基于第二代 Bandelet 变换的抗几何攻击图像水印

綦 科 [1, 2] 谢冬青 [1]

摘 要 抗几何攻击的鲁棒图像水印设计是目前水印技术研究的难点和热点之一. 文中分析了图像的 Bandelet 变换特性, 提出了一种以图像特征点矢量集为特征向量的回归支持向量机 (Support vector regression, SVR) 和第二代 Bandelet 变换的抗几何攻击图像水印算法, 采取的主要方法包括: 1) 在 Bandelet 变换提取的刻画图像局部特征的几何流系数上, 采用奇偶量化嵌入水印; 2) 利用 Harris-Laplace 算子从归一化的含水印图像中提取具有几何形变鲁棒性的图像特征点, 构造特征点矢量集作为特征向量, 应用回归支持向量机对几何变换参数进行训练学习; 3) 水印检测时, 先利用 SVR 训练模型得到待检测图像所受几何攻击的参数并作几何校正, 然后通过奇偶检测器盲提取水印. 仿真实验表明, 所提出的水印算法不仅具有良好的透明性, 而且对常规图像处理、一般性几何攻击和组合攻击均具有良好的鲁棒性.

关键词 图像水印, 几何攻击, Bandelet 变换, 回归支持向量机, 奇偶量化

引用格式 綦科, 谢冬青. 基于第二代 Bandelet 变换的抗几何攻击图像水印. 自动化学报, 2012, **38**(10): 1646−1653

DOI 10.3724/SP.J.1004.2012.01646

Watermarking Scheme Against Geometrical Attacks Based on Second Generation Bandelet

QI Ke[1, 2] XIE Dong-Qing[1]

Abstract Image watermarking against geometric attacks is the hotspot and challenging point in the present research on watermarking. This paper analyses the characteristics of the second generation Bandelet translation, and then proposes a novel Bandelet-domain watermarking scheme against geometric attacks based on support vector regression (SVR) with the vector of feature points. The proposed scheme includes three important techniques: 1) the Bandelet based image directional flow coefficient which depicts the characteristic of the image is used to embed watermarking bits with odd-even quantization; 2) the feature points robust to geometric deformation are extracted from the watermarking image using Harris-Laplace operator, and used as the eigenvectors to train the SVR model; 3) during detection, the parameters of geometric attacks are obtained using the well trained SVR, which is used for resynchronization, then an odd-even detector is used to extract the watermark blindly. Experiment results show that the proposed scheme is well transparent and is not only robust to common image processing but also robust against some geometric attacks as well as some combined attacks.

Key words Image watermarking, geometrical attacks, Bandelet transform, support vector regression (SVR), odd-even quantization

Citation Qi Ke, Xie Dong-Qing. Watermarking scheme against geometrical attacks based on second generation Bandelet. *Acta Automatica Sinica*, 2012, **38**(10): 1646−1653

近年来, 图像水印技术的研究取得了较大进展, 但是已有的多数水印算法无法有效抵抗一般性几何攻击, 包括: 全局仿射变换、剪切、行列去除、局部弯曲、几何变换组合等多种形式, 这是因为几何攻击破坏了载体和水印之间的同步性, 尽管水印信息依然存在于载体中, 但水印嵌入位置发生变化, 致使水印难以检测[1]. 因此, 抗几何攻击的高鲁棒图像水印设计依然是水印研究的难点之一.

目前, 抗几何攻击的水印算法大致分为: 基于仿射不变空间的方法[2], 基于模板的同步方法[3], 基于图像特征的同步方法[1, 4−8]. 其中: 基于图像特征的同步方法利用特征点提取算法提取图像重要特征进行水印同步, 例如文献 [4] 利用尺度不变特征变换 (Scale-invariant feature transform, SIFT) 进行水

收稿日期 2011-09-28 录用日期 2012-06-14
Manuscript received September 28, 2011; accepted June 14, 2012
广东省自然科学基金 (S2012010010004), 网络与数据安全四川省重点实验室 2011 开放项目, 广东省高等院校高层次人才项目资助
Supported by Natural Science Foundation of Guangdong Province (S2012010010004), 2011 Openning Projects of Network and Data Security Key Laboratory of Sichuan Province, and High-Level Talents Project of Guangdong Province
本文责任编委 戴琼海
Recommended by Associate Editor DAI Qiong-Hai
1. 广州大学计算机科学与教育软件学院 广州 510006 2. 网络与数据安全四川省重点实验室 成都 611731
1. Computer Science and Education Software College, Guangzhou University, Guangzhou 510006 2. Network and Data Security Key Laboratory of Sichuan Province, Chengdu 611731

印的同步, 文献 [1, 5−8] 基于图像 Harris-Laplace 特征点和特征尺度的水印同步, 在特征尺度范围内的系数上嵌入水印信息, 该类算法的优点是能有效抵抗旋转、缩放、平移 (Rotation, scale, translation, RST) 和剪切等去同步攻击, 不足是嵌入信息量较少, 而且对不等比例缩放的鲁棒性不佳.

近年来, 支持向量机 (Support vector machine, SVM) 理论为抗几何攻击提供了可能的解决方向, 成为抗几何攻击水印设计的研究热点, 文献 [9−11] 都是基于 SVM 模型的抗几何攻击水印算法, 分别在空域、Pseudo-Zernike 矩和空域嵌入水印信息, 这些算法都利用 SVM 模型对受攻击图像进行几何校正, 在一定程度上提升了水印抗几何攻击的鲁棒性, 但不足在于: 训练 SVM 模型所用的特征向量几何不变性较弱, 抵抗剪切、行列移除、局部弯曲的去同步攻击能力较差. 本文的基本思想是提取具有几何形变鲁棒性的图像特征点集, 用于 SVM 模型的训练和几何校正.

第二代 Bandelet 变换[12] 由法国学者 Pennec 等于 2005 年提出, 具有正交、无边界效应的特点, 能更好地提取图像复杂纹理和边缘等图像几何特征. 目前已设计出一些基于 Bandelet 变换的水印算法[13−14]. 文献 [13] 提出了一种基于 Bandelet 的全频域无损水印算法, 算法采用的是零水印的思想, 具有较好的抗常规图像攻击能力, 不足之处是没有应用隐藏技术, 抗几何攻击能力较弱; 文献 [14] 设计了一种基于第二代 Bandelet 变换的认证算法, 通过隐藏水印信息与从嵌入水印载体的 Bandelet 变换几何矢量方向流之间的相关性检测, 实现对图像的认证, 算法完全基于图像特征, 有较强的抗图像特效攻击的优点, 不足之处在于算法不能抵抗几何攻击.

本文结合 Bandelet 变换和 SVM 模型, 提出了一种以 Harris-Laplace 特征点矢量集为特征向量的回归支持向量机 (Support vector regression, SVR) 和第二代 Bandelet 变换的可有效抵抗一般性几何攻击的鲁棒图像水印算法. 算法在 Bandelet 变换提取的刻画图像局部特征的几何流系数上, 利用奇偶量化嵌入水印, 然后利用 Harris-Laplace 算子从归一化的含水印图像中提取具有几何形变鲁棒性的图像特征点矢量集作为特征向量, 用于 SVR 模型的训练. 检测时首先用 SVR 模型对待检测图像进行几何校正, 实现重同步后再检测水印. 实验证明该算法不仅具有水印图像质量高的优点, 而且对常规图像处理、一般性几何攻击及组合攻击均具有较强的鲁棒性.

1 第二代 Bandelet 变换

第二代 Bandelet 变换[12] 是一种建立在图像小波变换基础上的再次 Bandelet 化的多尺度几何分析方法, 具有算法过程简单、重构图像没有边缘效应的特点.

对于几何正则图像, 二维小波变换中高频子带大幅值系数主要沿图像的几何流分布, 可以用几何流来刻画. 第二代 Bandelet 变换的出发点就是对小波系数进行分块, 在每个子块中用直线逼近几何流, 这使得几何流只需一个称为几何流方向的参数控制, 从而实现图像的最佳稀疏表示.

第二代 Bandelet 变换原理是: 先对图像作规定级数的二维离散正交小波, 然后对高频子带分两种情况处理: 1) 对存在几何流的 Bandelet 块沿几何流方向进行曲波变换 (Warp wavelet), 将一维小波系数按 Mallat 规则重新排序为二维矩阵; 2) 对不存在几何流的 Bandelet 块保持原有小波系数.

给定一块正方形区域 S, 沿几何流方向 d 重排 S 内的小波系数, 得到一维信号. 如果方向 d 选择正确, 经一维小波变换可以对信号进一步处理得到的非零系数个数显著减少. 如果 S 和 d 选择不正确, 经一维小波变换, 量化后非零系数个数不会有显著减少. 区域 S 内的几何流角度的判定通过最小化 Lagrange 函数:

$$L(f_\theta, R) = \|f_\theta - \overline{f}_\theta\| + \lambda \cdot T^2(R_g + R_b) \qquad (1)$$

其中, $\overline{f}_\theta$ 表示由一致均匀量化后的 Bandelet 系数重构的一维信号, T 为量化阈值, R_g 表示几何流编码所需比特数, R_b 表示编码量化后的 Bandelet 系数所需比特数, λ 为 Lagrange 乘子, 按 Pennec 的优化结果实验中取值为 $\lambda = 3/28$. 获得最小化 Lagrange 系数的角度即为该区域内的最佳几何流方向 d.

在进行几何流方向 θ 的检测时, 对于尺寸为 $L \times L$ 的小方块, 一般将圆周角 $[0, \pi)$ 等角度离散为 $L^2 - 1$ 个, 即 θ 可能的取值为

$$\theta = \frac{k\pi}{L^2 - 1}, \quad k = 0, 1, \cdots, L^2 - 2 \qquad (2)$$

一般采用基于四叉树分割的自适应分块方式对中高频子带分块进行 Bandelet 变换[14], 但由于图像在遭受攻击后, 自适应的分块方式不一定能够完全再现, 此时将无法正确检测水印, 因此本文对图像的二维小波变换各中高频子带做固定分块, 然后利用 Bandelet 对图像固定分块进行几何流检测, 对存在几何流的 Bandelet 块沿几何流方向进行曲波变换, 得到刻画图像局部特征的 Bandelet 系数. 在几何流检测时, 取 $\{0, \pi/8, \pi/4, 3\pi/8, \pi/2, 5\pi/8, 3\pi/4, 7\pi/8\}$ 共 8 个有限离散角度搜索几何流方向, 如图 1 所示.

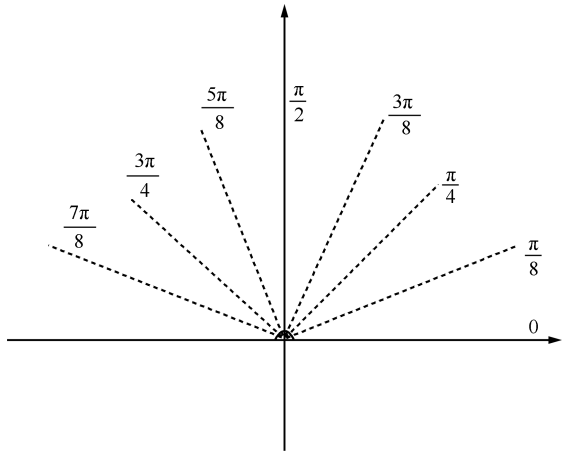


图 1 8 个离散角度几何流搜索

Fig. 1 Gometric flow searching of eight discrete angles

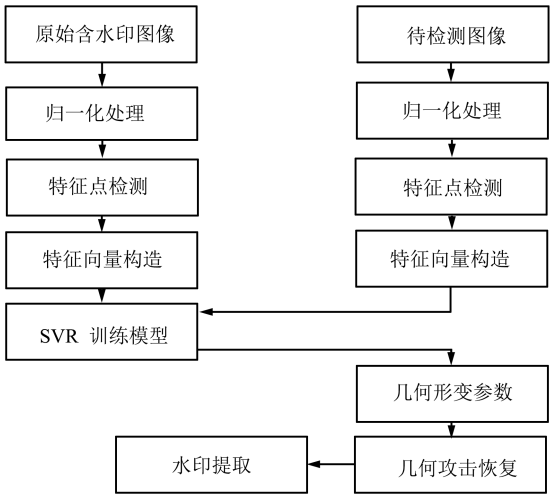


图 2 Bandelet 域水印嵌入

Fig. 2 Watermark embedding in Bandelet domain

2 数字水印的嵌入

基于小波系数固定分块和有限离散角度几何流检测的 Bandelet 变换, 本文提出的 Bandelet 域水印嵌入算法首先对原始图像小波分解的中高频子带进行固定分块, 然后利用第 1 节中的方法实施 8 个有限离散角度的几何流方向搜索, 最后对具有几何流方向的分块进行 Bandelet 变换, 在刻画图像局部特征的 Bandelet 系数上, 采用奇偶量化嵌入水印. 为增强鲁棒性, 水印信息被重复的嵌入到具有相同几何流方向的固定分块 Bandelet 系数中, 采用这种统计性的系数值修改, 形成水印信息与宿主信息的 $1:n$ 的关系, 即使嵌入水印的图像在遭受较强的攻击时, 也能够维持水印信息整体的稳定性; 同时, 由于水印被嵌入到对应于图像复杂纹理和边缘的大幅值 Bandelet 系数中, 所以算法具有良好的透明性和强鲁棒性. 水印嵌入算法如图 2 所示, 具体步骤如下:

步骤 1. 对原始图像做二维小波分解, 对各中高频子带系数做固定分块, 子块矩阵大小统一设为 $M \times N$, 得到中高频小波系数矩阵序列 $\{H^k|k=1, \cdots, n\}$, n 为固定分块数.

步骤 2. 对每一个分块 H^k, 按照第 1 节的方法实施 8 个角度的几何流方向搜索, 得到具有几何流方向的分块 $\{D_\theta^k|k=1,2,\cdots,m_\theta; m_\theta \le n;\ \theta \in (0, \pi/8, \pi/4, 3\pi/8, \pi/2, 5\pi/8, 3\pi/4, 7\pi/8)\}$, 共包含 u $(u \le 8)$ 个角度的几何流方向.

步骤 3. 对所有具有几何流方向的分块 $\{D_\theta^k\}$ 实施 Bandelet 变换, 得到各分块的 Bandelet 系数.

步骤 4. 将水印信息重复嵌入到具有相同几何流方向的固定分块 Bandelet 系数中, 对系数的修改通过奇偶量化的方式进行.

设待嵌入水印信息 $\{w_v|v=1,\cdots,l\}$ 是长度为 l 的伪随机序列, 取值为 $\{0,1\}$. 我们将水印信息 $\{w_v|\ v=1,\cdots,l\}$ 平均分为长度为 l/u 的 u $(u \le 8)$ 个子集合, 分别嵌入到 u $(u \le 8)$ 个几何流方向的固定分块 Bandelet 系数中, 过程如下:

1) 对具有几何流方向的分块 $\{D_\theta^k\}$, 按照 $\theta = 0,\ \pi/8, \pi/4, 3\pi/8, \pi/2, 5\pi/8, 3\pi/4, 7\pi/8$ 的顺序执行以下水印嵌入步骤.

2) 如果 $\{D_\theta^k\}$ 包含有角度 θ 的分块, 则提取所有具有角度 θ 的分块 $\{D_\theta^k|k=1,\cdots,m_\theta\}$; 否则转 1).

3) 对每一个具有角度 θ 的分块 $\{D_\theta^k|k=1,\cdots, m_\theta\}$ 的 Bandelet 系数, 按由大到小的方式选取前 $t=l/u$ 个系数 $\{B_\theta^k(t)|k=1,\cdots,m_\theta;\ t=1,\cdots, l/u\}$, 则长度为 l/u 的水印信息与每个分块中的前 l/u 个 Bandelet 系数一一对应, 并按照奇偶量化的方式嵌入到这些选取出来的前 l/u 个 Bandelet 系数中.

4) 对前 l/u 个系数中的每个系数 $B_\theta^k(t)$, 赋予符号 "0" 或 "1", 即:

$$q_\theta^k(t)=\begin{cases} 0, & KQ \le B_\theta^k(t) \le (K+1)Q, \\ & K=0,\pm2,\pm4,\cdots \\ 1, & KQ \le B_\theta^k(t) \le (K+1)Q, \\ & K=\pm1,\pm3,\cdots \end{cases} \tag{3}$$

其中, Q 为量化步长.

5) 计算前 $t=l/u$ 个系数中的每个系数 $B_\theta^k(t)$ 的量化噪声 $r_\theta^k(t)=B_\theta^k(t)-\lfloor B_\theta^k(t)/Q\rfloor \times Q$, 其中 $\lfloor\cdot\rfloor$ 表示向下取整.

6) 设第 i 个系数 $B_\theta^k(i)$ 中待嵌入的水印位为 $w(i)$, 为使修改后的 Bandelet 系数值处于量化区间的中间, 对每个分块 $\{D_\theta^k|k=1,\cdots,m_\theta\}$ 的第

i 个 Bandelet 系数 $B_\theta^k(i)$ 进行量化修改, 修改后的 Bandelet 系数值按照式 (4) 计算:

$$B_\theta^{'k}(i)=\begin{cases} B_\theta^k(i)-r_\theta^k(i)+\dfrac{Q}{2}, & q_\theta^k(i)=w(i) \\ B_\theta^k(i)-r_\theta^k(i)-\dfrac{Q}{2}, & q_\theta^k(i)\neq w(i) \end{cases} \tag{4}$$

通过以上奇偶量化的方式嵌入水印后, 所有具有相同几何流方向 θ 的分块中 (共 m_θ 个), 处于同一位置 i 的 Bandelet 系数值 $B_\theta^{'k}(i)$ 的量化函数值 $q_\theta^k(i)$ 都等于在该位置嵌入的水印 $w(i)$.

步骤 5. 将含有水印信息的修改系数 $\{B_\theta^{'k}(t)|k=1,\cdots,m_\theta;\ t=1,\cdots,l/u\}$, 结合未修改的系数一起进行逆 Bandelet 变换, 得到含水印图像.

3　基于图像特征点和 SVR 的几何攻击恢复水印检测

抗几何攻击水印算法的关键在于对水印信号进行同步, 使水印信息恢复到几何攻击前的位置. 本文应用 Harris-Laplace 特征点检测算子, 设计了一种基于 SVR 几何校正的水印检测算法, 算法程序框图如图 3 所示.

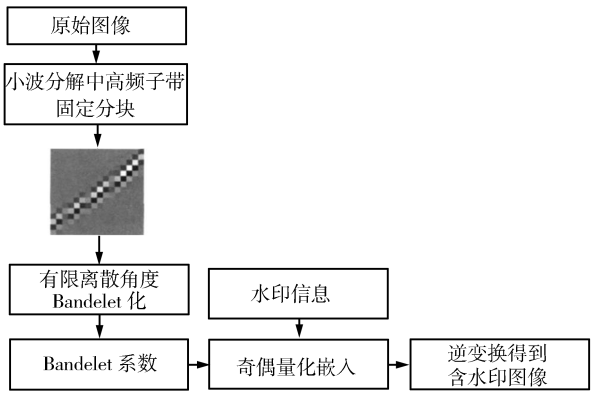


图 3　几何攻击恢复水印检测

Fig. 3　Watermark extracting based on geometric synchronous

算法主要步骤包括: 1) 图像尺度归一化处理, 提取图像 Harris-Laplace 特征点; 2) 选取图像的 Harris-Laplace 特征点, 构造以特征点为中心的特征矢量集作为特征向量, 通过 SVR 对旋转、缩放、平移及其组合攻击等几何变换参数进行训练学习, 获得训练模型; 3) 提取待检测图像的 Harris-Laplace 特征点, 以特征点矢量集作为特征向量, 利用训练模型预测几何变换参数, 利用预测输出结果对待检测图像进行几何校正; 4) 从几何校正后的图像内提取水印信息. 由于性能稳定的图像特征点具有几何形变鲁棒性, 将之用于构造 SVR 的特征向量, 既提高了图像对几何攻击的抵抗性, 又改善了 SVR 的分类性能.

3.1　特征向量的构造

由数字图像相关理论知, 特征点具有协变于图像几何形变的性质, 因此可作为参照系来矫正几何形变. Mikolajczyk 等[15] 提出的 Harris-Laplace 特征点检测算子对旋转、缩放、平移以及噪声干扰等均有较好的稳定性, 而且以特征点为中心的特征尺度反映了局部图像特征, 与图像局部结构具有协变特性, 考虑到本文重点讨论图像平移、缩放、旋转、剪切、局部弯曲等几何变换形式, 因此采用 Harris-Laplace 特征点集合 $\{p_k\}$ 及其相应的特征尺度内局部图像特征矢量 $\{v_k\}$ 来反映图像全局几何信息及局部图像信息, 并进一步将其作为特征向量.

Harris-Laplace 算子[15] 利用 Harris 算子在尺度 $\delta_n=s^n\delta_0$ 上建立 N 个尺度空间的描述, 其中 n 表示的是一系列尺度中的第 n 尺度, $n=1,2,\cdots,N$; s 表示尺度因子, 自适应调整尺度间的跨度. 在每一尺度空间描述上提取大于给定阈值且在邻域 Q 内的极值点, 然后验证该点能否在 N 尺度空间上的某一尺度获得局部极值, 获得极值则校验此点在该尺度空间上的 LOG 算子是否获得极值, 若能获得极值则是特征点, 否则舍弃. Harris 算子通过检测图像发生二维突变的位置提取特征点, 其检测方程为

$$R(x,y,\delta_I,\delta_D)=\det(M)-k\cdot[\mathrm{tr}(M)]^2 \tag{5}$$

其中, $R(x,y,\delta_I,\delta_D)$ 表示梯度因子, (x,y) 表示像素点坐标, δ_I 是积分尺度, δ_D 为微分尺度, M 为自相关矩阵, k 为常数, 一般取 0.04, $\det(M)$ 和 $\mathrm{tr}(M)$ 分别表示 M 的行列式和迹. 具体的 Harris-Laplace 算子特征点检测算法见文献 [15].

由于 Harris 特征点对图像的尺度变化敏感, 因此在提取图像特征点之前, 先对图像进行归一化处理, 以保证特征点在缩放攻击下的可重复检测性. 图像归一化是根据图像特征来获取图像的旋转、平移与缩放参数, 按照一种标准形式对图像进行几何变换, 将图像变换到一个标准尺寸.

本文采用的归一化方法是基于矩的归一化[16], 即对一幅图像 $I(x,y)$, 计算零阶几何矩 m_{00}:

$$m_{00}=\sum_x\sum_y I(x,y) \tag{6}$$

则归一化参数 $\alpha=\sqrt{\beta/m_{00}}$, 其中 β 为预先设置的常数, 归一化后的图像为 $I(x/\alpha,y/\alpha)$.

设 $f(x,y)$ 表示归一化处理后的图像, 则基于 Harris-Laplace 算子提取的特征点集 $\{p_k\}$ 及其相应的特征尺度内局部图像特征矢量集 $\{v_k\}$, 特征向量 $\{D_n\}$ 的构造方法如下:

步骤 1. 对 $\{p_k\}$ 中的特征点, 按照梯度因子 $R_k(x_k, y_k, \delta_I, \delta_D)$ 绝对值的大小, 从大到小排序.

步骤 2. 依次取出集合 $\{p_k\}$ 中的特征点, 以该点的特征尺寸 δ_k 为特征区域半径, 若其特征区域没有超出图像边缘且不与已存在的特征区域有重叠, 则该点是特征点, 并入有效特征点集 $\{f_k\}$ 中; 否则舍弃.

步骤 3. 对有效特征点集 $\{f_k\}$ 中的前 W 个特征点, 统计其特征区域的像素均值 A_k、均方差 S_k, 并与梯度因子 R_k、特征尺度 δ_k 构成以此特征点为中心的特征尺度内局部图像特征矢量集 $\{v_k|k = 1, 2, \cdots, W\}$, 并以此特征矢量集为特征向量. 其中, $A_k = \frac{1}{e}\sum_{x,y} I(x, y)$, $S_k = \frac{1}{e}\sum_{x,y}(I(x, y) - A_k)^2$, $v_k = (R_k, \delta_k, A_k, S_k)$, e 为特征区域的像素个数.

3.2 SVR 训练模型的获得

SVR 是支持向量机 SVM 在回归学习中的应用, 其基本思想是: 对于给定训练样本点集 (x_1, y_1), (x_2, y_2), $\cdots$, (x_n, y_n), 通过 SVR 训练一个回归函数 $f(x)$, 使得由该函数求出的每个输入样本的输出值和输入样本所对应的目标值相差不超过给定的阈值, 同时使回归函数 $f(x)$ 尽量平滑.

为了获得 SVR 训练模型, 我们在一定范围内随机平移 (包括 X 方向平移, Y 方向平移)、旋转、缩放原始图像 I, 产生 M 个训练样本图像 $\{I^m|m = 1, 2, \cdots, M\}$, 然后按照第 3.1 节所述方法提取每个训练样本图像 I^m 的特征向量 $\{v_k^m|k = 1, 2, \cdots, W; m = 1, 2, \cdots, M\}$, 并将其作为训练特征向量. 同时, 将相应的几何变换参数 $O^m = \{(t_x^m, t_y^m, \theta^m, \lambda^m)|m = 1, 2, \cdots, M\}$ 作为训练目标值, 其中, t_x^m, t_y^m, θ^m, λ^m 分别为 X 方向平移值, Y 方向平移值, 旋转角度, 缩放比例. 于是, 可以得到训练样本 $\Omega^m = \{(v_k^m, O^m)|m = 1, 2, \cdots, M\}$. 本文采用径向基函数 (Radial basis function, RBF) 作为 SVR 的核函数, 通过训练学习, 即可获得 SVR 训练模型.

3.3 待检测图像的几何校正

基于 SVR 的待检测图像 $\widetilde{I}$ 的几何校正过程如图 3 所示, 主要包括如下步骤:

步骤 1. 按照第 3.1 节所述方法, 对待检测图像 $\widetilde{I}$ 进行归一化处理.

步骤 2. 按照第 3.1 节所述方法, 计算待检测图像 $\widetilde{I}$ 的特征点矢量集 $\{\widetilde{v}_k\}$, 将其作为训练特征向量.

步骤 3. 以特征点矢量集 $\{\widetilde{v}_k\}$ 为输入向量, 利用已经获得的 SVR 训练模型对输出向量进行数据预测, 从而得到相应的输出向量值 $(\widetilde{t}_x, \widetilde{t}_y, \widetilde{\theta}, \widetilde{\lambda})$, 即待检测图像 $\widetilde{I}$ 的几何变换参数, 分别为 X 方向平移值、Y 方向平移值、旋转角度、缩放比例.

步骤 4. 利用所得到的几何变换参数, 对待检测图像 $\widetilde{I}$ 进行几何校正, 从而得到待检测图像 $\widetilde{I}$ 的校正结果 I^*.

3.4 数字水印的检测

设校正后的待检测图像为 I^*, 按照第 1 节所述方法, 首先对待检测图像的小波分解中高频子带进行 $M \times N$ 的固定分块; 然后搜索固定分块的几何流方向, 计算并提取相应的 Bandelet 系数; 最后按照 $\phi = 0, \pi/8, \pi/4, 3\pi/8, \pi/2, 5\pi/8, 3\pi/4, 7\pi/8$ 的顺序, 提取嵌入到各角度几何流 Bandelet 系数中的水印子序列:

步骤 1. 提取每一个具有角度 ϕ 的分块 $\{D_\phi'^k|k = 1, 2, \cdots, m_\phi'\}$ 及其相应的 Bandelet 系数, 按由大到小的方式选取前 l/u 个系数 $\{B_\phi'^k(t)|k = 1, 2, \cdots, m_\phi'; t = 1, 2, \cdots, l/u\}$.

步骤 2. 利用式 (3) 对所有的系数 $\{B_\phi'^k(t)|k = 1, 2, \cdots, m_\phi'; t = 1, 2, \cdots, l/u\}$ 进行奇偶量化, 得到奇偶量化值 $\{q_\phi'^k(t)|k = 1, 2, \cdots, m_\phi'; t = 1, 2, \cdots, l/u\}$.

步骤 3. 提取位置 i $(i = 1, 2, \cdots, l/u)$ 的水印 $w(i)'$: 遍历所有 m_ϕ' 个分块中位置 i 的奇偶量化值 $\{q_\phi'^k(i)|k = 1, 2, \cdots, m_\phi'\}$, 记量化函数值为 0 的像素个数为 $NUM_{i,0}$, 量化函数值为 1 的像素个数为 $NUM_{i,1}$, 通过式 (7) 的奇偶检测器提取水印 $w(i)'$:

$$w(i)' = \begin{cases} 0, & NUM_{i,0} > NUM_{i,1} \\ 1, & NUM_{i,0} < NUM_{i,1} \end{cases} \tag{7}$$

按照 $\phi = 0, \pi/8, \pi/4, 3\pi/8, \pi/2, 5\pi/8, 3\pi/4, 7\pi/8$ 的顺序, 重复步骤 1 ~ 步骤 3, 提取嵌入到各角度几何流 Bandelet 系数中的水印子序列, 最后将提取的水印子序列合成为最终的水印序列 $w(i)'$.

4 仿真实验

4.1 检测性能测试

为了评价水印算法的性能, 本文选取 512 像素 × 512 像素大小的标准灰度图像 Lena, Mandrill 和 House 进行透明性测试和抗攻击能力测试 (包括常规信号处理攻击和一般性几何攻击). 仿真实验中, 对原始图像进行一级小波变换, 得到 256 像素 × 256 像素大小的中高频子带, 对其进行 $M = N = 16$ 的固定分块, 然后对固定分块进行 8 个离散角度的几何流检测, 在相应的 Bandelet 变换系数中嵌入长度为 256 bits 的二元随机水印序列, 水印嵌入时的量化步长 $Q = \text{round}(0.7\,T)$, T 为所有嵌入水印的 Bandelet 系数中幅值最小的系数; 另外, 在含水印图像中提取 15 个图像特征点, 构成 $W = 15$ 的图像

特征点矢量集, 训练样本数目为 $M = 120$, SVR 训练时选用了 RBF 核函数.

图 4 给出了嵌入水印后的图像. 实验结果表明, 嵌入水印的图像峰值信噪比 (Peak signal to noise ratio, PSNR) 都在 46 dB 左右, 有良好的透明性, 并且检测时能够完全准确地提取出水印序列. 表 1 比较了本文算法与文献 [10−11, 14] 在图像 Lenna 和图像 Mandrill 的 PSNR 值, 可见本文算法与文献 [14] 的 PSNR 值相差不大, 而较文献 [10−11] 能够获得更高的 PSNR 值. 这是因为与文献 [10−11] 在 Pseudo-Zernike 矩和空域中嵌入水印相比较, 本文算法和文献 [14] 都是将水印嵌入到对应于图像复杂纹理和边缘的大幅值 Bandelet 系数中, 能更好地满足 HVS 理论中关于人眼对图像的纹理和边缘不敏感的特性, 使水印具有更好的透明性.

(a) 含水印图像 Lenna (b) 含水印图像 Mandrill (c) 含水印图像 House
(a) Watermarked Lenna (b) Watermarked Mandrill (b) Watermarked House

图 4　几何攻击恢复水印检测

Fig. 4　Watermarked images

表 1　算法 PSNR 值比较 (dB)

Table 1　Comparison of PSNR (dB)

PSNR 值	Lenna	Mandrill	House
本文算法	46.45	45.21	46.93
文献 [10]	43.59	44.28	44.14
文献 [11]	40.56	41.93	38.86
文献 [14]	44.97	45.73	45.36

4.2　抗攻击能力测试

为了验证本文算法的抗攻击能力, 我们用 Stirmark 4.0[17] 对加水印图像进行各种类型的攻击, 包括 JPEG 压缩、滤波、噪声攻击等常规图像攻击, 以及 RST 攻击及其组合攻击等几何攻击. 表 2 与表 3 分别给出了图像 Lenna 和 Mandrill 在常规图像攻击和几何攻击下的测试结果, 并且与文献 [10−11, 14] 的性能进行比较. 实验中, 使用比特误码率 (Bit error rate, BER) 来计算水印检测结果与原始水印之间的比特误差.

由表 2 可知, 本文算法在抵抗常规图像攻击时具有良好的鲁棒性, 性能优于文献 [10−11], 与文献 [14] 相差不大. 本文算法能够在图像遭受均值滤波、JPEG 压缩、高斯噪声和椒盐噪声等攻击时检测出水印信息, 这是因为算法中的奇偶检测器是一种基于统计的水印检测方法, 由于水印被重复地嵌入到分布于整个图像的大幅值 Bandelet 系数中, 这种统计性的系数值修改, 形成水印信息与宿主信息的 $1:n$ 的关系, 即使含水印图像遭受较强攻击, 也不会在整体性上改变 Bandelet 系数的奇偶统计性质. 本文算法中水印被嵌入到对应于图像复杂纹理和边缘的 Bandelet 系数中, 与文献 [10−11] 在 Pseudo-Zernike 矩和空域中嵌入水印相比较, 本文算法具有更强的鲁棒性. 而本文算法和文献 [14] 都是将水印嵌入到 Bandelet 系数中, 因此抵抗常规图像攻击的性能相差不大.

由表 3 可知, 本文算法在抗几何攻击中也具有较好的稳健性, 性能也优于文献 [10−11, 14]. 图 5 给出了检测时从未受攻击的含水印图像中提取出来的特征点, 图 6 给出了含水印图像 Lenna 遭受部分几何攻击后提取的特征点, 所有 15 个特征点都能够被正确提取, 可见特征点对几何攻击具有较强的稳健性. 这是因为本文利用图像特征点对大多数的图像几何操作不敏感的特性, 而且在对含水印图像尺度归一化的基础上利用 Harris-Laplace 算子提取特征点信息, 保证了特征点在缩放攻击下的可重复检测性, 进一步提高了特征点对抗几何攻击的稳健性. 因此本文算法选用抗几何攻击性能稳定的图像特征点构造特征向量, 用于待检测图像的几何攻击校正. 而文献 [14] 在遭受几何攻击后失去同步, 破坏了隐藏

(a) Lenna中提取的特征点 ($W = 15$)
(a) Feature points of Lenna ($W = 15$)
(b) Mandrill中提取的特征点 ($W = 15$)
(b) Feature points of Mandrill ($W = 15$)
(c) House中提取的特征点 ($W = 15$)
(c) Feature points of House ($W = 15$)

图 5　从含水印的图像中提取的特征点

Fig. 5　Feature points extracted from watermarked image

(a) 缩放 0.8
(a) Scale 0.8
(b) 缩放 0.8 + 旋转 5°
(b) Scale 0.8 + Rotation 5°
(c) 旋转 45° + 平移 (垂直 30 像素)
(c) Rotation 45° + Translation V30

图 6　含水印图像 Lenna 几何攻击后特征点

Fig. 6　Feature points of watermarked Lenna after geometric attacks

表 2 常规图像攻击时的算法比较 (BER)

Table 2 Watermark detection comparison for common signal processing (BER)

攻击方式	Lenna				Mandrill			
	本文算法	文献 [10]	文献 [11]	文献 [14]	本文算法	文献 [10]	文献 [11]	文献 [14]
无攻击	0	0	0	0	0	0	0.0078	0
JPEG 压缩 (70 %)	0.0273	0.0508	0.0898	0.0312	0.0351	0.0664	0.1211	0.0324
JPEG 压缩 (50 %)	0.0429	0.0742	0.1601	0.0495	0.0576	0.1094	0.2227	0.0497
JPEG 压缩 (30 %)	0.0781	0.1055	0.2422	0.0793	0.0936	0.1367	0.2813	0.0811
高斯滤波	0.0378	0.0837	0.1314	0.0297	0.0578	0.0856	0.0973	0.0528
均值滤波	0.0820	0.1484	0.2539	0.0765	0.0703	0.1172	0.2227	0.0633
高斯噪声	0.0395	0.0952	0.1385	0.0356	0.0534	0.0813	0.1172	0.0594
椒盐噪声 (1.5 %)	0.0313	0.0664	0.2148	0.0561	0.0491	0.0781	0.2383	0.0541
椒盐噪声 + 70 % JPEG 压缩	0.0969	0.1898	0.2734	0.0825	0.1225	0.2133	0.2422	0.1206
高斯滤波 + 70 % JPEG 压缩	0.1129	0.2138	0.2661	0.1027	0.1608	0.2455	0.3156	0.1508
高斯噪声 + 均值滤波	0.0786	0.1211	0.2378	0.0713	0.0842	0.1589	0.2695	0.0811
均值滤波 + 锐化	0.1208	0.1938	0.2792	0.1032	0.1025	0.2172	0.2561	0.1136

表 3 几何攻击时的算法比较 (BER)

Table 3 Watermark detection comparison for geometric attacks (BER)

攻击方式	Lenna			Mandrill		
	本文算法	文献 [10]	文献 [11]	本文算法	文献 [10]	文献 [11]
旋转 5°	0.0039	0.0078	0.0547	0.0039	0.0117	0.0664
旋转 45°	0	0.0039	0.0742	0.0039	0.0078	0.0898
缩放 0.8	0	0	0.0195	0	0	0.0352
缩放 2	0	0	0.0313	0	0	0.0586
平移 (水平 5 像素)	0	0	0.2344	0	0	0.2539
平移 (水平 30 像素)	0	0.0195	0.2109	0	0.0156	0.2266
平移 (垂直 5 像素)	0	0	0.2188	0	0	0.2422
平移 (垂直 30 像素)	0.0039	0.0234	0.2891	0	0.0157	0.3164
局部挤压弯曲	0.0117	0.0478	0.3359	0.0156	0.0352	0.3086
剪切 10 %	0.0156	0.0234	0.0586	0.0195	0.0352	0.0664
旋转 5° + 缩放 2	0.0078	0.0352	0.1758	0.0117	0.0429	0.1406
旋转 45° + 平移 (垂直 30 像素)	0.0039	0.0469	0.2617	0.0078	0.0507	0.2773

信息块序列, 提取水印时无法再现隐藏信息的位置, 因此不具备抵抗几何攻击的能力; 而文献 [10] 利用低阶 Krawtchouk 矩构造 SVR 特征向量, 文献 [11] 利用图像子块像素值方差与总和构造 SVR 特征向量, 这二组特征向量几何不变性较弱, 抵抗剪切、行列移除、局部弯曲的去同步攻击能力差, 因此, 正是基于图像特征点对几何攻击的稳健性和几何形变的协变性, 使本文算法具有较强的抗几何攻击能力.

5 结论和未来的工作

本文提出了一种以图像特征点矢量集为特征向量的回归支持向量机和第二代 Bandelet 变换的抗几何攻击图像水印算法, 对一般的图像攻击与几何攻击具有良好的稳健性. 算法具有如下特点: 1) 水印被嵌入到对应于图像复杂纹理和边缘的大幅值 Bandelet 系数中, 具有良好的透明性和较强的鲁棒性; 2) 抛弃了单纯的 Bandelet 系数操作, 利用统计原则来修改宿主信息, 进一步提高了水印鲁棒性; 3) 在归一化的含水印图像中利用 Harris-Laplace 算子提取具有几何形变鲁棒性的图像特征点, 提高图像对几何攻击的抵抗性; 4) 选用性能稳定的图像特征点构造特征向量, 改善了 SVR 的性能, 提高了水印系统的鲁棒性. 实验表明, 该算法是一种有效的抗几

何攻击鲁棒水印算法.

在今后的工作中, 我们仍然有很多问题亟待解决, 例如增加图像预处理步骤选取纹理丰富的图像, 以进一步提高水印的嵌入容量和鲁棒性; 深入研究神经网络、遗传算法等分类方法在抗几何攻击水印算法设计中的应用, 以进一步提高基于分类的图像几何校正方法的性能. 另外, 由于算法中的 Bandelet 变换、图像特征点提取、SVM 训练等都是比较耗时的过程, 考虑对图像分块等方法以减少 Bandelet 变换和特征点提取的耗时, 提高算法的速度和鲁棒性也将是未来的工作重点.

References

1 Lou Ou-Jun, Wang Zheng-Xuan. A contourlet-domain watermarking algorithm against geometric attacks based on feature template. *Chinese Journal of Computers*, 2009, **32**(2): 308−317
(楼偶俊, 王钲旋. 基于特征点模板的 Contourlet 域抗几何攻击水印算法研究. 计算机学报, 2009, **32**(2): 308−317)

2 Alghoniemy M, Tewk A H. Geometric invariance in image watermarking. *IEEE Transactions on Image Processing*, 2004, **13**(2): 145−153

3 Barni M. Effectiveness of exhaustive search and template matching against watermark desynchronization. *IEEE Signal Processing Letters*, 2005, **12**(2): 158−161

4 Lee H Y, Kim H S, Lee H K. Robust image watermarking using local invariant features. *Optical Engineering*, 2006, **45**(3): 1−10

5 Deng Cheng, Li Jie, Gao Xin-Bo. Geometric attacks resistant image watermarking in affine covariant regions. *Acta Automatica Sinica*, 2010, **36**(2): 221−228
(邓成, 李洁, 高新波. 基于仿射协变区域的抗几何攻击图像水印算法. 自动化学报, 2010, **36**(2): 221−228)

6 Wang Xiang-Yang, Wu Jun, Hou Li-Min. A feature-based digital image watermarking algorithm. *Acta Electronica Sinica*, 2007, **35**(7): 1318−1322
(王向阳, 邬俊, 侯丽敏. 一种基于图像特征点的数字水印嵌入方法. 电子学报, 2007, **35**(7): 1318−1322)

7 Li Lei-Da, Guo Bao-Long, Wu Xiao-Yue. A new spatial domain image watermarking scheme resisting geometric attacks. *Acta Automatica Sinica*, 2008, **34**(10): 1235−1242
(李雷达, 郭宝龙, 武晓钥. 一种新的空域抗几何攻击图像水印算法. 自动化学报, 2008, **34**(10): 1235−1242)

8 Seo J S, Yoo C D. Image watermarking based on invariant regions of scale-space representation. *IEEE Transactions on Signal Processing*, 2006, **54**(4): 1537−1549

9 Tsai H H, Sun D W. Color image watermark extraction based on support vector machines. *Information Sciences*, 2007, **177**(2): 550−569

10 Wang X Y, Xu Z H, Yang H Y. A robust image watermarking algorithm using SVR detection. *Expert Systems with Applications*, 2009, **36**(5): 9056−9064

11 Wang X Y, Yang H Y, Cui C Y. An SVM-based robust digital image watermarking against desynchronization attacks. *Signal Processing*, 2008, **88**(9): 2193−2205

12 Le Pennec E, Mallat S. Sparse geometric image representations with Bandelets. *IEEE Transactions on Image Processing*, 2005, **14**(4): 423−438

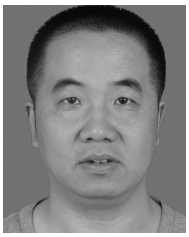
13 Yang Yue-Xiang, Luo Yong, Ye Zhao-Hui, Cheng Li-Zhi. A complete frequency lossless watermarking method via Bandelet and adaptive matrix norm. *Journal of Computer Research and Development*, 2007, **44**(12): 1996−2003
(杨岳湘, 罗永, 叶昭晖, 成礼智. 基于 Bandelet 与自适应矩阵范数的全频域无损水印方法. 计算机研究与发展, 2007, **44**(12): 1996−2003)

14 Liu Xu-Chong, Luo Yong, Wang Jian-Xin, Wang Jie. Watermarking algorithm for image authentication based on second generation Bandelet. *Journal on Communications*, 2010, **31**(12): 123−130
(刘绪崇, 罗永, 王建新, 汪洁. 基于第二代 Bandelet 变换的图像认证水印算法. 通信学报, 2010, **31**(12): 123−130)

15 Mikolajczyk K, Schmid C. Scale & affine invariant interest point detectors. *International Journal of Computer Vision*, 2004, **60**(1): 63−86

16 Alghoniemy M, Tewfik A H. Geometric invariance in image watermarking. *IEEE Transactions on Image Processing*, 2004, **13**(2): 145−153

17 Petitcolas F A P. Watermarking schemes evaluation. *IEEE Signal Processing Magazine*, 2000, **17**(5): 58−64



綦 科 广州大学计算机科学与教育软件学院副教授. 主要研究方向为数字水印, 信息隐藏及分析, 图像处理, 信息安全. E-mail: qikersa@163.com
(**QI Ke** Associate professor at the School of Computer Science and Educational Software, Guangzhou University. His research interest covers digital watermarking, steganography, image processing, and information security.)

谢冬青 广州大学计算机科学与教育软件学院教授. 主要研究方向为网络安全, 可信计算, 密码算法. 本文通信作者.
E-mail: xiedongqing@hotmail.com
(**XIE Dong-Qing** Professor at the School of Computer Science and Educational Software, Guangzhou University. His research interest covers network security, trusted computing and network, and cryptographic algorithm. Corresponding author of this paper.)