中图法分类号:TP391　　**文献标识码**:A　　**文章编号**:1006-8961(2024)12-3595-17

论文引用格式:Lin C, Huang K, Wen Y M and Lu W. 2024. Image copy-move forgery detection based on the clustering of matched pairs. Journal of Image and Graphics, 29(12):3595-3611(蔺聪, 黄轲, 温雅敏, 卢伟. 2024. 匹配对聚类的图像复制粘贴篡改检测. 中国图象图形学报, 29(12):3595-3611)[DOI:10.11834/jig.230454]

匹配对聚类的图像复制粘贴篡改检测

蔺聪[1*],黄轲[2],温雅敏[1],卢伟[3]

1. 广东财经大学统计与数学学院大数据与教育统计应用实验室,广州　510320; 2. 广东财经大学信息学院,广州　510320; 3. 中山大学计算机学院,广州　510006

摘　要:**目的**　图像篡改检测主要分为图像区域复制篡改、图像拼接和对象移除3个方向,其中图像复制粘贴篡改是图像篡改检测的重要研究方向之一。针对目前大多数复制粘贴篡改检测方法难以检测平滑和小的篡改区域,且虚警率较高等问题,提出了一种基于匹配对的密度聚类MP-DBSCAN(matched pairs——density based spatial clustering of applications with noise)和点密度过滤策略的图像复制粘贴篡改检测方法。**方法**　首先,在图像中提取大量关键点,根据关键点的灰度值分组后进行匹配。其次,提出了一种改进的密度聚类算法MP-DBSCAN,聚类对象为匹配对的一侧,并利用匹配对的另一侧约束聚类过程,即使篡改区域在空间上距离较近,或者篡改区域存在多个的情况,也能把不同的篡改区域较好地区分开来。此外,本文还提出了一种点密度过滤策略,通过删除低密度簇,降低了检测结果的虚警率。最后,通过估计仿射矩阵并使用ZNCC (zero-mean normalized cross-correlation)算法定位篡改区域。**结果**　消融实验表明了MP-DBSCAN算法和点密度过滤策略的有效性。在FAU、MICC-F600、GRIP和CASIA v2.0这4个数据集上与几个经典的和新颖的检测方法进行了对比实验,本文方法的F_1在4个数据集上像素层的实验结果分别是0.914 3、0.890 6、0.939 1和0.856 8。**结论**　本文提出的MP-DBSCAN聚类算法和点密度过滤策略能有效提高检测算法的性能,即使篡改区域经过旋转、缩放、压缩和添加噪声等处理,本文方法依然能够检测出大部分的篡改区域,性能优于当前的检测算法。

关键词:多媒体取证;图像取证;图像篡改检测;复制粘贴篡改;基于密度的带噪声空间聚类(DBSCAN)

Image copy-move forgery detection based on the clustering of matched pairs

Lin Cong[1*], Huang Ke[2], Wen Yamin[1], Lu Wei[3]

1. Applied Laboratory of Dig Data and Education Statistics, School of Statistics and Mathematics, Guangdong University of Finance and Economics, Guangzhou　510320, China; 2. School of Information, Guangdong University of Finance and Economics, Guangzhou　510320, China; 3. School of Computer Science and Engineering, Sun Yat-sen University, Guangzhou　510006, China

Abstract: **Objective** In recent years, with the development of the internet and computer technology, manipulating images

收稿日期:2023-07-07;**修回日期**:2023-12-18;**预印本日期**:2023-12-25

*通信作者:蔺聪　lincong0310@gmail.com

基金项目:国家自然科学基金项目(62072480);广东省普通高校特色创新项目(自然科学)(2022KTSCX041);广州市科技计划基础与应用基础研究项目(202102080316);广东省信息安全技术重点实验室开放基金(2020B1212060078);广州市海珠区科技计划项目(海科工商信计2022-45)

Supported by: National Natural Science Foundation of China(62072480); Characteristic Innovation Project of Regular Institutions of Higher Learning of Guangdong Province(Natural Science)(2022KTSCX041); Opening Project of Guangdong Province Key Laboratory of Information Security Technology(2020B1212060078)

and changing their content have become trivial tasks. Therefore, robust image tampering detection methods need to be developed. As passive forensic methods, image forgery methods can be categorized into copy-move, splicing, and inpainting methods. Copy-move involves copying part of the original image to another part of the same image. Many excellent copy-move forgery detection (CMFD) methods have been developed in recent years and can be categorized into block-based, keypoint-based, and deep learning methods. However, these methods have the following drawbacks: 1) they cannot easily detect small or smooth tampered regions; 2) a massive number of features leads to a high computational cost; and 3) false alarm rates are high when the tampered images involve self-similar regions. To solve these issues, a novel CMFD method based on matched pairs, namely, density-based spatial clustering of applications with noise (MP-DBSCAN), is proposed in this paper along with point density filtering. **Method** First, a large number of scale-invariant feature transform (SIFT) keypoints are extracted from the input image by lowering the contrast threshold and normalizing the image scale, thus allowing the detection of a sufficient number of keypoints in small and smooth regions. Second, the generalized two nearest neighbor (G2NN) matching strategy is employed to manage multiple keypoint matching, thus allowing the detection algorithm to perform smoothly even when the tampered region has been copied multiple times. A hierarchical matching strategy is then adopted to solve keypoint matching problems involving a massive number of keypoints. To accelerate the matching process, keypoints are initially grouped by their grayscale values, and then the G2NN matching strategy is applied to each group instead of the keypoints detected from the entire image. The efficiency and accuracy of the matching procedure can be improved without deleting the correct matched pairs. Third, an improved clustering algorithm called MP-DBSCAN is proposed. The matched pairs are grouped into different tampered regions, and the direction of the matched pairs are adjusted before the clustering process. The cluster objects only represent one side of the matched pairs and not all the extracted keypoints, and the keypoints from the other side are used as constraints in the clustering process. A satisfying detection result is obtained even when the tampered regions are close to one another. The proposed method obtains better F_1 measures compared with the state-of-the-art copy-move forgery detection methods. Fourth, the prior regions are constructed based on the clustering results. These prior regions can be regarded as the approximate tampered regions. A point density filtering policy is also proposed, where each point density of the region is calculated and the region with the lowest point density is deleted to reduce the false alarm rate. Finally, the tampered regions are located accurately using the affine transforms and the zero-mean normalized cross-correlation (ZNCC) algorithm. **Result** The proposed method is compared with the state-of-the-art CMFD methods on four standard datasets, including FAU, MICC-F600, GRIP, and CASIA v2.0. Provided by Christlein, the FAU dataset has an average resolution of about 3 000 × 2 300 pixels and includes tampered images under post-processing operations (e.g., additional noise and JPEG compression) and various geometrical attacks (e.g., scaling and rotation). This dataset involves 48, 480, 384, 432, and 240 plain copy-move, scaling, rotation, JPEG, and noise addition operations, respectively. The MICC-F600 dataset includes images in which a region is duplicated at least once. The resolutions of these images range from 800 × 533 to 3 888 × 2 592 pixels. Among the 600 images in this dataset, 440 are original images and 160 are forged images. The GRIP dataset includes 80 original images and 80 tampered images with a low resolution of 1 024 × 768 pixels. Some tampered regions on these images are very smooth or small. The size of the tampered regions ranges from about 4 000 to 50 000 pixels. The CASIA v2.0 dataset contains 7 491 authentic and 5 123 forged images, of which 1 313 images are forged using copy-move methods. Precision, recall, and F_1 scores are used as assessment criteria in the experiments. The F_1 scores of the proposed method on the FAU, MICC-F600, GRIP, and CASIA v2.0 datasets at the pixel level are 0.914 3, 0.890 6, 0.939 1, and 0.856 8, respectively. Extensive experimental results demonstrate the superior performance of the proposed method compared with the existing state-of-the-art methods. The effectiveness of the MP-DBSCAN algorithm and the point density filtering policy is also demonstrated via ablation studies. **Conclusion** To detect tampered regions accurately, a novel CMFD method based on the MP-DBSCAN algorithm and the point density filtering policy is proposed in this paper. The matched pairs of an image can be divided into different tampered regions by using the MP-DBSCAN algorithm to detect these regions accurately. The mismatched pairs are then discarded by the point density filtering policy to reduce false alarm rates. Extensive experimental results demonstrate that the proposed method exhibits a satisfactory accuracy and robustness compared with the existing state-of-the-art methods.

Key words: multimedia forensics; image forensics; image forgery detection; copy-move forgery; density based spatial clustering of applications with noise (DBSCAN)

0 引 言

随着图像编辑与美化软件的日益普及，人们可以通过简单的操作和极低的成本在网络上发布经过修改的图像。如果篡改图像用于非法目的，可能对个人隐私、社会秩序乃至国家安全造成重大威胁。因此，图像取证的研究尤为重要。图像取证是多媒体取证领域的一个分支（李晓龙 等，2021），目前主要存在以下几种图像篡改方式：拼接（splicing）、修复（inpainting）和复制粘贴（copy- move）。复制粘贴篡改是指将图像的一部分复制并粘贴到该图像的另一个区域。为了能够掩盖篡改痕迹并增加篡改检测的难度，篡改区域一般还会经过缩放、旋转、压缩、添加噪声和光照调整等操作。一般来说，经典复制粘贴篡改检测（copy-move forgery detection, CMFD）方法的检测流程总体可分为3个步骤：特征提取、特征匹配和后处理。目前，CMFD方法主要可以分为3种类型：基于块的方法，基于关键点的方法和基于深度学习的方法。

在基于块的方法中，首先将图像分为若干个规则的图像块，以获取图像的局部区域进行特征提取。在特征提取阶段，研究者尝试将多种特征提取算法引入CMFD过程中。Fridrich等人（2003）使用离散余弦变换（discrete cosine transform, DCT）对图像块进行特征提取，然而，这种特征几乎无法抵御几何、加噪和高斯模糊等攻击手段。为了解决这些问题，研究者们开始采用更加鲁棒的特征提取方法，例如离散小波变换（discrete wavelet transform, DWT）（Muhammad 等，2012）、极余弦变换（polar cosine transform, PCT）（Li, 2013）、极坐标复指数变换（polar complex exponential transform, PCET）（Emam 等，2016）、模糊矩不变量（blur moment invariants）（Mahdian 和 Saic, 2007）、Zernike 矩（zernike moments）（Ryu 等，2013）、圆谐傅里叶矩（radial harmonic Fourier moments, RHFMs）（秦娟 等，2013）和指数矩（exponent-fourier moments, EFMs）（赖玥聪等，2015）等特征提取方法。在特征匹配阶段，使用全局搜索思想的暴力匹配方法最简单，但由于基于分块方法提取的特征较多，会导致计算复杂度极高。为了提高匹配速度，研究者们提出了基于近似搜索思想的匹配算法。Cozzolino等人（2015）提出了一种改进的PatchMatch用于特征匹配，Bi和Pun（2018）使用增强相干敏感哈希（coherency sensitive hashing, CSH）进行匹配，极大地提高了算法的效率。除了基于近似搜索思想的匹配算法，Emam等人（2016）还提出了使用局部敏感哈希（locality-sensitive hashing, LSH）的方法，在加快匹配速度的同时获得了不错的检测准确率。由于基于分块思路的检测算法将图像分解为密集的局部区域，当图像分辨率较高时，计算时间复杂度过高，且对于大规模的几何变换，如旋转、缩放等，鲁棒性较差。

为了解决基于块的方法存在的问题，基于关键点的方法被提出。在特征提取阶段，尺度不变特征变换（scale-invariant feature transform, SIFT）特征（Lowe, 2004）广泛用于CMFD算法的特征提取步骤中，Pan和Lyu（2010）、Lin等人（2018）、Li和Zhou（2019）、Niu等人（2021）、Wang等人（2022）、Gan等人（2022）、Wang等人（2023）和Wang等人（2024）都采用了该特征。除了SIFT特征，加速鲁棒特征（speeded up robust features, SURF）（Silva等，2015）、KAZE（Yang等，2017）、Harris-Laplace（Lin等，2019）以及局部灰度序模式（local intensity order pattern, LIOP）（Lyu等，2021）等特征也被应用于CMFD方法的特征提取。基于关键点的算法具有较低的计算复杂度和更强的特征鲁棒性，能够抵抗几何攻击和尺度变换等后处理技术。然而，在某些分辨率低或者平滑的图像中，往往无法提取足够数量的关键点。针对这一问题，Li和Zhou（2019）通过放大图像并降低对比度阈值的方法获得更多的关键点，并提出了根据关键点的灰度值和尺度进行分组匹配的策略，从而加快了特征匹配的速度。即使通过降低对比度阈值的方法提取到的特征数量增加了，但是在平滑区域提取的特征数量依然达不到理想效果。为此，Gan等人（2022）移除了SIFT算法中对比度阈值对特征提取的约束，提取到了更多的关键点。在特征匹配阶段，有多种匹配方法相继提出并应用于复制粘贴篡改检测，例如传统的2NN（two nearest neighbor）

匹配(Pan和Lyu,2010)、适应于一个区域被复制多次的G2NN匹配(Amerini等,2011),以及其他变种如RG2NN(reversed generalized two nearest neighbor)匹配(Wang等,2017)和I2NN(imporved two nearest neighbor)匹配(Wang等,2023)等。在后处理阶段,通常使用随机样本一致性(random sample consensus, RANSAC)算法(Fischler和Bolles,1987)估计仿射矩阵。为了检测图像中的多对篡改区域,研究者使用聚类算法对匹配对进行分组,每个簇估计一个仿射矩阵。Lyu等人(2021)、Niu等人(2021)和Wang等人(2022)都在CMFD中使用了DBSCAN算法。Amerini等人(2011,2013)使用了凝聚层次聚类(agglomerative hierarchical clustering, AHC)算法和J-Linkage算法对匹配对分组。Dixit和Bag(2021)在CMFD中引入了模糊均值聚类(fuzzy c-means, FCM)算法。除了使用聚类算法之外,还可以使用图像分割算法将图像分为超像素块,达到对关键点分组的效果。如Li等人(2015)使用了简单线性迭代聚类(simple linear iterative clustering, SLIC)算法。基于关键点的方法对于平滑区域提取到的特征较少,JPEG压缩、添加噪声等后处理因素会严重影响特征的提取,进而影响检测效果。

近年来,随着人工智能的发展和深度学习技术的进步,很多学者提出了基于深度学习的CMFD方法。Rao和Ni(2016)提出使用卷积神经网络(convolutional neural network, CNN)检测图像是否经过篡改;Barni等人(2021)和Zhang等人(2023)分别提出了多分支卷积神经网络(multi-branch CNN)和CNN-T GAN(convolutional neural network-Transformer based generative adversarial network)模型来检测并区分篡改图像中的源区域和篡改区域。Liu和Pun(2018)提出了使用全卷积网络(fully convolutional network, FCN)的方法,并使用条件随机场的方法来对定位结果进行优化。Zhong和Pun(2020)以及Zhu等人(2020)分别将端到端的Dense-Inceptionnet和AR-Net(adaptive attention and residual refinement network)引入CMFD中。Abhishek和Jindal(2021)将深度卷积神经网络(deep convolution neural network)和语义分割(semantic segmentation)用于检测复制粘贴和拼接篡改的图像。Liu等人(2022)提出了一种两阶段的方法。第1阶段为主干自深匹配网络(backbone self deep matching network),第2阶段为Proposal SuperGlue,然后通过设计积分图的集成生成和细化方法,对两个阶段的结果进行集成,得到最优的结果。朱叶等人(2022)提出了一种使用端到端的高分辨率表示扩张注意力网络(high-resolution representation dilation attention network, HRDA-Net)的检测方法,来处理图像中包含拼接和复制粘贴等多种篡改方式的情况。刘丽颖等人(2022)提出了一个基于区域损失的U形网络来检测小篡改区域。Nazir等人(2022)提出了一个基于DenseNet-41的Mask-RCNN(mask region-based convolution neural network)模型以获取更好的图像特征。Weng等人(2024)提出了UCM-Net,将多个不对称跨层连接的新型类U-Net模型用于CMFD。基于深度学习模型的优点在于其具有强大的学习能力,可以自动地从数据中学习特征,并且可以选择适当的深度网络模型,构建端到端的图像篡改定位模型,以直接输出篡改定位结果,提升了检测效率。尤其在当今的大数据时代,深度学习模型可以充分发挥其潜力,因此基于深度学习的检测模型在大规模和复杂的取证场景中具有更好的前景。然而,就目前而言,基于深度学习的方法的泛化性和鲁棒性有待提高。

近年来,CMFD方法的检测准确性越来越高,但普遍存在以下几个问题:1)难以检测平滑和小的篡改区域;2)提取到的特征较多时,算法的运行效率较低;3)当图像内容相似度过高时,容易出现误报,虚警率较高。针对上述问题,本文提出一种新的基于MP-DBSCAN和点密度过滤的CMFD方法,具体贡献如下:1)提出一种新的基于匹配对的密度聚类算法MP-DBSCAN,针对匹配对的一侧进行聚类,并结合匹配对的另一侧较好地区分了空间上距离较近的簇,使得聚类效果得以提升,并可以有效地应对篡改区域存在多对等复杂情况;2)提出“先验”的概念,通过构造先验区域,确定了篡改区域的大致范围,为精确的篡改定位奠定了基础;3)提出“点密度”的概念,并设计了一种依据点密度过滤离群点的方法,通过删除低密度簇,降低虚警率。

1 本文方法

本文所提方法的流程如图1所示。首先,通过图像尺度标准化和降低对比度阈值提取大量SIFT关键点。然后,根据关键点的灰度值将关键点分成

不同的组，分别在每个组内进行关键点匹配，加快匹配速度。随后，提出了一种新的 MP-DBSCAN 聚类算法，聚类对象为匹配对的一侧，另一侧作为聚类过程的约束条件，即使篡改区域在空间上距离较近，也能有效地对关键点进行分组，其效果优于传统 DBSCAN。接下来，根据簇内的匹配对构建先验区域，确定篡改区域的大致范围，并根据先验区域的面积和先验区域中关键点的数量计算点密度。过滤点密度低的簇，降低检测结果的虚警率；在剩下的高密度簇内估计仿射变换，并进行篡改定位。

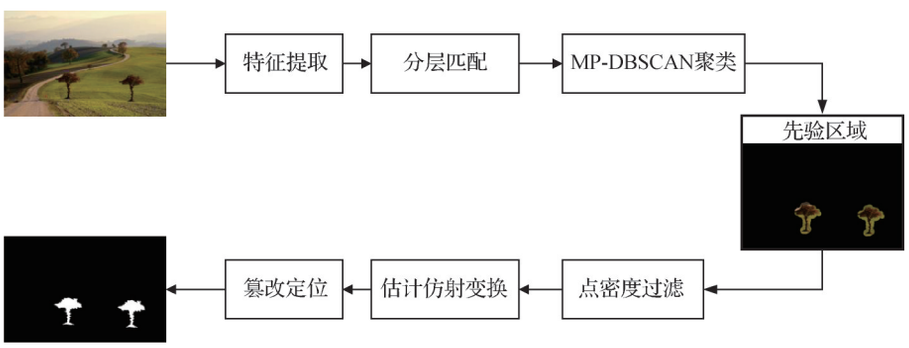


图 1　本文方法流程

Fig. 1　Framework of the proposed method

1.1　特征提取

由于 SIFT 特征提取算法在小篡改区域和平滑篡改区域提取到的特征较少，这类篡改区域很难被检测到。针对这一问题，通过将图像尺度标准化和降低对比度阈值以提取足够特征。其中标准化过程为将低分辨率图像放大，放大倍数 s 设置为

$$s=\begin{cases}\dfrac{3\,000}{\max(M,N)} & \max(M,N)<3\,000\\ 1 & \max(M,N)\geqslant 3\,000\end{cases} \tag{1}$$

式中，M,N 分别是输入图像的长和宽。调整后，该图像边长的最大值为 3 000，图像的边长比例不变。另外降低提取 SIFT 特征参数中的对比度阈值，本文实验中对比度阈值设为 0.1。提取到的特征集 $\boldsymbol{K}$ 表示为 $\boldsymbol{K}=\left\{\boldsymbol{k}_i,\boldsymbol{des}_i\middle|\boldsymbol{k}_i=(x_i,y_i,\sigma_i,\theta_i)\right\}$，其中 x_i,y_i 表示关键点 $\boldsymbol{k}_i$ 的坐标，σ_i,θ_i 表示关键点 $\boldsymbol{k}_i$ 的尺度和方向。$\boldsymbol{des}_i$ 是关键点 $\boldsymbol{k}_i$ 的描述子，是一个 128 维的向量。

1.2　分层匹配

1.2.1　关键点分层

在复制粘贴篡改图像中，正确匹配点的灰度值通常非常接近，因此可以根据关键点所在位置的灰度值进行分层，并在层内进行匹配。通过分层匹配的策略，可以加快匹配速度，同时减少错误匹配。在本文的实验中，将关键点分为 L 层，每层的灰度值范围 $[a_i,b_i]$ 为

$$\begin{cases}a_i=(i-1)\times(\omega_2-\omega_1)\\ b_i=\min(a_i+\omega_2,255)\end{cases} \tag{2}$$

式中，$i=1,\cdots,L,\omega_1=10$，代表层与层间的重叠度，$\omega_2=30$，代表每层的长度。每层内关键点的灰度值都在该层的范围之内。每一层的关键点集 $\boldsymbol{Q}_i$ 表示为

$$\boldsymbol{Q}_i=\left\{\boldsymbol{k}_j\middle|a_i\leqslant Gray(\boldsymbol{k}_j)\leqslant b_i,\boldsymbol{k}_j\in\boldsymbol{K}\right\} \tag{3}$$

式中，函数 $Gray$ 表示以该像素为中心的 3×3 区域的灰度均值。

1.2.2　关键点匹配

考虑到篡改区域可能被复制多次，一个关键点可能会存在多个匹配点；因此，本文中采取的匹配策略为 G2NN（Amerini 等，2011）。匹配过程在每一个分层的关键点集 $\boldsymbol{Q}_i$ 内，对于每一个关键点 $\boldsymbol{k}\in\boldsymbol{Q}_i$，计算该关键点与层内其他 $n-1$ 个关键点的欧氏距离并升序排序，即 $d_1\leqslant d_2\leqslant\cdots\leqslant d_{n-1}$。从 d_2 开始，依次计算每一个欧氏距离与它后面相邻的欧氏距离的比值，当且仅当

$$\frac{d_j}{d_{j+1}}<T_d,\ j=1,\cdots,n-1 \tag{4}$$

时停止。式中，$T_d=0.37$，此时欧氏距离 $d_1,\cdots,d_j$ 所对应的关键点为 $\boldsymbol{k}$ 的匹配点，将匹配对记为 $(\boldsymbol{k},\boldsymbol{k}')$，表示 $\boldsymbol{k}'$ 是 $\boldsymbol{k}$ 的匹配点。

1.3　MP-DBSCAN 聚类

本节提出了一种基于匹配对的密度聚类算法

MP-DBSCAN，该聚类算法与传统DBSCAN的区别如表1所示。

1）聚类半径的选取方法不同。传统DBSCAN中聚类半径的设定带有很大的主观性，在检测多幅图像时使用的是相同的半径。由于每幅图像的关键点分布情况不同，对所有图像使用相同的聚类半径带有一定的主观性，所以传统DBSCAN面对复杂的篡改取证场景效果不理想。而MP-DBSCAN根据每幅图像的关键点及其匹配点的分布情况，动态地生成聚类半径，能够达到较好的聚类效果。

2）聚类对象不同。传统DBSCAN的聚类对象是匹配后的所有关键点，当篡改区域越接近时，两个匹配的关键点之间的距离就越小，因此很容易将匹配对两侧的点聚在一起，影响最终检测结果。考虑到关键点成对存在，MP-DBSCAN使用匹配对的一侧进行聚类。一方面，便于分开相邻的成对区域；另一方面，聚类对象的数量只有原先的一半，提高了聚类速度。

3）聚类过程中计算点的邻域的方式不同。传统DBSCAN只使用距离条件来判定一个点的邻域，空间距离较近的关键点容易聚成一个簇，导致检测结果缺失；实际上，这些关键点可能属于不同的篡改区域。而MP-DBSCAN使用了关键点的匹配点来约束聚类过程。因此在MP-DBSCAN算法中，除了关键点要满足距离条件外，其匹配点附近还需满足特定的分布情况：取这两点的匹配点，并分别获取匹配点周围指定数量的点，得到两个点集；那么，这两个点集的交集所包含的点的数量需大于一定的阈值。采用这种方法，即使不同的篡改区域相距较近，也能够将属于不同区域的匹配对进行分组，从而改善了聚类效果。

结果表明，相比于传统的DBSCAN算法，MP-DBSCAN算法的聚类效果更好，可以有效地应对篡改区域存在多对或者篡改区域距离较近等复杂情况，提高了检测结果的准确性。下面，介绍MP-DBSCAN聚类算法的步骤。

表1　MP-DBSCAN和传统DBSCAN的区别

Table 1　The differences between MP-DBSCAN and traditional DBSCAN

区别	MP-DBSCAN	传统DBSCAN
聚类半径	动态选取半径	人为选取固定的半径
聚类对象	匹配对的一侧	所有匹配的关键点
邻域判定方式	关键点之间的距离以及关键点的匹配点附近的点构成点集的交集情况	关键点之间的距离

1.3.1　统一匹配对方向

因为匹配点成对存在，所以只对匹配对的一侧进行聚类依旧能够达到对匹配对分组效果。并且，使用单侧聚类可以避免由于匹配对之间距离过小，而将同一个匹配对中的关键点聚在一起的情况发生。由于在特征匹配过程中无法确定匹配对的某一个关键点是属于源区域还是目标区域，本文给匹配对设定了一个方向：匹配对左侧是源区域的点，右侧是目标区域的点。如图2（a）所示的理想情况，有4个匹配对$(\boldsymbol{p}_1,\boldsymbol{p}_1')$，$(\boldsymbol{p}_2,\boldsymbol{p}_2')$，$(\boldsymbol{p}_3,\boldsymbol{p}_3')$，$(\boldsymbol{p}_4,\boldsymbol{p}_4')$，所有匹配对的左侧都在源区域，而所有匹配对的右侧都在目标区域。在这种情况下，可以使用这4个匹配对估计一个仿射矩阵$\boldsymbol{H}_1$。但实际上，由于匹配过程无法区分关键点到底是属于源区域还是目标区域，所以实际得到的匹配对可能是$(\boldsymbol{p}_1',\boldsymbol{p}_1)$，$(\boldsymbol{p}_2,\boldsymbol{p}_2')$，$(\boldsymbol{p}_3,\boldsymbol{p}_3')$，$(\boldsymbol{p}_4',\boldsymbol{p}_4)$，如图2（b）所示，红色虚线的匹配对$(\boldsymbol{p}_1',\boldsymbol{p}_1)$和$(\boldsymbol{p}_4',\boldsymbol{p}_4)$与标准情况的方向不同，与实际需求不符，所以该种情况下估计的仿射矩阵$\boldsymbol{H}_2 \neq \boldsymbol{H}_1$，仿射矩阵的估计精度受到较大影响。并且红色连线的匹配对$(\boldsymbol{p}_1',\boldsymbol{p}_1)$，$(\boldsymbol{p}_4',\boldsymbol{p}_4)$满足的仿射变换关系与蓝色连线的匹配对$(\boldsymbol{p}_2,\boldsymbol{p}_2')$，$(\boldsymbol{p}_3,\boldsymbol{p}_3')$不同，红色连线的匹配对可能被当成错误匹配而删除，实际上红色连线的匹配对调换一下方向就是与正确的匹配对。因此需要将匹配对统一方向，让聚类对象全属于源区域或者目标区域，尽可能地将属于源区域和目标区域的关键点区分开，以提高仿射矩阵的估计精度。本文中规定，匹配对$(\boldsymbol{p},\boldsymbol{p}')$的方向总是$\boldsymbol{p}$到$\boldsymbol{p}'$的，即$\boldsymbol{p}$属于源区域，$\boldsymbol{p}'$属于目标区域，且满足

$$(x < x') \| (x = x', y < y') \tag{5}$$

式中，x，y是关键点$\boldsymbol{p}$的坐标，x'，y'是关键点$\boldsymbol{p}'$的坐标。否则，需要将方向对调，即将该匹配对中两个关键点的位置对调。值得注意的是，本文虽然假设了

匹配对的方向，但主要目的是尽可能区分源区域和目标区域中的关键点，提高仿射变换估计的准确性，并不能直接分辨出源区域和目标区域，因为传统的CMFD方法一般都不能区分源区域和目标区域，如Cozzolino等人(2015)、Li和Zhou(2019)、Lyu等人(2021)以及Wang等人(2023)都未能提供此类识别。

1.3.2　计算聚类半径

对于基于密度的聚类而言，聚类效果对于聚类半径的选取比较敏感，使用固定的聚类半径难以达到理想的聚类效果。本文提出的MP-DBSCAN算法，聚类半径根据关键点及其匹配点的分布情况得到，并且每幅图像的聚类半径都不相同，具体计算方法如下：

1)对于匹配对$(\boldsymbol{k}_i, \boldsymbol{k}_i')$中的$\boldsymbol{k}_i$侧，计算每个点与该侧其余所有点的第4近距离并升序排序，得到$d_1, \cdots, d_n$，同理，对于$\boldsymbol{k}_i'$侧，得到$d_1', \cdots, d_n'$；

2)一个点的第4近距离越大，说明该点是离群点的可能性也越大。为了排除离群点，取$d_1, \cdots, d_n$和$d_1', \cdots, d_n'$前半部分均值的α倍作为聚类半径，即

$$Eps = \alpha \times mean(d_1, d_1', \cdots, d_{\lceil n/2 \rceil}, d_{\lceil n/2 \rceil}') \tag{6}$$

式中，函数*mean*表示求均值，本文实验中α取5。

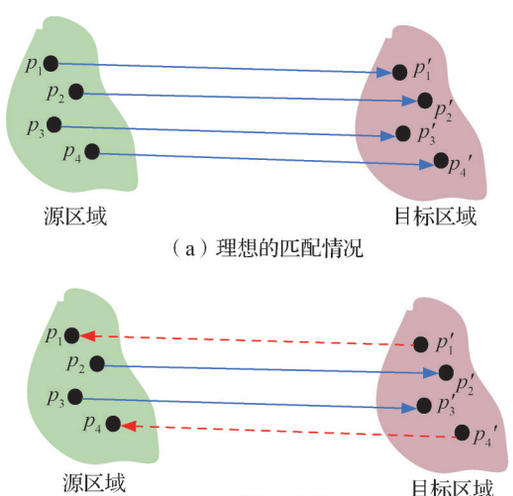


图2　匹配对的方向统一效果

Fig. 2　The effect of unifying the direction of matched pairs ((a) the ideal matching situation; (b) the actual matching situation)

1.3.3　聚类过程

本文提出的MP-DBSCAN算法聚类过程如算法1所示，首先从匹配对集$\boldsymbol{D}$中随机取一个未被访问的点，如果该点邻域内的点数量小于*Minpts*，则将该点标记为噪声点。*MinPts*是一个簇应该包含的最小点数，本文实验中将其设为4。否则就将该点分到当前的簇，并将该点邻域内的所有点执行入队操作。最后依次选取队列中的未被访问点，进行以上操作步骤，直到队列中所有的点都处理完毕，并且所有的点都被赋予簇标记或者被标记为噪声，则聚类结束。在聚类结束后，将包含点数量小于*MinPts*的簇内点作为噪声点删除。

算法1：MP-DBSCAN聚类算法流程。

输入：匹配对集$\boldsymbol{D}$，簇的最小包含点数*MinPts*，聚类半径*Eps*；

输出：匹配对的簇标记；

1)初始化*clusterId* = 0；

2)while 随机从$\boldsymbol{D}$中取一个点$\boldsymbol{p}$是未被访问过的点；

3)　if $\boldsymbol{p}$的邻域内点的数量小于*MinPts* then；

4)　　将$\boldsymbol{p}$标记为噪声点；

5)　else；

6)　　*clusterId*值加1；

7)　　将此时的*clusterId*值赋给$\boldsymbol{p}$的簇标记；

8)　　将$\boldsymbol{p}$的邻域内的点放进队列$\boldsymbol{Q}$；

9)　　while 队列$\boldsymbol{Q}$不为空时；

10)　　从队列中取出一个点$\boldsymbol{q}$；

11)　　将此时的*clusterId*值赋给$\boldsymbol{q}$的簇标记；

12)　　if $\boldsymbol{q}$的邻域内点的数量不小于*MinPts* then；

13)　　将$\boldsymbol{q}$的邻域内的点放进队列$\boldsymbol{Q}$；

14)　　end if；

13)　end while；

14)　end if；

15) end while。

与传统DBSCAN算法相比，MP-DBSCAN算法有以下几点不同：1)聚类半径的计算方法如1.3.2小节中式(6)所示；2)聚类对象是匹配对的一侧；3)确定一个点的邻域的方式不同，如算法2所示。

算法2：MP-DBSCAN聚类中获取点$\boldsymbol{p}_1$的邻域算法流程。

输入：点$\boldsymbol{p}_1$，匹配对集$\boldsymbol{D}$，聚类半径*Eps*，交集最小包含点数β；

输出：点$\boldsymbol{p}_1$的邻域；

1) for each $\boldsymbol{p}_2 \in$ ($\boldsymbol{D}$中$\boldsymbol{p}_1$所在一侧的所有点)；

2) if $\| \boldsymbol{p}_1 - \boldsymbol{p}_2 \| \leqslant Eps$ and;

$IntSect(NearP(\boldsymbol{p}_1'), NearP(\boldsymbol{p}_2')) \geqslant \beta$;

then;

3) $\boldsymbol{p}_2$在$\boldsymbol{p}_1$的邻域内;

4) else;

5) $\boldsymbol{p}_2$不在$\boldsymbol{p}_1$的邻域内;

6) end if;

7) end for。

传统DBSCAN判断两点间的欧氏距离满足

$$\| \boldsymbol{p}_1 - \boldsymbol{p}_2 \| \leqslant Eps \tag{7}$$

式中,Eps是聚类半径,则代表两点处于彼此的邻域内,表示两点在空间距离上是相邻的,这是判断两点属于同一个簇的前提条件。实际上,空间距离上相邻的两点未必属于同一个簇,因此单纯地根据关键点的空间距离进行聚类是不合理的。考虑到关键点成对存在,在聚类过程中利用关键点的匹配点使聚类过程得到约束,能够提高聚类结果的准确性。在MP-DBSCAN算法中,判定点$\boldsymbol{p}_2$是否处于点$\boldsymbol{p}_1$的邻域内,除了这两点间的距离要满足式(7)外,还需要满足

$$IntSect\left(NearP(\boldsymbol{p}_1'), NearP(\boldsymbol{p}_2')\right) \geqslant \beta \tag{8}$$

式中,$\boldsymbol{p}_1'$和$\boldsymbol{p}_2'$分别是$\boldsymbol{p}_1$和$\boldsymbol{p}_2$的匹配点,函数$NearP$表示获取与该点欧氏距离最小的12个点,函数$IntSect$表示求两个点集A和B的交集中点的数量,β在本文实验中取4。由于考虑到关键点成对存在的特性,因此,所提出的MP-DBSCAN聚类算法能够较好地区分空间距离较近的簇,并可以应对篡改图像中存在多对篡改区域的情况。

图3简要展示了MP-DBSCAN的聚类效果和原理。在MP-DBSCAN聚类过程中,对于点$\boldsymbol{p}_1$和$\boldsymbol{p}_2$,首先获得与$\boldsymbol{p}_1'$有最小欧氏距离的点构成的点集$\{\boldsymbol{p}_3', \boldsymbol{p}_4'\}$以及与$\boldsymbol{p}_2'$有最小欧氏距离的点构成的点集$\{\boldsymbol{p}_5', \boldsymbol{p}_6'\}$。由于$\{\boldsymbol{p}_3', \boldsymbol{p}_4'\} \cap \{\boldsymbol{p}_5', \boldsymbol{p}_6'\} = \varnothing$,因此$\boldsymbol{p}_1$和$\boldsymbol{p}_2$所在的匹配对不会分在同一个簇,同理可以判断其他匹配对之间的关系。聚类后,$\boldsymbol{p}_1, \boldsymbol{p}_3, \boldsymbol{p}_4$分到同一个簇,$\boldsymbol{p}_2, \boldsymbol{p}_5, \boldsymbol{p}_6$分到另一个簇,达到了理想的聚类效果。而传统的DBSCAN会将这些点都分到同一个簇。图中所示的情况仅为简要展示算法原理,实际情况远比图示复杂。

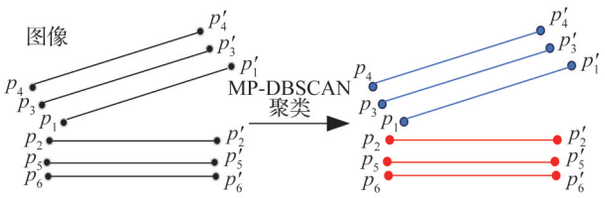


图3 MP-DBSCAN算法聚类效果

Fig. 3 Clustering effect of the MP-DBSCAN algorithm

1.3.4 构建先验区域

在聚类过程结束之后,可以根据簇内的匹配对拟合得到该簇所在篡改区域的大致范围,文中称为先验区域,由簇内匹配对的坐标和尺度计算得到,具体过程如下:

1)簇中的一个关键点$\boldsymbol{k} = (x, y, \sigma, \theta)$,其构成的区域$\boldsymbol{R}(u, v)$为

$$\boldsymbol{R}(u,v) = \begin{cases} 1 & (u-x)^2 + (v-y)^2 \leqslant (\lambda \times \sigma)^2 \\ 0 & (u-x)^2 + (v-y)^2 > (\lambda \times \sigma)^2 \end{cases} \tag{9}$$

式中,$u = [1, \cdots, M]$,$v = [1, \cdots, N]$,本文实验中$\lambda = 20$,M,N分别是输入图像的长和宽,即该点构成的区域图像是一幅二值图像,其中值为1的区域的形状为一个圆。

2)计算簇中其余关键点构成的区域并合并;同理,计算其他簇中关键点构成的区域,然后将所有簇构成的区域合并,得到先验区域,如图1所示。其中,每一个簇构成的先验区域大致标记出每一对篡改区域的所在位置。由于存在错误匹配对,先验区域不够精确,因此,本文提出了点密度过滤策略。

1.4 点密度过滤

在1.3节中,本文使用聚类结果构造了先验区域,确定了篡改区域的大致范围。篡改区域内匹配对的数量一般比非篡改区域内匹配对的数量多,且空间分布较密集。同时,匹配对的关键点都分布在先验区域之内。因此可以根据单位面积包含的关键点数量衡量每个先验区域的点密度,如果该先验区域包含篡改区域,则其点密度值应该较大。基于此,本文提出了一种点密度过滤策略,计算由各簇构成的先验区域的点密度值,若该值小于设定的阈值,则过滤该簇。点密度值DP的计算方法为

$$DP = \frac{NP}{S} \tag{10}$$

式中,NP代表该簇中关键点的数量,S为该簇构成的

先验区域的面积。为了提高点密度过滤策略的鲁棒性，点密度阈值的设定根据聚类后簇的数量分级设定，在本文的实验中，点密度阈值T_{dp}为

$$T_{\mathrm{dp}}=\begin{cases}0.000\,25 & NoC<4\\ 0.000\,30 & 4\leqslant NoC<6\\ 0.000\,40 & 6\leqslant NoC<8\\ 0.000\,45 & NoC\geqslant 8\end{cases} \tag{11}$$

式中，NoC为聚类后簇的数量。T_{dp}越大，保留下的簇的点密度越大，其构成的先验区域中包含真实篡改区域的可能性越大。

1.5 估计仿射矩阵

本文使用RANSAC算法来估计仿射矩阵并过滤错误匹配对。对于每一个簇，都可以得到一个对应的仿射矩阵

$$\boldsymbol{H}=\begin{bmatrix}t_{11} & t_{12} & t_x\\ t_{21} & t_{22} & t_y\\ 0 & 0 & 1\end{bmatrix} \tag{12}$$

式中，$t_{11}, t_{12}, t_{21}, t_{22}$是缩放和旋转系数，$t_x, t_y$是平移系数，这6个未知数可以根据3对匹配对的坐标计算得到。对于匹配对$\boldsymbol{k}=(x, y, 1), \boldsymbol{k}'=(x', y', 1)$，若满足

$$\left\|\boldsymbol{k}'-\boldsymbol{H}\boldsymbol{k}\right\|\leqslant T_o \tag{13}$$

则为正确的匹配对，否则为错误匹配对，并将这类匹配对删除。式中，$T_o=10$。

1.6 篡改定位

本文参考Wang等人(2023)的方法，通过簇内的关键点构建感兴趣区域(region of interest，ROI)热图，其像素值范围为[0, 1]。在检测图像中，只有对应位置的ROI热图像素值不为0的像素才参与定位过程。对于其中一个簇，通过该簇的仿射矩阵，得到像素$\boldsymbol{a}$的ZNCC(zero-mean normalized cross-correlation)相关系数，具体为

$$corr(\boldsymbol{a})=\frac{\sum\limits_{\mu\in\boldsymbol{\Omega}(\boldsymbol{a})}(I(\mu)-\bar{I})(V(\mu)-\bar{V})}{\sqrt{\sum\limits_{\mu\in\boldsymbol{\Omega}(\boldsymbol{a})}(I(\mu)-\bar{I})^2(V(\mu)-\bar{V})^2}} \tag{14}$$

式中，$I(\boldsymbol{a})$为像素$\boldsymbol{a}$的灰度值，$V(\boldsymbol{a})$为像素$\boldsymbol{a}$经过仿射矩阵变换位置后的对应像素的灰度值，$\boldsymbol{\Omega}(\boldsymbol{a})$为以像素$\boldsymbol{a}$为中心的5×5像素区域，$\bar{I}$代表以像素$\boldsymbol{a}$为中心的5×5像素区域灰度均值，$\bar{V}$代表以像素$\boldsymbol{a}$仿射变换后的对应像素为中心的5×5像素区域灰度均值。若$corr(\boldsymbol{a})\geqslant T_z$，则将该像素标记为篡改像素，本文实验中，$T_z=0.6$。

以相同的方法得到逆仿射变换检测结果和其余簇的检测结果，将所有结果合并。之后进行图像的形态学操作，如去除小面积、填充内部空洞等，得到最终的检测结果。

2 实验结果与分析

2.1 数据集

1)FAU数据集(Christlein等，2012)。此数据集包含的图像分辨率较高，平均分尺寸为3 000×2 300像素。其中所有类型的篡改图像都是由48幅原始图像经过不同的篡改方式得到。本文实验中，使用了该数据集的1 584幅篡改图像，其中基础平移篡改图像48幅，旋转篡改图像384幅，缩放篡改图像480幅，JPEG篡改图像432幅，添加噪声篡改图像240幅，具体情况如表2所示。

表2 攻击的参数设置

Table 2 Setting of the attacks

篡改类型	篡改程度	参数标准
旋转(rotation)	2, 4, 6, 8, 10, 20, 60, 180	角度(angle)
缩放(scale)	91∶2∶109	尺度(%)
压缩(JPEG compression)	20∶10∶100	质量因子(QF)
噪声(noise)	0.02∶0.02∶0.10	标准差(standard deviation)

2)MICC-F600数据集(Amerini等，2013)。此数据集共包含了600幅图像，其中440幅是原始的未篡改图像，另外160幅是经过篡改的图像。该数据集的图像分尺寸从800×533像素到3 888×2 592像素不等。本文实验中，使用了该数据集的160幅篡改图像，其中基础平移篡改图像40幅，旋转篡改图像40幅，缩放篡改图像40幅，一对多篡改图像40幅。

3)GRIP数据集(Cozzolino等，2015)。此数据集包含80幅原始图像和80幅平移篡改图像，图像尺

寸皆为768 × 1 024像素，本文实验中使用了其中的80幅篡改图像。

4）CASIA v2.0数据集。此数据集包含7 491幅原始图像和5 123幅篡改图像，主要有拼接和复制粘贴两种类型的篡改图像。本文实验中使用了其中的1 313幅复制粘贴篡改图像（Wu等，2018），其尺寸从240 × 180像素到900 × 600像素不等。

2.2 实验对比分析

为了检测本文提出的CMFD方法性能，进行了参数验证实验和消融对比实验，并在FAU、MICC-F600、GRIP和CASIA v2.0这4个数据集上与其他几个经典和最近的CMFD方法进行对比，这几个方法分别是：传统的方法，如Cozzolino等人（2015）、Zandi等人（2016）、Li和Zhou（2019）、Lyu等人（2021）和Wang等人（2023）；深度的检测方法，如Wu等人（2018）和Chen等人（2021），两个深度方法的运行和实验参照Chen等人（2021）文中的实验设置。本文使用精确率*precision*、召回率*recall*和综合评价指标F_1分数对实验结果进行评估。最后，给出了各检测方法的可视化检测结果对比，并对各方法的计算效率进行了对比。

2.2.1 参数验证

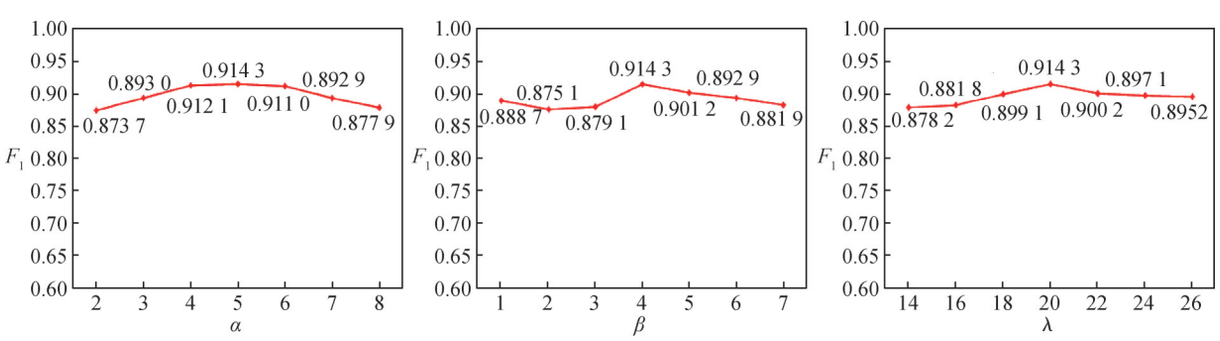
本节对本文方法提出的MP-DBSCAN和点密度过滤策略中的主要参数进行验证实验，如表3所示，以证明参数选取的可靠性。

在MP-DBSCAN算法中，主要的参数有式（6）中求聚类半径的扩大系数α、式（8）中交集最小包含点数β以及式（9）中构建先验区域的关键点尺度半径的扩大系数λ，其实验参数设计及结果如图4所示。从图4（a）可以看出，α的取值设为2～8，步长为1，并在α取5时的实验结果最好。以5为基准，随着α的增大和减小，F_1分数大致为下降趋势，尤其是α取2或者8时，检测结果下降得较多，这是因为聚类半径过小或者过大会对聚类结果产生较大的影响，从而影响定位效果。从图4（b）可以看出，β值设为1～7，步长为1，并在β取4时效果最好。以4为基准，随着β的增大或减小，F_1分数大致为下降趋势。这是因为β越小，在不同的篡改区域相距较近时，交集包含的点数很容易超过较小的β值，容易将属于不同篡改区域的匹配对聚在一起；而β越大，在篡改区域提取的匹配点较少时，交集包含的点数很难超过较大的β值，因此有些本属于相同篡改区域的匹配对因不满足阈值条件，反而不能聚在一起。从图4（c）可以看出，λ的值设为14～26，步长为2，并在λ取20时效果最好。使用不同的λ值构建的先验区域不同，同时该先验区域的点密度值也会不同。因此，不合适的λ值会影响点密度过滤阶段，进而影响定位结果。如表4所示，实验中将点密度阈值T_{dp}设置了7种不同的组合，在设计的第1种情形中，当簇的数量$Noc \in [1,2)$时，点密度阈值T_{dp}设为0.000 25；当

表3 主要参数设置

Table 3 Setting of the main parameters

参数	取值
聚类半径扩大系数α	5
交集最小包含点数β	4
关键点尺度扩大系数λ	20
点密度阈值T_{dp}	$T_{dp}=\begin{cases}0.000\,25 & NoC<4\\0.000\,30 & 4\leqslant NoC<6\\0.000\,40 & 6\leqslant NoC<8\\0.000\,45 & NoC\geqslant 8\end{cases}$



(a) 不同α值的结果　(b) 不同β值的结果　(c) 不同λ值的结果

图4 MP-DBSCAN在FAU基础平移数据集的参数验证实验结果

Fig. 4 The experimental results of parameter calibration of MP-DBSCAN on plain copy move (FAU)

((a) detection results of varying α; (b) detection results of varying β; (c) detection results of varying λ)

表 4　不同 T_{dp} 在 FAU 平移篡改数据集的实验结果

Table 4　The detection results on plain copy move (FAU) of varying T_{dp}

T_{dp}	*NoC*						
	#1	#2	#3	#4	#5	#6	#7
0.000 20	–	–	[1, 4)	–	–	–	–
0.000 25	[1, 2)	[1, 3)	–	[1, 4)	[1, 4)	[1, 5)	[1, 6)
0.000 30	[2, 4)	[3, 5)	[4, 6)	[4, 6)	[4, 6)	[5, 7)	[6, 9)
0.000 35	[4, 6)	[5, 8)	–	–	–	[7, 9)	[9, 11)
0.000 40	[6, 8)	[8, 10)	[6, 8)	[6, 8)	[6, 8)	[9, 11)	[11, 14)
0.000 45	[8, +∞)	[10, +∞)	[8, +∞)	[8, +∞)	–	[11, +∞)	[14, +∞)
0.000 50	–	–	–	–	[8,+∞)	–	–
precision	0.893 8	0.874 4	0.914 2	**0.925 2**	0.887 7	0.918 9	0.905 1
recall	0.917 8	0.918 9	0.917 2	0.915 6	0.915 2	0.915 0	**0.919 7**
F_1	0.899 3	0.889 7	0.910 3	**0.914 3**	0.893 6	0.910 6	0.905 3

注：加粗字体表示每行最优值。“–”表示无相关内容。

簇的数量 $Noc \in [2,4)$ 时，T_{dp} 设为 0.000 3；当簇的数量 $Noc \in [4,6)$ 时，T_{dp} 设为 0.000 35；当簇的数量 $Noc \in [6,8)$ 时，T_{dp} 设为 0.000 4；当簇的数量 $Noc \in [8,+\infty)$ 时，T_{dp} 设为 0.000 45。其余 6 种情形类似，使用不同的 *Noc* 区间设置不同的阈值 T_{dp}。从实验结果看，其中第 4 种组合获得了最佳的 F_1 分数。

2.2.2　消融实验

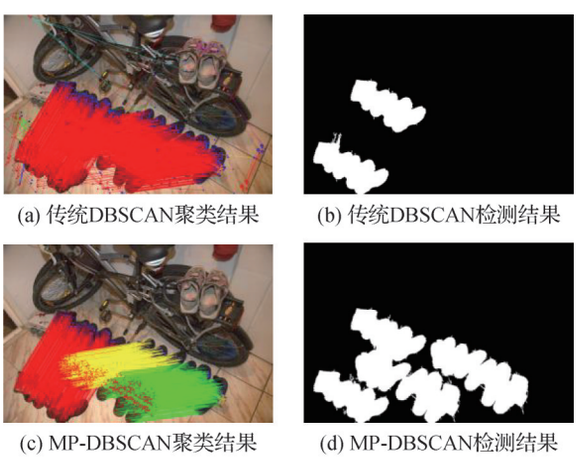
为了验证本文提出的 MP-DBSCAN 聚类算法和点密度过滤策略的有效性，本文在 FAU 数据集上进行消融实验，对比结果如表 5 所示。通过分析表 5 发现，相比传统的 DBSCAN 算法，使用 MP-DBSCAN 算法可以获得更高的 *precision*、*recall* 和 F_1 分数，因为 MP-DBSCAN 能够更好地对匹配对进行分组，尤其是在篡改图像存在多对篡改区域的情况下，如图 5 所示。图 5(a)和图 5(b)分别展示了传统 DBSCAN 的聚类和篡改定位结果，图 5(c)和图 5(d)分别展示了 MP-DBSCAN 的聚类和篡改定位结果。

表 5　FAU 平移篡改消融实验的像素层检测结果

Table 5　The ablation study of the proposed method on plain copy move (FAU) at the pixel level

检测方法	*precision*	*recall*	F_1
传统 DBSCAN	0.874 0	0.820 9	0.831 2
MP-DBSCAN	0.894 2	0.899 2	0.879 0
MP-DBSCAN +点密度过滤	**0.925 2**	**0.915 6**	**0.914 3**

注：加粗字体表示各列最优结果。



(a) 传统DBSCAN聚类结果　(b) 传统DBSCAN检测结果

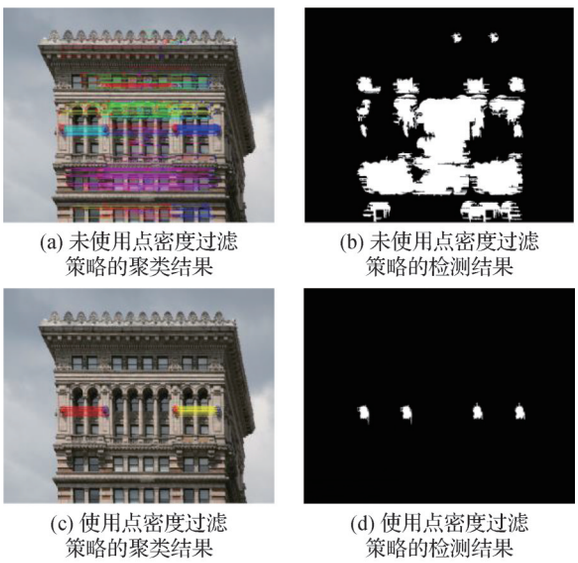
(c) MP-DBSCAN聚类结果　(d) MP-DBSCAN检测结果

图 5　传统 DBSCAN 与 MP-DBSCAN 检测结果

Fig. 5　Detection results between traditional DBSCAN and MP-DBSCAN ((a) the clustering result of traditional DBSCAN; (b) the detection result of traditional DBSCAN; (c) the clustering result of MP-DBSCAN; (d) the detection result of MP-DBSCAN)

从图 5 可以看出，由于传统的聚类方法采用固定聚类半径，将相邻的多个簇合并在一起，导致检测结果较差；而 MP-DBSCAN 的聚类半径是根据关键点及其匹配点的分布情况计算的，该策略能够使匹配对分组更加合理，改善了检测结果。在应用了点密度过滤之后，表 4 检测结果的 *precision*、*recall* 和 F_1 分数都达到了最优值。有无点密度过滤策略的检测结果对比如图 6 所示。图 6(a)和图 6(b)是未使用点密度过滤策略的聚类和篡改定位结果，图 6(c)和

图6(d)为使用了点密度过滤策略的聚类和篡改定位结果。从图6可以看出,点密度过滤策略删除了大量错误的匹配对,提高了检测精度。



(a) 未使用点密度过滤策略的聚类结果　(b) 未使用点密度过滤策略的检测结果

(c) 使用点密度过滤策略的聚类结果　(d) 使用点密度过滤策略的检测结果

图6　有无点密度过滤策略检测结果对比

Fig. 6　Detection results between using the filtering of the point density and without using the filtering of the point density ((a) the clustering result without using the filtering of the point density; (b) the detection result without using the filtering of the point density; (c) the clustering result of using the filtering of the point density; (d) the detection result of using the filtering of the point density)

2.2.3　FAU数据集实验结果

表6展示了在FAU数据集上像素层的检测结果,共使用了48幅平移篡改图像。对比的多个方法的实验结果与Li和Zhou(2019)、Wang等人(2023)文中的数据接近。从表中可以看出,本文方法的*recall*和F_1分数在几种方法中最高,分别达到了0.915 6和0.914 3;本文方法的*precision*为第二高,仅次于Cozzolino等人(2015)方法。本文方法检测结果较好的原因是,所提出的MP-DBSCAN聚类能够更好地对匹配对进行分组,从而最大程度地检测出篡改区域。此外,由于提出的点密度过滤策略尽可能地删除了一些错误匹配,降低了虚警率,进一步增加了检测结果的准确率。

为了验证本文方法对各种类型的篡改图像的鲁棒性,实验分为旋转、缩放、JPEG压缩和添加噪声等4种类型,并分别评估了*precision*、*recall*和F_1分数这3个指标,实验结果如图7所示。通过对图中数据的分析,可以发现本文方法在旋转和缩放这两种类型

表6　FAU平移篡改的像素层检测结果

Table 6　The detection results of plain copy move (FAU) at the pixel level

检测方法	*precision*	*recall*	F_1
Cozzolino等人(2015)	**0.939 5**	0.893 4	0.908 3
Zandi等人(2016)	0.760 7	0.895 3	0.795 2
Li和Zhou(2019)	0.899 9	0.889 6	0.884 6
Lyu等人(2021)	0.893 1	0.848 8	0.841 6
Wang等人(2023)	0.905 8	0.891 4	0.880 9
Wu等人(2018)	0.320 0	0.374 7	0.298 3
Chen等人(2021)	0.376 3	0.271 2	0.275 4
本文方法	0.925 2	**0.915 6**	**0.914 3**

注:加粗字体表示各列最优结果。

的攻击中的*recall*和F_1分数是最高的;本文方法在篡改图像添加噪声攻击情况下,其F_1分数是最高的。在篡改图像经历JPEG压缩的情况下,本文方法的性能在JPEG压缩程度较高时,表现为最好;在JPEG压缩程度较低时,表现也仅次于Cozzolino等人(2015)方法。从图中可以看出,随着压缩程度的增加,各种检测方法的性能都急剧下降,这是因为经过压缩后的图像可提取到的特征减少,并且经过压缩后图像内容失真。本文方法的优势体现在以下几个方面:1)提出的MP-DBSCAN算法能够较好地将属于不同篡改区域的匹配对进行分组,在应对包含多区域篡改以及篡改区域较近等复杂情况下有明显的优势。2)虽然图像经过JPEG压缩和添加噪声等攻击后,篡改区域能够提取到的特征数量大大降低,由于MP-DBSCAN的自适应半径选取策略,在较好地将匹配对进行分组的同时,最大程度地保留了正确的匹配对,提高了这类图像检测结果的准确率。3)提出的点密度过滤策略能够有效地过滤错误匹配对,进一步提高检测精度。总体来看,本文提出的方法能够有效地检测出篡改区域,并且对平移、旋转、缩放、JPEG压缩和添加噪声等攻击具有较好的鲁棒性。

2.2.4　MICC-F600数据集实验结果

为了进一步验证本文方法的有效性,本节展示了多个方法在MICC-F600数据集上的对比实验结果,对比的多个方法的实验结果与Li和Zhou(2019)、Niu等人(2021)和Wang等人(2023)文中的数据接近。MICC-F600数据集包含了多种篡改方式,例如一对多、缩放和旋转等,这些篡改类型对于

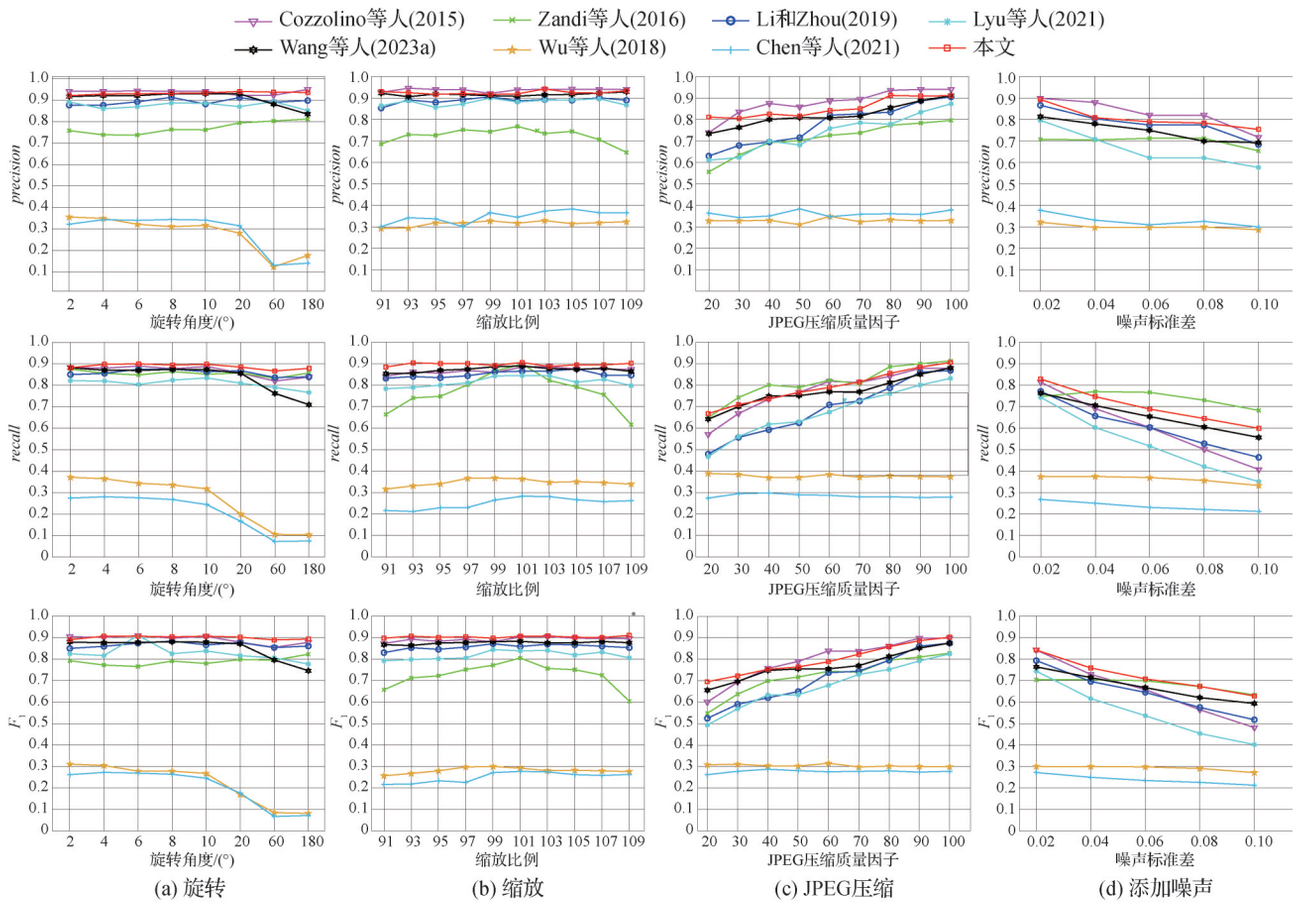


图 7　不同攻击和不同方法在 FAU 中的 *precision*，*recall* 和 F_1 曲线

Fig. 7　*Precision*, *recall*, and F_1 curves for different methods on FAU with various attacks ((a) rotation; (b) scale; (c) JPEG compression; (d) additional noise)

CMFD 方法来说具有较高的挑战性。表 7 列出了各种方法在 MICC-F600 数据集上的实验结果。从表中数据可以看出，在 MICC-F600 数据集上，本文方法的 *recall* 和 F_1 分数均位居首位，并且也具有较高的 *precision*；这是因为 MP-DBSCAN 算法能够有效地对匹配对进行分组，从而能够检测出篡改图像中存在的多对篡改区域。

2.2.5　GRIP 数据集实验结果

GRIP 数据集中的图像则具有较低的分辨率，并且其中的篡改区域较为平滑，给 CMFD 检测带来较高的挑战。表 8 显示了各种方法在 GRIP 数据集上的实验结果，对比的多个方法的实验结果与 Li 和 Zhou(2019)、Gan 等人(2022)以及 Wang 等人(2023)文中的数据接近。从表中数据可知，本文方法的 *recall* 和 F_1 分数分别达到了 0.960 8 和 0.939 1，在所有方法中排名第 1；这是因为本文采用了点密度过滤策略能够准确地过滤错误匹配对，从而降低了虚警率。总体而言，本文方法在此数据集上的 F_1 分数位居首位，表明本文方法能够有效地检测图像中的篡改区域，且性能优于当前的方法。

表 7　MICC-F600 数据集像素层检测结果

Table 7　The detection results of MICC-F600 at the pixel level

检测方法	*precision*	*recall*	F_1
Cozzolino 等人(2015)	**0.911 0**	0.827 3	0.853 4
Zandi 等人(2016)	0.668 8	0.704 1	0.646 3
Li 和 Zhou(2019)	0.855 6	0.807 3	0.819 8
Lyu 等人(2021)	0.859 5	0.834 8	0.826 8
Wang 等人(2023)	0.870 4	0.841 0	0.832 4
Wu 等人(2018)	0.242 7	0.259 3	0.204 3
Chen 等人(2021)	0.304 0	0.170 6	0.177 7
本文	0.907 5	**0.874 4**	**0.890 6**

注：加粗字体表示各列最优结果。

表8 GRIP数据集像素层检测结果

Table 8 The detection results of GRIP at the pixel level

检测方法	*precision*	*recall*	F_1
Cozzolino等人(2015)	0.901 8	0.925 3	0.906 1
Zandi等人(2016)	0.790 4	**0.967 2**	0.842 4
Li和Zhou(2019)	0.902 4	0.952 3	0.923 0
Lyu等人(2021)	0.826 6	0.844 4	0.824 0
Wang等人(2023)	0.890 3	0.937 0	0.893 2
Wu等人(2018)	0.227 4	0.368 7	0.242 7
Chen等人(2021)	0.340 3	0.342 1	0.288 7
本文	**0.918 3**	0.960 8	**0.939 1**

注:加粗字体表示各列最优结果。

2.2.6 CASIA v2.0数据集实验结果

表9展示了本文方法与几个传统检测方法和深度学习检测方法在CASIA v2.0数据集上的检测结果,对比的多个方法的实验结果与Zhong和Pun(2020)以及Wang等人(2023)文中的数据接近。CASIA v2.0数据集中的篡改图像尺寸从240×180像素到900×600像素不等,并且包含了多种篡改方式,如旋转和缩放等。从表中数据所示,本文方法的*recall*和F_1分数分别达到了0.943 5和0.856 7,超过其他的对比方法。这是由于本文方法通过图像尺度标准化和降低提取特征时的对比度阈值,在分辨率较低的图像中提取到了大量关键点,并且通过MP-DBSCAN算法进行聚类,在较好地将匹配对进行分组的同时,最大程度地保留了正确的匹配对。另外,本文所提出的点密度过滤策略能够准确地过滤错误匹配对,进一步降低了虚警率,提升了本文方法的整体检测性能。

2.2.7 可视化检测结果对比

图8展示了本文方法与其他对比方法在4个数据集检测结果的可视化比较。图8中的第1、2行是FAU数据集上的检测结果,第3、4行是MICC-F600数据集上的检测结果,第5、6行是GRIP数据集上的检测结果,最后两行是CASIA v2.0数据集上的检测结果。从可视化的结果可以看出,即使篡改区域较小且平滑,甚至篡改区域被复制多次,或者篡改区域经过一些后处理攻击,本文方法依然能够检测出大部分篡改区域。相比于其他方法,定位结果更好,证明了本文方法的有效性。

表9 CASIA v2.0数据集像素层检测结果

Table 9 The detection results of CASIA v2.0 at the pixel level

检测方法	*precision*	*recall*	F_1
Cozzolino等人(2015)	0.474 7	0.489 0	0.474 5
Zandi等人(2016)	0.508 3	0.690 2	0.552 9
Li和Zhou(2019)	0.580 6	0.659 9	0.595 3
Lyu等人(2021)	0.787 6	0.758 8	0.749 2
Wang等人(2023)	**0.807 4**	0.803 2	0.780 1
Wu等人(2018)	0.415 9	0.582 3	0.444 3
Chen等人(2021)	0.520 2	0.546 2	0.498 9
本文方法	0.803 6	**0.943 6**	**0.856 8**

注:加粗字体表示各列最优结果。

2.2.8 计算效率对比分析

图9给出了各检测方法的平均单幅图像的计算效率对比结果,从图中可以看出,与传统的方法相比,本文方法的计算效率介于Wang等人(2023)和Zandi等人(2016)方法之间。另外,从图10可以看出,造成本文方法计算效率不高的原因是提取大量的特征后,关键点的匹配过程较慢,导致整体检测流程时间较长。因此,未来可以优化匹配过程,以加快整体检测流程。从实验结果来看,本文方法在4个公开的数据集上的实验结果都是最好,即使图像的篡改区域较小或者平滑,甚至经过了一些后处理攻击,如旋转、缩放、JPEG压缩和添加噪声等,本文方法都可以较好地检测出大部分的篡改区域,并且效果优于现有的方法。

3 结 论

为了准确地检测篡改区域并降低虚警率,本文提出了一种基于MP-DBSCAN聚类和点密度过滤的CMFD方法。首先,通过图像尺度标准化和降低特征提取的对比度阈值来获取大量关键点,并根据关键点的灰度值进行分层,以加快匹配速度。其次,提出了基于匹配对的密度聚类算法MP-DBSCAN,能够有效地将匹配对分组。然后,利用簇内的关键点构建先验区域,标记出篡改区域的大致范围,并提出了点密度过滤策略来过滤错误匹配对,即删除点密度较低的簇。最后,通过估计各个簇的仿射矩阵,并使用ZNCC算法计算原始像素点与根据仿射矩阵转换

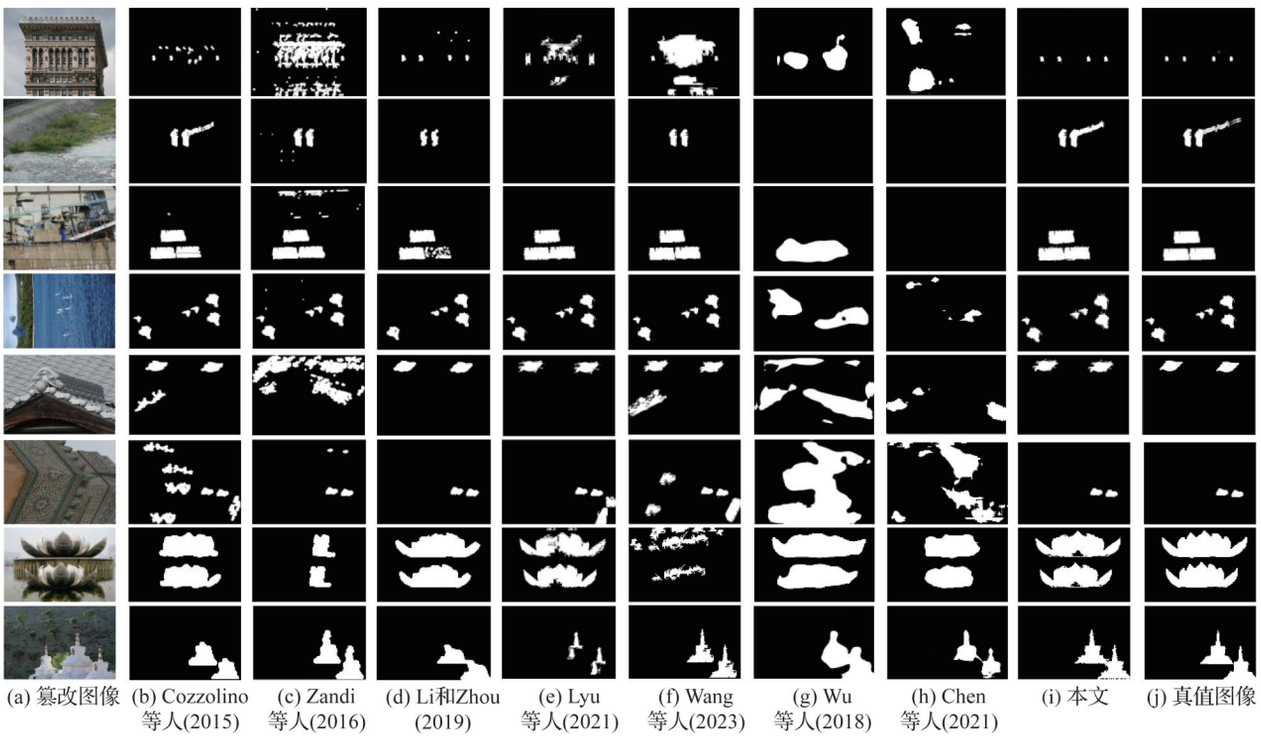


图 8　本文方法与其他方法的检测结果可视化比较

Fig. 8　Visual comparison of the proposed method and other methods ((a) forged images; (b) Cozzolino et al. (2015); (c) Zandi et al. (2016); (d) Li and Zhou (2019); (e) Lyu et al. (2021); (f) Wang et al. (2023); (g) Wu et al. (2018); (h) Chen et al. (2021); (i) our; (j) ground truths)

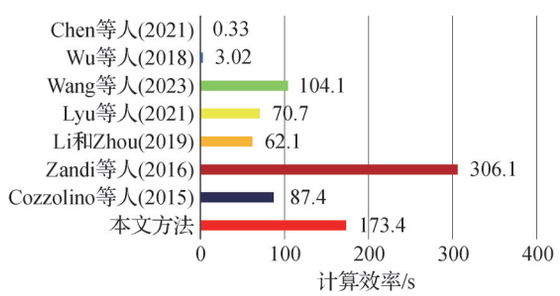


图 9　计算效率对比

Fig. 9　The comparison result of computational efficiency

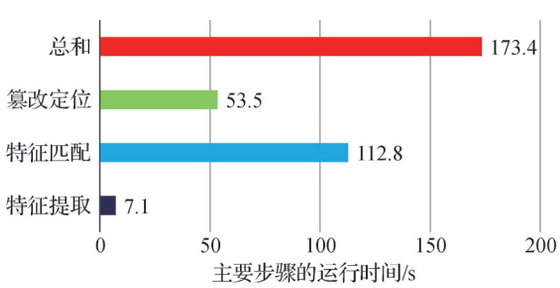


图 10　本文方法的主要步骤运行时间

Fig. 10　The computational time of main steps of the proposed method

后的像素点之间的相关系数，对篡改像素点进行标记，从而定位篡改区域。在 4 个公开数据集上验证了本文方法的性能，实验结果表明，即使篡改图像经过平移、缩放、旋转、JPEG 压缩和添加噪声等攻击，本文方法仍然展现出良好的性能，优于一些经典方法和最近的方法。

虽然与现有的主要方法相比，本文方法在各数据集的整体表现较好，但是，本文方法对于经过 JPEG 压缩和添加噪声的篡改图像检测效果并不十分理想，造成这种情况的原因之一是这类图像的篡改区域能够提取的特征较少。此外，本文方法未能提供源区域和目标区域的识别，并且计算效率不够高。未来的工作将对特征提取进一步优化，以获取更多稳定的特征，并优化特征匹配过程，提高检测效率。同时，进一步探索识别源区域和目标区域的方法，如统计篡改区域边界的纹理信息，为图像篡改检测领域提出更为完善的方案。

参考文献(References)

Thakur A and Jindal N. 2021. Copy move and splicing forgery detection using deep convolution neural network, and semantic segmentation. Multimedia Tools and Applications, 80 (3): 3571-3599

[DOI: 10.1007/s11042-020-09816-3]

Amerini I, Ballan L, Caldelli R, Del Bimbo A, Del Tongo L and Serra G. 2013. Copy-move forgery detection and localization by means of robust clustering with J-Linkage. Signal Processing: Image Communication, 28(6): 659-669 [DOI: 10.1016/j.image.2013.03.006]

Amerini I, Ballan L, Caldelli R, Del Bimbo A and Serra G. 2011. A sift-based forensic method for copy-move attack detection and transformation recovery. IEEE Transactions on Information Forensics and Security, 6(3): 1099-1110 [DOI: 10.1109/TIFS.2011.2129512]

Barni M, Phan Q T and Tondi B. 2021. Copy move source-target disambiguation through multi-branch CNNs. IEEE Transactions on Information Forensics and Security, 16: 1825-1840 [DOI: 10.1109/TIFS.2020.3045903]

Bi X L and Pun C M. 2018. Fast copy-move forgery detection using local bidirectional coherency error refinement. Pattern Recognition, 81: 161-175 [DOI: 10.1016/j.patcog.2018.03.028]

Chen B J, Tan W J, Coatrieux G, Zheng Y H and Shi Y Q. 2021. A serial image copy-move forgery localization scheme with source/target distinguishment. IEEE Transactions on Multimedia, 23: 3506-3517 [DOI: 10.1109/TMM.2020.3026868]

Christlein V, Riess C, Jordan J, Riess C and Angelopoulou E. 2012. An evaluation of popular copy-move forgery detection approaches. IEEE Transactions on Information Forensics and Security, 7(6): 1841-1854 [DOI: 10.1109/TIFS.2012.2218597]

Cozzolino D, Poggi G and Verdoliva L. 2015. Efficient dense-field copy-move forgery detection. IEEE Transactions on Information Forensics and Security, 10(11): 2284-2297 [DOI: 10.1109/TIFS.2015.2455334]

Dixit A and Bag S. 2021. A fast technique to detect copy-move image forgery with reflection and non-affine transformation attacks. Expert Systems with Applications, 182: #115282 [DOI: 10.1016/j.eswa.2021.115282]

Emam M, Han Q and Niu X M. 2016. PCET based copy-move forgery detection in images under geometric transforms. Multimedia Tools and Applications, 75(18): 11513-11527 [DOI: 10.1007/s11042-015-2872-2]

Fischler M A and Bolles R C. 1981. Random sample consensus: a paradigm for model fitting with applications to image analysis and automated cartography. Communications of the ACM, 24(6): 381-395 [DOI: 10.1145/358669.358692]

Fridrich A J, Soukal B D and Lukáš A J. 2003. Detection of copy-move forgery in digital images//Proceedings of Digital Forensic Research Workshop. Cleveland, OH, USA: 19-23

Gan Y F, Zhong J L and Vong C. 2022. A novel copy-move forgery detection algorithm via feature label matching and hierarchical segmentation filtering. Information Processing and Management, 59(1): #102783 [DOI: 10.1016/j.ipm.2021.102783]

Lai Y C, Huang T Q and Jiang R X. 2015. Image region copy-move forgery detection based on Exponential-Fourier moments. Journal of Image and Graphics, 20(9): 1212-1221 (赖玥聪, 黄添强, 蒋仁祥. 2015. 采用指数矩的图像区域复制粘贴篡改检测. 中国图象图形学报, 20(9): 1212-1221) [DOI: 10.11834/jig.20150908]

Li J, Li X L, Yang B and Sun X M. 2015. Segmentation-based image copy-move forgery detection scheme. IEEE Transactions on Information Forensics and Security, 10(3): 507-518 [DOI: 10.1109/TIFS.2014.2381872]

Li X L, Yu N H, Zhang X P, Zhang W M, Li B, Lu W, Wang W and Liu X L. 2021. Overview of digital media forensics technology. Journal of Image and Graphics, 26(6): 1216-1226 (李晓龙, 俞能海, 张新鹏, 张卫明, 李斌, 卢伟, 王伟, 刘晓龙. 2021. 数字媒体取证技术综述. 中国图象图形学报, 26(6): 1216-1226) [DOI: 10.11834/jig.210081]

Li Y M and Zhou J T. 2019. Fast and effective image copy-move forgery detection via hierarchical feature point matching. IEEE Transactions on Information Forensics and Security, 14(5): 1307-1322 [DOI: 10.1109/TIFS.2018.2876837]

Li Y N. 2013. Image copy-move forgery detection based on polar cosine transform and approximate nearest neighbor searching. Forensic Science International, 224(1/3): 59-67 [DOI: 10.1016/j.forsciint.2012.10.031]

Lin C, Lu W, Huang X C, Liu K, Sun W and Lin H H. 2019. Region duplication detection based on hybrid feature and evaluative clustering. Multimedia Tools and Applications, 78(15): 20739-20763 [DOI: 10.1007/s11042-019-7342-9]

Lin C, Lu W, Sun W, Zeng J H, Xu T H and Lai J H. 2018. Region duplication detection based on image segmentation and keypoint contexts. Multimedia Tools and Applications, 77(11): 14241-14258 [DOI: 10.1007/s11042-017-5027-9]

Liu B and Pun C M. 2018. Locating splicing forgery by fully convolutional networks and conditional random field. Signal Processing: Image Communication, 66: 103-112 [DOI: 10.1016/j.image.2018.04.011]

Liu L Y, Wang J X, Cao S L, Zhao L and Zhang X Q. 2022. U-Net for detecting small forgery region. Journal of Image and Graphics, 27(1): 176-187 (刘丽颖, 王金鑫, 曹少丽, 赵丽, 张笑钦. 2022. 检测小篡改区域的U型网络. 中国图象图形学报, 27(1): 176-187) [DOI: 10.11834/jig.210438]

Liu Y Q, Xia C, Zhu X B and Xu S W. 2022. Two-stage copy-move forgery detection with self deep matching and proposal SuperGlue. IEEE Transactions on Image Processing, 31: 541-555 [DOI: 10.1109/TIP.2021.3132828]

Lowe D G. 2004. Distinctive image features from scale-invariant keypoints. International Journal of Computer Vision, 60(2): 91-110 [DOI: 10.1023/B:VISI.0000029664.99615.94]

Lyu Q Y, Luo J W, Liu K, Yin X L, Liu J R and Lu W. 2021. Copy Move Forgery Detection based on double matching. Journal of Visual Communication and Image Representation, 76: #103057 [DOI: 10.1016/j.jvcir.2021.103057]

Mahdian B and Saic S. 2007. Detection of copy-move forgery using a method based on blur moment invariants. Forensic Science International, 171(2/3): 180-189 [DOI: 10.1016/j.forsciint.2006.11.002]

Muhammad G, Hussain M and Bebis G. 2012. Passive copy move image forgery detection using undecimated dyadic wavelet transform. Digital Investigation, 9(1): 49-57 [DOI: 10.1016/j.diin.2012.04.004]

Nazir T, Nawaz M, Masood M and Javed A. 2022. Copy move forgery detection and segmentation using improved mask region-based convolution network (RCNN). Applied Soft Computing, 131: #109778 [DOI: 10.1016/j.asoc.2022.109778]

Niu P, Wang C, Chen W, Yang H and Wang X. 2021. Fast and effective keypoint-based image copy-move forgery detection using complex-valued moment invariants. Journal of Visual Communication and Image Representation, 77: #103068 [DOI: 10.1016/j.jvcir.2021.103068]

Pan X Y and Lyu S W. 2010. Region duplication detection using image feature matching. IEEE Transactions on Information Forensics and Security, 5(4): 857-867 [DOI: 10.1109/TIFS.2010.2078506]

Qin J, Li F, Xiang L Y and Yin C M. 2013. Detection of image region copy-move forgery using radial harmonic Fourier moments. Journal of Image and Graphics, 18(8): 919-923 (秦娟, 李峰, 向凌云, 殷茗茗. 2013. 采用圆谐—傅里叶矩的图像区域复制粘贴篡改检测. 中国图象图形学报, 18(8): 919-923) [DOI: 10.11834/jig.20130805]

Rao Y and Ni J Q. 2016. A deep learning approach to detection of splicing and copy-move forgeries in images//2016 IEEE International Workshop on Information Forensics and Security (WIFS). Abu Dhabi, United Arab Emirates: IEEE: 1-6 [DOI: 10.1109/WIFS.2016.7823911]

Ryu S J, Kirchner M, Lee M J and Lee H K. 2013. Rotation invariant localization of duplicated image regions based on Zernike moments. IEEE Transactions on Information Forensics and Security, 8(8): 1355-1370 [DOI: 10.1109/TIFS.2013.2272377]

Silva E, Carvalho T, Ferreira A and Rocha A. 2015. Going deeper into copy-move forgery detection: exploring image telltales via multi-scale analysis and voting processes. Journal of Visual Communication and Image Representation, 29: 16-32 [DOI: 10.1016/j.jvcir.2015.01.016]

Wang C, Huang Z Q, Qi S R, Yu Y S, Shen G H and Zhang Y S. 2023. Shrinking the semantic gap: spatial pooling of local moment invariants for copy-move forgery detection. IEEE Transactions on Information Forensics and Security, 18: 1064-1079 [DOI: 10.1109/TIFS.2023.3234861]

Wang X Y, Chen W C, Niu P P and Yang H Y. 2022. Image copy-move forgery detection based on dynamic threshold with dense points. Journal of Visual Communication and Image Representation, 89: #103658 [DOI: 10.1016/j.jvcir.2022.103658]

Wang X Y, Li S, Liu Y N, Niu Y, Yang H Y and Zhou Z L. 2017. A new keypoint-based copy-move forgery detection for small smooth regions. Multimedia Tools and Applications, 76(22): 23353-23382 [DOI: 10.1007/s11042-016-4140-5]

Wang X Y, Wang X Q, Niu P P and Yang H Y. 2024. Accurate and robust image copy-move forgery detection using adaptive keypoints and FQGPCET-GLCM feature. Multimedia Tools and Applications, 83(1): 2203-2235 [DOI: 10.1007/s11042-023-15499-3]

Weng S W, Zhu T G, Zhang T C and Zhang C Y. 2024. UCM-Net: a U-Net-like tampered-region-related framework for copy-move forgery detection. IEEE Transactions on Multimedia, 26: 750-763 [DOI: 10.1109/TMM.2023.3270629]

Wu Y, Abd-Almageed W and Natarajan P. 2018. BusterNet: detecting copy-move image forgery with source/target localization//Proceedings of the 15th European Conference on Computer Vision. Munich, Germany: Springer: 170-186 [DOI: 10.1007/978-3-030-01231-1_11]

Yang F, Li J W, Lu W and Weng J. 2017. Copy-move forgery detection based on hybrid features. Engineering Applications of Artificial Intelligence, 59: 73-83 [DOI: 10.1016/j.engappai.2016.12.022]

Zandi M, Mahmoudi-Aznaveh A and Talebpour A. 2016. Iterative copy-move forgery detection based on a new interest point detector. IEEE Transactions on Information Forensics and Security, 11(11): 2499-2512 [DOI: 10.1109/TIFS.2016.2585118]

Zhang Y L, Zhu G P, Wang X, Luo X Y, Zhou Y C, Zhang H L and Wu L G. 2023. CNN-Transformer based generative adversarial network for copy-move source/target distinguishment. IEEE Transactions on Circuits and Systems for Video Technology, 33(5): 2019-2032 [DOI: 10.1109/TCSVT.2022.3220630]

Zhong J L and Pun C M. 2020. An end-to-end dense-InceptionNet for image copy-move forgery detection. IEEE Transactions on Information Forensics and Security, 15: 2134-2146 [DOI: 10.1109/TIFS.2019.2957693]

Zhu Y, Chen C F, Yan G, Guo Y C and Dong Y F. 2020. AR-Net: adaptive attention and residual refinement network for copy-move forgery detection. IEEE Transactions on Industrial Informatics, 16(10): 6714-6723 [DOI: 10.1109/TII.2020.2982705]

Zhu Y, Yu Y L and Guo Y C. 2022. HRDA-Net: image multiple manipulation detection and location algorithm in real scene. Journal on Communications, 43(1): 217-226 (朱叶, 余宜林, 郭迎春. 2022. HRDA-Net: 面向真实场景的图像多篡改检测与定位算法. 通信学报, 43(1): 217-226) [DOI: 10.11959/j.issn.1000-436x.2022016]

作者简介

蔺聪，男，讲师，主要研究方向为信息安全、多媒体取证和数字图像取证。E-mail: lincong0310@gmail.com

黄轲，男，硕士研究生，主要研究方向为图像篡改检测。E-mail: jacobi0727@163.com

温雅敏，女，教授，主要研究方向为信息安全。E-mail: wenyamin@gdufe.edu.cn

卢伟，男，教授，博士生导师，主要研究方向为多媒体信息安全、数字取证、信息隐藏、隐私保护和多媒体大数据智能。E-mail: luwei3@mail.sysu.edu.cn