第 59 卷 第 2 期/2022 年 1 月/激光与光电子学进展 研究论文

激光与光电子学进展 先进成像

基于递进式混合特征的篡改图片识别算法

彭一航，叶武剑*，刘怡俊

广东工业大学信息工程学院，广东 广州 510006

摘要 针对现有检测算法难以抵抗组合攻击的缺点，提出一种基于混合特征的复制-粘贴篡改识别算法。与传统算法使用固定阈值不同，所提算法采用无阈值相似子块提取方法来选择具有高相关性的子块。同时，为获取更多的局部信息，提出一种自适应子块合成方案以避免子块出现混叠。另外，针对尺度不变特征变换（SIFT）特征无法区分自然相似区域与篡改区域的问题，所提算法结合矩特征的优点，提取合成子块的递进式混合特征以此来降低算法的虚警率。实验结果表明，所提算法在MICC-F2000数据集上的灵敏度（TPR）与F1分别为97.2%与92.9%，在MICC-F220数据集上的TPR与F1为98.2%与95.1%，说明所提算法具有良好的检测能力。

关键词 成像系统；复制-粘贴篡改；混合特征；图片篡改识别；尺度不变特征变换；Hu矩

中图分类号 0436 **文献标志码** A **doi**：10.3788/LOP202259.0211001

Tampered Image Recognition Algorithm Based on Progressive Hybrid Feature

Peng Yihang, Ye Wujian*, Liu Yijun

School of Information Engineering, Guangdong University of Technology, Guangzhou, Guangdong 510006, *China*

Abstract Aiming at the disadvantage that the existing detection algorithms are difficult to resist combined attacks, a copy-move forgery recognition algorithm based on mixed features is proposed. Different from the traditional algorithm using fixed threshold, the proposed algorithm uses the similar sub-block extraction method without threshold to select the sub-block with high correlation. At the same time, in order to obtain more local information, an adaptive sub-block synthesis scheme is proposed to avoid sub-block aliasing. In addition, aiming at the problem that scale-invariant feature transform (SIFT) features cannot distinguish natural similar regions from tampered regions, the proposed algorithm combines the advantages of moment features to extract the progressive hybrid features of synthetic sub-blocks, so as to reduce the false alarm rate of the algorithm. The experimental results show that the true positive rate (TPR) and F1 of the proposed algorithm are 97.2% and 92.9% on MICC-F2000 data set and 98.2% and 95.1% on MICC-F220 data set, respectively, indicating that the proposed algorithm has good detection ability.

Key words imaging systems; copy-move forgery; hybrid feature; image tamper recognition; SIFT; Hu moment

1 引 言

随着图像编辑技术的不断发展，如今人们可以随意地利用如Photoshop，AI等软件对图片进行不留痕迹的篡改并进行传播，因此如何确认图像的真实性已经成为了一个备受关注的课题。复制-粘贴

收稿日期：2020-12-19；**修回日期**：2021-01-31；**录用日期**：2021-03-09

基金项目：广东省重点区域研究开发计划（2018B030338001，2018B010107003，2018B010115002）、广东省教育厅创新人才项目和广东工业大学青年百人项目（220413548）

通信作者：*yewjian@126.com

是指从某个图像中复制一个区域并粘贴到该图像的另一个区域，是一种常见的篡改方式。现有的复制-粘贴篡改检测算法可大致分为两类：1）基于图像子块的检测算法；2）基于特征点的检测算法。

基于图像子块的检测算法首先把图像分成重叠、固定大小的子块，然后提取子块的特征，最后进行特征匹配以寻找相似子块。Fridrich 等[1]使用离散余弦变化（DCT）系数作为图像子块的特征，并对 DCT 系数进行匹配以找出相似区域。为降低计算复杂度，主成分分析（PCA）[2]、奇异值分解（SVD）[3]等技术被用于 DCT 系数的降维。DCT 系数的优点在于简单高效，但 DCT 系数无法抵抗旋转、拉伸、加噪等攻击手段，因此研究人员开始寻找鲁棒性更强的特征表示方法，例如 RGB 通道融合信息[4]，离散小波变换（DWT）[5]等。其中 Zernike 矩[6]、解析傅里叶-梅林变换（AFMT）[7]、极坐标余弦变换（PCT）[8]、PECT-SVD[9]、CMF-iteMS[10]这一类特征通过把图像的空域信息映射至正交的高阶特征空间，使特征具有较强的旋转不变性及伸缩不变性，但无法抵抗组合攻击，如对某一个局部区域进行先旋转后拉伸。在特征匹配阶段，暴力匹配算法是一种常见的算法，该算法实现简单但计算代价过大且容易导致虚警率偏高。为改善这一缺点，许多近似最优匹配算法被应用于特征匹配阶段，如字典排序[11]、PatchMatch[12]及局部敏感哈希（LSH）[13]等。基于图像子块的检测算法主要有两个问题：1）计算复杂度高。由于被检测图像需要被分成重叠的小块，算法的计算复杂度会随着图像尺寸的增大而增大。2）算法鲁棒性不强。基于图像块的匹配算法对经过伸缩、旋转、加噪等攻击的复制-粘贴图片识别效果差。

基于特征点的检测算法首先检测图像中的局部关键点并形成描述子，然后进行特征匹配以寻找匹配关键点。Amerini 等[14]对尺度不变特征变换（SIFT）关键点进行聚类，使得算法可以检测多重复制-粘贴的区域。Xu 等[15]则采用 speeded up robust features（SURF）特征以降低算法复杂度，SURF 特征维度为 SIFT 的一半，故算法实时性更好。赵洁等[16]提取 Harris 点并计算 local binary pattern（LBP）特征，LBP 算法比 SURF 算法更快速，但鲁棒性不强。Silva 等[17]在使用 SURF 特征的基础下，对图像进行了高斯金字塔分解并提取疑似篡改区域的 HSV 颜色特征，提高了算法的缩放不变性及定位精确度。为解决由特征点稀疏性导致的篡改区域信息缺失问题，Li[18-19]等在提取关键点前使用 simple linear iterative clustering（SLIC）算法对图片进行语义分割，但由于 SLIC 算法的分割性能与图像特性相关，固定的阈值会导致算法能力泛化能力弱。Vaishnavi 等[20]利用特征点的几何对称性检测篡改区域。基于特征点的检测算法计算复杂度低且抵抗几何攻击的能力强，但对平坦区、小物体等产生角点数目少的局部区域检测效果不佳。

为结合分块与特征点两种思想的优点，Soni 等[21]提出了一种把分块思想及特征点思想混合的算法，该算法首先对图像进行不重叠的分块，然后对子块提取 SURF 特征并通过简单的阈值判断方法找出匹配图像子块。为获取更多的局部信息，对子块的 8 邻域进行组合并提取图像块的 maximally stable extremal regions（MSER）特征与 SURF 特征以完成识别。该算法计算复杂度低，但仍然具有泛化性差、虚警率高的问题。

针对 Soni 算法的不足，本文对 Soni 算法进行改进，并提出了一种基于混合特征的复制-粘贴篡改图片识别算法。采用一种无阈值相似子块提取法以解决固定阈值方法识别准确率不高的问题；采用一种自适应子块组合方法合成子块，避免子块混叠；为解决单独使用 SIFT 特征虚警率高的问题，采用一种递进式特征混合提取方法。

2 基于混合特征的复制粘贴图像篡改识别算法

所提算法流程如图 1 所示，主要分为 2 个阶段。第 1 阶段，把目标图像转换成灰度图并进行非重叠均匀式分割，对于每一个子块，提取 SIFT 特征并使用 2-最近邻（2NN）算法进行匹配，使用无阈值相似子块提取法获取相似子块。第 2 阶段，使用所提自适应子块组合方案以避免组合子块之间产生混叠。最后采用一种递进式的混合特征提取方案判断该区域是否为篡改区域。

2.1 预处理

待检测图片一般为彩色图片，而 SIFT 特征只需要图像的梯度信息。因此，首先把彩色图像转换为灰度图以降低计算复杂度。

$$I(x,y)=0.2989R+0.587G+0.114B, \tag{1}$$

式中：R、G、B 代表 3 个颜色分量。在转换为灰度图后，对灰度图进行非重叠均匀式分割，图 2 为分割尺寸为 8×8 的分割过程示意图。非重叠均匀式分割可以更关注图像的局部特性，有利于提升识别精度。

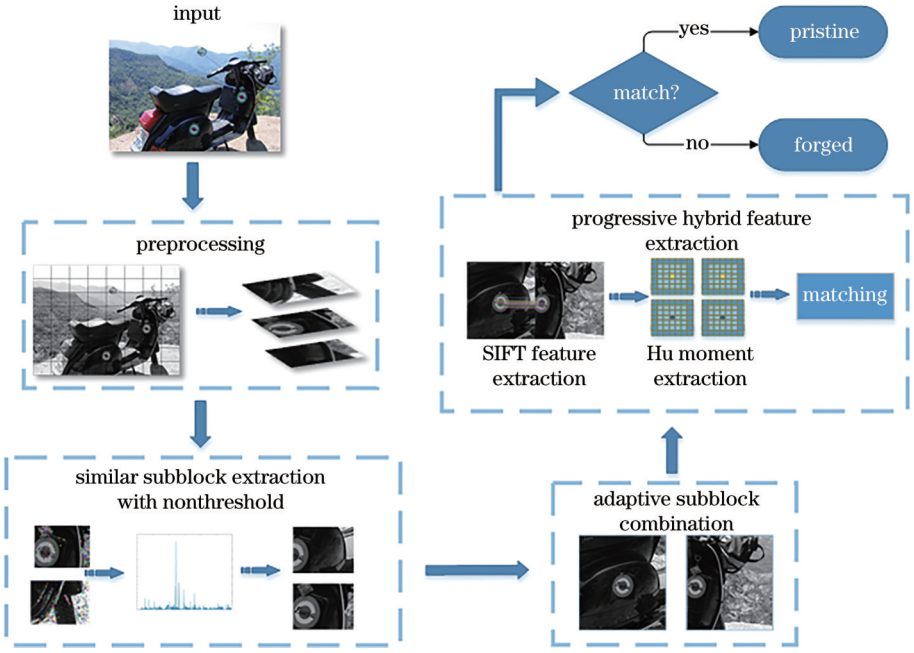

图 1　算法流程图

Fig. 1　Flow chart of proposed algorithm

图 2　非重叠均匀式分割

Fig. 2　Non-overlapping uniform segmentation

2.2　无阈值相似子块提取法

经过复制-粘贴的图片往往存在着高度相似的局部区域，具有此类区域的子块为相似子块匹配对。无阈值相似子块提取法主要分为两个阶段：特征提取与相似子块获取。

在特征提取阶段，首先提取每一个图像子块的 SIFT 关键点与描述子。然后对于任意两个子块的 SIFT 关键点集合，采用 2NN 算法对关键点进行匹配。设匹配后的距离向量为 $\{d_1, d_2, d_3, \cdots, d_n\}$，则 2NN 的计算表达式为

$$\frac{d_i}{d_{i+1}} \leqslant \delta, i = 1, 2, \cdots, n, \tag{2}$$

式中：δ 为一个固定的阈值。在完成关键点匹配后，使用随机抽样一致性（RANSAC）算法[22]进一步清除错误匹配点。在相似子块获取阶段，由于篡改区域包含高度相似区域，相似子块对应包含较多的匹配点数。Soni 算法采用固定的匹配点数阈值来判断两个子块是否为相似子块匹配对，如图 3 所示。

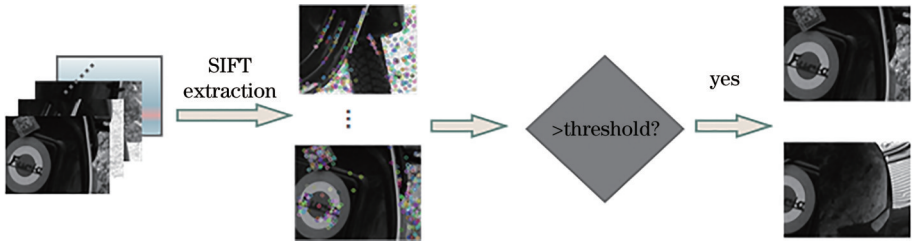

图 3　Soni 算法的相似子块提取过程

Fig. 3　Similar sub-block extraction process of Soni algorithm

然而，几何变换、加噪等后处理导致的像素失真往往会使一部分的匹配点数丢失，故固定阈值的处理方法并没有充分考虑篡改图像的特征，适用性差。针对上述缺点，提出一种无阈值相似子块提取法，如图 4 所示。

设图像经过预处理后得到的子块集合为

$(b_1, b_2, b_3, b_4, \ldots, b_i)$, $i=1, 2, 3, \ldots, n$, 其中 n 表示图像子块的总数。该方法首先在子块间进行特征匹配并记录子块的特征点匹配数目及对应的子块编号 b_i 与 b_j, 最后形成匹配点数分布图。在寻找相似子块时, 因为由于包含篡改区域的相似子块之间的匹配点数会明显多于不相似子块, 所以选择点数匹配分布图的峰值及次峰值所对应的子块对作为相似子块对。该方法利用包含篡改区域子块之间的高相关性来获取相似子块, 无需阈值。然而, 相似子块匹配对往往只包含一部分的篡改区域信息, 所提算法采用自适应子块组合方法以获取更多的局部区域信息。

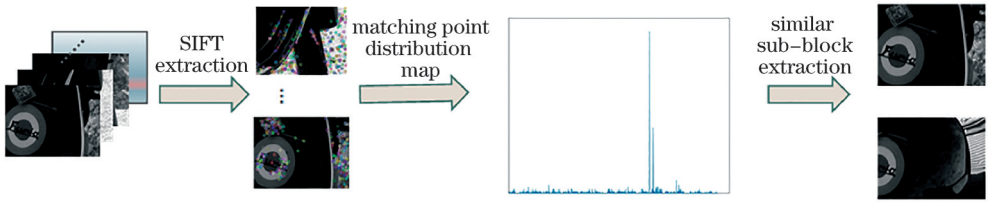

图 4　无阈值相似子块提取过程

Fig. 4　Similar sub-block extraction process with non-threshold

2.3　自适应子块组合方法

在获得相似匹配子块后, 对邻域子块进行组合以获取完整的篡改区域。Soni 算法中的 8 邻域子块组合法并没有考虑相似匹配子块之间的位置关系, 导致虚警率较高。为解决这一问题, 所提算法在图像分块后对每一个分块进行标号以表示每一个子块的位置, 图 5(a)表示以分割尺寸为 8×8 的标号信息。

设图像分块的尺寸为 $L \times L$, 图像子块的位置为 i, 则子块之间的相对位置 d 的表达式为

$$d=\mathrm{abs}(i_1-i_2), \tag{3}$$

式中: abs(·)为绝对值函数。子块间的相对位置关系可大致分为 2 种情况: 1) 匹配子块对中有子块处于边缘位置; 2) 匹配子块对中没有子块处于边缘位置。对于情况 1), 由于处于边缘位置的子块无法采用 8 邻域合成子块, 因此取 3 邻域, 即 4 个子块合成, 如图 5(b)所示。对于情况 2), 选取子块的组合个数 n 的规则为

$$n=\begin{cases}6, & d=1, L, L+1, L-1, L+2, L-2, 2L-1, 2L+1, 2L+2, 2L-2\\ 8, & \text{else}\end{cases}。 \tag{4}$$

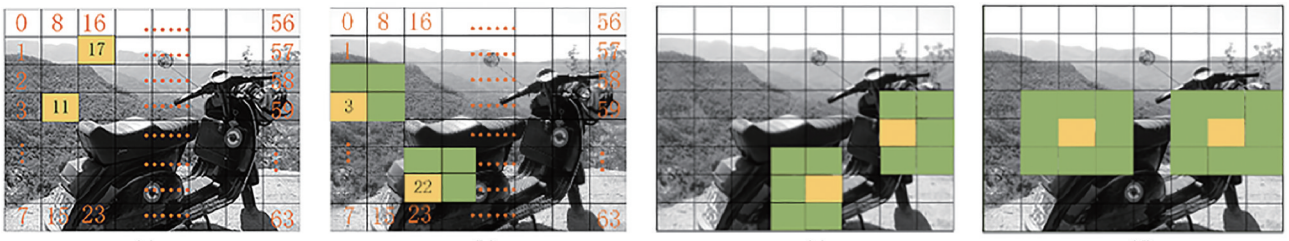

图 5　自适应子块组合。(a)子块标号; (b)子块处于边缘; (c) n=6 的情况; (d) n=8 的情况

Fig. 5　Adaptive sub-block combination. (a) Label for each sub-block; (b) sub-block on edge; (c) case of n=6; (d) case of n=8

即当相似子块的相对位置过近时, 取 6 邻域的子块进行合成, 图 5(c)表示 n 取 6 时情况; 当两个相似子块间隔足够远时, 取 8 邻域子块合成, 图 5(d)表示 n 取 8 的情况。

所提自适应邻域子块组合方法充分地考虑子块匹配对的相对位置信息, 可以有效避免子块混叠现象, 降低虚警率。但原始图片中会存在局部自然相似区域, 该区域会导致虚警率升高。为精确区分自然相似区域与篡改区域, 所提算法使用一种递进式混合特征提取方法对合成子块进行识别。

2.4　递进式混合特征提取

经过复制-粘贴篡改的图片会具有极高的局部相关性, 然而原始图片中也会存在自然高度相似的区域, 如图 6 中圆圈部分所示。自然高度相似的区域往往会干扰算法, 造成虚警率过高。

由于良好的鲁棒性, 特征点现已被广泛应用于复制-粘贴的篡改识别算法中。然而, 局部特征点的单独使用并无法准确区分自然相似区域与篡改区

域。原因在于局部特征点的特征一般是通过计算关键点邻域的梯度信息得到的，而自然相似区域也具有高度相似的梯度信息，这说明仅仅使用基于梯度信息的特征具有一定的局限性。为改善特征点的这一问题，提出一种递进式混合特征提取方法，如图7所示。

图6　自然相似区域

Fig. 6　Natural similar areas

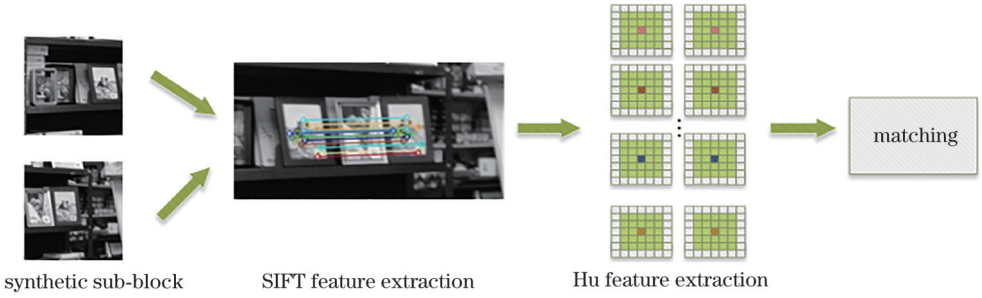

图7　递进式混合特征提取

Fig. 7　Progressive hybrid feature extraction

所提递进式混合特征提取方法首先提取两个合成子块的SIFT特征点并进行匹配，得到匹配点集合。为了弥补SIFT特征的局限性，该方法计算了每一对匹配特征点邻域信息的Hu矩特征。几何矩由像素值的积分计算而来，更关注像素值本身而非像素的梯度信息，可以捕捉自然相似区域之间如亮度变化等细微的差异，可以弥补SIFT特征点的缺陷。Hu矩作为矩阵特征的一种，是通过计算像素的几何矩来构成的7维特征向量，具有鲁棒性强、计算复杂度低等优点。

在得到每一对特征点邻域Hu矩后，采用欧式距离计算特征点邻域之间Hu矩特征相似性。若相似子块为自然相似区域，则匹配点集合中应包含大量的误匹配点。因此，若匹配特征点集合中有一定数量Hu矩特征不匹配，则该区域属于自然相似区域。递进式的特征混合方式可以有效结合SIFT特征与Hu矩特征的优点，在保证图像鲁棒性的同时区分篡改区域和原始相似区域，降低了算法的虚警率。

3　实验部分

3.1　数据集简介

实验在由Amerini等[14]提供的两个数据集：MICC-F200与MICC-F2000中完成。MICC-F220数据集共包含220张图片，其中原始图片有110张，篡改图片有110张，图片分辨率为800×600；MICC-F2000数据集共包含2000张图片，其中原始图片有1300张，篡改图片有700张，图片分辨率为2048×1536。MICC-F200数据集与MICC-F2000数据集中对篡改区域的后处理主要为几何变换，包括平移、拉伸、旋转及三者的组合攻击。设在后处理过程中对粘贴区域进行旋转的角度为θ，x轴方向的缩放系数为L_x，y轴方向的缩放系数为L_y。MICC-F220数据集、MICC-F2000数据集中的后处理攻击类型G如表1和表2所示。

两个数据集的几何攻击方式均以等比例缩放为主，其中MICC-F2000中的攻击类型更符合现实情况，包含不等比例缩放及“不等比例缩放＋旋转结合”的组合攻击，对算法的鲁棒性要求更高。将所提算法与文献[26-28]中的相关算法进行了比较，并分析了实验结果。

3.2　评价标准

采用灵敏度(TPR)、假正率(FPR)及F1值来评价所提算法的性能，各指标的表达式分别为

$$R_{\mathrm{TPR}}=\frac{N_{\mathrm{FT}}}{N_{\mathrm{F}}},\tag{6}$$

表 1　MICC-F220 数据集几何攻击类型

Table 1　Type of geometric attack in MICC-F220 dataset

Parameter	G1	G2	G3	G4	G5	G6	G7	G8	G9	G10
θ /(°)	0	10	20	30	40	0	0	0	10	20
L_x	1	1	1	1	1	1.2	1.3	1.4	1.2	1.4
L_y	1	1	1	1	1	1.2	1,3	1.4	1.2	1.4

表 2　MICC-F2000 数据集几何攻击类型

Table 2　Type of geometric attack in MICC-F2000 dataset

Parameter	G1	G2	G3	G4	G5	G6	G7	G8	G9	G10	G11	G12	G13	G14
θ /(°)	0	5	25	70	90	0	0	0	0	0	0	0	40	30
L_x	1	1	1	1	1	1.2	1.5	2.0	0.7	0.5	1.4	2.6	3.4	1.4
L_y	1	1	1	1	1	1.2	1,5	2.0	0.7	0.5	1.7	1.3	1.2	0.7

$$R_{\mathrm{FPR}}=\frac{N_{\mathrm{FF}}}{N_{\mathrm{P}}},\tag{7}$$

$$S_{\mathrm{F1}}=\frac{2\times R_{\mathrm{TPR}}\times P}{R_{\mathrm{TPR}}+P},\tag{8}$$

式中：N_{F} 为篡改图片的总数量；N_{FT} 为篡改图片中被正确分类的总数量；N_{FF} 为篡改图片中被错误分类的总数量；N_{P} 为原始图像总数量；P 为准确率。TPR 表示算法识别篡改图片的灵敏度，TPR 越高表示算法识别篡改图片的能力越强。FPR 又被称为虚警率，是衡量算法是否容易产生误判的一个标准，值越小表示误判量越少。F1 值可衡量算法的整体分类性能，值越高说明整体分类性能越好。

3.3　鲁棒性测试

在 4 种攻击情况下来验证所提算法抵抗攻击的能力：a 篡改区域未经过几何攻击；b 篡改区域只经过旋转攻击；c 篡改区域只经过缩放攻击；d 篡改区域经过旋转与缩放的组合攻击。4 种情况与数据集攻击类型对应如表 3 所示。

表 3　攻击种类

Table 3　Attack type

Dataset	a	b	c	d
MICC-F220	G1	G2, G3, G4, G5	G6, G7, G8	G9, G10
MICC-F2000	G1	G2, G3, G4, G5	G6,G7,G8,G9,G10,G11,G12	G13, G14

其中情况 c 在 MICC-F220 数据集中均为等比例缩放，而在 MICC-F2000 数据集中包含不等比例缩放（G11, G12）。所提算法在 MICC-F220 和 MICC-F2000 上的 TPR 指标如图 8 和图 9 所示。

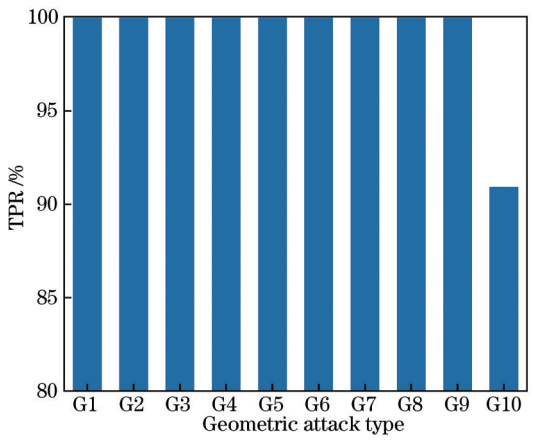

图 8　MICC-F220 鲁棒性测试

Fig. 8　Robust test in MICC-F220

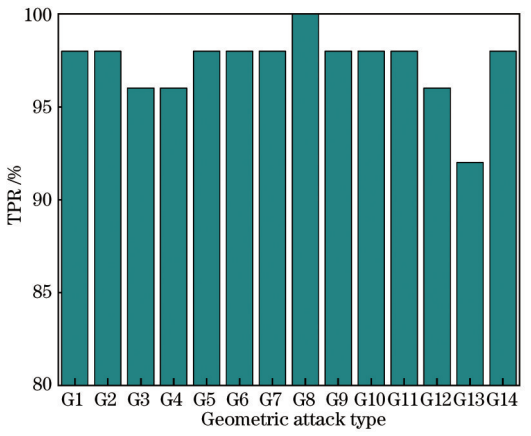

图 9　MICC-F2000 鲁棒性测试

Fig. 9　Robust test in MICC-F2000

从图 8 中可以看出：在 MICC-F220 数据集中，所提算法在 G1～G9 类几何攻击下的识别准确率较高，说明所提算法可以有效抵抗 a，b，c 3 种情况下的几何攻击；对 G10 类别的识别准确率有所下降，表

明所提算法对组合攻击的抵抗能力还需提高，但仍能达到90%的准确率。从图9中可以看出，所提算法在G11～G14类几何攻击下的TPR指标分别为98%，96%，92%，98%，表明所提算法在面对不等比例缩放及“不等比例缩放＋旋转”这两种具有挑战性的后处理攻击时，也能保持较高的识别准确率。

3.4　自动阈值方案与混合特征的有效性

通过MICC-F220数据集来验证自动阈值方案与混合特征的有效性。实验结果如表4所示。

表4　各阶段实验结果

Table 4　Experimental results of each stage

Algorithm	TPR /%	FPR /%	F1 /%
Soni	97.5	8.5	94.7
Non-threshold method	98.2	9.09	94.6
Non-threshold method＋hybrid feature	98.2	8.1	95.1

从表4中可以看出，无阈值方法，与Soni算法相比TPR上升了0.7个百分点，但同时FPR上升了0.59个百分点，F1值下降了0.1个百分点，说明算法在增强识别篡改图片能力的同时出现了过拟合现象，整体分类性能下降。FPR上升的原因在于自然相似纹理区的干扰。无阈值方法关注匹配点数分布图中的峰值与次峰值，因此原始图片中包含相似纹理区的子块更容易被判定为匹配子块。另外，在经过邻域子块组合后，仅仅使用SIFT特征无法区分自然相似区域和复制-粘贴区域，从而出现误判。在使用混合特征后，与无阈值方法及Soni算法相比，FPR指标分别下降0.99个百分点和0.4个百分点，F1指标分别提升了0.5个百分点与0.4个百分点，说明混合特征方法可以在不影响识别能力情况下有效降低算法的虚警率。

3.5　算法运行时间分析

在MICC-F2000数据集中随机选取50张图片（25张原始图与25张篡改图），取50张图片的运行均值并与相关的算法进行对比。实验结果如表5所示。

Soni算法及所提算法均在本机平台进行实验，其余算法的运行时间来源于Pun[19]。从表5可知，所提算法的运行时间远少于Pun[19,27]和Ryu[6]，但多于Soni[21]与Sliva[17]。Sliva[17]算法采用了SURF特征与HSV颜色域结合的方法，对比所提算法采用的SIFT特征与Hu矩特征具有一定的速度优势，但

表5　运行时间对比

Table 5　Comparison of running time

Algorithm	Time /s
Silva[17]	39
Pun[19]	399
Pun[27]	123
Ryu[6]	565
Soni[21]	38
Proposed algorithm	47

SURF特征与HSV特征的特征组合抵抗攻击的能力不强，在CMH数据集上仅有83%的识别准确率。Soni算法采用固定阈值的方法获取相似子块，无需对子块进行全局搜索，在降低了复杂度的同时也降低了识别准确率。所提算法对相似子块进行全局搜索以实现无阈值方案，并采用了混合特征的组合形式，提高了算法的识别率，降低了虚警率，同时无需过多时间。

3.6　与传统算法的对比

为突出所提算法的优势，对所提算法与现有的传统算法性能进行对比，实验结果如图10和图11所示。

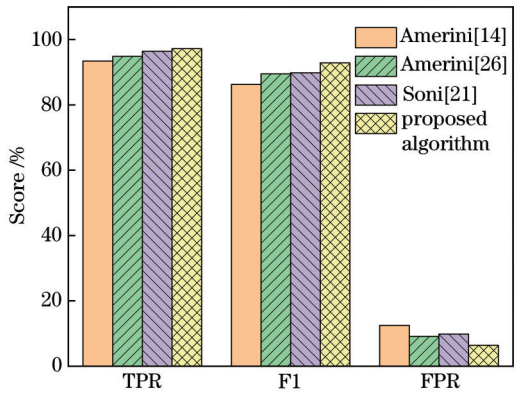

图10　MICC-F220数据集上的结果对比

Fig. 10　Comparison of results on MICC-F220 dataset

从图10中可以看出，所提算法的TPR与F1指标均为最高，说明所提算法识别篡改图片的能力及整体分类性能均优于其余算法。文献[15]的Bo算法的TPR与F1指标均为最低，说明该算法在对图片进行判别时更为保守，只把少数的图片被判定为篡改图片，从而造成识别效果不理想的现象。从图11中可以看出，在MICC-F2000数据集中，所提算法在TPR较高的情况下FPR较低，且F1指标取得最好，说明所提算法在识别高分辨率篡改图像上的性能出色。

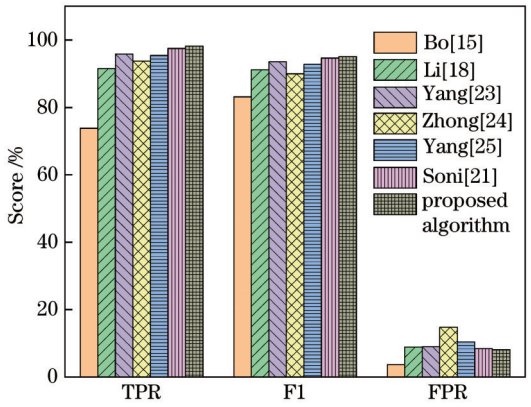

图 11　MICC-F2000 数据集上的结果对比

Fig. 11　Comparison of results on MICC-F2000 dataset

3.7　与基于深度学习识别算法的对比分析

近年来，基于深度学习的取证算法大部分是针对异源拼接的，针对复制-粘贴的深度学习方法数量较少[28]。Wu 等[29]提出了一种双流网络 BusterNet，该算法的研究重点在于如何进一步鉴定可疑区域的属性，算法的识别准确率并不理想。为了使深度特征具有较强的不变性，Liu 等[30]提出了一种可供 GPU 训练的核卷积神经网络（CKN）网络。所提算法与 CKN 网络在 MICC-F2000 数据集的对比结果如表 6 所示。

表 6　所提算法与 CKN 算法的性能对比

Table 6　Performance comparison between proposed algorithm and CKN algorithm

Algorithm	TPR /%	FPR /%	F1 /%
CKN	93	11	87.2
Proposed algorithm	97.2	6.4	92.9

基于深度学习网络的取证算法主要有以下几个缺点：1）对训练机器的要求高；2）网络的训练过程需要较多的时间；3）对训练数据集的制作要求高。所提算法对硬件环境、数据集均无依赖且不需要训练。另外，从表 6 中可以看出，所提算法的 TPR 比 CKN 网络高 4.2 个百分点，FPR 比 CKN 低 4.6 个百分点，说明所提算法的对篡改图片的识别性能更优异。

4　总　　结

提出了一种基于混合特征的复制-粘贴篡改识别算法。采用一种无阈值相似子块提取法解决固定阈值方法识别准确率不高的问题；采用一种个自适应子块组合方法合成子块，避免子块混叠；为解决单独使用 SIFT 特征虚警率高的问题，提出了一种递进式特征混合提取方法。实验结果表明，在 MICC-F2000 数据集中，G13、G14 类型攻击的识别准确率为 92% 与 98%，所提算法可以有效抵抗旋转及不等比例缩放等具有挑战性的几何攻击。另外，在 MICC-F220 数据集中，与无阈值方法相比，所提算法的 FPR 指标下降 0.99 个百分点，说明混合特征方法可以在保证准确率的前提下降低虚警率。但是，所提算法对平坦区及小区域的复制-粘贴检测性能还有待提高，另外混合特征的聚合方式也是下一步将要重点研究的问题。

参　考　文　献

[1] Fridrich A J, Soukal B D, Lukáš A J. Detection of copy-move forgery in digital images[C]//in Proceedings of Digital Forensic Research Workshop, August, 2003, Cleveland, OH, USA. [S.l.: s.n.], 2003: 342-358.

[2] Popescu A C, Farid H. Exposing digital forgeries by detecting duplicated image regions[R]. Cambridge: Technical Report, 2004.

[3] Zhao J, Guo J C. Passive forensics for copy-move image forgery using a method based on DCT and SVD[J]. Forensic Science International, 2013, 233(1/2/3): 158-166.

[4] Luo W Q, Huang J W, Qiu G P. Robust detection of region-duplication forgery in digital image[C]//18th International Conference on Pattern Recognition (ICPR '06), August 20-24, 2006, Hong Kong, China. New York: IEEE Press, 2006: 746-749.

[5] Muhammad G, Hussain M, Bebis G. Passive copy move image forgery detection using undecimated dyadic wavelet transform[J]. Digital Investigation, 2012, 9(1): 49-57.

[6] Ryu S J, Kirchner M, Lee M J, et al. Rotation invariant localization of duplicated image regions based on Zernike moments[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(8): 1355-1370.

[7] Gan Y F, Zhong J L. Application of AFMT method for composite forgery detection[J]. Nonlinear Dynamics, 2016, 84(1): 341-353.

[8] Yap P T, Jiang X D, Kot A C. Two-dimensional polar harmonic transforms for invariant image representation[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2010, 32(7): 1259-1270.

[9] Wang Y L, Kang X B, Chen Y J. Robust and accurate detection of image copy-move forgery using PCET-SVD and histogram of block similarity

measures[J]. Journal of Information Security and Applications, 2020, 54: 102536.

[10] Warif N B A, Idris M Y I, Wahab A W A, et al. CMF-iteMS: an automatic threshold selection for detection of copy-move forgery[J]. Forensic Science International, 2019, 295: 83-99.

[11] Wang J W, Liu G J, Zhang Z, et al. Fast and robust forensics for image region-duplication forgery[J]. Acta Automatica Sinica, 2009, 35(12): 1488-1495.
王俊文, 刘光杰, 张湛, 等. 图像区域复制篡改快速鲁棒取证[J]. 自动化学报, 2009, 35(12): 1488-1495.

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

[13] Emam M, Han Q, Niu X M. PCET based copy-move forgery detection in images under geometric transforms[J]. Multimedia Tools and Applications, 2016, 75(18): 11513-11527.

[14] Amerini I, Ballan L, Caldelli R, et al. 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.

[15] Xu B, Wang J W, Liu G J, et al. Image copy-move forgery detection based on SURF[C]//2010 International Conference on Multimedia Information Networking and Security, November 4-6, 2010, Nanjing, China. New York: IEEE Press, 2010: 889-892.

[16] Zhao J, Guo J C. Passive forensics for region duplication image forgery using Harris feature points and annular average representation[J]. Journal of Data Acquisition and Processing, 2015, 30(1): 164-174.
赵洁, 郭继昌. 利用Harris特征点和环形均值描述的图像区域复制篡改的被动取证[J]. 数据采集与处理, 2015, 30(1): 164-174.

[17] Silva E, Carvalho T, Ferreira A, et al. Going deeper into copy-move forgery detection: Exploring image telltales via multi-scale analysis and voting processes[J]. Journal of Visual Communication and Image Representation, 2015, 29: 16-32.

[18] Li J, Li X L, Yang B, et al. Segmentation-based image copy-move forgery detection scheme[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(3): 507-518.

[19] Pun C M, Chung J L. A two-stage localization for copy-move forgery detection[J]. Information Sciences, 2018, 463/464: 33-55.

[20] Vaishnavi D, Subashini T S. Application of local invariant symmetry features to detect and localize image copy move forgeries[J]. Journal of Information Security and Applications, 2019, 44: 23-31.

[21] Soni B, Das P K, Thounaojam D M. Geometric transformation invariant block based copy-move forgery detection using fast and efficient hybrid local features[J]. Journal of Information Security and Applications, 2019, 45: 44-51.

[22] Fischler M A, Bolles R C. Random sample consensus[J]. Communications of the ACM, 1981, 24(6): 381-395.

[23] Yang B, Sun X M, Guo H L, et al. A copy-move forgery detection method based on CMFD-SIFT[J]. Multimedia Tools and Applications, 2018, 77(1): 837-855.

[24] Zhong J L, Gan Y F, Young J, et al. A new block-based method for copy move forgery detection under image geometric transforms[J]. Multimedia Tools and Applications, 2017, 76(13): 14887-14903.

[25] Yang F, Li J W, Lu W, et al. Copy-move forgery detection based on hybrid features[J]. Engineering Applications of Artificial Intelligence, 2017, 59: 73-83.

[26] Amerini I, Ballan L, Caldelli R, et al. Copy-move forgery detection and localization by means of robust clustering with J-Linkage[J]. Signal Processing: Image Communication, 2013, 28(6): 659-669.

[27] Pun C M, Yuan X C, Bi X L. Image forgery detection using adaptive oversegmentation and feature point matching[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(8): 1705-1716.

[28] Wang J, Zhang Y C, Huo Z Q, et al. Image tampering detection method based on approximate nearest neighbor search[J]. Laser & Optoelectronics Progress, 2020, 57(10): 101102.
王静, 张雨辰, 霍占强, 等. 基于近似最近邻搜索的图像篡改检测方法[J]. 激光与光电子学进展, 2020, 57(10): 101102.

[29] Wu Y, Abd-Almageed W, Natarajan P. BusterNet: detecting copy-move image forgery with source/target localization[M]//Ferrari V, Hebert M, Sminchisescu C, et al. Computer vision-ECCV 2018. Lecture notes in computer science. Cham: Springer, 2018, 11210: 170-186.

[30] Liu Y Q, Guan Q X, Zhao X F. Copy-move forgery detection based on convolutional kernel network[J]. Multimedia Tools and Applications, 2018, 77(14): 18269-18293.