包装印刷

基于 SIFT 的 NSCT 域抗几何攻击水印算法

陈青，王飞
（上海理工大学，上海 200093）

摘要：目的 针对基于尺度不变特征变换(SIFT)的抗几何攻击图像水印算法在图像匹配时容易产生误匹配，影响提取水印的鲁棒性，提出一种改进的 SIFT 图像水印算法。**方法** 先对载体图像进行两级非下采样 Contourlet 变换(NSCT)，利用中间值量化算法把水印信息嵌入低频系数的方向子带中。图像匹配时利用广义霍夫变换删除误匹配特征点对，提高匹配精度。根据筛选后的特征点匹配对估算几何失真参数，对含水印的载体图像进行几何校正并提取水印，从而实现水印的抗几何攻击。**结果** 实验数据表明对原始特征点匹配对进行筛选后,至少提高了 6.8%的匹配精度,提取水印的 NC 值平均达到 0.9 以上。**结论** 文中提出的改进算法不仅对几何攻击和常规信号攻击均具有较好的鲁棒性，还能保证水印的不可见性。

关键词：尺度不变特征变换；非下采样 Contourlet 变换；广义霍夫变换；几何攻击
中图分类号：TS801.1 **文献标识码：**A **文章编号：**1001-3563(2017)05-0178-05

NSCT-domain Watermarking Algorithm Robust to Geometric Attacks Based on SIFT

CHEN Qing, *WANG Fei*
(University of Shanghai for Science and Technology, Shanghai 200093, China)

ABSTRACT: The work aims to propose an improved SIFT image watermarking algorithm with respect to the mismatching caused by the image watermarking algorithm robust to geometric attacks based on scale invariant feature transform (SIFT) when the images are matching. Firstly, the carrier image was subject to two-stage non-subsampled Contourlet transform (NSCT) and the watermarking information was embedded into the directional subbands with low-frequency coefficient through mean-value quantitative algorithm. When the images are matching, the generalized Hough transform was used to remove the mismatched feature point pairs to improve the matching accuracy. The geometric distortion parameters were estimated according to the screened feature point pairs. The carrier images with watermarks were subject to geometric correction and watermark extraction, so as to achieve the watermarking robust to geometric attacks. The experimental data indicated that, after the matching pairs of the original feature points were screened, the matching precision was improved at least by 6.8% and the average NC values of extracted watermark were all above 0.9. The results show that the improved algorithm proposed herein can not only resist the geometric attacks and normal signal attacks, but also guarantee the invisibility of watermarks.

KEY WORDS: SIFT; NSCT; generalized Hough transform; geometric attack

随着互联网和信息技术的日益发展，保护数字多媒体作品版权、保证信息安全和可进行内容认证的数字水印技术一直是热门研究方向，其中，抗几何攻击水印技术一直是鲁棒水印技术研究中的热点和难点。目前大多数水印算法对噪声、滤波等常规信号攻击有很好的鲁棒性，但抗旋转、缩放、平移、剪切等几何攻击的鲁棒性不太理想，这是因为几何攻击破坏了载体图像和水印之间的同步性，水印信息虽然存在于载体图像中，但水印的嵌入位置发生了变化，导致水印难以被提取。由于图像特征点无论受到常规攻击还是

收稿日期：2016-07-06
基金项目：上海自然科学基金（12ZR1420800）；上海理工大学国家级项目培育基金（16HJPY-MS06）
作者简介：陈青（1962—），女，博士，上海理工大学副教授，主要研究方向为图像处理。

几何攻击均能保持较好的稳定性，因此基于图像特征点的第 2 代数字水印技术得到广泛的应用。

常见的图像特征点[1—4]有 Harris，SUSAN，Harris-Laplace，SIFT 等。其中，SIFT 特征点由于在对旋转、缩放、尺度、光照、噪声等因素均具有不变性和实时性被广泛地应用在目标识别、医学图像、图像水印、人脸识别等方面。文献[5]是将水印信息嵌入载体图像的 DCT 域中，并且从空域提取特征点进行特征点匹配，求出仿射变换参数，从而对失真图像进行几何校正，并提取出水印信息。文献[6]是将水印信息嵌入载体图像的 DWT 域中，并从重构小波参数中提取特征点，实现图像匹配后水印信息的提取。文献[7]算法是选择载体图像的内切圆的内接正方形作为水印的嵌入区域，通过量化图像小波域的分块奇异值矩阵进行水印嵌入，最后利用 SIFT 特征点对图像可能遭受的几何攻击进行校正。以上文献算法均具有不足之处，在空域提取出的图像特征点容易受到滤波、光照、噪声等影响，图像匹配时形成错误的匹配对，会造成仿射参数的求解结果有一定的误差；小波变换的方向表示性非常有限，无法有效地表示图像轮廓及边缘信息，因此利用小波域提取图像特征点估算仿射变换参数值具有不稳定性。针对以上问题，文中提出一种基于 SIFT 的 NSCT 域数字图像水印算法，算法在图像的 NSCT 域低频系数中选取 SIFT 特征点，并对匹配特征点进行筛选，提高匹配结果准确性的同时又能有效提高水印抗几何攻击的鲁棒性和不可见性。

1　相关理论

1.1　SIFT 算法

SIFT 算法[8]是一种图像局部特征的提取方法，提取的图像特征对图像的旋转、尺度缩放、亮度变化等均具有不变性。

1.1.1　构建高斯差分(DOG)尺度空间

首先建立图像 $I(x, y)$的尺度空间 $L(x, y, \delta)$，二维图像的尺度空间是由图像和不同尺度 δ 的高斯核函数 $G(x, y, \delta)$的卷积：

$$L(x,y,\delta)=G(x,y,\delta)\cdot I(x,y)$$

$$G(x,y,\delta)=\frac{1}{2\pi\delta^2}\exp(-\frac{x^2+y^2}{2\delta^2})$$

为了提取有效而且稳定的 SIFT 特征点，需要构建高斯差分(DOG)尺度空间，DOG 尺度空间是由相邻尺度的尺度空间之差组成的。

1.1.2　提取特征点

DOG 尺度空间的每个采样点要和它同尺度 8 个相邻点以及上下相邻尺度的 18 个相邻点进行比较，如果这个点在这 26 个点中是最大或最小值时，该采样点可以被当作图像当前尺度的一个特征点。为了保证提取的特征点具有稳定的匹配和抗噪声能力，对提取的特征点集运用拟合三维二次函数去除低对比度的特征点和不稳定的边缘响应点。

1.1.3　生成特征点描述子

首先为每个特征点计算一个方向，根据这个方向利用特征点邻域像素的梯度方向分布特性为每个特征点指定方向参数，使特征点描述子具有旋转不变性。然后对坐标轴进行旋转，使其方向为特征点的方向，并以特征点为中心选取 16×16 像素大小的模块，将模块划分为 16 个 4×4 像素大小的子块，每个子块可以看成一个种子点，计算每个种子点的梯度方向直方图，绘制每个梯度方向的累加值，且每个种子点具有 8 个方向向量信息，这样就产生了 128 个数据来描述一个特征点，即形成 128 维的 SIFT 特征点描述子，最后对描述子进行归一化，用以消除光照对图像的影响。

1.2　几何校正

利用仿射变换模型可以校正几何失真后的图像。仿射变换模型可以通过一系列原子变换的复合实现图像经常遭受的旋转、缩放、平移等几何攻击，其变换矩阵为：

$$\boldsymbol{T}=\begin{bmatrix} s\cos\theta & s\sin\theta & 0 \\ -s\sin\theta & s\cos\theta & 0 \\ \delta_x & \delta_y & 1 \end{bmatrix}$$

式中：s 为尺度变换参数；θ 为旋转角度；δ_x，δ_y 分别为 x 与 y 方向上的平移量。失真前图像像素坐标(w, z)和失真后像素坐标(x, y)之间的映射关系为：

$$\begin{bmatrix} x \\ y \end{bmatrix}=\begin{bmatrix} \sigma_x \\ \sigma_y \end{bmatrix}+\begin{bmatrix} s\cos\theta & s\sin\theta \\ -s\sin\theta & s\cos\theta \end{bmatrix}\begin{bmatrix} w \\ z \end{bmatrix}$$

首先利用失真前后图像进行匹配得出特征点匹配对集合，通过特征点匹配对集合求出仿射变换矩阵的相关参数值，对失真后的图像进行几何校正。

1.3　广义霍夫变换

霍夫变换[9]是图像处理中用于识别图像区域边界形状的方法，常用来检测图像中直线、圆、椭圆等形状，广义霍夫变换[10]是霍夫变换的改进，可以检测任意形状。运用广义霍夫变换可以检测目标图像是否包含已知图像的相关信息。具体实现方法是将在图像空间的检测转换到参数空间中去，通过参数空间的转换，可以把对目标图像的检测问题转换为查找转换矩阵的问题，通过该转换矩阵可以检测到目标图像中包含已知图像相关信息的位置，从而目标图像和已知图像可实现信息的位置匹配，即只要求出转换矩阵的参数值，那么已知图像的相关信息在目标图像中的位置也就确定了。广义霍夫变换是按照局部度量来计算全

面描述参数，因此具有很高的容错性和鲁棒性。

1.4 NSCT

非下采样 Contourlet 变换是由 Cunha 等[11]于 2005 年提出的一种新的多尺度变换，该变换不仅具有小波变换的所有优点，还具有多方向性、各向异性和平移不变性，同时还注重图像的相位信息和幅值信息，不会出现 Contourlet 变换中的频谱混淆现象，具有良好的时频局部化特征。NSCT 所有高频系数以及低频系数尺寸大小都和原始图像尺寸大小相同，这样对图像的细节信息有着很好的表达，并能提高图像分解和重构的精度，便于水印的嵌入，因此被广泛应用于数字水印领域。NSCT 首先对图像运用非采样塔式滤波器组进行多尺度分解，然后对得到的各尺度子带图像用非抽样方向滤波器组进行方向分解。NSCT 滤波器结构和方向滤波器组见图 1。

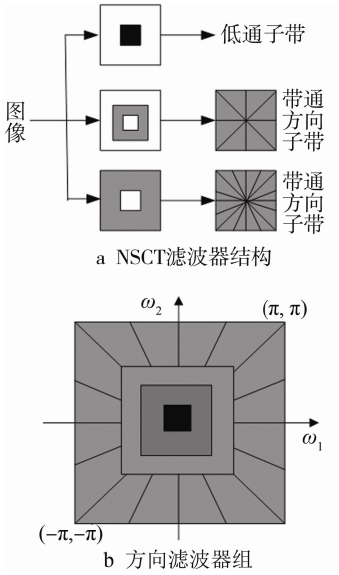

图 1 非下采样 Contourlet 变换

Fig.1 Nonsubsampled contourlet transform

1.5 中间值量化算法

文中采用中间值量化算法[12]向载体图像嵌入水印信息，该算法是利用相同尺度下 3 个不同的方向子带的小波系数值之间的关系，同时生成一个密钥来指定子带嵌入水印的确切位置，密钥包含的是随机生成一组 0，1 序列，0 表示该位置不能嵌入水印，1 表示该位置可以嵌入水印。具体量化方法如下所述。

1) 对原始图像进行 L 级 NSCT 变换，在第 l 尺度下选择 3 个方向子带，其中，方向子带的分辨率和载体图像分辨率相同。假设第 k 个子带图像为 $f_{l,k}$，其中 k={1, 2, 3}。

2）当密钥值为 1 时，表示方向子带坐标(m, n)处可以嵌入水印信息，否则表示当前坐标(m, n)不能嵌入水印信息。

3）当向坐标(m, n)嵌入水印信息时，需要比较 3 个方向子带在坐标(m, n)处系数值的大小关系。对当前位置坐标(m, n)上的 3 个子带的系数值进行排序，满足关系式：

$$f_{l,k_1}(m,n) \le f_{l,k_2}(m,n) \le f_{l,k_3}(m,n)$$

式中：k_1, k_2, k_3∈{1，2，3}且 k_1, k_2, k_3 取值各不相同。

4)计算量化步长 Δ。$\Delta=(f_{l,k_3}(m,n)-f_{l,k_1}(m,n))/(q-1)$，对中间值 $f_{l,k_2}(m,n)$ 进行量化，见图 2。其中 q 值是根据实际情况决定的，一般情况下 q 值取 8。q 值越大，表示量化步长越小，水印的不可见性越好，但抗攻击性越差。

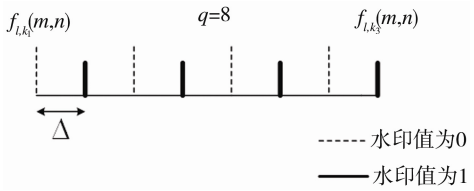

图 2 水印量化

Fig.2 Quantization watermarking

5）当水印值为 1 时，将中间值 $f_{l,k_2}(m,n)$ 量化到图 2 中黑实线所对应的值；当水印值为 0 时，则量化到虚线所对应的值。

2 水印嵌入和提取算法

文中算法是在参考相关文献[13—17]的基础上，采用将水印信息嵌入载体图像 NSCT 域低频系数的方向子带中，同时利用 SIFT 算法实现水印的抗几何攻击。载体图像经过两级 NSCT 变换后，利用中间值量化算法将水印信息嵌入低频系数的方向子带上，可以进一步提高算法的鲁棒性和不可见性。当含水印的载体图像遭到几何攻击时，分别从受攻击后载体图像和原始载体图像的 NSCT 域低频系数中提取 SIFT 特征点，进行图像匹配，并对几何失真的载体图像进行校正，从而实现水印信息具有抵抗几何攻击的能力。

2.1 水印的嵌入

设载体图像 I 尺寸大小为 M×N，水印图像 w 尺寸大小为 m×n。首先对水印图像 w 进行为 Arnold 置乱，置乱后水印图像为 w_0，保存置乱次数；然后对图像 I 进行两级 NSCT 变换，将水印信息 w_0 利用中间值量化算法嵌入低频系数的 3 个方向子带中；再对低频系数和该尺度下的已嵌入水印信息的方向子带进行重构，对重构后的新尺度的低频系数进行 SIFT 特征点提取，并把提取的特征点和特征向量作为密钥 key 进行保存；最后继续重构，得到嵌入水印信息的

载体图像。

2.2　水印的提取

水印的提取是水印嵌入的逆过程，其具体步骤为：对待检测图像进行一级 NSCT 变换，并对低频系数进行 SIFT 检测，提取其特征点和特征向量，结合密钥 key 中保存含水印信息的载体图像的特征点和特征向量进行匹配，得出特征点匹配对；运用广义霍夫变换对特征点匹配对进行提纯，删除错误的特征点匹配对；利用筛选后匹配的特征点对求出仿射变换参数，使用仿射变换的逆变换校正待检测图像；对校正后的待检测图像进行两级 NSCT 变换获得低频系数的方向子带，提取出加密的水印信息；根据保存的置乱次数解密被加密的水印信息。

3　实验结果及分析

该实验采用尺寸大小为 32×32 的二值水印图像，载体图像采用尺寸大小为 512×512 的 Lena 灰度图像，置乱次数 M 取 20，q 取值为 4。同时，采用峰值信噪比 PSNR 度量水印图像质量，相关系数 NC 值检测水印相关性。

1）水印的嵌入和提取。Lena 载体图像、水印图像、嵌入水印的 Lena 图像和从未受攻击的含水印图像中提取出来的水印图像见图 3a—d，从视觉上看，Lena 原始图像和嵌入水印的 Lena 图像几乎没有差别；从 PSNR 值和 NC 值上看，Lena 原始图像和嵌入水印后的 Lena 图像的 PSNR 值为 41.33，NC 值为 1.0，表明了水印具有较好的鲁棒性和不可见性；以旋转

a 载体图像　b 水印　c 含水印的图像　d 原图中提取的水印

e 旋转 30° 的含水印图像　f 校正后的含水印图像　g 校正后提取的水印

图 3　水印的嵌入和提取

Fig.3 Watermark embedding and extracting

30°的含水印载体图像为例，先对攻击后的图像进行几何校正，再从校正后的图像提取水印，见图 3e—g。

2）旋转攻击。对嵌入水印的载体图像进行各个角度的旋转攻击，旋转 0°，20°，40°，60°，80°，90°攻击后提取的水印的 NC 值分别为 1.0，0.94，0.977，0.952，0.939，1.0，说明对各个角度的旋转攻击均有很好的鲁棒性。

3）缩放攻击。对嵌入水印的载体图像进行缩放攻击，插值方法采用双 3 次插值，缩放 0.5，0.75，1.25，1.5 攻击后提取的水印 NC 值分别为 0.866，0.989，1.0，1.0。

4）平移攻击。对嵌入水印的载体图像进行平移攻击，平移(0, 0)，(10, 10)，(25, 25)，(−10, −10)，(−25, −25)，(0, −25)，(25, 0)攻击后提取的水印 NC 值分别为 1.0，0.931，0.911，0.957，0.923，0.968，0.970。

5）组合攻击。对嵌入水印的载体图像进行旋转、缩放和平移的组合攻击，组合攻击类型分别是旋转 30°＋缩放 0.75，旋转 30°＋缩放 1.25，旋转 30°＋平移(10, 10)，旋转 30°＋平移(25, 25)，平移(10, 10)＋缩放 0.75，平移(10, 10)＋缩放 1.25，旋转 30°＋平移(10, 10)＋缩放 0.75，旋转 30°＋平移(10,10)＋缩放 1.25，相对应提取水印的 NC 值分别为 0.910, 0.867, 0.948, 0.935, 0.920, 0.942, 0.885, 0.845。实验结果表明，对于组合攻击，提取的水印也具有较好的鲁棒性。

6）常规攻击。常规攻击包括压缩、噪声、滤波等。实验结果见表 1，结果表明，该算法对于常规信号攻击也具有很好的鲁棒性。

表 1 常规攻击实验结果
Tab.1 Result of conventional attacks' experiment

攻击方式	攻击参数	NC值
高斯噪声	0.005	0.961
椒盐噪声	0.01	0.978
高斯滤波	3×3	0.998
	5×5	0.968
	7×7	0.937
中值滤波	3×3	0.965
	5×5	0.841
	7×7	0.770
JPEG压缩	40	1.000
	30	1.000
	20	0.965
剪切	左上1/4	0.929
	中间1/4	0.938
	右下1/4	0.991

7）未采用广义霍夫变换筛选匹配对和采用广义霍夫变换后的数据对比见表 2。结果表明，采用广义霍夫变换对图像特征点匹配对进行筛选后，提高了匹配的正确率和降低了匹配耗时。其中匹配正确率是指正确匹配对数与总的匹配对数的比值，匹配阈值 distRatio 取 0.6，表 2 中试验项的结果是该试验项多个不同试验求出结果后统计出的平均值。

表 2 匹配结果分析
Tab.2 Analysis of matching results

试验项	原匹配对数	筛选后匹配对数	原正确率%	筛选后正确率/%
物体遮挡	107	95	81.3	91.6
仿射变换	39	36	82.1	88.9
光照变化	68	60	82.4	93.3

4 结语

文中算法利用 SIFT 算法实现水印具有抗几何攻击的能力；广义霍夫变换删除误匹配对，提高匹配精度；中间值量化算法实现了水印的嵌入和提取，降低了水印信号嵌入和提取的错误率；使用 Arnold 变换对水印图像进行置乱，提高了安全性和抗干扰性。为了提高仿射变换参数值精度，水印提取时，利用筛选后的特征点匹配对和最小二乘法估算仿射变换参数值，减少求解误差。大量实验结果表明，文中算法对旋转、缩放及常规信号攻击都具有很好的鲁棒性和不可见性。

参考文献：

[1] BAS P, CHASSERY J M, MACQ B. Geometrically Invariant Watermarking Using Feature Points[J]. IEEE Transactions on Image Processing A Publication of the IEEE Signal Processing Society, 2002, 11(9): 1014—1028.
[2] SMITH S M, BRADY J M. S. A New Approach to Low Level Image Processing[J]. International Journal of Computer Vision, 1997, 23(1): 45—78.
[3] WANG W, LUO D, LI W. Algorithm for Automatic Image Registration on Harris-Laplace Features[J]. Journal of Applied Remote Sensing, 2009, 3(1): 554—567.
[4] LOWE D G. Distinctive Image Features from Scale-Invariant Keypoints[J]. International Journal of Computer Vision, 2004, 60(6): 91—110.
[5] 刘军, 王海卫, 谢长生, 等. 使用 SIFT 图像校正的彩色图像水印算法[J]. 小型微型计算机系统, 2009, 30(9): 1838—1842.
LIU Jun, WANG Hai-wei, XIE Chang-sheng, et al. Digital Watermarking Algorithm for Color Image Using SIFT Image Correction[J]. Journal of Chinese Computer Systems, 2009, 30(9): 1838—1842.
[6] YAN W, HU Y, SHOU G, et al. The Algorithm of Color Image Watermarking Based on SIFT[C]// International Conference on E-Business and Information System Security, 2010.
[7] YE X, CHEN X, DENG M, et al. A SIFT-based DWT-SVD Blind Watermark Method against Geometrical Attacks[C]// International Congress on Image and Signal Processing, 2014.
[8] LUO H, SUN X, YANG H, et al. A Robust Image Watermarking Based on Image Restoration Using SIFT[J]. Radio Engineering, 2011, 20(2): 525—532.
[9] GALAMBOS C, KITTLER J, MATAS J. Gradient Based Progressive Probabilistic Hough Transform[J]. Vision, Image and Signal Processing, 2001, 148(3): 158—165.
[10] BALLARD D H. Generalizing the Hough Transform to Detect Arbitrary Shapes[J]. Pattern Recognition, 1981, 13(2): 111—122.
[11] CUNHA A L D, ZHOU J, DO M N. Nonsubsampled Contourilet Transform: Filter Design and Applications in Denoising[C]// IEEE International Conference on Image Processing, 2005: 749—752.
[12] KUNDUR D, HATZINAKOS D. Digital Watermarking Using Multiresolution Wavelet Decomposition[C]// Proceedings of the 1998 IEEE International Conference, 1998.
[13] THORAT C G, JADHAV B D. A Blind Digital Watermark Technique for Color Image Based on integer Wavelet Transform and SIFT[J]. Procedia Computer Science, 2010, 2(2): 236—241.
[14] YANG L, GUO B, LYU J. A Modified Feature Based Image Watermarking Scheme in NSCT Domain[C]// International Conference on Information Assurance and Security, 2009.
[15] GAO G, CAI B, XU S, et al. Watermark Performance Contrast between Contourlet and Non-subsampled Contourlet Transform[C]// International Conference on Information and Automation, 2012.
[16] YANG H Y, WANG X Y, CHEN L L. Geometrically Invariant Image Watermarking Using SVR Correction in NSCT Domain[J]. Computers & Electrical Engineering, 2011, 37(5): 695—713.
[17] TING M A, HUNG J H, ZHAO Y, et al. Study on the Digital Watermarking Algorithm Based on NSCT and SVD[J]. Journal of Yunnan University of Nationalities, 2011(1): 49—55.