} 是标准几何矩不变量, $\{a_{k,n,p}\}$ 是由式(6)决定的加权系数。通过式(9)可以计算任意阶 Krawtchouk 矩不变量。

3 奇异值分解

设任意的矩阵 A 的阶是 $m \times n$, 等价于 $A \in R^{m \times n}$, A 的 n 个特征值的非负平方根叫做 A 的奇异值,则存在正交矩阵 U 和 V , 分别有 $U = [u_1, u_2, \dots, u_m] \in R^{m \times m}$ 和 $V = [v_1, v_2, \dots, v_n] \in R^{n \times n}$, 使得

$$U^T A V = \text{diag}(\lambda_1, \lambda_2, \dots, \lambda_g, 0, \dots, 0) = S \quad (11)$$

对式(11)两边分别乘正交矩阵 U 和 V^T , 则有矩阵 A 的奇异值分解公式

$$A = U S V^T \quad (12)$$

奇异值分解的重要特性:a)稳定性;b)二次奇异值分解不变性;c)转置和旋转不变性。由于这些特性,将水印信息嵌入奇异值中,可以提高水印的鲁棒性。

4 水印嵌入算法

4.1 Logistic 混沌序列

Logistic 混沌映射是一种形式简单的混沌序列,只需给其传递系统初值和控制参数就能按照确定的方程产生具有 δ -like 型自相关函数和互相关性为零的混沌序列。经过混沌置乱前后的图像如图 2 所示。

Logistic 混沌序列的定义为

$$\alpha_{k+1} = \mu \alpha_k (1 - \alpha_k) \quad k = \{0, 1, 2, \dots\} \quad (13)$$

其中: μ 为混沌控制参数,取值范围为 $1 \leq \mu \leq 4$ 。实验证明 $\mu \in$

[3.9,4]时,系统将进入混沌状态。

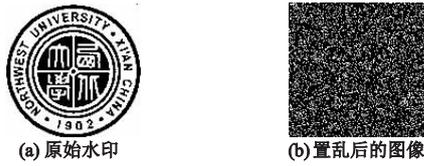


图2 对水印图像进行混沌置乱

4.2 水印嵌入过程

将二值水印图像嵌入到彩色载体图像中,具体步骤如下:

a) 对原始图像 $Img(R, G, B)$ 进行像素三分量的分解,提取其中绿色分量 $Img(:, G, :)$, 将其作为新的图像 IG 。

b) 选取预测算子式(3)和更新算子式(5)对图像 IG 进行二级提升小波变换, $split(IG) = (e_{j-1}, o_{j-1})$ (e_{j-1} 为偶数序列, o_{j-1} 为奇数序列, $j=512, d_{j-1} = o_{j-1} - p(e_{j-1}), d_{j-1}$ 是 IG 的高频部分, $s_{j-1} = e_{j-1} + U(d_{j-1}), s_{j-1}$ 是 IG 的低频部分)。

c) 计算图像低频区域的七个 Krawtchouk 低阶不变量 $[q_{01}, q_{10}, q_{11}, q_{02}, q_{20}, q_{12}, q_{21}]$, 构成函数 $F^{[10]}$:

$$F = [3(q_{01} + q_{10}) + 2(q_{11} + q_{02} + q_{20}) + (q_{12} + q_{21})] / 14$$

F 即为构造出的一个水印。

d) 然后取图像 IG 中频部分 (129:256, 129:256) 对其作奇异值分解, 对水印图像 M 进行混沌置乱得到图像 I , 混沌序列初值 0.3256 和混沌控制参数 3.9 作为密钥保存, 并对置乱后的图像作奇异值分解。

e) 根据水印嵌入的加性规则 $I' = I + rW$ 将水印信息的奇异值嵌入到中频系数的奇异值中, 其中嵌入强度 r 为 0.1。

f) 将得到的新的中频系数赋给 IG 图像变换后的图像中, 对图像进行二级提升小波逆变换, $e_{j-1} = s_{j-1} - U(d_{j-1}), o_{j-1} = d_{j-1} + P(e_{j-1}), S_j = merge(e_{j-1}, o_{j-1}), S_j$ 为重构出的图像。

g) 得到嵌有水印的绿色分量 $Im(:, G, :)$, 最终得到含水水印信息的彩色图像 $Im(R, G, B)$ 。

4.3 水印提取过程

水印提取是水印嵌入的逆过程, 具体步骤如下:

a) 对含水水印图像 $Im(R, G, B)$ 进行像素三分量的分解, 提取其中绿色分量 $Im(:, G, :)$, 用 Ig 表示。

b) 对图像 Ig 进行二级提升小波变换, 计算其低频子图 Krawtchouk 矩不变量 F' , 并比较其与 F 的绝对偏差值 E , 即 $E = |F - F'|$ 。若 $E \leq \varepsilon$, 则认为水印存在, 否则不存在。 ε 为容忍度, 实验中一般取 0.2 ~ 0.3。

c) 若第一水印存在, 则取图像 Ig 的中频系数, 并对它进行奇异值分解。

d) 根据加性原则的逆运算 $W = (I' - I) / r$ 得到水印的奇异值, 利用公式 $A = USV^T$ 对其进行重组。

e) 将得到的水印图像进行反置乱恢复, 得到最终的水印图像。

5 算法仿真及抗攻击性能测试

5.1 算法仿真

本文采用 512×512 的 Lena 彩色图像作为载体图像, 如图 3(a) 所示; 采用 128×128 西北大学校徽的二值图像作为水印图像, 如图 3(b) 所示; 嵌入水印后的图像如图 3(c) 所示; 提取出来的水印图像如图 3(d) 所示。利用峰值信噪比 (PSNR) 来评价水印系统的透明性, 而水印系统的鲁棒性一般用归一化相

关系数 (NC) 来评价。计算可得载体图像与含水水印图像的峰值信噪比 $PSNR = 40.5109$ dB, 原水印图像与提取出的水印图像的 $NC = 0.9999$ 。



图3 载体图像和水印图像

5.2 抗攻击性能测试

含水水印的图像被攻击后实验结果如图 4 所示, 受攻击后的图像与原含水水印图像 Krawtchouk 不变矩的比较如表 1 所示, 与其他文献的比较结果如表 2 所示。



图4 受攻击的含水水印图像和提取出的水印

表 1 图像受攻击后绝对偏差值 E

攻击类型	E
椒盐噪声 (0.05)	0.037 7
高斯噪声 (0.1)	0.026 3
JPEG 压缩 ($Q=80$)	0.042 6
旋转 30°	0.062 3
剪切	0.023 3

表 2 图像受攻击后与其他文献的参数对比

攻击方式	文献[7] NC	文献[8] NC	本文 NC
椒盐噪声 (0.05)	0.945 63	0.978	0.988 5
高斯噪声 (0.1)	0.889 07	0.867	0.989 3
JPEG 压缩 ($Q=80$)	0.982 45	0.872	0.983 7
旋转 30°	0.481 42	0.582	0.629 3
剪切	0.963 54	0.976	0.999 8

通过以上实验说明,在非结构去中心化的 P2P 网络中的节点增加人工免疫系统后,正常节点抵抗恶意节点的能力显著增强,并且在一个可以容忍的误报范围里,能够尽快地将恶意节点隔离。

3 结束语

通过在节点中添加人工免疫系统,对于 20 个节点的非结构去中心化的 P2P 网络,当人工免疫系统中的请求状态循环队列的长度 k 为 5 时,正常节点能发现恶意节点,且误报率低,但是由于非常严格的阈值,使得节点要花费很长的时间才能真正发现恶意节点;当选择 k 为 8 时,节点能在较短的时间发现恶意节点,但误报节点有所增加;当选择 $k=10$ 时,虽然找到恶意节点,误报的节点直线上升。

对于非结构去中心化的 P2P 网络带来的 DDoS 攻击,取状态循环队列长度 $k=8$ 、阈值为 0.333 33 时,误报的节点数在一定的容忍范围内,可以有效地降低恶意节点带来 DDoS 攻击的风险。在选择请求状态队列的长度 k 时,可以适当放宽误报节点的数目;而在检测器进化时,需要权衡节点上检测器进化的时间是否能够节点所容忍,这个进化的结果是否能够适应后期出现的恶意节点的检测,这有待继续研究。

参考文献:

- [1] NAOUMOV N, ROSS K. Exploiting P2P systems for DDoS attacks [C]//Proc of the 1st International Conference on Scalable Information Systems. New York: ACM Press,2006.
- [2] DASWANI N, GARCIA-MOLINA H. Query flood DoS attacks in Gnutella networks[C]//Proc of the 9th ACM Conference on Computer and Communications Security. New York: ACM Press,2002:181-192.
- [3] 李俊青,潘全科,王文宏,等. 蚁群优化在 P2P 网络防范 DDoS 攻击中的应用研究[J]. 计算机应用研究,2009,26(1):339-341.
- [4] 谭艳霞,吴灏. 基于免疫的对等网络 DoS 攻击防御系统[J]. 计算机工程与设计,2006,27(22):4204-4206.

(上接第 4617 页)

表 1 证明了 Krawtchouk 不变矩的差值只有十分微小的变化,可见它们对平移、旋转、镜面以及尺度变换具有不变性。从表 2 中可以看出,在椒盐噪声、高斯噪声、JPEG 压缩、旋转和剪切的攻击下,本文算法比文献[7,8]的算法提取出的水印图像更清晰,NC 值略大。本文算法采用双水印系统,在透明性、鲁棒性、稳定性和抗攻击能力上与其他两个文献算法相比都略胜一筹。

6 结束语

本文算法充分利用了 Krawtchouk 不变矩、提升小波变换和奇异值分解的优势,通过两级提升小波变换后提取其奇异值,再将水印奇异值有效加入。考虑到水印嵌入低频分量,其不可见性好,鲁棒性较差;嵌入到高频分量,其不可见性较差。因此,本文选取其中频分量,兼顾了不可见性和鲁棒性。另外,通过计算 Krawtchouk 不变矩作为另一验证标志,双重水印保证了其鲁棒性。通过实验证明,该算法不可见性好,对常见攻击和几何攻击都具有较好的鲁棒性,具有一定的应用价值。

参考文献:

- [1] ZHOU Bo, CHEN Jian. A geometric distortion resilient image watermarking algorithm based on SVD[J]. Chinese Journal of Image and Graphics,2004,9(4):506-512.

- [5] MA Xin-xin, ZHAO Yang, QIN Zhi-guang. Improving resilience against DDoS attack in unstructured P2P networks [J]. Journal of Electronic Science and Technology of China,2007,5(1):18-22.
- [6] ATHANASOPOULOS E, ANAGNOSTAKIS K G, MARKATOS E P. Misusing unstructured P2P systems to perform DoS attacks the network that never forgets [C]//Proc of the 4th International Conference on Applied Cryptography and Network Security. 2006:130-145.
- [7] 莫宏为. 人工免疫系统原理与应用[M]. 哈尔滨:哈尔滨工业大学出版社,2003.
- [8] 莫宏为,左兴权. 人工免疫系统[M]. 北京:科学出版社,2009.
- [9] 李敏强,寇纪淞,林丹,等. 遗传算法的基本理论与应用[M]. 北京:科学出版社,2009.
- [10] ZEINALIPOUR-YAZTI D. Exploiting the security weaknesses of the Gnutella protocol [D]. Riverside: University of California,2002.
- [11] LIU Yun-hao, LIU Xiao-mei, WANG Chen, et al. Defending P2Ps from overlay flooding-based DDoS [C]//Proc of International Conference on Parallel Processing. 2007.
- [12] WEI Dong, YANG Shou-bao, LIU Xiao-qian. Artificial immunology based anti-pollution P2P file sharing system grid and cloud computing [C]//Proc of the 6th International Conference on Grid and Cooperative Computing. 2007:82-87.
- [13] SUN Xin, TORRES R, RAO S G. On the feasibility of exploiting P2P systems to launch DDoS attacks[J]. Peer-to-Peer Networking and Applications,2010,3(1):36-51.
- [14] CHOLEZ T, HENARD C, CHRISMENT I, et al. A first approach to detect suspicious peers in the KAD P2P network [C]//Proc of Network and Information Systems Security. 2011:1-8.
- [15] 刘丹,李毅超,余三超,等. 面向 P2P 网络的 DDoS 攻击抑制方法[J]. 电子科技大学学报,2011,40(1):85-89.
- [16] QWASMI N, AHMED F, LISCANO R. Simulation of DDoS attacks on P2P networks [C]//Proc of the 13th IEEE International Conference on High Performance Computing and Communications. 2011:610-614.

- [2] 王丽娜,于戈,王国仁. 基于混沌特性改进的小波数字水印算法[J]. 电子学报,2001,29(10):1424-1426.
- [3] 刘瑞祯,谭铁牛. 基于奇异值分解的数字图像水印方法[J]. 电子学报,2001,29(2):168-171.
- [4] 刘连山,李人厚,高琦. 一种基于彩色图像绿色分量的数字水印嵌入方法[J]. 西安交通大学学报,2004,38(12):1256-1259.
- [5] SWELDENS W. The lifting scheme: a new philosophy in biorthogonal wavelet constructions [C]//Proc of SPIE on Wavelet Applications in Signal and Image Processing III. [S. l.]: SPIE, 1995: 68-79.
- [6] FRIDRICH J, GOLJAN M, HOGEA D. Attacking the outguess [C]//Proc of ACM MULTIMEDIA '02 Workshop on Multimedia and Secrecy, and Steganalysis. New York: ACM Press,2002:3-6.
- [7] 徐国荣,王礼平. 基于奇异值与提升小波的彩色图像水印算法[J]. 计算机应用研究,2011,28(5):1982-1986.
- [8] 赵玉霞,康宝生. 基于混沌系统与提升小波的彩色图像盲水印算法[J]. 计算机应用研究,2010,27(1):247-250.
- [9] 张力,肖薇薇,钱恭斌,等. 基于 Krawtchouk 不变矩的仿射攻击不变性局部水印算法[J]. 电子学报,2007,7(7):1403-1408.
- [10] 吴一全,谢静,庞磊. 基于 Krawtchouk 矩和 Contourlet 变换的多目的水印[J]. 光子学报,2009,38(8):2160-2164.
- [11] 王春桃,倪江群,卓华硕,等. 基于可变形多尺度变换的几何不变鲁棒图像水印算法[J]. 自动化学报,2011,37(11):1368-1380.
- [12] 夏冕,鲁宏伟,赵小厦. 鲁棒性数字图像水印技术[J]. 小型微型计算机系统,2011,2(2):356-360.