

基于 U 型检测网络的图像篡改检测算法

王珠珠

(西安电子科技大学网络与信息安全学院, 陕西 西安 710071)

摘 要: 针对图像篡改检测算法依赖单一图像属性、适用度不高以及当前基于深度学习的检测算法时间复杂度过高、精度较低等缺陷, 提出了一种基于 U 型检测网络的图像篡改检测算法。该算法首先利用连续的卷积层和最大池化层提取图像中多阶段的特征信息, 然后将得到的特征信息通过上采样操作恢复至输入图像的分辨率大小。同时, 为保证在提取图像高级语义信息的同时实现更高的检测精度, U 型检测网络中各阶段的输出特征会和对应的通过上采样层的输出特征进行合并。U 型检测网络在一般网络展现出来的特性上, 进一步探究了图像中篡改与非篡改区域间的隐藏特征信息, 利用其端到端的网络结构和提取图像上下文间较强关联信息的属性, 可以实现快速且高精度的检测效果。最后利用全连接条件随机场对 U 型检测网络的输出结果进行优化, 以获得更精细的检测效果。实验结果表明, 所提算法效果优于传统的基于图像单一属性的篡改检测算法和当前基于深度学习的检测算法, 并且具有较好的顽健性。

关键词: U 型检测网络; 隐藏特征信息; 全连接条件随机场; 图像篡改检测

中图分类号: TP302

文献标识码: A

doi: 10.11959/j.issn.1000-436x.2019086

Image forgery detection algorithm based on U-shaped detection network

WANG Zhuzhu

School of Cyber Engineering, Xidian University, Xi'an 710071, China

Abstract: Aiming at the defects of traditional image tampering detection algorithm relying on single image attribute, low applicability and current high time-complexity detection algorithm based on deep learning, an U-shaped detection network image forgery detection algorithm was proposed. Firstly, the multi-stage feature information in the image by using the continuous convolution layers and the max-pooling layers was extracted by U-shaped detection network, and then the obtained feature information to the resolution of the input image through the upsampling operation was restored. At the same time, in order to ensure higher detection accuracy while extracting high-level semantic information of the image, the output features of each stage in U-shaped detection network would be merged with the corresponding output features through the upsampling layer. Further the hidden feature information between tampered and un-tampered regions in the image upon the characteristics of the general network was explored by U-shaped detection network, which could be realized quickly by using its end-to-end network structure and extracting the attributes of strong correlation information among image contexts that could ensure high-precision detection results. Finally, the conditional random field was used to optimize the output of the U-shaped detection network to obtain a more exact detection results. The experimental results show that the proposed algorithm outperforms those traditional forgery detection algorithms based on single image attribute and the current deep learning-based detection algorithm, and has good robustness.

Key words: U-shaped detection network, hidden feature information, conditional random field, image forgery detection

收稿日期: 2019-01-02; 修回日期: 2019-03-01

基金项目: 陕西省自然科学基金基础研究计划基金资助项目 (No.2016JM6074)

Foundation Item: The Natural Science Basic Research Plan in Shaanxi Province of China (No.2016JM6074)

1 引言

由于图像编辑软件的大量出现和数字媒体监管力度的缺乏,人们可以轻易更改图像的内容信息,导致更改后的图像可能会传递完全不同的信息,这一有害趋势已经在很多领域引起了严重的不良后果。针对这一系列问题,许多学者对其进行了深入性的研究。总体来说,图像内容篡改操作可分为 2 类:复制粘贴篡改和剪切组合篡改。在复制粘贴篡改中,一幅图像里的某一部分内容会被复制粘贴到同一幅图像的另一个部分,以达到掩盖或增加图像内容的目的。剪切组合篡改是指将一幅图像的一个或几个区域复制到另一幅图像中以生成一幅新的图像。一组剪切组合篡改示例如图 1 所示,其中,图 1(a)为原始图像,图 1(b)为篡改图像,图 1(c)为篡改图像中的真实篡改区域。本文所研究的篡改类型为剪切组合篡改,并提出了一种有效的检测算法实现剪切组合篡改检测。传统的剪切组合篡改检测算法主要是根据图像中篡改与非篡改区域之间的属性差异进行判断,基于这些属性差异的检测算法大致可分为 4 类:1) 基于图像本质属性的检测方法^[1-3];2) 基于成像设备属性的检测方法^[4-7];3) 基于图像压缩属性的检测方法^[8-12];4) 基于图像散列的检测方法^[13-16]。由于每种检测算法只针对一种特定的图像属性,当这种属性不明显或不存在时,会出现检测失效的情况。例如,当被篡改图像和篡改图像产自相同品牌和模型的成像设备时,它们具有相同的噪声信息,那么基于图像本质属性的检测方法就会失效;而基于图像散列技术的检测方法则需要利用原始图像的散列值才能进行判断,严格来说,这并不算一种盲检测算法。



图 1 剪切组合篡改示例

近年来,由于卷积神经网络可自动学习高维数据间的映射关系,并且具有平移不变性等属性,使其在图像分类、图像语义分割、图像生成等计算机视觉领域都取得较大成功。目前,基于卷积神经网络的检测算法可实现不依赖于图像单一属性的图像篡改检测,弥补了传统算法依赖于图像单一属

性、适用度不高等缺陷。文献[17]将卷积神经网络首次应用于图像篡改检测,可用于判断当前图像是否被篡改,但不能定位篡改区域的具体位置。文献[18]提出了一种基于图像块的检测算法,但仅能大致定位图像中的篡改区域。为实现篡改区域的像素级定位,文献[19-20]都使用了不重叠的图像块作为神经网络的输入进行判断。由于大多数基于卷积神经网络的图像篡改检测算法主要是对图像中的每个块进行判断分类来得到最终检测结果,缺少利用图像上下文中的特征关联信息进行匹配和判断的条件(图像中的上下文关联信息是图像篡改检测中较为重要的部分),导致最终检测结果难以达到理想状况。同时,这些方法都是由多个阶段操作混合完成的,具有较高的时间复杂度。针对以上问题,本文首先利用 U 型检测网络^[21]针对图像上下文间的关联信息进行定位的特点实现图像篡改检测,然后再使用全连接条件随机场^[22]对 U 型检测网络的检测结果进行进一步的优化精细,最终得到较好的实验效果。

2 U 型检测网络与条件随机场

基于 U 型检测网络的图像篡改检测算法主要由两部分组成:U 型检测网络^[21]和全连接条件随机场^[22]后处理。首先利用 U 型检测网络对输入图像中的篡改区域进行较为精细的定位得到疑似篡改区域,然后利用全连接条件随机场对上述疑似区域进行进一步的精细优化以获得最终精确的检测结果。基于 U 型检测网络的检测示例如图 2 所示,其中,图 2(a)为待检图像,图 2(b)为通过 U 型检测网络检测得到的疑似篡改区域,图 2(c)为通过全连接条件随机场后处理的最终检测结果。



图 2 基于 U 型检测网络的检测示例

2.1 卷积神经网络

一般来说,在图像分类任务中,网络结构由若干个卷积层和池化层交替组成,通过全连接层和 softmax 激活函数得到最终的预测类别。由于全连接层会丢失特征的空间位置信息来完成特征的分类和回归,因此在图像分割任务中,为保留输出特

征能映射回输入图像的空间位置信息，需要舍弃全连接层，并利用上采样层或反卷积层来输出高分辨率的预测特征图。

2.1.1 卷积层

卷积层由一系列卷积核组成，每个卷积核负责不同的特征信息提取，这些特征信息包含了图像中的纹理信息、边缘信息、亮度分布、噪声信息等，对网络的判断起着重要作用。同时，由于卷积核权重共享的特点，可使特征提取的效率更高，整体参数更少。卷积层的计算方式为

$$y_i = w_i x + b_i \quad (1)$$

其中， x 为采样输入， w_i 为第 i 个卷积核的权重参数， b_i 为第 i 个神经元的偏置项， y_i 为第 i 个神经元的输出。

2.1.2 池化层

池化层也称为下采样层，一般在卷积层之后进行操作，可以通过池化层使卷积层输出的特征向量降维。池化层的具体作用有 4 个：1) 维持输出特征的不变形，这些不变形包括平移不变形、旋转不变性、尺度不变性等；2) 减小下一个卷积层的输入数据大小、减小计算量和参数大小；3) 可获得固定大小的输出，例如全局均值池化可以得到输出为 1×1 的特征图，这对某些输入数据大小不固定的情况较为重要；4) 由于池化操作可降低网络的参数大小，进一步地也可预防网络出现过拟合的情况。

2.1.3 上采样层

上采样层一般应用于图像分割任务中，利用插值方法，将低分辨率的语义级信息放大至较高分辨率，以获得可视化结果。

2.2 U 型检测网络

U 型检测网络本质上是一种卷积神经网络，于 2015 年由 Ronneberger 等^[21]提出，被广泛应用于医学图像处理领域，相较于传统的神经结构分割算法，不论是检测速率还是检测精度都有较大提升。U 型检测网络的结构如图 3 所示，图中数字表示当前的特征个数。U 型检测网络首先利用连续的卷积层和最大池化层来获取图像中的上下文特征信息，然后使用一系列上采样层将得到的特征信息进行插值放大以得到高分辨率特征图，最后利用层与层之间特征的横向传播，以达到减少特征的细节信息损失和精准定位篡改区域的目的。

图像篡改检测实际上也可被看作一个复杂的图像分割问题，同理，适用于图像分割问题的方法也可用于图像篡改区域检测中。在图像篡改检测中，由于图像中篡改区域与非篡改区域之间的可鉴别特征较为隐蔽和虚弱，当网络结构较深时，这些可鉴别特征会出现梯度消失的情况，为解决这一问题，需在 U 型检测网络中卷积层后加入批归一化^[23]操作。批归一化的具体计算步骤如算法 1 所示。

算法 1 批归一化操作

输入 批处理输入 $x: h = \{x_1, \dots, x_m\}$

输出 归一化后的结果 $\hat{y}_i = \text{BN}_{\gamma, \beta}(\hat{x}_i)$

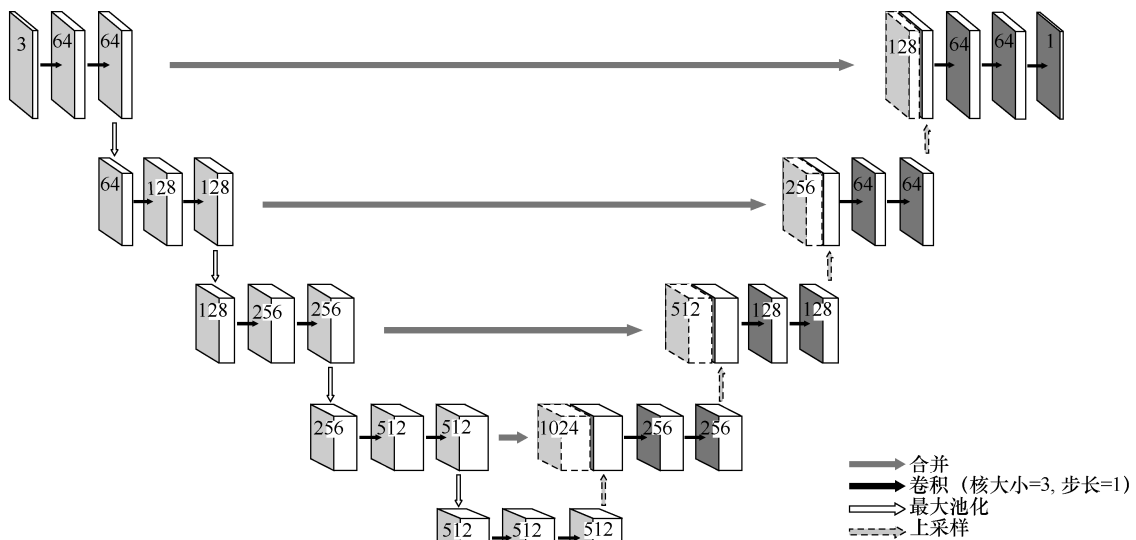


图 3 U 型检测网络的结构

- 1) $\mu_h \leftarrow \frac{1}{m} \sum_{i=1}^m x_i$ //计算批数据均值
- 2) $\sigma_h^2 \leftarrow \frac{1}{m} \sum_{i=1}^m (x_i - \mu_h)^2$ //计算方差
- 3) $\hat{x}_i \leftarrow \frac{x_i - \mu_h}{\sqrt{\sigma_h^2 + \varepsilon}}$ //归一化
- 4) $\hat{y}_i \leftarrow \gamma \hat{x}_i + \beta = \text{BN}_{\gamma, \beta}(\hat{x}_i)$

由于批归一化后输入数据会被限制在正态分布下,使网络的表达能力下降,为了解决这一问题,引入学习得到的 γ 和 β 进行尺度变换和偏移。同时,为解决图像中篡改区域和非篡改区域间的隐蔽特征难以学习的问题,引入 focal loss^[24] 作为网络的损失函数。focal loss 在交叉熵^[25]的基础上,进一步研究了简单样本和困难样本之间的关系及其对损失值的影响,从而解决了以往网络主要针对简单样本的特征进行学习却忽略困难样本的重要性的问题。focal loss 计算式为

$$L = -\alpha_i (1 - p_i)^\gamma \ln p_i \quad (2)$$

其中, α_i 为可调的权重控制参数, γ 为聚焦参数, p_i 为正确预测的概率。

2.3 全连接条件随机场后处理

在通过 U 型检测网络检测后,得到的疑似篡改区域仍包含了部分误判区域。基于此,利用全连接条件随机场^[22]后处理对 U 型网络的检测结果进行进一步的精细优化以得到最终的检测结果。全连接条件随机场作为一种经典的判别式模型,可更好地反映观测集中所有变量之间的相互联系和依赖关系。全连接条件随机场后处理在 U 型检测网络检测结果的基础上,不仅可进一步精细化检测结果,同时还可以剔除那些较小的误判区域,输出结果即为最终的篡改区域检测结果。

全连接条件随机场符合吉布斯分布,如式(3)所示。

$$P(X = x | I) = \frac{1}{Z(I)} \exp(-E(x | I)) \quad (3)$$

其中, $\frac{1}{Z(I)}$ 为归一化项, I 为包含观测集 $\{I_1, I_2, \dots, I_k\}$ 的随机场, I_k 为像素 k 的特征向量; X 为一个包含隐藏状态集 $\{X_1, X_2, \dots, X_k\}$ 的随机场, X_k 为像素 k 的标签; P 为预测的概率分布; $E(x | I)$ 为能量函数(为便于显示,后续推导中省略全局观

测集 I), 可表示为

$$E(x) = \sum_i \Psi_u(x_i) + \sum_{i < j} \Psi_p(x_i, x_j) \quad (4)$$

其中, i 为像素 i ; $\sum_i \Psi_u(x_i)$ 为一元势函数,代表 U 型检测网络的输出结果; $\sum_{i < j} \Psi_p(x_i, x_j)$ 为二元势函数,计算式为

$$\sum_{i < j} \Psi_p(x_i, x_j) = u(x_i, x_j) \sum_{m=1}^M w^{(m)} k_G^{(m)}(f_i, f_j) \quad (5)$$

其中, $u(x_i, x_j)$ 用于监督相邻且特征向量相似的像素被标记为不同类型, f 表示特征函数, M 表示共有 M 个特征函数, $k_G^{(m)}$ 表示第 m 个特征函数, $w^{(m)}$ 表示与特征函数对应的权重值。全连接条件随机场在传统的仅利用 4 连接或 8 连接邻域的条件随机场的基础上,利用二元势函数描述每一个像素与其他所有像素间的关系,并最终得到全图的概率分布。

3 实验数据及对比分析

数据集 CASIA v2.0^[26]是一个篡改图像复杂真实且不易被人眼判断的篡改图像数据集。为保证实验的客观性和实际性,本文选择 CASIA v2.0 作为实验数据集。CASIA v2.0 数据集中包含了复制粘贴和剪切组合这 2 种图像篡改类型,由于本文仅针对图像的剪切组合篡改,因此从 CASIA v2.0 数据集中筛选出共计 1 082 组剪切组合篡改图像数据作为实验数据,其中,随机选取 900 组图像数据作为训练数据,142 组图像数据作为验证数据,余下的 40 组作为测试数据。同时由于 CASIA v2.0 数据集中数据量的限制,实验部分采用十折交叉验证法来对实验效果进行客观公正的评估。在第 3.1 节中将会列出本文算法各个步骤的具体参数设置和对比实验的评价参数。进一步地,为客观验证本文所提算法的有效性及其稳健性,本文从传统的基于图像单一属性的篡改检测算法和当前基于深度学习的检测算法中分别挑选出几种检测效果较好的算法作为对比算法,并在第 3.2 节中列出几种算法的具体实验效果及其在各种攻击条件下的检测效果。

3.1 算法参数及实验评价参数

在训练过程中, U 型检测网络的初始学习率被设定为 0.1 进行训练,在迭代 50 轮后,学习率会被

降低到 0.01 进行训练, 再次迭代 50 轮后, 学习率会被降低至 0.001 继续训练, 直至网络趋于平稳状态。U 型检测网络选用随机梯度下降作为网络的优化器, focal loss 作为网络的损失函数, focal loss 中超参数 $\alpha_i=0.25$, $\gamma=2$ 。在全连接条件随机场后处理的推断过程中, 迭代更新次数为 5。本文所提算法使用 Python 作为编程语言, 利用 PyTorch 深度学习库实现 U 型检测网络, 实验部分中传统的基于单一属性的检测算法的实现平台为 Matlab, 基于深度学习的检测算法的实现框架为 Tensorflow, 并且以上对比算法都已调至最优参数。

本文对比实验部分所参考的评价参数为精确率、召回率和 F , 其中, 精确率的计算如式(6)所示, 召回率的计算如式(7)所示, F 的计算如式(8)所示。

$$\text{精确率} = \frac{\text{真阳性}}{\text{真阳性} + \text{伪阳性}} \quad (6)$$

$$\text{召回率} = \frac{\text{真阳性}}{\text{真阳性} + \text{伪阴性}} \quad (7)$$

$$F = \frac{2 \times \text{精确率} \times \text{召回率}}{\text{精确率} + \text{召回率}} \quad (8)$$

其中, 真阳性表示检测结果中正确检测为篡改区域的像素总量, 伪阳性表示检测结果中错误检测为篡改区域的像素总量, 伪阴性表示检测结果中错误检测为非篡改区域的像素总量。

3.2 评价实验及对比分析

为评价本文所提算法的实际效果, 本文选择 BLK 算法^[27]、GHO 算法^[28]、DCT 算法^[9]、CFAE 算法^[29]、NADQ 算法^[30] (以上算法由 Zampoglou 等^[31]复现)、C2R-Net 算法和 U-Net 算法为对比实验算法。由于原始 CASIA v2.0 数据集的图像数据为 TIFF 格式, 而 BLK 算法、GHO 算法、DCT 算法以及 NADQ 算法是基于 JPEG 图像格式的压缩属性进行检测的, 为保证对比实验的公平性, 需将 TIFF 格式的图像数据转化为零压缩的 JPEG 格式的图像数据。

从测试数据中随机挑选 5 组数据作为示例, 如图 4 所示。其中, 每一列表示一组示例及不同方法的检测结果, 第 a 行表示篡改图像, 第 b 行表示对应的真实篡改区域图像, 第 c 行表示 BLK 算法的检测结果, 第 d 行表示 GHO 算法的检测结果, 第 e 行表示 DCT 算法的检测结果, 第 f 行表示 CFAE 算法的检测结果, 第 g 行表示 NADQ 算法的检测结

果, 第 h 行表示 C2R-Net 算法的检测结果, 第 i 行表示 U-Net 算法的检测结果, 第 j 行表示本文所提算法的检测结果。从主观视觉角度出发, 在 5 种传统的基于图像单一属性的篡改检测算法中, BLK 算法、GHO 算法、CFAE 算法以及 NADQ 算法的检测结果趋于失效状态, DCT 算法也仅能大致定位出图像中的篡改内容; 基于深度学习的 C2R-Net 算法虽然能定位出图像中的篡改内容, 但仍存在少量误检及较多漏检情况; 原始 U-Net 算法能较好地定位图像中的篡改区域, 但存在少量多检及误检情况; 而本文所提算法在 U-Net 算法的基础上精细了检测结果, 筛掉了误检区域, 最终展示了较好、较稳定的检测效果。

表 1 展示了本文所提算法及 7 种对比算法通过十折交叉验证在 40 组图像数据上的检测结果的精确率、召回率和 F 的平均值。由表 1 可知, 本文所提算法的检测效果在精确率及 F 上都优于其他 7 种对比算法, 但召回率略低于 DCT 算法及 NADQ 算法。尽管 DCT 算法和 NADQ 算法的检测结果的召回率较高, 但从主观视角来判断, 2 种算法的检测结果存在较多的误检, 且出现大范围失效问题 (如图 4 第 e 行和第 g 行所示)。进一步地, 为验证本文所提算法的顽健性 (由于图 4 中已展示了原始 U-Net 算法和本文所提算法在非攻击条件下的实验效果, 这里不再做 U-Net 算法顽健性实验的展示), 本文测试了 7 种算法在不同攻击情况下的检测效果, 结果如图 5 所示, 并分别计算精确率、召回率及 F 的平均值。图 5(a)、图 5(c)和图 5(e)表示本文所提算法及 6 种对比算法在不同品质因子的 JPEG 图像压缩攻击下的检测结果, 图 5(b)、图 5(d)和图 5(f)表示各算法在不同方差 (均值默认为 0) 的高斯噪声攻击下的检测结果, 图 5(a)和图 5(b)表示各算法在不同类型、不同程度攻击下的检测结果的精确率, 图 5(c)和图 5(d)表示各算法在不同攻击情况下的检测结果的召回率, 图 5(e)和图 5(f)表示各算法在不同攻击情况下的检测结果的 F 。从图 5 可以看出, 在 JPEG 图像压缩攻击下, 对比算法中仅 DCT 算法和 C2R-Net 算法有一定的抗攻击能力, 当品质因子为 80 以下时, DCT 算法呈检测失效状态; 在高斯噪声攻击下, 仅 C2R-Net 能完成检测。而本文所提算法不仅在 JPEG 图像压缩攻击下展示了较好、较稳定的检测结果, 在高斯噪声攻击下仍维持了较好的检测效果。

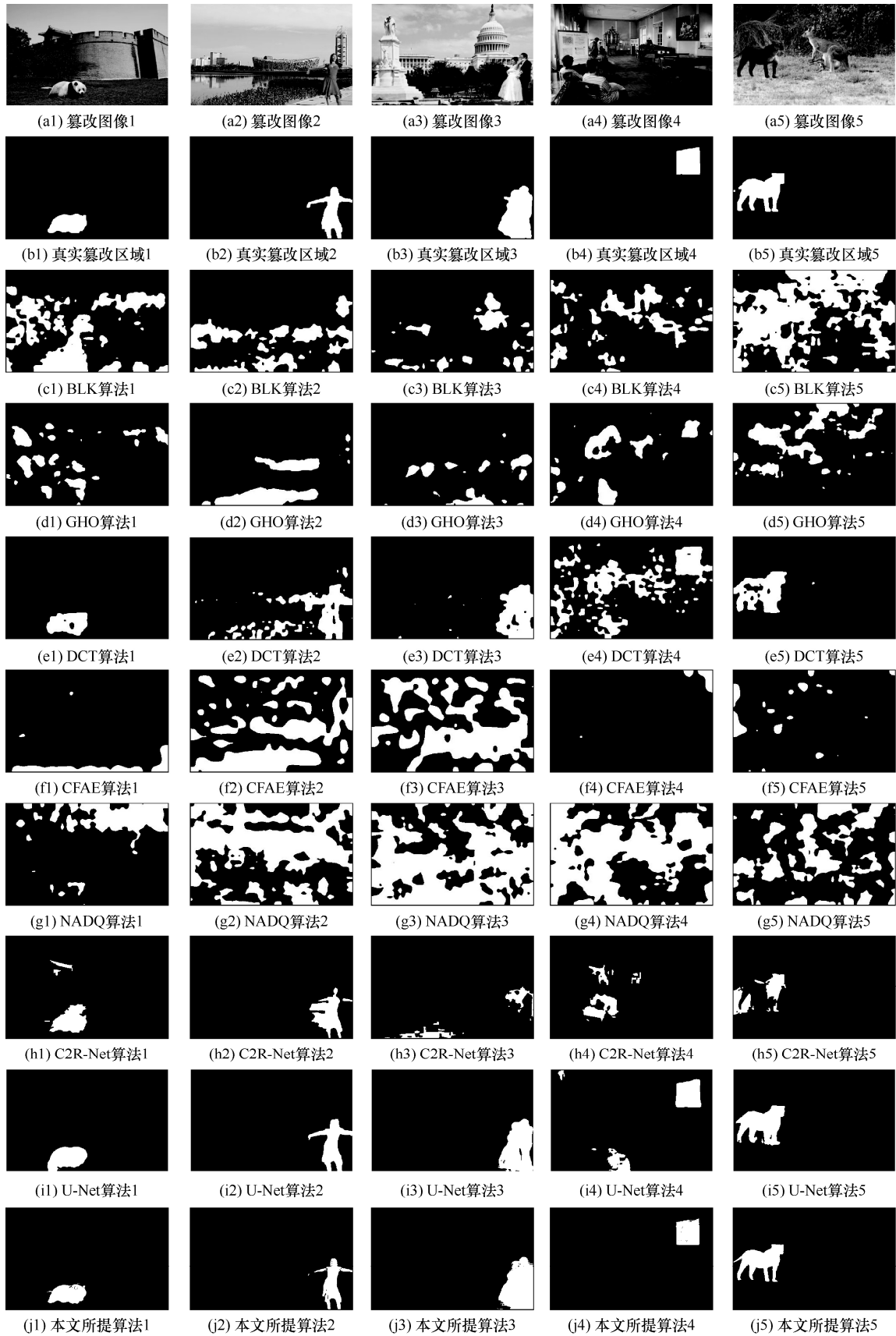


图 4 5 组对比实验示例

表 1 本文所提算法及 7 种对比算法在 40 组图像数据上的检测结果精确率、召回率和 F 的平均值

算法	精确率	召回率	F
BLK 算法	0.17	0.33	0.22
GHO 算法	0.19	0.25	0.22
DCT 算法	0.45	0.79	0.57
CFAE 算法	0.11	0.28	0.16
NADQ 算法	0.13	0.68	0.22
C2R-Net 算法	0.60	0.44	0.51
U-Net 算法	0.79	0.62	0.69
本文所提算法	0.90	0.67	0.77

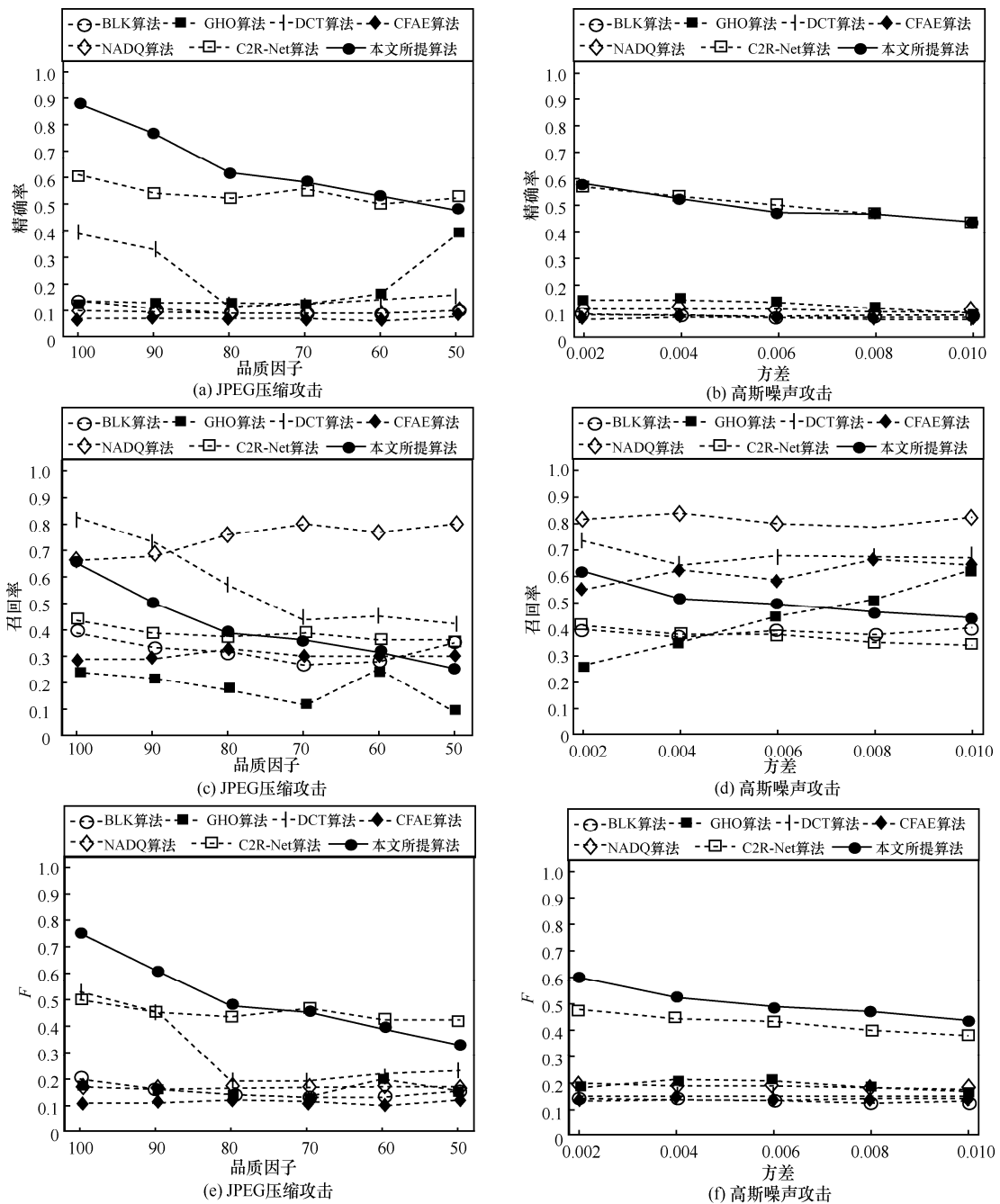


图 5 本文算法及 6 种对比算法的检测结果

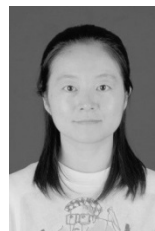
4 结束语

本文提出了一种基于 U 型检测网络的图像篡改检测算法, 首先利用 U 型检测网络检测图像中的疑似篡改区域, 接着为进一步优化精细 U 型网络的检测结果, 本文使用全连接条件随机场后处理进行处理并得到最终的检测结果。为评价本文所提算法的有效性及其实际性, 将其与传统的基于图像单一属性的篡改检测算法和当前基于深度学习的检测算法进行实验对比, 实验结果表明, 本文所提算法的检测效果优于其他几种对比算法。

参考文献:

- [1] CHEN W, SHI Y Q, SU W. Image splicing detection using 2-D phase congruency and statistical moments of characteristic function[C]//Security, Steganography, & Watermarking of Multimedia Contents IX. International Society for Optics and Photonics. 2007, 6505: 65050R.
- [2] WANG W, DONG J, TAN T. Effective image splicing detection based on image chroma[C]//IEEE International Conference on Image Processing. IEEE, 2009: 1257-1260.
- [3] ZHAO X, LI J, LI S, et al. Detecting digital image splicing in chroma spaces[J]. Lecture Notes in Computer Science, 2010, 6526: 12-22.
- [4] GOU H, SWAMINATHAN A, WU M. Noise features for image tampering detection and steganalysis[C]//IEEE International Conference on Image Processing. IEEE, 2007, 6: VI-97.
- [5] HSU Y F, CHANG S F. Detecting image splicing using geometry invariants and camera characteristics consistency[C]//IEEE International Conference on Multimedia & Expo. IEEE, 2006: 549-552.
- [6] MAHDIAN B, SAIC S. Detection of resampling supplemented with noise inconsistencies analysis for image forensics[C]//International Conference on Computational Sciences and its Applications. 2008: 546-556.
- [7] JOHNSON M K, FARID H. Exposing digital forgeries through specular highlights on the eye[C]//Information Hiding, Lecture Notes in Computer Science. Springer, 2007: 311-325.
- [8] JOHNSON M K, FARID H. Exposing digital forgeries in complex lighting environments[J]. IEEE Transactions on Information Forensics and Security, 2007, 2(3): 450-461.
- [9] YE S, SUN Q, CHANG E C. Detecting digital image forgeries by measuring inconsistencies of blocking artifact[C]//IEEE International Conference on Multimedia & Expo. IEEE, 2007: 12-15.
- [10] LIN Z, HE J, TANG X, et al. Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis[J]. Pattern Recognition, 2009, 42(11): 2492-2501.
- [11] LUO W, HUANG J, QIU G. JPEG error analysis and its applications to digital image forensics[J]. IEEE Transactions on Information Forensics and Security, 2010, 5(3): 480-491.
- [12] BIANCHI T, DE ROSA A, PIVA A. Improved DCT coefficient analysis for forgery localization in JPEG images[C]//IEEE International Conference on Acoustics. IEEE, 2011: 2444-2447.
- [13] ZHAO Y, WANG S, ZHANG X, et al. Robust hashing for image authentication using zernike moments and local features[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(1): 55-63.
- [14] WANG X, PANG K, ZHOU X, et al. A visual model-based perceptual image hash for content authentication[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(7): 1336-1349.
- [15] TANG Z, ZHANG X, LI X, et al. Robust image hashing with ring partition and invariant vector distance[J]. IEEE Transactions on Information Forensics and Security, 2015, 11(1): 200-214.
- [16] YAN C P, PUN C M, YUAN X C. Quaternion-based image hashing for adaptive tampering localization[J]. IEEE Transactions on Information Forensics and Security, 2016, 12(9): 2144-2158.
- [17] RAO Y, NI J. A deep learning approach to detection of splicing and copy-move forgeries in images[C]//IEEE International Workshop on Information Forensics & Security. IEEE, 2017: 1-6.
- [18] ZHANG Y, WIN L L, GOH J, et al. Image region forgery detection: a deep learning approach [C]//The Singapore Cyber-Security Conference (SG-CRC). 2016: 1-11.
- [19] BAPPY J H, ROYCHOWDHURY A K, BUNK J, et al. Exploiting spatial structure for localizing manipulated image regions[C]//IEEE International Conference on Computer Vision. IEEE Computer Society, 2017: 4970-4979.
- [20] YANG W, BI X L, XIAO B. C2R net: the coarse to refined network for image forgery detection[C]//The International Conference on Big Data Science and Engineering. IEEE, 2018: 1656-1659.
- [21] RONNEBERGER O, FISCHER P, BROX T. U-Net: convolutional networks for biomedical image segmentation[C]//International Conference on Medical Image Computing & Computer-assisted Intervention. IEEE, 2015: 234-241.
- [22] KR H H, KOLTUN V. Efficient inference in fully connected CRFs with Gaussian edge potentials[C]//Conference and Workshop on Neural Information Processing Systems. 2012: 109-117.
- [23] IOFFE S, SZEGEDY C. Batch normalization: accelerating deep network training by reducing internal covariate shift[J]. arXiv: 1502.03167.
- [24] LIN T Y, GOYAL P, GIRSHICK R, et al. Focal loss for dense object detection[C]//The IEEE International Conference on Computer Vision. 2017: 2980-2988.
- [25] SHORE J, JOHNSON R. Axiomatic derivation of the principle of maximum entropy and the principle of minimum cross-entropy[J]. IEEE Transactions on Information Theory, 1980, 26(1): 26-37.
- [26] CASIA. CASIA tampered image detection evaluation database(TIDE): v2.0[S]. Institute of Automation, Chinese Academy of Sciences, 2015.
- [27] LI W, YUAN Y, YU N. Passive detection of doctored JPEG image via block artifact grid extraction[J]. Signal Processing, 2009, 89(9): 1821-1829.
- [28] FARID H. Exposing digital forgeries from JPEG ghosts[J]. IEEE Transactions on Information Forensics & Security, 2009, 4(1): 154-160.
- [29] DIRIK A E, MEMON N D. Image tamper detection based on demosaicing artifacts[C]//The International Conference on Image Processing. IEEE, 2009: 1497-1500.
- [30] BIANCHI T, PIVA A. Image forgery localization via block-grained analysis of JPEG artifacts[J]. IEEE Transactions on Information Forensics & Security, 2012, 7(3): 1003-1017.
- [31] ZAMPOGLOU M, PAPADOPOULOS S, KOMPATSIARIS Y. Large-scale evaluation of splicing localization algorithms for web images[J]. Multimedia Tools & Applications, 2017, 76(1): 1-34.

[作者简介]



王珠珠 (1981-), 女, 山东曹县人, 西安电子科技大学博士生, 主要研究方向为数据安全、人工智能安全。