文章编号：2095-4980(2020)03-0483-08

基于色彩制约耦合距离惩罚的图像篡改检测

王亚子[1a]，孙怀波[*2]，马远坤[1b]

(1.周口师范学院 a.数学与统计学院，b.网络工程学院，河南 周口 466001；2.阜阳师范大学 数学与统计学院，安徽 阜阳 236037)

摘 要：当前较多图像篡改检测方法主要通过对图像特征间的距离进行测量来完成特征匹配，忽略了图像的色彩信息，导致检测结果中存在较多的误检测和漏检测现象。对此，本文将色彩信息引入到图像特征匹配过程中，设计了一种采用色彩制约模型的篡改检测算法。利用 Laplacian 算子与 Harris 算子提取图像特征，并利用像素点的红(R)、绿(G)、蓝(B)三原色信息，结合特征描述符建立色彩制约模型，对特征点间的色彩信息进行度量，再借助该度量值与特征点间的距离测量值共同完成图像特征匹配，充分剔除误匹配现象，有效提高匹配准确度。该算法还根据特征点间距离方差构造距离惩罚模型，对匹配后的图像特征进行聚类，准确识别篡改内容。通过实验结果发现，与其他篡改检测算法相比，本文算法不仅对伪造内容具备更高的检测准确度，而且对模糊及旋转等内容操作也具有更好的适应性。

关键词：复制–粘贴篡改检测；Laplacian 算子；Harris 算子；灰度差异信息；色彩制约模型；距离惩罚

中图分类号：TN911.73；TP391 **文献标志码：**A **doi：**10.11805/TKYDA2019262

Image copy-paste tampering detection algorithm based on color constrained coupling distance penalty model

WANG Yazi[1a]，SUN Huaibo[*2]，MA Yuankun[1b]

(1a.School of Mathematics and Statistics，b.School of Network Engineering，Zhoukou Normal University，Zhoukou Henan 466001，China；2.School of Mathematics and Statistics，Fuyang Normal University，Fuyang Anhui 236037，China)

Abstract：At present，many image tampering detection methods mainly measure the distance between image features to complete feature matching，ignoring the color information of the image，resulting in more false detection and missed detection in the detection results. In this paper，color information is introduced into the process of image feature matching，and a tamper detection algorithm based on color constraint model is designed. The Laplacian operator and Harris operator are utilized to extract the image features. The R，G and B primary color information of the pixels，as well as the image feature descriptor are adopted to form a color restriction model for measuring the color information between feature points. Then the image feature matching is accomplished by using the distance measurement between the measure value and the feature points to fully eliminate the mismatch phenomenon and effectively improve the matching accuracy. Additionally，the distance penalty model is constructed according to the distance variance between feature points to cluster the matched image features for identifying the tampered content accurately. The experimental results show that compared with other tamper detection algorithms，the proposed algorithm not only has higher detection accuracy for forgery content，but also has better adaptability for content operations such as blur and rotation.

Keywords：copy-paste tampering detection；Laplacian operator；Harris operator；gray difference information；color constraint model；distance penalty

收稿日期：2019-07-23；**修回日期：**2019-08-21

基金项目：国家自然科学基金资助项目(31702232)；河南省高等学校重点科研资助项目(17A110038)

作者简介：王亚子(1978–)，男，硕士，副教授，主要研究方向为图像处理、信息安全、智能算法。email:wangyzi1978pro@sina.com

[*]**通信作者：**孙怀波 email:sunhuaibo7788@163.com

计算机技术的快速发展为数字图像的处理带来了便利，利用图像处理类的计算机应用软件可以便捷地对数字图像进行编辑等操作[1]。图像处理类应用软件的出现在一定程度上推动了数字图像的广泛应用，但若经过编辑的数字图像应用不当，也将给人们的生活带来多方面的困扰。如：当篡改后的数字图像被用于案件侦查时，可能会引起错误的侦查结果；当篡改后的数字图像被用于保险理赔时，可能会引起错误的理赔结果；当篡改后的数字图像被用于新闻传播时，可能会传播错误的新闻信息[2]。由此可见，对篡改图像进行检测已成为当前信息安全研究领域中的一项重要工作。

近些年出现了多种篡改图像检测方法。如 Emam 等[3]将伪造的图像分割成重叠的圆形块，采用极复指数变换(Polar Complex Exponential Transform，PCET)提取子块的不变特征，再利用局部敏感哈希(Locality Sensitive Hashing，LSH)方法与近似最近邻(Approximate Nearest Neighbor，ANN)搜索方法来识别潜在的相似块，采用形态学运算去除错误的相似块，进而完成伪造检测。由于近似最近邻搜索方法在获取相似块时，仅对图像块的距离信息进行测量，忽略了图像的色彩信息，而且将伪造的图像分割成重叠的圆形块，可能引起伪造内容的重复检测，易使检测结果出现误检测。朱叶等[4]通过在高斯差分区域中提取图像特征，利用混合灰度序模式方法对图像特征进行描述，采用欧几里德距离比值的方法获取特征匹配结果，并通过随机抽样一致性(Random Sample Consensus，RANSAC)方法去除无匹配实现篡改检测。由于采用欧几里德距离比值的方法获取特征匹配结果，需要依赖阈值进行，而且没有考虑图像的色彩信息，使匹配结果正确度下降，限制了检测准确性。Tao 等[5]研究了基于图像边缘信息的基本水印算法，将加密后的水印转换成二进制值并嵌入到边缘中，使用翻转不变的筛选功能定位关键内容区域，利用帐篷图和散列函数进一步保护秘密水印，进而实现伪造检测。这种采用水印加密的方法能实现伪造图像的检测，但其将加密水印嵌入到图像中，会对图像的原始信息造成一定程度的破坏。

为了改善篡改内容的识别准确性，本文设计了一种彩色制约耦合距离惩罚模型的篡改检测算法。在利用 Harris 算子检测图像特征前，先将图像的每个尺度空间进行 Laplacian 算子计算，以锐化图像特征，使图像特征的检测结果更为准确。在特征匹配过程中，利用像素点的色彩信息构造色彩制约模型，通过图像的色彩与距离双重信息完成特征匹配，提高特征匹配的正确度。

1 复制—粘贴篡改检测算法

本文算法的检测过程如图 1 所示。由图 1 可见，算法可分为图像特征检测、图像特征描述以及图像特征匹配、匹配特征聚类 4 部分，分别如下：

1) 通过高斯核函数计算出图像的多尺度空间，利用 Laplacian 算子对多尺度空间进行锐化，并在每一个尺度空间通过 Harris 算子检测出图像的特征。

2) 利用特征点邻域圆中 Haar 小波信息，计算出特征点的主方向，并通过计算主方向上特征点邻域中像素点的灰度差异信息，求取特征向量。

3) 通过像素点的三原色信息构造色彩制约模型，并通过其与欧氏距离测量模型完成图像特征匹配。

4) 利用匹配点间欧氏距离的方差信息，构造距离惩罚模型，用以对匹配点进行聚类，完成篡改内容的检测。

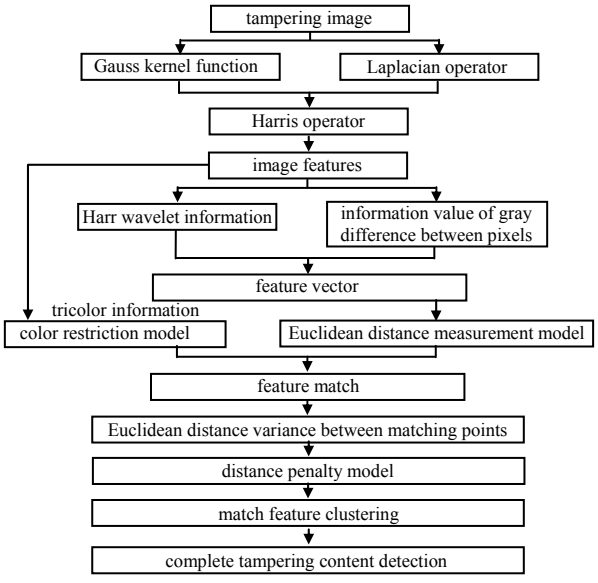


Fig.1 Process of image tampering detection algorithm in this paper
图 1 本文图像篡改检测算法的过程

1.1 图像特征检测

令坐标为 (x,y) 的像素点 p 对应的灰度值为 $H(x,y)$。U 代表以 p 为中心的邻域，将其平移 (Z,J) 后，U 中像素点对应的灰度变化量 $C(Z,J)$ 为[6]：

$$C(Z,J)=\sum \eta_{Z,J}\left[H(x+Z,y+J)-H(x,y)\right]^2 \tag{1}$$

式中 $\eta_{Z,J}$ 为高斯滤波器，用以对 U 进行高斯平滑处理，滤除噪声信息。

通过 p 点在 8×8，$F(x,y)$ 方向上的导数 $\frac{\partial p}{\partial x}$ 和 $\frac{\partial p}{\partial y}$ 建立实对称矩阵 $\boldsymbol{S}$：

$$\boldsymbol{S}=\sum\eta_{Z,J}\begin{bmatrix}\left(\dfrac{\partial p}{\partial x}\right)^2 & \left(\dfrac{\partial p}{\partial x}\times\dfrac{\partial p}{\partial y}\right)\\ \left(\dfrac{\partial p}{\partial x}\times\dfrac{\partial p}{\partial y}\right) & \left(\dfrac{\partial p}{\partial y}\right)^2\end{bmatrix} \tag{2}$$

令 $Det(\boldsymbol{S})$ 和 $Tra(\boldsymbol{S})$ 分别表示实对称矩阵 $\boldsymbol{S}$ 对应的列式值和迹，则图像特征的响应模型 M 为：

$$M=\frac{Det(\boldsymbol{S})}{Tra(\boldsymbol{S})+\alpha} \tag{3}$$

式中 α 为任意一个不为零的常数。

将像素点 p 对应的响应值 M 与响应阈值 β 相比较，若满足 $M\geqslant\beta$，则认为像素点 p 为图像的特征点。但 Harris 算子不具备尺度不变性，图像特征检测过程鲁棒性较差。对此，本文将获取图像的多尺度空间，在每个尺度空间上进行 Harris 计算，以检测图像特征，提高图像特征检测过程的鲁棒性。

令 δ 为尺度因子，求取图像 $I(x,y)$ 的多尺度空间 $L(x,y,\delta)$ 的过程为：

$$L(x,y,\delta)=G(x,y,\delta)*I(x,y) \tag{4}$$

式中：*为卷积运算；$G(x,y,\delta)$ 为高斯核函数，其表述为：

$$G(x,y,\delta)=\frac{1}{2\pi\delta^2}\mathrm{e}^{-\frac{x^2+y^2}{2\delta^2}} \tag{5}$$

为了增强图像的特征，提高 Harris 算子的检测正确度，本文利用 Laplacian 算子 $\nabla^2 I$ 对每个尺度空间进行锐化处理：

$$\nabla^2 I=[I(x+1,y)+I(x-1,y)+I(x,y-1)+I(x,y+1)]-4I(x,y) \tag{6}$$

式中 ∇ 为梯度算子。经过式(6)锐化处理后的每个尺度空间，再利用 Harris 算子求取图像的特征点，检测的图像特征如图 2 所示。观察图 2(b)可见，该方法对图像特征能够进行较为准确的检测。

(a) tampering image　(b) feature detection result

Fig.2 Detection results of image feature

图 2 图像特征检测结果

1.2 图像特征描述

获取图像的 Haar 小波特征，计算图像特征的方向信息，并以此为依据建立特征点邻域，通过求取该邻域中像素点的灰度差异信息，生成特征向量。

选取任一特征点 p，将其作为中心，6δ 作为半径，构建圆域 Q。再求取各 60°扇形窗口中 Haar 小波值的总和，将 Haar 小波值总和最大的方向作为主方向 θ[7−8]。然后构建一个大小为 6×6 的 p 的邻域 B。以 B 中像素点 q 为圆心，θ 为参考方向，建立一个直径为 6δ 的圆域 o，求取 o 中每一个像素点 r_i 与像素点 q 的灰度差值 $D(r_i,q)$。利用 $D(r_i,q)$ 值建立二值模型 $E(r_i,q)$，并通过 $E(r_i,q)$ 计算出邻域圆 o 中像素点间的灰度差异信息值 $V(r_i,q)$：

$$E(r_i,q)=\begin{cases}1, D(r_i,q)\geqslant 0\\ 0, D(r_i,q)<0\end{cases} \tag{7}$$

$$V(r_i,q)=\sum_{i=0}^{k-1}E(r_i,q)2^{i-1} \tag{8}$$

式中 k 为邻域圆 o 中像素点的总数。

最后，求矩形邻域 B 中所有像素点与其邻域圆的灰度差异信息值 $V(r_i,q)$，并将所有灰度差异信息值执行归一化运算，从而得到一个 36 元素的特征向量 $\boldsymbol{F}$，该特征向量的示意图如图 3 所示。

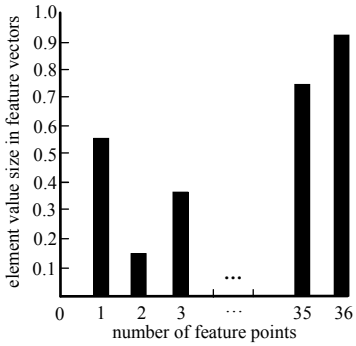


Fig.3 Eigenvectors corresponding to feature points

图 3 特征点对应的特征向量

$$\boldsymbol{F}=\{V_1,V_2,V_3,\cdots,V_{36}\} \tag{9}$$

1.3 图像特征匹配

图像特征匹配是篡改检测的关键步骤，在此利用像素点的 R，G，B 三原色信息，构造色彩制约模型，将图像的色彩信息引入到特征匹配的过程中。由于仅通过特征点间的距离信息判断其匹配性，容易产生一对多的匹配现象，使匹配出错。因此本文利用色彩制约模型与欧氏距离测量模型，对图像的色彩与距离信息进行测量，

制约一对多匹配现象的出现，提高图像特征匹配的正确性。

令 $\boldsymbol{F}_{p_i}$ 与 $\boldsymbol{F}_{q_i}$ 分别为特征点 p 与 q 的特征向量，则特征点 p 与 q 对应的欧氏距离测量模型 $EU(p,q)$ 为[9]：

$$EU(p,q)=\left[\sum_{i=1}^{36}\left(\boldsymbol{F}_{p_i}-\boldsymbol{F}_{q_i}\right)^2\right]^{1/2} \tag{10}$$

以特征点 p 与 q 为中心，分别构建一个尺寸为 $w\times w$ 的邻域 Lp 与 Lq，且利用 $R(\cdot),G(\cdot),B(\cdot)$ 分别表示 Lp 与 Lq 中像素点 R，G，B 三原色信息值，则色彩制约模型 $CR(p,q)$ 为：

$$CR(p,q)=\sum_{a\in L_p}\sum_{b\in L_p}[(R(a)-R(b))^2+(G(a)-G(b))^2+(B(a)-B(b))^2]^{1/2} \tag{11}$$

当 2 个特征点相匹配时，不仅 $EU(p,q)$ 值最小，其 $CR(p,q)$ 值也应该最小。对此可利用式(10)和式(11)计算特征点 p 与其他特征点的 $EU(p,q)$ 值和 $CR(p,q)$ 值，并选取与特征点 p 同时具有最小 $EU(p,q)$ 值和最小 $CR(p,q)$ 值的特征点 q 作为其匹配点。通过色彩制约模型与欧氏距离测量模型对图 2(b)中特征点进行匹配，结果如图 4 所示。观察图 4 可见，该方法总体匹配结果正确性较高，仅存在少许错误匹配。

Fig.4 Feature matching results
图 4 特征匹配结果

1.4 匹配特征聚类

为了对伪造内容进行准确的辨别，需要对匹配的图像特征进行聚类[10−11]。以匹配点间欧氏距离的方差值为基础，构建距离惩罚模型，对匹配点进行聚类。

令 T 为匹配特征的集合，$EU(p,q)$ 为匹配点对 p 与 q 的欧氏距离，则 p 与 q 的欧氏距离方差 $VA(p,q)$ 为：

$$VA(p,q)=\frac{1}{k}\sqrt{\sum_{(p,q)\in T}\left|AG(p,q)-EU(p,q)\right|^2} \tag{12}$$

式中：k 为匹配点对数；$AG(p,q)$ 为 p 与 q 欧氏距离的均值：

$$AG(p,q)=\frac{1}{k}\sum_{(p,q)\in T}EU(p,q) \tag{13}$$

通过 $VA(p,q)$ 构造的距离惩罚模型 $PU(p,q)$ 为：

$$PU(p,q)=\sum_{(p,q)\in T}\frac{1}{2\pi VA(p,q)}\exp^{-\frac{1}{2(VA(p,q))^2}} \tag{14}$$

利用距离惩罚模型对匹配特征聚类时，先将所有匹配特征点视为独立的聚类，利用式(14)计算每个类的 $PU(p,q)$ 值，并选取最小 $PU(p,q)$ 值对应的类进行聚合，形成一个新类 nw。对 nw 的中心进行更新，形成新的聚类中心 CN，迭代此过程，直至聚类完毕。

$$CN=\frac{1}{N}\sum_{i=1}^{N}\sum_{j=0}^{36}p_i(\boldsymbol{F}_{pj}) \tag{15}$$

式中：N 为 nw 中特征点总数；p_i 为 nw 中第 i 个特征点，$p_i(\boldsymbol{F}_{pj})$ 为 p_i 特征向量中第 j 个元素。利用距离惩罚模型对图 4 所示匹配特征聚类所得的篡改内容识别结果如图 5 所示。从图 5 可见，将匹配特征经过距离惩罚模型聚类后，能够较为准确地识别出篡改内容。

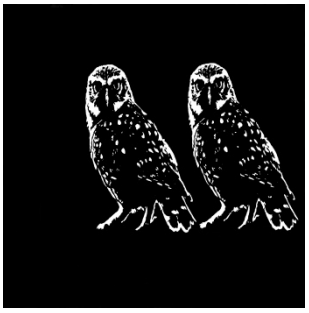


Fig.5 Recognition results of tampered content
图 5 篡改内容的识别结果

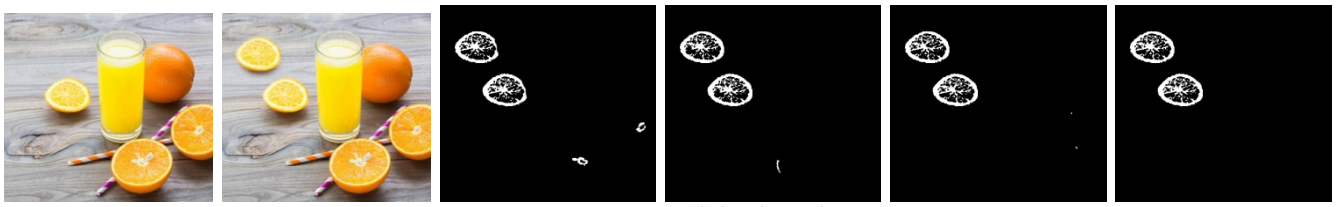
2 实验结果

实验硬件为 Intel Celeron 2.6 GHz CPU,4 GB 内存 PC 机，采用 Windows 7 操作系统、Matlab 7 及 OPENCV 3.0 软件。实验时设置本文算法中的响应阈值 β=1 200，并将文献[12−14]作为对照组。

2.1 单一的复制—粘贴篡改图像检测

不同算法对单一的复制—粘贴篡改图像的检测结果及统计数据分别如图 6 和表 1 所示。从图 6 可以看出，文献[12]算法检测的结果中，篡改内容“橙子”的边缘存在检测不完整现象，而且还存在错误检测现象。文献[13]算法检测的结果中，篡改内容“橙子”的内部存在漏检测现象，且存在一处错误检测内容。文献[14]算法检

测的结果中，篡改内容“橙子”的内部也存在漏检测现象。而本文算法，篡改内容“橙子”的边缘和内部都较为完整，不存在错误检测内容。通过对比表 1 中的统计数据发现，本文算法的检测正确度高于文献[12−14]中的算法。



(a) initial image　(b) copy−paste tampered image　(c) detection results of reference [12]　(d) detection results of reference [13]　(e) detection results of reference [14]　(f) detection results of this algorithm

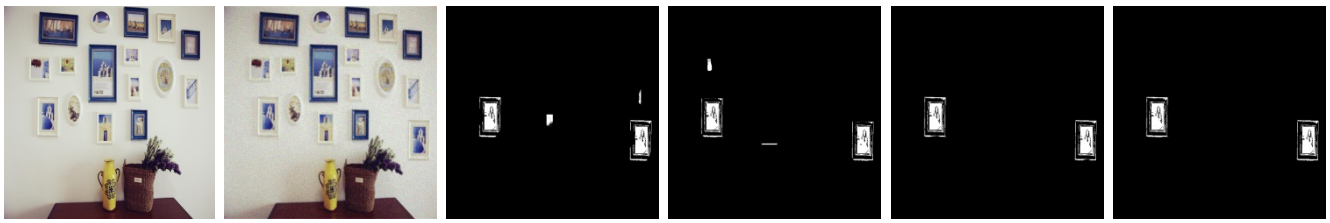
Fig.6 Detection results of copy−paste tampered images by different algorithms
图 6 不同算法对复制−粘贴篡改图像检测结果

表 1 图 6 中不同算法检测结果的统计数据
Table1 Statistical data of detection results of different algorithms in Fig.6

algorithm	forged content area(pixels)	detection of forged content area(pixels)	detection accuracy/%
reference [12] algorithm	4 780	4 308	90.13
reference [13] algorithm	4 780	4 497	94.08
reference [14] algorithm	4 780	4 529	94.75
this algorithm	4 780	4 680	97.91

2.2 不同几何变换下的复制—粘贴篡改图像检测

为了进一步验证本文算法的检测有效性以及鲁棒性，利用不同算法分别对添加了模糊和噪声、旋转以及缩放处理的复制—粘贴篡改图像进行检测。其中，不同算法对复制—粘贴+模糊+噪声篡改图像的检测效果如图 7 所示，其对应的统计数据如表 2 所示。观察图 7 可见，文献[12]算法检测的结果中，篡改内容存在检测不完整现象，而且检测结果中还存在错误检测。文献[13]算法检测结果中，篡改内容相框顶部存在漏检测现象，其余部分也存在错误检测。文献[14]算法检测结果中，篡改内容相框底部存在漏检测现象。本文算法检测结果中不存在错误检测内容，且篡改内容检测的完整度也较高。由表 2 中的统计数据可见，较文献[12−14]算法，本文算法检测出的伪造内容最多，其准确度达到 97.25%。图 8 为不同算法对复制—粘贴+旋转篡改图像的检测效果，其对应的统计数据如表 3 所示。从图 8 中可见，文献[12−14]的检测结果中都存在错误检测，以及较多的漏检测内容，而本文算法的检测结果中不存在错误检测，且漏检测内容也较少。对比表 3 中的统计数据发现，本文算法的检测正确度为 92.04%，检测正确度最高。图 9 为不同算法对复制—粘贴+缩放篡改图像的检测效果，其对应的统计数据如表 4 所示。从图 9 可见，本文算法的检测结果比文献[12−14]算法具有更高的检测完整度以及更少的错误检测。从表 4 可见，本文算法、文献[12−14]的检测正确度分别为 91.16%,85.51%,89.01%, 90.04%，这也验证了本文算法检测结果的正确度优于文献[12−14]。

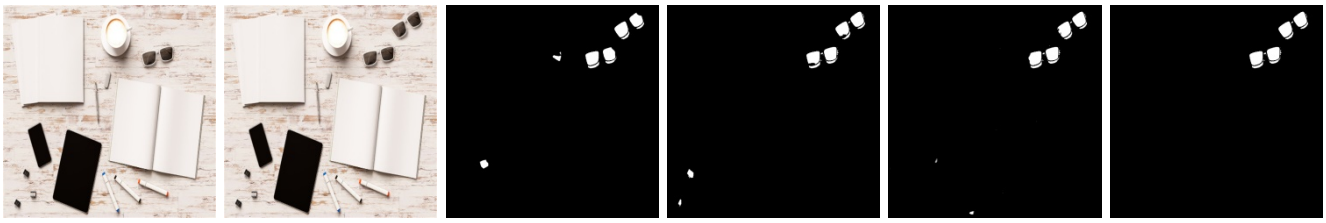


(a) initial image　(b) copy−paste+blur+ noise tampered image　(c) detection results of reference [12]　(d) detection results of reference [13]　(e) detection results of reference [14]　(f) detection results of this algorithm

Fig.7 Detection results of copy−paste+blur+noise tampering images by different algorithms
图 7 不同算法对复制−粘贴+模糊+噪声篡改图像检测结果

表 2 图 7 中不同算法检测结果的统计数据
Table2 Statistical data of detection results of different algorithms in Fig.7

algorithm	forged content area(pixels)	detection of forged content area(pixels)	detection accuracy/%
reference [12] algorithm	12 272	11 013	89.74
reference [13] algorithm	12 272	11 357	92.54
reference [14] algorithm	12 272	11 415	93.02
this algorithm	12 272	11 935	97.25



(a) initial image (b) copy−paste+rotate tampered image (c) detection results of reference [12] (d) detection results of reference [13] (e) detection results of reference [14] (f) detection results of this algorithm

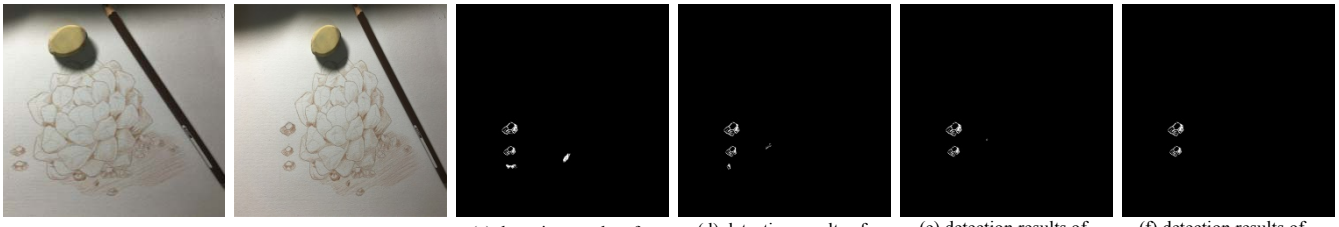
Fig.8 Detection results of copy−paste+rotation tampering images by different algorithms

图 8 不同算法对复制−粘贴+旋转篡改图像检测结果

表 3 图 8 中不同算法检测结果的统计数据

Table3 Statistical data of detection results of different algorithms in Fig.8

algorithm	forged content area(pixels)	detection of forged content area(pixels)	detection accuracy/%
reference [12] algorithm	5 615	4988	88.83
reference [13] algorithm	5 615	5019	89.39
reference [14] algorithm	5 615	5052	89.97
this algorithm	5 615	5168	92.04



(a) initial image (b) copy−paste+scaling tampered image (c) detection results of reference [12] (d) detection results of reference [13] (e) detection results of reference [14] (f) detection results of this algorithm

Fig.9 Detection results of copy−paste+scaling tampered images by different algorithms

图 9 不同算法对复制−粘贴+缩放篡改图像检测结果

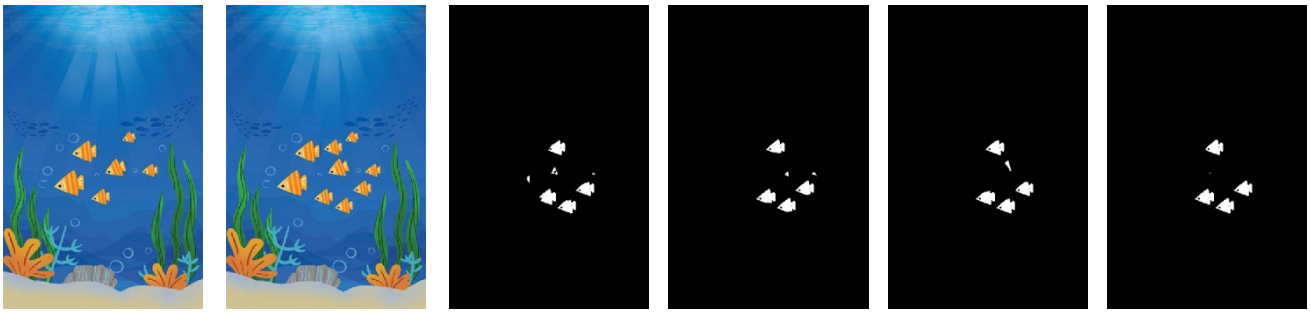
表 4 图 9 中不同算法检测结果的统计数据

Table4 Statistical data of detection results of different algorithms in Fig.9

algorithm	forged content area(pixels)	detection of forged content area(pixels)	detection accuracy/%
reference [12] algorithm	2 229	1 906	85.51
reference [13] algorithm	2 229	1 984	89.01
reference [14] algorithm	2 229	2 007	90.04
this algorithm	2 229	2 032	91.16

2.3 多次复制—粘贴篡改图像检测

不同算法对多次复制—粘贴篡改图像的检测结果及统计数据分别如图 10 和表 5 所示。从图 10 可以看出，文献[12]算法的检测结果中，存在 3 处错误检测和较多的漏检测；文献[13]算法的检测结果中，也具有几处错误检测和漏检测；文献[14]算法的检测结果中，具有漏检测现象，以及一处较大的错误检测；而本文算法的检测结果中，仅存在少量的漏检测。对比表 5 中的数据可见，本文算法的检测正确度要高于文献[12−14]。



(a) initial image (b) copy−paste tampered image (c) detection results of reference [12] (d) detection results of reference [13] (e) detection results of reference [14] (f) detection results of this algorithm

Fig.10 Detection results of multiple copy−paste tampered images by different algorithms

图 10 不同算法对多次复制−粘贴篡改图像检测结果

表 5 图 10 中不同算法检测结果的统计数据

Table5 Statistical data of detection results of different algorithms in Fig.10

algorithm	forged content area(pixels)	detection of forged content area(pixels)	detection accuracy/%
reference [12] algorithm	2 618	2 256	86.17
reference [13] algorithm	2 618	2 301	87.89
reference [14] algorithm	2 618	2 335	89.19
this algorithm	2 618	2 403	91.79

根据上述伪造图像检测效果可见，本文算法不仅能有效检测出伪造图像中的篡改内容，而且对多种后处理操作具有较强的稳健性。

2.4 量化分析

MICC-F220 数据集中包含了经过缩放、旋转等操作的伪造图像以及原图像[15−16]。在此，从中选取一幅经过旋转后处理的伪造图像，将伪造内容进行不同角度的旋转，从而形成 10 幅伪造图像。利用不同算法对这 10 幅图像进行检测，并记录其检测结果的准确度及平均耗时。

不同算法的篡改检测准确度如图 11 所示。从图 11 中可见，与对照组算法相比，本文算法检测结果的准确度最高。当旋转角度为 70° 时，本文算法的检测准确度为 91.02%，文献[12−14]算法的检测准确度分别为 81.19%, 86.20%及 88.53%。不同算法的篡改检测平均耗时如表 6 所示。从表 6 可见，文献[12]具有更高的检测效率，其耗时最低，仅为 3.38 s。本文算法也具有较高的效率，其平均耗时为 4.16 s。而文献[13]的检测效率最低，平均耗时约为 8.72 s。说明本文算法的检测性能较好，耗时较少。本文算法以特征点邻域中的像素点构造了圆域，并通过求取该圆域中像素点的灰度差异信息值获取了鲁棒性较好且仅包含 36 个元素的特征向量，降低了检测耗时。同时本文算法还利用像素点的三原色信息构造了色彩制约模型，利用其与欧氏距离测量模型准确地获取了图像特征的匹配结果，提高了算法的检测性能。

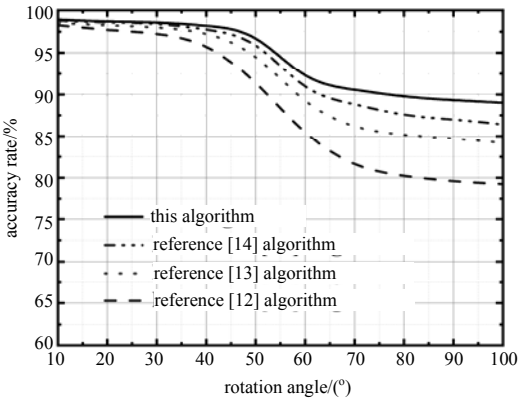


Fig.11 Accuracy test results of different algorithms

图 11 不同算法检测结果准确度测试结果

表 6 不同算法的篡改检测平均耗时

Table6 Average time of tamper detection for different algorithms

algorithm	average time/s
reference [12] algorithm	3.38
reference [13] algorithm	8.72
reference [14] algorithm	6.45
this algorithm	4.16

3　结论

本文通过高斯核函数求取图像的多尺度空间，并在每一层尺度空间上，利用 Laplacian 算子对图像进行锐化，以增强图像特征，在锐化后的图像上利用 Harris 算子准确提取了图像特征。通过图像的 Harr 小波信息计算了特征点的主方向，并利用其建立了像素点的邻域圆，利用邻域圆中像素点的灰度差异信息值，计算出特征点的特征向量。通过像素点的三原色信息，构造了色彩制约模型，利用其与欧氏距离测量模型，对特征点间距离与色彩信息进行测量，将图像的色彩信息引入到匹配过程，提高了特征匹配的正确性。采用匹配点间欧氏距离的方差值，构造了距离惩罚模型，对匹配点进行聚类检测篡改内容。在实验测试中，通过对单一的复制－粘贴篡改图像，以及经过了模糊及旋转等后处理的复制－粘贴篡改图像进行识别，结果表明本文算法具有理想的检测准确度与鲁棒性。

参考文献：

[1] 李芬. 基于归一化和 Bessel−Fourier 矩的鲁棒水印算法[J]. 太赫兹科学与电子信息学报, 2014,12(4):584−588. (LI Fen. Robust watermarking algorithm based on normalization and Bessel−Fourier moments[J]. Journal of Terahertz Science and Electronic Information Technology, 2014,12(4):584−588.)

[2] WARIF N B A,WAHAB A W A,IDRIS M Y I. Copy−move forgery detection:survey,challenges and future directions[J]. Journal of Network and Computer Applications, 2016,75(1):259−278.

[3] EMAM Mahmoud,HAN Qi,NIU Xiamu. PCET based copy−move forgery detection in images under geometric transforms[J]. Multimedia Tools and Applications, 2016,75(18):11513−11527.

[4] 朱叶,申铉京,陈海鹏. 基于混合灰度序模式的图像复制-粘贴篡改盲鉴别算法[J]. 吉林大学学报(工学版), 2017, 47(4):1280-1285. (ZHU Ye,SHEN Xuanjing,CHEN Haipeng. Copy-move forgery detection based on mixed intensity order pattern[J]. Journal of Jilin University(Engineering and Technology Edition), 2017,47(4):1280-1285.)

[5] TAO Rui,SUN Yanjing,LIU Weidong. Forgery detection using chaotic watermarking in image key areas[J]. Tehnicki Vjesnik-Technical Gazette, 2017,24(4):1263-1268.

[6] 孙红,李晶. 融合 Harris 角点检测算法的肺实质分割方法[J]. 小型微型计算机系统, 2019,40(4):818-822. (SUN Hong, LI Jing. Lung CT image segmentation based on Harris corner detection algorithm[J]. Journal of Chinese Computer Systems, 2019,40(4):818-822.)

[7] ZHILA Bahrami,FARDIN Akhlaghiantab. A new robust video watermarking algorithm based on SURF features and block classification[J]. Multimedia Tools and Applications, 2018,77(1):327-345.

[8] 陈甜甜,姚璜,魏艳涛. 基于融合特征的人体动作识别[J]. 计算机工程与设计, 2019,40(5):1394-1400. (CHEN Tiantian,YAO Huang,WEI Yantao. Human action recognition based on fusion features[J]. Computer Engineering and Design, 2019,40(5):1394-1400.)

[9] 高煜妤,王春芳. 基于欧氏距离图的随机 Hough 变换椭圆检测方法[J]. 现代电子技术, 2016,39(21):61-64,69. (GAO Yuyu,WANG Chunfang. Ellipse detection method based on random Hough transform and Euclidean distance graph[J]. Modern Electronics Technique, 2016,39(21):61-64,69.)

[10] MANU V T,MEHTRE B M. Copy-move tampering detection using affine transformation property preservation on clustered keypoints[J]. Signal Image and Video Processing, 2018,12(3):549-556.

[11] WANG Huan,WANG Hongxia,SUN, Xingming. A passive authentication scheme for copy-move forgery based on package clustering algorithm[J]. Multimedia Tools and Applications, 2017,76(10):12627-12644.

[12] MAHMOOD Toqeer,IRTAZA Aun,MEHMOOD Zahid. Copy-move forgery detection through stationary wavelets and local binary pattern variance for forensic analysis in digital images[J]. Forensic Science International, 2017,279(1):8-21.

[13] WANG Xiangyang,LI Shuo,LIU Yunan. A new keypoint-based copy-move forgery detection for small smooth regions[J]. Multimedia Tools and Applications, 2017,76(22):23353-23382.

[14] MOHAMED A E,HEBA A,MOHAMED M D. Two stages object recognition based copy-move forgery detection algorithm[J]. Multimedia Tools and Applications, 2019,78(11):15353-15373.

[15] AMERINI I,BALLAN L,CALDELLI R. A SIFT-based forensic method for copy-move attack detection and transformation recovery[J]. IEEE Transactions on Information Forensics and Security, 2011,6(3):1099-1110.

[16] 独智序,王晓峰. 基于稳健关键点的图像 Copy-move 篡改检测算法[J]. 云南大学学报(自然科学版), 2019,41(1):61-67. (DU Zhixu,WANG Xiaofeng. Copy-move forgery detection algorithm based on robust keypoints[J]. Journal of Yunnan University (Natural Science Edition), 2019,41(1):61-67.)