包装印刷

基于 SIFT 特征点匹配的抗几何攻击水印算法

陈青，柯婷婷
（上海理工大学，上海 200093）

摘要：目的 为了有效抵抗几何攻击，实现水印图像的嵌入与检测的同步。**方法** 将水印嵌入到图像小波分解后的奇异值中，然后利用 SIFT（scale invariant feature transform）特征点所具有的旋转、缩放和平移不变性进行宿主图像和受攻击图像的匹配，并估计受攻击图像的几何攻击参数，对可能失真的图像进行几何校正。**结果** 图像经过几何失真、常规图像处理攻击或 JPEG 压缩后，嵌入的水印依然能被可靠地检测和提取。**结论** 理论分析和大量实验结果表明，该算法校正精度高，具有良好的不可见性和鲁棒性。

关键词：几何攻击；数字水印；SIFT；几何校正
中图分类号：TP391 **文献标识码：**A **文章编号：**1001-3563(2016)23-0146-05

An Image Watermarking Algorithm Resistant to Geometric Distortion Matched Based on SIFT Feature Points

CHEN Qing, KE Ting-ting
(University of Shanghai for Science and Technology, Shanghai 200093, China)

ABSTRACT: The work aims to effectively resist geometric attack, so as to achieve the synchronization between embedding and detection of watermark image. The watermark was embedded into the singular values after wavelet decomposition. Then, SIFT (scale invariant feature transform) feature points characterized by invariance of rotation, scaling and translation were used to match host image and attacked image. The geometric distortion parameters of the attacked image were estimated and the images likely to be distorted were subject to geometric correction. The embedded watermark of the images subjected to geometric distortion, general image processing attacks or JPEG compression could still be reliably detected and extracted. Theoretical analysis and experimental results show that the algorithm has high precision and good invisibility and robustness.

KEY WORDS: geometric attack; digital watermarking; SIFT; geometric correction

近年来，随着数字水印的迅速发展，许多复杂的抗攻击水印系统应运而生，但应对旋转、平移和缩放等几何攻击仍存在很大的困难。设计一种能有效抵抗几何攻击的算法是目前数字水印技术中的热点，也是难点，其中基于图像的不变变换设计水印系统被视为一种有效抵抗几何攻击的方法。Bas[1]通过特征点构造了三角形细分平面，由于提取的特征点过多，稳定性不佳，会导致水印嵌入的三角区域和提取的不匹配。Tang[2]利用 Mexican Hat 小波得到特征点，将水印归一化后嵌入特征点构造的局部圆形区域，由于圆形区域的半径是常数，因而无法有效抵抗缩放攻击。JING Li 等[3,11]根据仿射变

收稿日期：2016-06-01
基金项目：上海自然科学基金(12ZR1420800)；国家 863 计划（2012AA050206）；上海理工大学国家级项目培育课题（16HJPY-MS06）
作者简介：陈青（1962—），女，上海人，博士，上海理工大学副教授、硕导，主要研究方法为信号处理。

换公式矩阵，这种算法精度直接受 3 对匹配特征点精度的影响，会导致算法的随机性较大。CHEN Ning 等[4]根据提取的特征点求得几何参数，由于缩放校正算法中利用尺度因子只能计算同等比例缩放参数，因而对于不同等比例缩放并未考虑。

该算法结合 DWT-SVD 对常规信号攻击具有很好鲁棒性的特点将水印嵌入到宿主图像，利用图像 SIFT 匹配点对应坐标之间的直接关系，计算出几何攻击的参数，并进行校正，校正后的图像只会造成微小的几何攻击，降低了水印提取带来的误差。实验结果表明，此水印图像在经受了几何失真和常规信号处理攻击仍可有效地检测出水印。

1　SIFT 特征点匹配

1.1　SIFT 特征点生成

SIFT 算法在空间尺度寻找最佳极值点，提取位置，尺度，旋转不变量，获得图像的局部特征。一副二维图像的尺度空间定义为：

$$L(x,y,\sigma)=G(x,y,\sigma)*I(x,y) \tag{1}$$

式中：*为卷积运算；(x,y)为图像的像素坐标；σ 为尺度空间因子；$G(x,y,\sigma)$为尺度可变高斯函数，其定义见式(2)。

$$G(x,y,\sigma)=\frac{1}{2\pi\sigma^2}\mathrm{e}^{-(x^2+y^2)/2\sigma^2} \tag{2}$$

为了有效地在尺度空间检测到稳定的关键点，提出了高斯差分尺度空间（DOG scale-space），利用不同尺度的高斯差分核与图像卷积生成，见式(3)。

$$D(x,y,\sigma)=(G(x,y,k\sigma)-G(x,y,\sigma))*I(x,y)=L(x,y,k\sigma)-L(x,y,\sigma) \tag{3}$$

DOG 空间的每个像素点要与它相邻尺度域内的 8 个相邻点和上下对应的 18 个点共 26 个点进行比较，局部极大值和极小值组成了关键点。由于 DOG 算子会产生较强的边缘效应，因此可以通过获取特征点处的 Hessian 矩阵剔除不稳定的边缘点。矩阵 $\boldsymbol{H}$ 如下:

$$\boldsymbol{H}=\begin{bmatrix} D_{xx} & D_{xy} \\ D_{xy} & D_{yy} \end{bmatrix} \tag{4}$$

特征点稳定性表示如下：

$$S=\frac{(D_{xx}+D_{yy})^2}{D_{xx}D_{yy}-D_{xy}^2}<\frac{(r+1)^2}{r} \tag{5}$$

式中：r 为 Hessian 最大特征值和最小特征值的比率，用来控制特征点的稳定性；D_{xx}，D_{yy}，D_{xy} 为尺度空间图像的二阶导数。

1.2　特征点的描述子

为了使描述子具有旋转不变性，利用图像的局部特征给每个特征点指定一个主方向，局部结构的稳定方向通过图像梯度的方法求取。梯度的模值和方向如下：

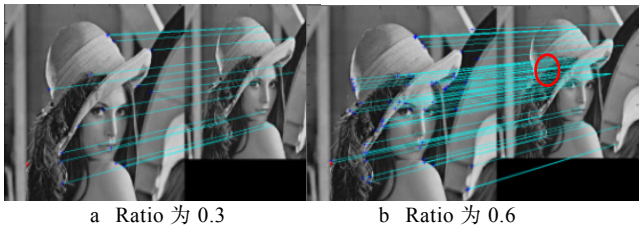
$$m(x,y)=\sqrt{[L(x+1,y)-L(x-1,y)]^2+[L(x,y+1)-L(x,y-1)]^2} \tag{6}$$

$$\theta(x,y)=\arctan\frac{L(x,y+1)-L(x,y-1)}{L(x+1,y)-L(x-1,y)} \tag{7}$$

计算出主方向后，将特征点所在尺度空间的像素均旋转一个主方向的角度，确保图像的旋转不变性。此后，把周围的像素点分为 4×4 个子块，然后计算 8 个方向的梯度强度的直方图，共 128 维的信息表征。

1.3　SIFT 特征点匹配

SIFT 特征描述子的欧式距离作为 2 幅图像特征点的相似性判定度量。取原图像的某个关键点，并找出与其要匹配图像欧式距离最近的前 2 个关键点，在这 2 个关键点中，如果最近的距离除以次近的距离小于阈值 Ratio，则匹配成功。大量实验表明，Ratio 取值在 0.3 ~ 0.6 之间最适宜，ratio 越小 SIFT 匹配点数目越少，但匹配点更加稳定，反之，匹配点数目增加，但是误匹配点的数量也随之增加。Ratio 分别为 0.3 和 0.6 的 512×512 和 384×384 Lena 图像匹配情况见图 1。图 1b 中圆圈处，原图像多个不同的特征点匹配到了一点，显然有大量的误匹配点，而图 1a 就已经去除了这些误匹配点。



a　Ratio 为 0.3　　b　Ratio 为 0.6

图 1　阈值不同时的图像匹配点

Fig.1 Image match points at different threshold values

2　SIFT 特征点几何校正

设原图像特征点集 $\boldsymbol{R}$ 中任意两特征点 $r_i(x_i,y_i)$ 和 $r_j(x_j,y_j)$，几何攻击后的失真图像匹配的特征点为 $r_i'(x_i',y_i')$和 $r_j'(x_j',y_j')$

2.1 旋转校正

根据上述方法提取图像的 SIFT 特征点并进行匹配后，假设嵌入水印后的图像与攻击后的图像之间的匹配对个数为 R，易知图像旋转角度也是 2 幅图像特征点分别所成向量的旋转角度，利用向量夹角式(8)，求出每组旋转角度。由于会存在误匹配点，利用折线图去掉差异较大的旋转角度，然后求取平均角度，见式(9)。

$$\beta_i=\arccos\frac{(x_i-x_j)(x_i'-x_j')+(y_i-y_j)(y_i'-y_j')}{\sqrt{(x_i-x_j)^2+(y_i-y_j)^2}\sqrt{(x_i'-x_j')^2+(y_i'-y_j')^2}} \tag{8}$$

$$\beta=\frac{1}{n}\sum_{i-1}^{n}\beta_i, i\le R-1, n\le R-1 \tag{9}$$

2.2 缩放校正

文献[4]利用尺度因子只能校正等比例缩放的图像。图像长宽的缩放倍数与 2 幅图像每组特征点向量横纵坐标的比值是等同的。根据任意 2 组匹配点之间对应的位置关系估计长宽的缩放参数，记为 α_x，α_y。对于每一组(α_x, α_y)，都在斜率为 α_x/α_y 的正比例函数上，去掉偏离函数较大的点即误匹配点，然后分别求取长宽缩放的平均值，见式(10)。

$$\partial_x=\frac{|x_i-x_j|}{|x_i'-x_j'|}\ ,\partial_y=\frac{|y_i-y_j|}{|y_i'-y_j'|} \tag{10}$$

2.3 平移校正

图像平移的距离也是 2 幅图像每对匹配点横纵坐标的差值。由于会存在错误的匹配点，利用横纵坐标 2 条折线图，去掉波动较大的值，然后求取横纵坐标平移的平均值：

$$\begin{cases}\Delta x=x_i-x_i'\\ \Delta y=y_i-y_i'\end{cases} \tag{11}$$

3 水印算法

3.1 水印嵌入

1）水印数据相关性较强，不适合直接嵌入。利用混沌序列对水印数据进行调制，使得水印信号具有伪随机性，从而增强了水印的随机性和安全性。

2）对宿主图像进行一级小波变换，将低频子带 LL 按 8×8 分块，则低频子带最大能嵌入水印为 1024 bit，对每个分块进行 SVD 处理，$\boldsymbol{B}_i=\boldsymbol{U}_i\boldsymbol{S}_i\boldsymbol{V}_i^{\mathrm{T}}$，$\boldsymbol{U}$ 为一个 $N\times N$ 的方阵，$\boldsymbol{V}^{\mathrm{T}}$($\boldsymbol{V}$ 的转置)为一个 $N\times N$ 的矩阵，将对角矩阵 $\boldsymbol{S}_i$ 的奇异值按降序排列。

3）按下列算法修改每一个分块的第一个奇异值，其中 $Z=\sigma_1\bmod(q)$。当 $W_{(i,j)}'=0$，则有：

$$\begin{cases}\sigma_1'=\sigma_1-Z+\dfrac{5q}{4}, Z\ge 3q/4\\ \sigma_1'=\sigma_1-Z+\dfrac{q}{4}, \text{else}\end{cases} \tag{12}$$

当 $W_{(i,j)}'=1$，则有：

$$\begin{cases}\sigma_1'=\sigma_1-Z+\dfrac{3q}{4}, Z\ge q/4\\ \sigma_1'=\sigma_1-Z-\dfrac{q}{4}, \text{else}\end{cases} \tag{13}$$

q 为量化步长，$W_{(i,j)}'$混沌加密后的水印信息，嵌入后的图像分块为 $\boldsymbol{B}_i'=\boldsymbol{U}_i\boldsymbol{S}_i'\boldsymbol{V}_i^{\mathrm{T}}$。

4）重复步骤 3），嵌入所有水印后，进行小波重构，得到嵌入水印信息宿主图像。

5）提取嵌入水印后图像的特征点，记特征点集为 $\boldsymbol{T}$。

3.2 水印嵌提取

该算法水印的提取不需要宿主图像的参与，提取过程如下所述。

1）对受攻击的图像提取特征点，与特征点集 $\boldsymbol{T}$ 进行匹配，然后按照 2 节的方法进行几何校正，校正后的图像只是受到了微小的几何攻击，极大降低了几何失真的程度。

2）攻击后的图像进行一级小波变换，将低频子带 LL 按 8×8 分块，对每一个 8×8 块进行 SVD 处理，$\boldsymbol{B}_i'=\boldsymbol{U}_i\boldsymbol{S}_i'\boldsymbol{V}_i^{\mathrm{T}}$，将对角矩阵 $\boldsymbol{S}_i'$的奇异值按降序排列。

3）按如下规则提取水印信号，其中 $Z=\sigma_1'\bmod(q)$。

$$\begin{cases}W_{(i,j)}'=0, Z\le q/2\\ W_{(i,j)}'=1, \text{else}\end{cases} \tag{14}$$

4）重复步骤 2），3），直到提取出所有的水印信息。将提取出的 W'进行解密即可得到最终恢复出的水印图像。

4 实验结果与分析

4.1 几何攻击校正测试

512×512 的灰度图像 Lena 作为原始图像，32×32 的二值图像作为水印图像。表 1 列出了旋转校正测试得到的数据，以不改变图像大小的逆时针

旋转为例，采用双线性差值。对比文献[4]和[5]的数据，可以看出该旋转校正算法具有很高的准确性。

表 1　旋转校正测试
Tab.1 Rotation correction test

(°)

实际旋转角度	校正角度		
	文中	文献[5]	文献[4]
10	10.0118	9.8517	9.995
20	19.9905	20.1487	—
30	29.9968	30.0125	30.060
40	39.9788	40.0086	—
60	60.9466	—	—
80	80.3621	—	—
90	90.1393	—	90.344

该算法考虑了长宽方向同等比例和不同等比例的缩放，大大增强了几何攻击的鲁棒性。实验随机选取几组缩放后的图像数据进行校正。表 2 是实际缩放值与计算所得值的对比，算法具有较高的准确率。由于图像缩小过程中的抽样导致了部分图像像素信息的丢失，因此准确率相对图像放大时较低。

表 2　缩放校正测试
Tab.2 Scale correction test

实际缩放像素大小	实际缩放比例矩阵	校正缩放比例矩阵
320×240	[1.6125,2.15]	[1.6156,2.1756]
256×512	[2,1]	[2.0181,1.0318]
384×384	[1.3333,1.3333]	[1.3114,1.4224]
640×500	[0.8,1.024]	[0.8023,1.0414]
640×640	[0.8,0.8]	[0.8154,0.8127]

平移校正的数据见表 3。由于图像的平移只能以像素为单位，所以对计算的值取整得到校正量。大量实验表明，当横纵方向平移量之比为 1∶1 时，校正量的精确度为 100%。对比文献[4], [12]的数据，明显有了很大的提高。

表 3　平移校正测试
Tab.3 Translation correction test

实际平移矩阵[*x*, *y*]	校正平移矩阵	取整校正值
[150,100]	[149.9931,99.9871]	[150,200]
[220,70]	[219.9277,69.9784]	[220,70]
[150,240]	[149.9816,239.9848]	[150,240]
[200,284]	[198.5763,284.5518]	[199,285]
[120,120]	[120,120]	[120,120]

4.2　抗攻击实验结果

实验采用 516×516 的 Lena 灰度图像作为原始图像，水印图像采用大小为 32×32 的二值图像，见图 2。大量实验表明，当 q=115 时，水印的不可见性和鲁棒性达到一个平衡点，图 2d 为嵌入水印信息后的图像。含水印图像与原始载体间的峰值信噪比为 41.887，图像质量没有明显下降。

a 载体图像　b 原始水印图像
c 提取出的水印　d 含水印图像

图 2　数字水印嵌入提取图像比较
Fig.2 The comparison of watermark embedding and extracting

归一化相关系数 NC 度量实验抗攻击的效果。NC 值越大，提取出的水印越完整，水印的鲁棒性越好。实验结果与文献[6]进行数据比较，见表 4。从结果可知，文中算法大部分 NC 值都大于文献[6]的 NC 值，尤其是在缩放攻击方面具有绝对的优势。

表 4　旋转攻击实验结果
Tab.4 Results of rotation attack

旋转角度/(°)	NC值	
	文中算法	文献[6]
0	1.000	1.000
20	0.989	0.971
40	0.989	0.986
60	0.989	0.989
80	0.986	0.988
90	0.994	1.000

缩放攻击中，由于图像缩小，丢失了像素信息，会给图像带来比较大的失真，所以缩放尺度等于 0.5 时，得到的 NC 值都不高。文中算法还考虑了不同等比例的缩放，实验结果也比较理想，见表 5。

组合攻击中，加入了平移攻击，比文献[6]考虑的情况更多，也更加说明了文中算法的可行性，其中 R, S, T 分别代表旋转、缩放、平移攻击，结果见表 6。

表 5 缩放攻击实验结果
Tab.5 Results of scale attack

缩放尺度比例	NC值	
	文中算法	文献[6]
0.5×0.5	0.7506	0.618
0.75×0.75	0.9304	0.898
1.25×1.25	1.0000	1.000
2.0×2.0	1.0000	1.000
1.5×0.5	0.8607	—
0.5×1	0.8909	—

表 6 组合攻击实验结果
Tab.6 Results of compounding attack

组合攻击	NC值	
	文中算法	文献[6]
R: 10°, S: 0.75×0.75	0.8945	0.886
R: 30°, S: 1.5×0.5	0.9536	0.978
R: 50°, S: 0.75×0.75	0.9042	0.886
R: 50°, S: 1.5×0.5	0.9230	0.952
R: 30°, T: [100,150]	0.9548	—
S: 0.75×0.75, T: [220,70]	0.9788	—

常规信号处理攻击包括有损压缩、添加噪声、图像滤波等。对各类型攻击选择不同参数进行实验，结果见表 7。结果表明该算法对于信号处理攻击同样具有很好的鲁棒性，比文献[7—10]效果更好，也说明了该算法本身具有对噪声不敏感的优良特性。

表 7 常规信号攻击实验结果
Tab.7 Results of common signal attack

	参数	NC值	
		文中算法	文献[6]
高斯噪声	0.010	0.9751	0.9751
	0.015	0.8872	0.8872
	0.020	0.8758	0.8758
中值滤波	3×3	0.9921	1.000
	5×5	0.9392	0.967
	7×7	0.9114	0.719
JPEG压缩	50	1.0000	1.000
	30	1.0000	1.000
	20	0.9912	0.984

5 结语

文中针对抗几何攻击鲁棒性差的问题，在基于图像 SIFT 变换的基础上结合 DWT-SVD（效果比文献[13—15]更佳）算法对常规信号具有较好鲁棒性的特点，实现了水印的盲提取。SIFT 算子提取出的图像局部特征点能在几何攻击及常规信号攻击下保持一定的稳定性，利用这种稳定的特征点作为几何失真校正的模板，能够有效估计几何变换参数。同时在频域中嵌入水印，既保证了图像的不可见性又增强了图像的鲁棒性。大量实验数据表明，该算法对几何攻击及三者的组合攻击都具有很好的鲁棒性，同时也适用于应对常规信号处理攻击。

参考文献：

[1] BAS P, CHASSERY J M, MACQ B. Geometrically Invariant Watermarking Using Feature Points[J]. IEEE Transactions on Image Processing, 2002, 11(9): 1014— 1028.

[2] TANG C W, HANG H M. A Feature-Based Robust Digital Image Watermarking Scheme[J]. Signal Processing IEEE Transactions on, 2003, 51(4): 950—959.

[3] JING Li. Robust Image Watermarking Method in Wavelet Domain Based on SIFT Features[J]. Application Research of Computers, 2009, 26(2): 766—768.

[4] CHEN Ning, HUANG Lu, MA Hui-jie. Anti Geometric Attacks Watermarking Algorithm Based on SIFT Feature Point Matching Correction[J]. Journal of Circuit and System, 2013, 18(2): 159—165.

[5] 何利英, 李智勇, 刘伟灵, 等. 基于 SIFT 特征点的几何失真数字水印算法[J]. 计算机工程与应用, 2007, 43(13): 58—60.
HE Li-ying, LI Zhi-yong, LIU Wei-ling, et al. Watermarking Algorithm Robust to Geometic Distortion Based on SIFT Feature Points[J]. Computer Engineering and Application, 2007, 43(13): 58—60.

[6] CHEN Qing, WENG Xu-feng. Novel Blind Image Watermarking Based on Pseudo Zernike Moments[J]. Application Research of Computers, 2016(9): 1—5.

[7] LIAO Qi-nan. Based on SIFT Feature Point Matching Watermark Image Geometric Correction Algorithm[J]. Computer Applications, 2011, 28(6): 2247—2249.

[8] GAO Hu-ming, LI Kai-jie, WANG Ying-juan. Digital Watermarking Algorithm Based on SIFT Resistance to Geometric Attack[J]. Journal of Computer Applications, 2013, 33(3): 748—751.

[9] WANG Ruo-yu. Digital Watermarking Algorithm Based on SIFT Research[D]. Wuhan: Huazhong University of Science and Technology, 2011.

[10] 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, SUN Liu-jie, JIANG Zhe-wei, et al. A Watermarking Algorithm Against Geometric Attack in DWT Domain[J]. Packaging Engineering, 2015, 36(21): 102—107.

[11] OWALLA F O, MWANGI E. A Colour Image Watermarking Technique Resistant to Affine Geometric Attacks[J]. AFRICON, 2013: 1—5.

[12] ZHAO Li-hui, YANG Hong-zhe, GUO Dong, et al. Method to Reduce Matching Range in Print Detection Based on SIFT Algorithm[J]. Packaging Engineering, 2013, 34(17): 104—107.

[13] SINGH C, RANADE S K. Image Adaptive and High-capacity Watermarking System Using Accurate Zernike Moments[J]. Institution of Engineering and Technology, 2014, 8(7): 373—382.

[14] 王瑶, 尤丽华, 吴静静, 等. 基于改进 SIFT 的图像快速自适应匹配算法[J]. 包装工程, 2014, 35(11): 96—104.
WANG Yao, YOU Li-hua, WU Jing-jing, et al. Fast Adaptive Image Matching Algorithm Based on Improved SIFT[J]. Packaging Engineering, 2014, 35(11): 96—104.

[15] YE Tian-yu. Perfectly Blind Self-embedding Robust Quantization-based Watermarking Scheme in DWT-SVD Domain[J]. Journal of Image and Graphics, 2012, 17(6): 644—650.