

包装印刷

一种新的 SIFT 几何校正的抗几何攻击水印算法

陈青, 陈祥, 姚绍华

(上海理工大学, 上海 200093)

摘要: **目的** 为了提高抗几何攻击水印算法的鲁棒性, 提出一种新的 SIFT 几何校正的抗几何攻击水印算法。**方法** 利用尺度不变特征变换算法分别提取原始图像和受几何攻击图像的特征点, 在水印提取前, 将原始图像和受几何攻击图像进行特征点匹配, 按照匹配的特征点对受几何的攻击图像进行几何校正。在水印嵌入过程中, 结合奇异值分解(SVD)特征值的稳定性和非负矩阵分解(NMF)线性无关性来增强水印图像的鲁棒性。**结果** 文中算法在剪切、JPEG、噪声等攻击下具有很好的鲁棒性, 提取出来的水印图像 NC 值均大于 0.98, 在 RST 攻击下水印图像的 NC 值也能达到 0.97 以上。**结论** 提出的抗几何攻击算法能有效的抵抗各类几何攻击, 具有很好的鲁棒性。

关键词: 数字水印; 小波变换; 奇异值分解; 非负矩阵分解; 特征点匹配; 几何校正; 抗几何攻击

中图分类号: TP391 **文献标识码:** A **文章编号:** 1001-3563(2017)01-0169-05

A New Watermarking Algorithm Against Geometric Attack Based on SIFT Geometric Correction

CHEN Qing, CHEN Xiang, YAO Shao-hua

(University of Shanghai for Science and Technology, Shanghai 200093, China)

ABSTRACT: The work aims to improve watermarking algorithm robustness against geometric attack and propose a new watermarking algorithm against geometric attack based on SIFT geometric correction. First, the feature points of the original image and attacked image were respectively extracted with SIFT. Before watermark extraction, the feature points of the original image and attacked image were matched and the geometric correction of the attacked image was carried out based on the matched feature points. In the embedding process, the robustness of the watermark image was enhanced in combination with the stability of the singular value decomposition (SVD) eigenvalue and the linear independence of non-negative matrix factorization (NMF). The algorithm in the paper was robust in shear, JPEG, noise and other attacks, and the NC value of the extracted watermark was higher than 0.98. The NC value of watermark image under attack of RST could also reach over 0.97. The proposed algorithm against geometric attack can resist all kinds of geometric attacks effectively and also is robust.

KEY WORDS: digital watermarking; DWT; SVD; NMF; feature points match; geometric correction; anti-geometric attacks

数字水印作为一种在网络环境中保护图像、文本、视频版权使用有效的手段, 已经成为了国内外研究的一个热点^[1]。在水印技术中, 由于小波变换(DWT)多分辨率等特性使得小波领域的水印技术近年来广受关注^[2]。小波变换本身不具备几何不变性, 抗几何干扰的效果很差, 对原始图像进行轻微的几何

变换都能够达到破坏水印信息的目的, 因此, 提出一种能够抵抗几何攻击算法尤为重要^[3]。

郑秋梅和顾国民等^[4]提出一种基于 LBS 和图像同步性的抗几何攻击水印算法, 具有很好的抗几何攻击能力, 但在常规攻击下鲁棒性较差。陈青和翁旭峰^[5]提出基于伪 Zernike 矩的图像盲水印算法, 在

收稿日期: 2016-06-14

基金项目: 国家 863 计划 (2012AA050206)

作者简介: 陈青 (1962—), 女, 博士, 上海理工大学副教授、硕导, 主要研究方向为信号处理。

抗旋转攻击上具有很好的鲁棒性。文中提出的水印算法就是在水印提取之前,首先对受到几何攻击的图像利用尺度不变特征变换进行特征点匹配之后进行几何校正,然后提取图像水印信息。在水印嵌入前,对图像分别进行 NMF 变换和 SVD 变换,增强了水印图像的鲁棒性^[6]。同时,在对水印图像小波分解之前,将水印图像进行 Arnold 置乱,从而增强水印图像的安全性。在水印嵌入位置的选择上,基于水印图像不可见性和鲁棒性的综合考虑,将水印图像进行一层小波分解,取其垂直分量 wLH_1 , 水平分量 wHL_1 和近似分量 wLL_1 分别嵌入至载体图像三层小波分解后的第 2 层垂直分量 LH_2 , 第 2 层水平分量 HL_2 和第 3 层近似分量 LL_3 上^[7]。

1 水印算法思想

1.1 非负矩阵分解

非负矩阵分解是一种新的矩阵分解方法,它的目标就是将一个非负矩阵分解成 2 个小矩阵,而数字图像的像素点的值基本上都是非负值^[8-9]。所谓非负矩阵分解就是将一个非负矩阵 A 进行如下转换: $A \approx W \times H$ ^[10]。式中: A 为 $M \times N$ 矩阵; W 为 $M \times r$ 矩阵; H 为 $r \times N$ 矩阵; r 为事先给定的值且 r 小于 M, N 。非负矩阵分解算法提供了一种求解 2 个非负矩阵 W, H 的方法,在 W 和 H 是非负矩阵的约束条件下,使函数 $\|A - W \times H\|^2$ 取极小值,通过对函数的 W, H 分别求导迭代来得到 W, H 的值。此时 $A - W \times H$ 的值为误差矩阵 E ,其迭代过程的收敛性能够保证在复原之后的矩阵 A 依旧为非负矩阵。该算法通过将高维的数据矩阵降维处理,得到一个特定维度的矩阵。算法适合大规模数据处理^[11],因其非负的限制条件,导致了原始图像像素之间只允许进行非负和加性的操作,因此 NMF 算法得到的非负矩阵 W 拥有稀疏性和线性无关性。

1.2 奇异值分解

奇异值分解是一种能满足任意形式的矩阵分解的矩阵分解方式。所谓奇异值分解,就是将一个矩阵进行式(1)转换^[12]。

$$A = USV^T \quad (1)$$

式中: U, V 为正交矩阵,分别为左奇异值阵和右奇异值矩阵; S 为对角矩阵,其对角线上的值就是 A 的奇异值。对于一个图像矩阵,图像的奇异值发生细微的变化并不会影响图像的质量,而且图像遭受攻击之后,其奇异值也不会发生很大的变化,所以奇异值分解具有很好的稳定性^[13]。利用奇异值分解的稳定性可以提高嵌入水印的鲁棒性以及不可见性。

1.3 尺度不变特征变换

尺度不变特征变换(SIFT)是一种用来检测局部

特征的算法, SIFT 特征除了具有尺度不变性之外,还具有一些其他特性,比如改变图像旋转角度或者亮度,仍然能够检测得到好的检测效果^[14-15]。尺度不变特征变换的本质是在构建尺度空间并搜索特征点。该算法实现几何校正的步骤见图 1。提取原始图像和几何攻击之后图像的特征点;对每个特征点附加详细的信息;对比提取出的 2 幅图像的特征点找出相互匹配的特征点;根据匹配的特征点进行几何校正。

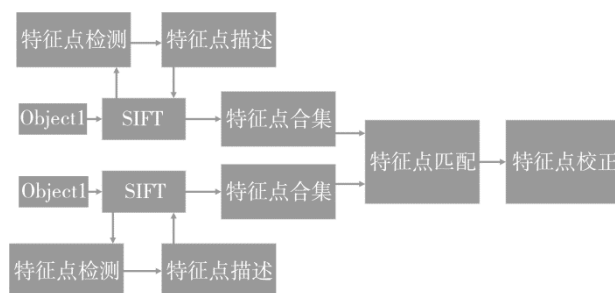


图 1 IFT 算法实现过程

Fig.1 Process block diagram of SIFT algorithm

1.3.1 SIFT 特征值匹配

SIFT 特征匹配是借助特征点之间的相似性度量来进行的^[16]。采用欧氏距离对 SIFT 的特征向量进行匹配,在获取特征向量值后,采用优先 k-d 树进行优先搜索来查找每个特征点的近似最近邻特征点。检测 2 个特征点,如果较短的距离除以次短的距离不高于某个上限值,则接受这一对匹配点。通过更改这个上限值的值,可以控制特征匹配点的数量。上限值变大时匹配点数目变多,产生较多的误匹配点,匹配稳定性变差,反之亦然。大量的实验表明,当比例阈值,即上限值处于 0.4 ~ 0.6 之间时,匹配效果最好。

1.4.2 SIFT 几何校正方式

1) 缩放校正。分别选取 Object1, Object2 中距离最远的 2 个匹配特征点进行欧式计算即可得到其缩放参数 k 的估计^[17]。假设 Object1 所选取的特征点为 $A(a_1, a_2), B(b_1, b_2)$, Object2 所选取的特征点为 $C(c_1, c_2), D(d_1, d_2)$ 。根据式(2)可以得到其缩放参数 k 。

$$k = \frac{\sqrt{(a_1 - b_1)^2 + (a_2 - b_2)^2}}{\sqrt{(c_1 - d_1)^2 + (c_2 - d_2)^2}} \quad (2)$$

2) 旋转校正。旋转过程中,当旋转中心为图像中心点,图像的中心点不会随着图像旋转而产生变换;当旋转中心点不是图像中心点时,旋转过程等价于先将原始图像进行平移,使得旋转点被平移到原始图像的中心点,然后再对图像进行绕中心点的旋转。因此可以利用特征点与图像中心之间的夹角的变化来校正图像的旋转角度。假设图像旋转角度为 θ , Object1 的特征点与 Object1 的中心点之间的夹角为 θ_1 , Object2 的特征点与 Object2 的中心点之间的夹角

为 θ_2 。根据式(3)可以得到其旋转角度 θ 。

$$\theta = |\theta_1 - \theta_2| \quad (3)$$

3) 平移校正。分别选取 Object1 和 Object2 中一对匹配的坐标 $A(a_1, a_2)$, $B(b_1, b_2)$ 。假设图像 Object1 和 Object2 的大小分别为 $M \times N$, $M' \times N'$, Object1 和 Object2 的中心坐标, 即图像的中心点坐标分别为 $O(x, y)$, $O_1(x_1, y_1)$, 其中 $x=M/2$, $y=N/2$, $x_1=M'/2$, $y_1=N'/2$ 。根据式(4)可以得到其平移校准量 Δx , Δy 。

$$\begin{cases} \Delta x = (b_1 - x_1) - (a_1 - x) \\ \Delta y = (b_2 - y_1) - (a_2 - y) \end{cases} \quad (4)$$

2 水印的嵌入与提取

2.1 水印嵌入算法

水印嵌入步骤见图 2。

1) 将二值图像 X 进行 K 次 Arnold 置乱, 解除水印图像像素点之间的空间相关性, 得到 x_1 。

2) 将原始图像进行三层 haar 小波分解, 得到第 3 层近似分量 LL_3 , 第 2 层水平细节分量 HL_2 和第 2 层垂直细节分量 LH_2 。

3) 对 LL_3 , HL_2 , LH_2 进行 NMF 分解, 分别得到 $LL_3 = W_1 \times H_1$, $HL_2 = W_2 \times H_2$, $LH_2 = W_3 \times H_3$, 误差值 $E_1 = LL_3 - W_1 \times H_1$, $E_2 = HL_2 - W_2 \times H_2$, $E_3 = LH_2 - W_3 \times H_3$ 。分别对 W_1 , W_2 , W_3 进行奇异值分解。 $W_1 = U_1 S_1 V_1^T$, $W_2 = U_2 S_2 V_2^T$, $W_3 = U_3 S_3 V_3^T$

4) 将置乱后的二值图像 X_1 进行一层 haar 小波分解, 得到其近似分量 wLL_1 , 水平细节分量 wHL_1 , 垂直细节分量 wLH_1 。

5) 将水印图像 haar 小波分解后的近似分量 wLL_1 嵌入到 LL_3 中, $K_1 = S_1 + a \times wLL_1$; wHL_1 嵌入到 HL_2 中, $K_2 = S_2 + a \times wHL_1$; wLH_1 嵌入到 LH_2 中, $K_3 = S_3 + a \times wLH_1$ 。其中 a 为水印的嵌入强度。

6) 对 K_1 , K_2 , K_3 再进行奇异值分解, 分别得到奇异值矩阵 S'_1 , S'_2 , S'_3 。然后得到嵌入水印之后的 W'_1 , W'_2 , W'_3 。

7) 利用误差值 E_1 , E_2 , E_3 合成非负矩阵, $LL'_3 = W_1 \times H_1 + E_1$, $HL'_2 = W_2 \times H_2 + E_2$, $LH'_2 = W_3 \times H_3 + E_3$ 。

8) LL'_3 , HL'_2 , LH'_2 分别替换原始图像分解之后的第 3 层近似分量 LL_3 , 第 2 层水平细节分量 HL_2 和第 2 层垂直细节分量 LH_2 。然后进行二维小波逆变换得到含水信息的载体图像。

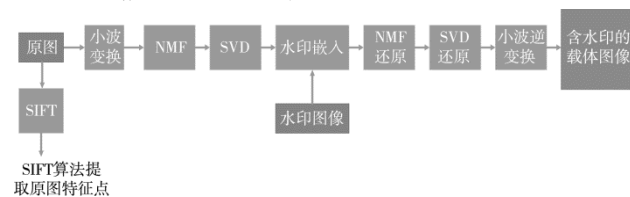


图 2 抗几何攻击水印嵌入过程

Fig.2 Watermark embedding process against geometric attack

2.2 水印提取算法

水印提取步骤见图 3。

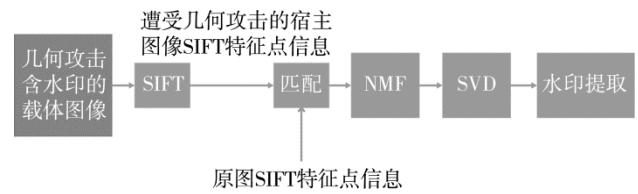


图 3 抗几何攻击水印提取过程

Fig.3 Watermark extracting process against geometric attack

对嵌入水印的载体图像进行三层 haar 小波分解, 得到第 3 层近似分量 LL'_3 , 第 2 层水平细节分量 HL'_2 和第 2 层垂直细节分量 LH'_2 。

对 LL'_3 , HL'_2 , LH'_2 进行 NMF 分解, 分别得到 $LL'_3 = W'_1 \times H'_1$, $HL'_2 = W'_2 \times H'_2$, $LH'_2 = W'_3 \times H'_3$ 。然后分别对 W'_1 , W'_2 , W'_3 进行奇异值分解。 $W'_1 = U'_1 S'_1 V'^T_1$, $W'_2 = U'_2 S'_2 V'^T_2$, $W'_3 = U'_3 S'_3 V'^T_3$ 通过得到的奇异矩阵和原始图像左右奇异矩阵合成 K'_1 , K'_2 , K'_3 。 $K'_1 = U'_1 S'_1 V'^T_1$, $K'_2 = U'_2 S'_2 V'^T_2$, $K'_3 = U'_3 S'_3 V'^T_3$ 计算 wLL'_1 , wHL'_1 , wLH'_1 。 $wLL'_1 = (K'_1 - S_1)/a$, $wHL'_1 = (K'_2 - S_2)/a$, $wLH'_1 = (K'_3 - S_3)/a$ 。

将 wLL'_1 , wHL'_1 , wLH'_1 替换嵌入时置乱后的二值水印图像 W_1 进行一层 haar 小波分解的近似分量 wLL_1 , 水平细节分量 wHL_1 和垂直细节分量 wLH_1 , 利用小波反变换得到未反置乱的二值水印图像 X'_1 。

将 X'_1 进行 Arnold 反置乱, 获得水印图像 X_1 。

对于几何攻击的水印提取算法和上述过程略有不同。在水印嵌入之前, 用 SIFT 算法检测并保存原始图像的特征点; 在含水信息的载体图像遭受几何攻击之后, 利用尺度不变特征变换算法检测并保存检测到的特征点; 利用原始图像的特征点和遭受几何攻击的载体图像的特征点进行特征值匹配并校正; 对已校准的图像利用上述水印提取算法提取水印。

3 实验结果

文中选取 512×512 的 bmp 格式的灰度图“woman”作为原始图像, 选择 64×64 的二值图像“wm64”作为水印图像, 嵌入强度 $a=0.01$, NMF 选用的中间维数 $r=32$ 。通过峰值信噪比 (PSNR) 来直观测量水印图像的不可见性, 通过归一化相关系数 (NC) 来定量分析提取出来的水印图像的鲁棒性。

原始图像和水印图像见图 4a,b, 嵌入水印之后的载体图像见图 5a, 从视觉效果上看, 与原始图像没有明显变化, 计算其 PSNR 值为 46.12, 图像性能良好。在无攻击的情况下提取出来的水印图像见图 5b, 视觉上和原始水印图像无明显变化, 计算其 NC 值为 1, 证明该算法是行之有效的。



图4 原始图像和水印图像
Fig.4 Original image and watermark image



图5 算法结果
Fig.5 The picture of algorithm results

表1 抗常规攻击测试实验结果

Tab.1 Results of experiment against traditional attacks

攻击方式	PSNR	NC值
椒盐噪声(0.01)	24.95	0.9857
高斯噪声(0.01)	20.09	0.9814
JPEG压缩(50%)	38.28	0.9895
裁剪(1/4)	9.28	0.9807
中值滤波	36.97	0.9923
均值滤波	6.22	0.9939
直方图均衡化	18.62	0.9964

表1给出了7种常规的攻击方式,在文中算法下都能完成水印的提取,且其NC值都在0.980以上,证明该算法鲁棒性较好,对常规攻击有很好的抵抗能力。单独测试算法的抗几何攻击能力。未遭受几何攻击时,载体图像有354个匹配特征点。载体图像遭受几何攻击之后进行SIFT算法匹配校正,选择的比例阈值为0.60。

缩放攻击特征点匹配见图6a,含水印的载体图像被放大2倍。放大后的图像像素数量变为 1024×1024 。经过SIFT特征点匹配有237个匹配点,进行几何校正之后提取出来的水印NC值为1。旋转攻击特征点匹配见图6b,旋转角度为 30° 。旋转后的图像像素数量变大,以像素值0填充增大部分,这也导致了特征点无法匹配。经过SIFT特征点匹配有19个匹配点,进行几何校正之后提取出来的水印NC值为0.9983。平移攻击特征点匹配见图6c,将图像平移了[20, 20]像素距离。平移后的图像像素数量变大,以像素值0填充增大部分,这也导致了特征

点无法匹配。经过SIFT特征点匹配后有147个匹配点,进行几何校正之后提取出来的水印NC值为0.9926。旋转平移组合攻击方式特征点匹配见图6d,旋转角度为 30° ,且将图像平移了[20, 20]像素距旋转平移后的图像像素变大。经过SIFT特征点匹配后有16个匹配点,进行几何校正之后提取出来的水印NC值为0.9852。

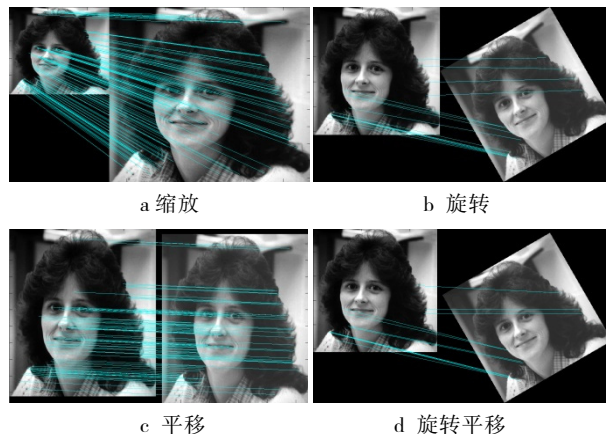


图6 击特征点匹配
Fig.6 Hit feature point matching

表2给出了各种几何攻击方式包括旋转和平移的组合攻击方式,在水印提取之前利用SIFT算法进行几何校正,之后提取出来的水印NC值都比较可观,在面对单一几何攻击时,水印NC值都在0.987以上,表现出了很好的抗攻击能力。

表2 抗几何攻击测试实验结果

Tab.2 Results of experiment against geometric attack

攻击方式(旋转、平移、组合)	NC值(SIFT校正后)
旋转 15°	0.9975
旋转 30°	0.9983
旋转 45°	0.9987
放大2倍	1
放大0.5倍	0.9769
平移[10, 10]	0.9991
平移[20, 20]	0.9926
平移[25, 25]	0.9876
旋转 30° +平移[20, 20]	0.9852
旋转 45° +平移[10, 10]	0.9835

与文献[16]中算法进行比较发现,当攻击方式为旋转攻击,旋转角度为 45° 时,文献[16]提取出水印的NC值为0.9973,而文中算法提取出的水印NC值为0.9987;攻击方式放大2倍攻击时,文献[16]提取出水印的NC值为0.9955,而文中算法提取出的NC值为1,水印图像能够完整的提取出来;当攻击方式为平移攻击时,平移程度为[25, 25]时,文中算法提取出水印的NC值为0.9876,也优于文献[16]提取出

的水印 NC 值。证明文中算法鲁棒性优于前者, 也印证了文中算法的有效性和优越性。

4 结语

文中利用原始图像和受几何攻击图像的特征点, 在水印提取前, 将原始图像和受几何攻击图像进行特征点匹配, 根据匹配的特征点对受几何的攻击图像进行几何校正, 从而校准受几何攻击的图像。同时在水印嵌入过程中, 巧妙地将小波分解嵌入、奇异值分解和非负矩阵相结合, 大大增强了算法的鲁棒性。大量仿真实验结果显示该算法不仅对于常规攻击具有很好的鲁棒性, 对于几何攻击也具有很好的抵抗性, 改善了小波域水印本身所不具备的几何不变性。

参考文献:

- [1] 石永福, 杨得过, 李智. 一种基于小波变换的数字图像水印新算法[J]. 华中师范大学学报(自然科学版), 2013, 47(4): 479—482.
SHI Yong-fu, YANG De-guo, LI Zhi. A New Algorithm of Digital Image Watermarking Based on Wavelet Transform[J]. Journal of Huazhong Normal University (Natural Sciences), 2013, 47(4): 479—482.
- [2] 何冰. 一种基于 DWT 域的彩色图像数字水印算法[J]. 计算机与数字工程, 2011, 39(6): 126—130.
HE Bing. A Color Image Digital Watermarking Algorithm based on DWT Domain[J]. Computer and Digital Engineering, 2011, 39(6): 126—130.
- [3] 陈宁, 黄璐, 马会杰, 等. 基于 SIFT 特征点匹配校正的抗几何攻击水印算法[J]. 电路与系统学报, 2013, 18(2): 158—165.
CHEN Ning, HUANG Lu, MA Hui-jie, et al. An Anti-geo-metric Attack Watermarking Algorithm Based on SIFT Feature Point Matching Correction[J]. Journal of Circuits and Systems, 2013, 18(2): 158—165.
- [4] 郑秋梅, 顾国民, 王玉菲, 等. 一种新的抗几何攻击的数字算法[J]. 中国石油大学学报(自然科学版), 2012, 36(1): 188—192.
ZHENG Qiu-mei, GU Guo-min, WANG Yu-fei, et al. A New Digital Algorithm Against Geometric Attacks[J]. Journal of China University of Petroleum(Edition of Natural Science), 2012, 36(1): 188—192.
- [5] 陈青, 翁旭峰. 一种新的基于伪 Zernike 矩的图像盲水印算法[J]. 计算机应用研究, 2016(9): 1—5.
CHEN Qing, WENG Xu-feng. Novel Blind Image Watermarking Based on Pseudo Zernike Moments[J]. Application Research of Computers, 2016(9): 1—5.
- [6] THIND D K, JINDAL S. A Semi Blind DWT-SVD Video Watermarking[J]. Procedia Computer Science, 2015, 46: 1661—1667.
- [7] 于艳敏. 基于小波域的水印最佳嵌入位置的研究[J]. 数字技术与应用, 2013(10): 88—89.
- [8] 刘如京, 王玲. 一种 NMF 和 SVD 相结合的鲁棒水印算法[J]. 计算机科学, 2011, 38(2): 271—273.
LIU Ru-jing, WANG Ling. A Robust Watermarking Algorithm Combining NMF and SVD[J]. Computer Science, 2011, 38(2): 271—273.
- [9] LEE D D, SEUNG H S. Learning the Parts of Objects by Non-negative Matrix Factorization[J]. Nature, 1999, 401(21): 788—791.
- [10] LI Le, ZHANG Yu-jin. Survey of Non-negative Matrix Factorization Algorithm[J]. Acta Electronica Sinica, 2008, 36(4): 737—743.
- [11] DAN K. A Singularly Valuable Decomposition: The SVD of a Matrix[J]. College Mathematics Journal, 2010, 27(1): 2—23.
- [12] 邱丽红, 张丽艳, 李笑, 等. 基于 DCT-SVD 的抗几何攻击图像水印算法[J]. 大连交通大学学报, 2014, 35(6): 93—96.
QIU Li-hong, ZHANG Li-yan, LI Xiao, et al. An Image Watermarking Algorithm Against Geometric Attack based on DCT-SVD[J]. Journal of Dalian Jiaotong University, 2014, 35(6): 93—96.
- [13] 赵丽红, 王永军, 王佳禾. 双正交提升小波和奇异值分解的彩色水印算法研究[J]. 计算机应用研究, 2014, 31(2): 568—570.
ZHAO Li-hong, WANG Yong-jun, WANG Jia-he. A Research on Color Watermarking Algorithm based on Bi-orthogonal Lifting Wavelet and Singular Value Decomposition[J]. Application Research of Computers, 2014, 31(2): 568—570.
- [14] ZOU Xin-guo, LI Na, NAWEI J. Robust Watermarking Algorithm for Digital Image Based on SIFT Feature Points[C]//Software Engineering and Service Science (ICSESS), 2014 5th IEEE International Conference on, 2014: 27—29.
- [15] 高虎明, 李凯捷, 王英娟. 基于 SIFT 抗几何攻击的数字水印算法[J]. 计算机应用, 2013, 33(3): 748—751.
GAO Hu-ming, LI Kai-jie, WANG Ying-juan. Digital Watermarking Algorithm Against Geometric Attacks Based on SIFT[J]. Computer Applications, 2013, 33(3): 748—751.
- [16] 汪祖辉, 孙刘杰, 蒋哲薇, 等. 一种抗几何攻击的小波域水印算法[J]. 包装工程, 2015, 36(21): 102—107.
WANG Zu-hui, LIU Sun-jie, JIANG Zhe-wei, et al. A Watermarking Algorithm Against Geometric Attacks based on Wavelet Domain[J]. Packaging Engineering, 2015, 36(21): 102—107.
- [17] 廖琪男. 基于 SIFT 特征点匹配的水印图像几何校正算法[J]. 计算机应用研究, 2011, 28(6): 2247—2249.
LIAO Qi-nan. New Watermarked Image Geometric Correction Algorithm based on SIFT Feature Points Matching[J]. Application Research of Computers, 2011, 28(6): 2247—2249.