

## 复制粘贴篡改图像检测技术综述

丁远晴<sup>1,2</sup>

1 四川警察学院, 四川 泸州 646000

2 刑事检验四川省高校重点实验室, 四川 泸州 646000

**[摘要]** 复制粘贴篡改是一种常见的图像篡改方式, 其恶意使用和广泛传播造成了严重的社会影响。首先介绍了复制粘贴篡改的概念, 原理和模型。随后, 将现有复制粘贴篡改检测算法大致分为了基于图像块的方法、基于关键点的方法和深度学习的方法, 并分别对这三类方法进行了综述。此外, 还介绍了用于评价复制粘贴篡改检测技术的常用数据集和客观评价标准。最后, 总结了当前图像复制粘贴篡改检测技术的优势和劣势, 并给出了发展方向, 以期对该领域的后续研究有所裨益。

**[关键词]** 图像篡改; 复制粘贴; 检测; 数据集

DOI: 10.33142/sca.v6i3.8823

中图分类号: TP3

文献标识码: A

## Overview of Copy Paste Tampering Image Detection Technology

DING Yuanqing<sup>1,2</sup>

1 Sichuan Police College, Luzhou, Sichuan, 646000, China

2 Key Laboratory of Criminal Inspection in Sichuan Provincial Universities, Luzhou, Sichuan, 646000, China

**Abstract:** Copy paste tampering is a common method of image tampering, which has caused serious social impact due to its malicious use and widespread dissemination. Firstly, the concept, principle, and model of copy paste tampering were introduced. Then, the existing copy paste tamper detection algorithms are roughly divided into image block based methods, keypoint based methods, and deep learning methods, and these three types of methods are reviewed respectively. In addition, common datasets and objective evaluation criteria for evaluating copy paste tamper detection techniques were also introduced. Finally, the advantages and disadvantages of current image copying, pasting, and tamper detection technologies were summarized, and the development direction was given, with the aim of benefiting future research in this field.

**Keywords:** image tampering; copy paste; testing; data set

### 引言

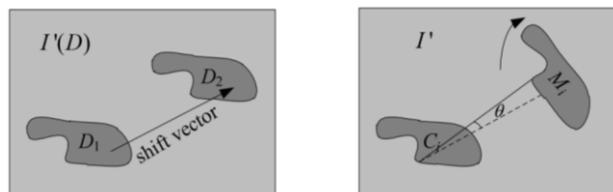
随着数字图像技术的发展与广泛应用, 数字图像的篡改变得十分便捷且普遍。在人人都是自媒体的时代, 图像的恶意篡改及其传播会造成严重的社会问题, 甚至引发政治危机。数字图像篡改主要有两种类型, 即拼接篡改和复制粘贴篡改。拼接篡改是指将源图像的部分区域复制粘贴到目标图像上, 对于拼接篡改图像的检测往往根据目标图像的性质、特征的不连续性判定篡改区域。不同于拼接篡改, 复制粘贴篡改是将图像自身的一部分区域复制粘贴在同一幅图像中的其他区域, 以便于隐藏或增加信息。同时, 篡改者为了增加伪造图像的真实性, 会对图像的粘贴区域进行亮度变换、旋转、压缩、模糊化、加噪等操作。

本文主要聚焦于数字图像的复制粘贴篡改方式。一种有效的复制粘贴篡改检测 (Copy Move Forgery Detection, CMFD) 技术, 必须考虑许多因素。首先, 需要 CMFD 方法提供高精度、高可靠性的检测结果。此外, 在实际应用中, 所开发的方法在速度和计算复杂度方面也应具有较高的效率。因此, 解决速度-精度权衡的问题是目前具有挑战性的。此外, 一个有效的 CMFD 方法应该对各种类型的攻击和操作技术有很强的鲁棒性 (例如, 噪声添

加、压缩、缩放和旋转)。

### 1 图像复制粘贴篡改模型

在<sup>[3]</sup>中, 作者通过对 100 张自然图像的分析, 发现一张图像不可能有两个大于图像面积的 0.85%相似的区域。因此, 复制粘贴篡改检测的目标是在可疑图像中寻找两个相似的大面积区域, 如图 1 (a) 所示。



(a) Luo 的模型

(b) Liu 的模型

图 1 复制粘贴篡改的两种模型

给定源图像为  $I$ , 篡改图像为  $I'$ ,  $D_1$  是源区域,  $D_2$  是粘贴的区域,  $d = (dx, dy)$  表示转向向量, 应满足:  $D_1$  和  $D_2$  都是  $D$  的子集,  $D_2 = D_1 + d$ , 如果  $(x, y) \notin D_2$ ,  $I'(x, y) = I(x, y)$ ; 如果  $(x, y) \in D_2$ ,  $I'(x, y) = I(x - dx, y - dy)$ 。然而, Luo 的模型无法描述复制区域粘贴到两个或多个地方, 或者复制区域在粘贴前进行旋转的篡改方式。

为了弥补 Luo 模型的缺陷, Liu 等人<sup>[4]</sup>提出了一个更全面的复制粘贴篡改检测模型, 如图 1 (b) 所示。假设旋转向量阈值是  $\mathbf{V}_r = [V_r, V_r]$ , 复制区域的阈值是  $A_r$ 。图像  $I$  复制粘贴篡改后为  $I'$ , 需要满足: (1) 复制区域  $C_i$  是单连通的并且内部无孔, 复制区域的面积比  $A_r \cdot a(I)$  大, 其中  $a(I)$  表示图像  $I$  的面积。(2) 假设复制区域  $C_i$  的粘贴区域为  $M_i$ , 存在多个复制区域对  $\{C_1 \parallel M_1, C_2 \parallel M_2, \dots, C_n \parallel M_n\}, C_i, M_i \in I'$ , 满足  $C_i \neq C_j, \forall i \neq j, i, j \in \{1, 2, \dots, n\}$  及  $C_i \cap C_j = \emptyset$ 。对于任意的  $C_i \parallel M_i$  对, 定义参照系统的起源为旋转中心, 复制粘贴篡改可以被认为是旋转后的变形, 描述如下:

$$\left\{ \begin{array}{l} \forall (x, y) \in C_i, f(x, y) = f'(x', y') \\ x' = x \cos \theta - y \sin \theta + \Delta_x \\ y' = x \sin \theta + y \cos \theta + \Delta_y \\ \sqrt{\Delta_x^2 + \Delta_y^2} \geq |\mathbf{V}_r| \\ a(C_i) > A_r \cdot a(I) \end{array} \right. \quad (1)$$

其中,  $f$  表示在位置  $(x, y)$  的像素值,  $\Delta_x$  和  $\Delta_y$  分别是沿着  $x$  和  $y$  轴的平移距离;  $\theta$  是旋转角度。

## 2 复制粘贴篡改图像检测的主流方法

### 2.1 基于图像块的篡改检测方法

基于图像块的篡改检测方法, 一般将图像分割为相同大小的图像块, 然后对每个图像块进行特征提取, 生成二维特征向量矩阵, 再进行特征匹配。若不同图像块的特征向量相同, 表明这两个图像块异常, 则判断为复制粘贴篡改区域。基于图像块检测的经典算法由 Fridrich 等人在 2003 年提出, 算法对分割后的图像块进行离散余弦变换 (Discrete Cosine Transform, DCT), 获得特征系数, 组成特征向量, 最后基于字典排序检测算法对所有特征向量进行排序, 字典中位置相近的两个块认为是复制粘贴的源区域和目标区域。在此基础上出现了许多改进算法, AC. Popescu 和 H. Farid 在 2004 年提出使用主成分分析法 (Principal Component Analysis, PCA) 代替了 DCT, 获得了更小的特征系数, 提升了图像块特征向量匹配的效率。此类算法对加性噪声和 JPEG 压缩具有很好的鲁棒性, 但是在旋转、缩放等几何变换攻击下性能较差。由于 log-polar 变换对几何变换具有较好的不变性, 同时也能对特征向量进行降维。Myna 等人提出对图像进行 DWT 变换, 并对图像块进行 log-polar 变换, 通过穷举法搜索相似的图像块, 提高了算法对几何变换的鲁棒性。

基于图像块的方法具有很好的鲁棒性, 可以对加入了噪声和经过压缩的图像进行判定。由于判定区域也是由图像块为单位组成, 所以检测的区域的精度与块大小有直接关系。

### 2.2 基于关键点的篡改检测方法

基于关键点的篡改检测方法, 以像素点为处理单元, 利用相邻像素的颜色、纹理等局部不变性获取特征点描述

向量, 然后对其进行特征匹配, 当相似的特征值积累到达一定阈值时, 判定该图像经过了篡改操作。Huang<sup>[20]</sup>等人利用尺度不变特征变换 (Scale-Invariant Feature Transform, SIFT)<sup>[2]</sup>检测复制粘贴篡改图像, 通过匹配 SIFT 特征点识别篡改区域。对于基于关键点的特征提取, 不可否认的是, 尺度不变特征变换是该领域的经典方法, 但仍然很流行。SIFT 提供了一种具有 128 个元素长度的特征描述技术。生成的特征对缩放和旋转变换都具有鲁棒性, 使其特征描述符特别适用于复制粘贴篡改图像的检测。但 SIFT 存在计算成本高、复杂度高等问题, 这使得它不适合一些需要处理大量图像或要求实时处理速度的实际应用。为了克服这个问题, 提出了许多加快或改进 SIFT 各个方面的算法<sup>[12-19]</sup>。文献[15]中, Muzaffer 和 Ulutas 提出了一种使用二值化 SIFT 的 CMFD 技术, 该技术将 SIFT 描述符中每个元素的值二值化为 0 或 1。由于特征描述符的简化, 使得匹配过程效率更高, 从而提高了检测的整体速度。对 SIFT 算法无法处理平滑区域的问题, Jin 和 Wan<sup>[16]</sup>提出了一种改进 SIFT 算法, 使用 Opponentsift 算法来提高描述符在对比度低的关键点上的辨别能力。此外, 在 2016 年, Shahrudnejad 和 Rahmati<sup>[17]</sup>提出了一种使用仿射-SIFT (Affine SIFT, ASIFT) 检测 CMF 的有趣方法。该方法将在 SIFT 算法之前应用了仿射相机模型, 以模拟并获得更多可能的仿射失真信息。该方法被认为是完全仿射不变的, 并且对 CMF 篡改区域的变换和变形具有鲁棒性。

针对复杂的复制粘贴篡改检测及定位的精确度问题, 有研究学者提出了更为系统的检测框架。Ardizzone 等人<sup>[25]</sup>对 SIFT 变换后的关键点进行聚类, 采用类匹配的方法检测篡改区域多次粘贴的情况。Shivakumar<sup>[22]</sup>提出利用加速鲁棒性特征 (Speeded-Up Robust Features, SURF)<sup>[21]</sup>提取关键点, 检测篡改区域。Jaberi M 等人<sup>[23]</sup>提出利用 MIFT 获得关键点特征进行篡改区域检测。Ardizzone 等人<sup>[26]</sup>利用提取的 SIFT 特征点来构建 Delaunay 划分, 然后利用每个三角形块的颜色信息和角度信息作为三角形区域的特征向量进行匹配。Shivakumar<sup>[24]</sup>提出了一种利用 SIFT 特征向量与 harris 角点有效检测复制粘贴篡改区域的方法, 但是对经过旋转、加高斯噪声等后处理的篡改检测性能不理想。

和基于块匹配的检测方法相比, 基于关键点匹配的方法避免了全局搜索, 大大提高了检测效率, 且对几何变换具有更好的鲁棒性。

### 2.3 基于深度学习的篡改检测方法

传统的复制粘贴篡改检测算法需要根据先验知识人工设计特征, 检测篡改区域, 算法性能往往受限于特定的篡改方式。近年来, 利用深度学习进行图像篡改检测的研究也取得了不错的效果, 并展现出了优于传统算法的鲁棒性和泛化性。

Rao 等<sup>[27]</sup>首次将卷积神经网络 (Convolutional

Neural Network, CNN) 用于检测图像的拼接篡改和复制粘贴篡改,该方法利用 CNN 自动学习输入 RGB 图像的特征层表示,并采用空间丰富模型(Spatial Rich Model, SRM) 初始化网络参数。2017 年 Ouyang 等人<sup>[28]</sup>提出了一种基于 CNN 的复制粘贴篡改检测方法。该模型在 ImageNet 上进行预训练,再使用复制粘贴篡改数据集训练,对网络参数进行微调。该方法有效解决了复制粘贴篡改数据集数据量太小的问题,但对真实场景图像的鉴别准确度不理想。2018 年 Wu 等人<sup>[29]</sup>针对图像复制粘贴篡改提出了一种端到端的篡改检测与定位方法。该方法通过特征提取、自相关计算、逐点特征提取、解码四个阶段,首次实现了像素级别的复制粘贴区域定位,识别精度优于传统算法。不久 Wu 等人<sup>[30]</sup>在此基础上提出了可以检测源目标和篡改目标的端到端的 BusterNet。该模型有两个支路,称为 Mani-Det 分支和 Simi-Det 分支。实验表明,该方法具有较好的鲁棒性,在多个数据集上取得了最佳的效果。Chen 等人<sup>[35]</sup>提出一种串行分支网络模型,包含相似性检测网络 CMSDNet 和源与目标鉴别网络 STRDNet。STRDNet 研究 CMSDNet 获得的相似块的分类问题,相对于 BusterNet 的分支更加简单且准确率更高。

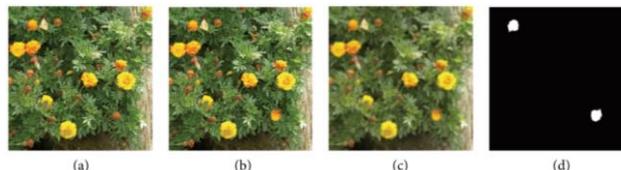
Zhou 等人<sup>[31]</sup>将图像篡改检测视为图像检测任务,提出一种端到端由 RGB 流和噪声流组成的双流 Faster R-CNN 网络模型。实验表明该模型能够识别复制粘贴、拼接和去除等篡改方式,具有先进的性能和较好的鲁棒性,但无法实现像素级定位。Wu 等人<sup>[32]</sup>提出了一个不需要额外的预处理和后处理的篡改检测网络 ManTra-net,用一个自监督学习的方式从 385 篡改类型中学习特征。大量的实验结果表明,无论对于单个类型的篡改方式或是多种篡改方式叠加的图像,ManTra-net 都具有良好的泛化性、鲁棒性和更好的性能。Barni 等人<sup>[33]</sup>提出了多分支网络 DisTool 对图像复制粘贴篡改进行检测并识别源区域和目标区域,该网络在真实的测试场景中也表现良好。Zhong 等人<sup>[34]</sup>提出了基于 Dense-InceptionNet 的检测方案,充分使用了多尺度的信息和稠密特征链接,该算法对几何变换操作和 JPEG 压缩都有一定的鲁棒性。Islam A 等人<sup>[36]</sup>提出了 DOA-GAN,一个具有双阶注意力模型的生成对抗网络来检测和定位复制移动区域。

### 3 常用数据集

本小节简要介绍用于解决 CMFD 问题的主流数据集。通常,研究人员只使用许多公共数据集中的几个进行实验。如图 2 展示了 CoMoFoD 数据集的一组样例。

表 1 中罗列了评估复制移动篡改算法所使用的主流数据集。CASIA 取证数据集是用于图像篡改检测问题的最主流的数据集。CoMoFoD 数据集是一个复制移动图像的数据集,由 200 组小图像 512×512 和 60 组大图像 3000×2000 组成。GRIP 数据集由 80 张复制粘贴图像和 80 张对

应的扩展图像阵列(Extended Graphics Array, XGA)的真实图像组成。COVERAGE 是一个复制粘贴图像数据集,在复制区域中具有相似的真实对象。MICC-F600 数据集由 440 张真实图像和 160 张带有相应真实掩码图像的复制粘贴图像组成。FAU 数据集从 MICC-F600 数据集选取 48 张中高分辨率真实图像的基础上,创建了一个手工复制粘贴图像集。



(a) 源图像, (b) 篡改图像, (c) 篡改图像经过模糊处理, (d) ground truth 图

图 2 CoMoFoD 数据集样例

表 1 数据集比较

数据集	图像数量 (篡改图像数; 真实图像数)	ground truth 图	格式(大小)
GRIP[6]	80; 80	是	PNG (1024×768; 768×1024)
MICC-F600 [9]	152; 448	是	PNG; JPG (722×480 至 800×600)
FAU[7]	48; 48	是	PNG; JPG (1632× 1224; 3039×2014)
CoMoFoD[8]	200; 60	是	PNG; JPG (512× 512; 3000×2000)
CASIA TIDE v1.0[10]	921; 800	否	JPG (384×256)
CASIA TIDE v2.0[10]	5123; 7491	否	TIF; JPG (240×160 至 900×600)
COVERAGE[11]	100; 100	是	TIF (400×486)

### 4 质量评价指标

复制粘贴篡改检测算法的性能通常从图像级和像素级两个方面进行评估。最为常用的性能评价指标是精确度  $p$  和召回率  $r$ <sup>[7]</sup>, 它们的计算方式分别如下:

$$p = \frac{T_p}{T_p + F_p} \quad (2)$$

$$r = \frac{T_p}{T_p + F_N} \quad (3)$$

图像级评估中,  $T_p$  表示篡改图像正确检测为篡改图像的数量,  $F_p$  表示真实图像错误的检测为篡改图像的数量,  $F_N$  表示篡改图像错误检测为真实图像的数量;  $p$  表示预测为篡改图像数中预测正确的图像数所占比例, 也称为查准率。  $r$  表示篡改图像被正确预测的比例, 也称为查全率。同样, 在像素级评估中,  $T_p$ 、 $F_p$  和  $F_N$  所指的是相关的像素个数,  $p$  表示预测的篡改区域中预测准确的像

素数所占比例,  $r$  表示篡改区域被正确预测的像素所占比例。理想情况下,  $P$ 、 $r$  两个指标都是越高越好, 但一般情况下,  $P$  和  $r$  之间存在权衡, 因此, 评价篡改检测算法时会考虑这两种指标的调和平均数 (Harmonic Mean, MF), 即  $F_1$  值<sup>[7]</sup>, 计算如式 (4) 所示, 显然  $F_1$  越大, CMFD 方案的准确度越高。

$$F_1 = 2 \cdot \frac{P \cdot r}{P + r} \quad (4)$$

Zhao 和 guo<sup>[5]</sup> 给出了另一种像素级的评价准则, 检测准确率  $R_{DA}$  和错误正例率  $R_{FP}$ , 其计算方法分别如式 5-6 所示。

$$R_{DA} = \frac{|\Psi_C \cap \tilde{\Psi}_{DC}| + |\Psi_P \cap \tilde{\Psi}_{DP}|}{|\Psi_C| + |\Psi_P|} \quad (5)$$

$$R_{FP} = \frac{|\tilde{\Psi}_{DC} - \Psi_C| + |\tilde{\Psi}_{DP} - \Psi_P|}{|\tilde{\Psi}_{DC}| + |\tilde{\Psi}_{DP}|} \quad (6)$$

其中  $|\cdot|$  表示复制区域或者粘贴区域的面积,  $\cap$  表示两个区域的交集,  $-$  表示两个区域的差值,  $\Psi_C$  表示复制区域的像素,  $\Psi_P$  表示粘贴区域的像素,  $\tilde{\Psi}_{DC}$  表示预测为复制区域的像素,  $\tilde{\Psi}_{DP}$  表示预测为粘贴区域的像素。  $R_{FP}$  越接近于 0,  $R_{DA}$  越接近于 1, 则 CMFD 方案的准确度越高。

#### 4 结语

本文分析了国内外复制粘贴篡改检测技术的发展前沿, 检测方法可以分为: 基于图像块的方法, 基于关键点的方法和基于深度学习的方法。前面两种检测方法是通过手工设计的特征, 当前在精度上能够达到不错的效果, 但由于图像篡改技术日新月异, 篡改的方式也从单一变为复杂, 基于手工设计的特征很容易受到攻击。基于深度学习的方法通常采用端到端的训练方式自动学习特征, 这种方法避免了人工设计特征, 使得模型的鲁棒性和泛化性更好。

与图像篡改的“矛”相比, 图像内容被动取证的“盾”发展情况要落后很多。面对深度学习网络基于真实区域与缺失区域相关性预测出的“虚假”图像, 如何进行检测, 是当前亟须解决的问题。如何利用少量的数据集, 精简模型参数, 提高模型检测效率也是未来的研究方向。希望本文能够为该领域的研究人员提供最新的信息和研究的见解。

基金项目: 刑事检验四川省高校重点实验室开放基金研究项目 (2019YB02)。四川省高校人文社会科学重点研究基地——反恐怖主义研究中心资助 (FK2020QN03)。

#### [参考文献]

[1] Fridrich A J, Soukal B D, AJ Luk á š . Detection of copy-move forgery in digital

images[J]. Proceedings of Digital Forensic Research Workshop, 2003(2):102.

[2] Lowe D G . Distinctive Image Features from Scale-Invariant Keypoints[J]. International Journal of Computer Vision, 2004, 60(2):91-110.

[3] Luo W, Huang J, Qiu G . Robust Detection of Region-Duplication Forgery in Digital Image[J]. International Conference on Pattern Recognition. IEEE, 2006(2):102.

[4] Liu G, Wang J, Lian S, et al. A passive image authentication scheme for detecting region-duplication forgery with rotation[J]. Journal of Network and Computer Applications, 2011, 34(5):1557-1565.

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

[6] Cozzolino D, Poggi G, Verdoliva L . Efficient Dense-Field Copy - Move Forgery Detection[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(11):11.

[7] Christlein, Vincent, Riess, et al. An Evaluation of Popular Copy-Move Forgery Detection Approaches[J]. Information Forensics and Security, IEEE Transactions on, 2012(2):14-15.

[8] Tralic D, Zupancic I, Grgic S, et al. CoMoFoD - New Database for Copy-Move Forgery Detection[S]. ELMAR 2013.

[9] G. Serra, “MICC-F600, MICC-F220, MICC-F2000, and MICC-F8multi, ” [S]. Available: <http://giuseppeserra.com/content/sift-based-forensic-method-copy-move-detection>.

[10] National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Science, “CASIA image tampering detection evaluation database (CASIA TIDE) v1.0, v2.0, ” [S]. Available: <http://forensics.idealtest.org>.

[11] Wen B, Ye Z, Subramanian R, et al. COVERAGE - A novel database for copy-move forgery detection[J]. IEEE International Conference on Image Processing. IEEE, 2016(2):105.

[12] Alberry H A, Hegazy A, Salama G I . A fast SIFT based method for copy move forgery detection[J]. Future Computing & Informatics

- Journal, 2018(3):114.
- [13] Yadav N , Kapdi R . Copy move forgery detection using SIFT and GMM[J].2015 5th Nirma University International Conference on Engineering (NUICONE). IEEE, 2015(2):146.
- [14] Das T , Hasan R , Azam M R , et al. A Robust Method for Detecting Copy-Move Image Forgery Using Stationary Wavelet Transform and Scale Invariant Feature Transform[S]. 2018.
- [15] Muzaffer G , Ulutas G . A fast and effective digital image copy move forgery detection with binarized SIFT[J].International Conference on Telecommunications & Signal Processing. IEEE, 2017(2):595-598.
- [16] Jin G , Wan X . An improved method for SIFT-based copy - move forgery detection using non-maximum value suppression and optimized J-Linkage[J].Signal Processing: Image Communication, 2017(3):113-125.
- [17] Shahroudnejad A , Rahmati M . Copy-move forgery detection in digital images using affine-SIFT[J]. 2016 2nd International Conference of Signal Processing and Intelligent Systems (ICSPIS). IEEE, 2016(3):101.
- [18] Resmi M R , Vishnukumar S . A novel segmentation based copy-move forgery detection in digital images[J]. 2017 International Conference on Networks & Advances in Computational Technologies (NetACT), 2017(1):105.
- [19] Li Y , Zhou J . Fast and Effective Image Copy-Move Forgery Detection via Hierarchical Feature Point Matching[J]. IEEE Transactions on Information Forensics and Security, 2019(8):1-1.
- [20] Huang H , Guo W , Zhang Y . Detection of Copy-Move Forgery in Digital Images Using SIFT Algorithm[J]. Workshop on Computational Intelligence & Industrial Application. IEEE, 2009(2):131.
- [21] Bay H , Tuytelaars T , Van Gool L . Surf: Speeded up robust features[J].Lecture notes in computer science, 2006(3951):404-417.
- [22] Shivakumar B L , Baboo S S . Detection of region duplication forgery in digital images using SURF[J].International Journal of Computer Science Issues (IJCSI), 2011,8(4):199.
- [23] Jaberi M , Bebis G , Hussain M , et al. Accurate and robust localization of duplicated region in copy - move image forgery[J].Machine vision and applications, 2014(25):451-475.
- [24] Shivakumar B , Baboo S S . Automated forensic method for copy-move forgery detection based on Harris interest points and SIFT descriptors[J].International Journal of Computer Applications, 2011,27(3):9-17.
- [25] Ardizzone E , Bruno A , Mazzola G . Detecting multiple copies in tampered images[J].2010 IEEE International Conference on Image Processing. IEEE, 2010(2):2117-2120.
- [26] Ardizzone, Edoardo, Mazzola, et al. Copy-Move Forgery Detection by Matching Triangles of Keypoints[J]. IEEE Transactions on Information Forensics & Security, 2015(5):121.
- [27] Yuan R , Ni J . A deep learning approach to detection of splicing and copy-move forgeries in images[J].2016 IEEE International Workshop on Information Forensics and Security (WIFS). IEEE, 2017(2):141.
- [28] Ouyang J , Liu Y , Miao L . Copy-move forgery detection based on deep learning[J].2017 10th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI), 2017(3):145.
- [29] Yue W , Abd-Elmageed W , Natarajan P . Image Copy-Move Forgery Detection via an End-to-End Deep Neural Network[J].2018 IEEE Winter Conference on Applications of Computer Vision (WACV). IEEE, 2018(5):146.
- [30] Yue W , Abd-Elmageed W , Natarajan P . BusterNet: Detecting Copy-Move Image Forgery with Source/Target Localization[J].European conference on computer vision, 2018(2):46.
- [31] Zhou P , Han X , Morariu V I , et al. Learning Rich Features for Image Manipulation Detection[J]. 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). IEEE, 2018(15):184.
- [32] Wu Y , Abdalmageed W , Natarajan P . ManTra-Net: Manipulation Tracing Network for Detection and Localization of Image Forgeries With Anomalous Features[J]. 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR).

IEEE, 2019 (15):140.

[33] Barni M , Phan Q T , Tondi B . Copy Move Source-Target Disambiguation through Multi-Branch CNNs[J]. IEEE Transactions on Information Forensics and Security, 2020 (99):1-1.

[34] Zhong J L , Pun C M . An End-to-End Dense-InceptionNet for Image Copy-Move Forgery Detection[J]. IEEE Transactions on Information Forensics and Security, 2020 (15):2134-2146.

[35]Chen B, Tan W, Coatrieux G, et al. A serial image copy-move forgery localization scheme with

source/target distinguishment[J]. IEEE Transactions on Multimedia, 2020 (23):3506-3517.

[36]Islam A, Long C, Basharat A, et al. Doa-gan: Dual-order attentive generative adversarial network for image copy-move forgery detection and localization[J]. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2020 (2):4676-4685.

作者简介：丁远晴，女，(1992.12-)，毕业于西南交通大学，数字取证方向，当前就职于四川警察学院，讲师。