

DOI:10.16136/j.joel.2023.03.0263

基于卷积神经网络的随机因子重采样图像检测

刘 洋¹, 张玉金^{1*}, 张 涛², 王永琦¹, 袁国龙¹

(1. 上海工程技术大学 电子电气工程学院, 上海 201600; 2. 常熟理工学院 计算机科学与工程学院, 江苏 常熟 215500)

摘要: 图像重采样检测是图像取证领域的重要任务, 其目的是检测图像是否经过重采样操作。现有的基于深度学习的重采样检测方法大多只针对特定的重采样因子进行研究, 而较少考虑重采样因子完全随机的情况。本文根据重采样操作中所涉及的插值技术原理设计了一组高效互补的图像预处理结构以避免图像内容的干扰, 并通过可变形卷积层和高效通道注意力机制 (efficient channel attention, ECA) 分别提取和筛选重采样特征, 从而有效提高了卷积神经网络整合提取不同重采样因子的重采样特征的能力。实验结果表明, 无论对于未压缩的重采样图像还是 JPEG 压缩后处理的重采样图像, 本文方法都可以有效检测, 且预测准确率相比现有方法均有较大提升。

关键词: 图像取证; 重采样检测; 可变形卷积; 高效通道注意力 (ECA); 卷积神经网络

中图分类号: TP391 **文献标识码:** A **文章编号:** 1005-0086(2023)03-0232-09

Image resampling detection with random factor based on convolutional neural network

LIU Yang¹, ZHANG Yujin^{1*}, ZHANG Tao², WANG Yongqi¹, YUAN Guolong¹

(1. School of Electronic and Electrical Engineering, Shanghai University of Engineering Science, Shanghai 201600, China; 2. School of Computer Science and Engineering, Changshu Institute of Technology, Changshu, Jiangsu 215500, China)

Abstract: Image resampling detection is an important task in the field of image forensics. The purpose is to detect whether the image is resampled. Current methods based on deep learning are mostly aimed at fixed resampling factors. However, they rarely consider the case that the resampling factors are completely random. In this paper, according to the principle of interpolation involved in resampling operation, an efficient preprocessing structure is designed to avoid the interference of image content. Then resampling features are extracted and screened by deformable convolutional layer and efficient channel attention mechanism respectively, so as to effectively improve the performance of convolutional neural network in extracting resampling features with different resampling factors. The experimental results show that whether for uncompressed resampling images or resampling images after JPEG compression, the method can detect effectively, and the prediction accuracy is greatly improved compared with the current methods.

Key words: image forensics; resampling detection; deformable convolution; efficient channel attention (ECA); convolutional neural network

0 引 言

随着图像处理工具的快速发展, 数字图像的可信度越来越低。被恶意修改的图像可能反映着

与原始图像完全相反的内容, 从而造成信息的混淆、舆论的反转, 严重影响信息的真实性。因此, 对于数字图像的篡改取证受到越来越多技术人员的关注。

* E-mail: yjzhang@sues.edu.cn

收稿日期: 2022-04-12 修订日期: 2022-06-15

基金项目: 国家自然科学基金(62072057)、上海市自然科学基金(17ZR1411900)资助项目

数字图像篡改往往会破坏原始图像中某些固有的性质,或者生成一些新的不属于原始图像的操作痕迹,被动取证技术^[1]利用这些信息鉴别数字图像是否被篡改。近年来,针对图像拼接检测^[2]、中值滤波检测^[3]、JPEG压缩检测^[4]和重采样检测^[5]等多种不同情况的篡改检测已成为热点研究问题。其中,涉及图像尺寸的操作均与图像重采样技术有关。一方面,图像重采样可以使图像获得更精美的视觉反馈;另一方面,通过调整图像尺寸可以使伪造区域更加贴合于背景图像,达到以假乱真的效果。因此,检测图像是否被重采样是数字图像取证研究的重要环节。

近年来,研究人员从时域和频域等角度提出了一些基于手工特征分析的图像重采样取证方法。POPESCU^[6]从空间域考虑重采样像素和相邻像素间存在的相关性,用期望最大化(expectation maximum, EM)算法来提取这种线性关系,在没有任何数字水印和数字签名的情况下检测图像重采样痕迹。GALLAGHER^[7]通过计算图像的二阶导数,并用傅里叶变换凸显由重采样操作引起的周期性痕迹,发现了重采样图像的频谱峰值特性。在周期性和频谱特性等启发下,研究者们将机器学习方法^[8]引入重采样取证领域, FENG等^[9]通过归一化具有交替特性的能量密度,推导出一个19维的特征向量,输入支持向量机以检测重采样图像。此外, FAN等^[10]将高斯混合模型(Gaussian mixture model, GMM)用在小图像块中学习图像操作痕迹,实现了包括滤波检测、JPEG压缩检测和重采样检测在内的通用图像处理检测器。

随着神经网络的再度兴起,基于深度学习的重采样取证方法迎来蓬勃发展,与基于手工特征提取的传统方法相比,神经网络能够提取更高级的特征以实现更好的检测性能。BAYAR等^[5]在卷积神经网络架构中添加一个约束卷积层计算输入图像的残差,使网络能够自动学习对重采样有鉴别能力的残差特征,但对于JPEG压缩后的重采样图像适用性不高。CHEN等^[11]考虑到大部分的图像操作具有方向不变性,引入了各向同性卷积层处理网络的输入,并借鉴DenseNet^[12]的结构设计网络,实现了通用图像操作检测。CAO等^[13]通过两个低阶高通滤波器构造了一种双流卷积神经网络,提高了在JPEG压缩图像上重采样检测的准确率,但网络结构比较复杂,需要较高算力。LIANG等^[14]以残差模块(residual block)为基础设计卷积神经网络进行重采样操作痕迹检测,使网络对不同重采样因子的重采样图像均具

有较高的检测准确率。DING等^[15]则根据上采样能量稀疏而下采样能量紧密的特性,构建了可测量的能量层以消除与重采样检测无关的纹理和其他信息,从而对重采样因子做有效预测。在针对不同图像尺寸的重采样检测问题中, LAMBA^[16]设计了一种具有迭代池和分支网络的模型以处理不同分辨率的重采样图像,提高了模型的适用性。PENG等^[17]对重采样因子估计问题做了公式化的描述,并设计了一种双滤波结构的卷积神经网络用于估计重采样因子。

上述研究工作大多只针对特定的重采样因子进行,实际中被检测的图像往往具有未知的重采样因子。因此,研究能够高效检测随机因子重采样图像的网络模型具有更大的现实意义。针对这个问题,本文设计了一种基于可变形卷积和高效通道注意力机制(efficient channel attention, ECA)的卷积神经网络架构,通过预处理层提供高频信息输入流,使用可变形卷积从输入中提取重采样特征,接着利用ECA结构对特征通道进行筛选,提取能够更有效刻画重采样特性的深度特征。

1 数字图像重采样

数字图像重采样主要通过插值技术实现,一般分为图像上采样(放大)和下采样(缩小)操作。重采样后的图像每个像素都是插值后的像素,其值由原始图像中的邻域像素的像素值加权求得。图1是一幅示例图像及其局部区域的上/下采样结果。

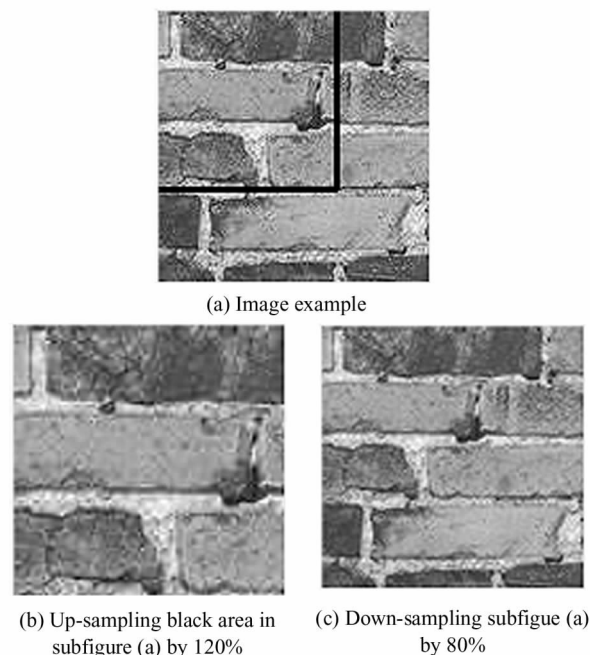


图1 重采样操作对图像的影响

Fig. 1 Effects of resampling operation on an image

目前常用的重采样插值算法有3种,分别是最近邻插值法、双线性插值法及双三次插值法,这3种方法的侧重范围各不相同,它们的计算复杂度和插值质量依次提高。

2 本文方法

本文将重采样检测视为模式分类问题,通过深度学习方法中针对图像的卷积神经网络模型来解决。重采样图像的检测会受到图像内容的严重干扰,后续实验表明,这种干扰在随机采样因子的重采样图像中更为明显。因此未处理的图像不能直接作为卷积神经网络的输入。本文首先用一组由两个互补的高通滤波器组成的预处理结构计算图像的残差,再将得到的高频信息流通过可变形卷积结构等提取重采样特征,在各卷积结构中插入ECA模块筛选特征通道,最终通过分类结构预测图像类别。

2.1 预处理层

卷积神经网络通过提取重采样特征对重采样图像进行预测,而重采样痕迹通常存在于与图像内容无关的高频信息之中。因此,预处理层的作用是计算图像残差,图像残差表示抑制了图像内容后的高频信息流,其结果由图像像素与其邻域像素的差异计算得到。根据计算函数 $f(\cdot)$ 的不同,得到的残差结果也不同。该过程可以表示为式(1):

$$Res = f(I) - I, \quad (1)$$

式中, Res 表示残差输出, I 表示输入图像或图像块。

由于重采样后的像素是由其原始图像邻域插值得到的像素,而在计算残差时邻域像素的重要程度未知。因此本文设计了一种如式(2)所示的考虑4邻域的残差滤波器 K_1 ,表示由距离像素最近的4个相邻像素以相同的权重计算残差。

$$K_1 = \begin{bmatrix} 0 & 0.25 & 0 \\ 0.25 & 1 & 0.25 \\ 0 & 0.25 & 0 \end{bmatrix}. \quad (2)$$

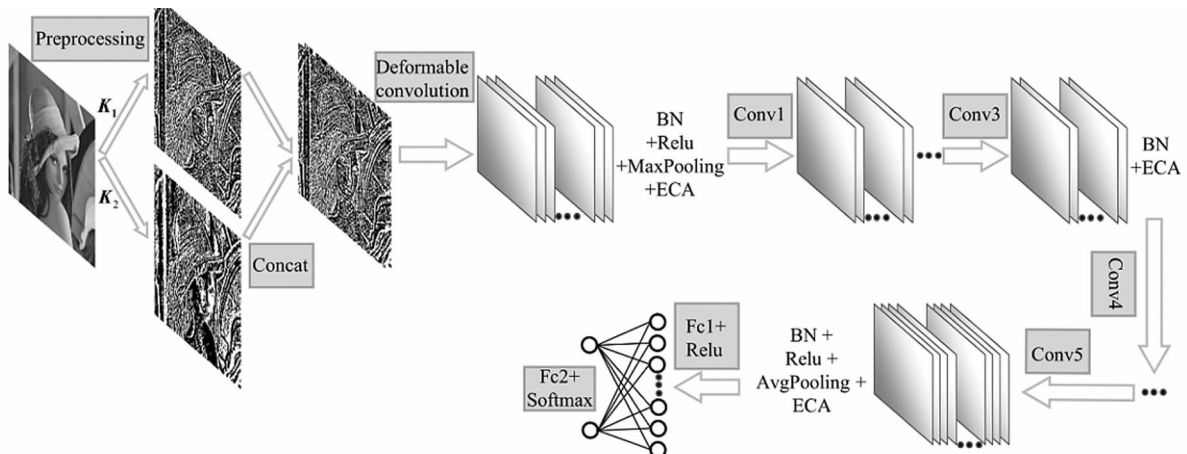


图3 本文模型架构图

Fig. 3 The detailed structure of the proposed model

图2是滤波器 K_1 对一幅示例图像的处理效果,可以看出,处理后的图像,内容被抑制,而大量的边缘、角点等高频信息被凸显。

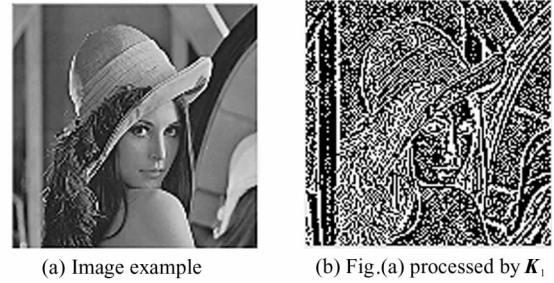


图2 被 K_1 处理图像的可视化效果

Fig. 2 Visualization of preprocessing on image by K_1

为了区分在残差计算时邻域像素的重要程度,本文另外设计了一种如式(3)所示的1邻域残差滤波器 K_2 作为补充,其含义为由距离像素最近的1个相邻像素计算残差。

$$K_2 = [1, -1, 0]. \quad (3)$$

上述两个滤波器以并行连接的方式共同构成网络的预处理层以获取更多能够体现重采样特性的处理痕迹。具体来讲,就是在将灰度图像输入卷积神经网络之前,首先用 K_1 和 K_2 这两个滤波器进行卷积,滤波器的步长为1,填充为1,然后将处理后的图像在通道维度拼接作为卷积结构的输入。

2.2 网络架构

2.2.1 卷积神经网络

卷积神经网络是一种常见的深度学习模型,它可以自动学习图像的内部特征从而实现图像分类、图像预测等功能。本文使用卷积神经网络作为主干网络,如图3所示。

该网络由预处理结构、卷积结构和分类结构顺序连接组成,网络结构及相关参数如表1所示。其中,预处理结构用于接收和预处理图像数据,包含预处理层利用 K_1 和 K_2 滤波器分别对输入图像进行处理,拼接函数 Concat 将得到的残差信息按通道维度拼接。卷积结构用于提取重采样特征,在可变形卷积结构中,卷积核大小为 7×7 的可变形卷积层、批标准化层、Relu 激活层、窗口大小为 3×3 的最大值池化层和 ECA 模块依次相连。卷积结构1和卷积结构2具有类似的设计,由卷积核大小为 5×5 的标准卷积层和批标准化层、Relu 激活函数、窗口大小为 3×3 的最大值池化层、ECA 模块依次相连。为了防止特征消失,卷积核大小分别为 5×5 和 3×3 的卷积结构3和卷积结构4并未设计激活层和池化层,在最后的卷积结构5中,其卷积核大小为 1×1 ,并设计了窗口大小为 3×3 的平均值池化层来减少模型参数。在各卷积结构中,图像数据在经过其卷积层和池化层处理前后,其尺寸会发生改变,表1所示输入和输出尺寸是以 128×128 的灰度图像作为初始输入得到的。最后,分类结构用于结果的预测,两层全连接层用于实现数据降维,并最终通过 Softmax 函数预测图像类别。

2.2.2 可变形卷积层

本文引入可变形卷积层^[18]作为网络的第一层卷积。与传统图像分类问题相比,图像重采样检测问题中卷积结构的初始输入不是未经处理的原始图像,而是被抑制了内容后的残差图像。传统的方形卷积较难处理残差图像中所包含的不规则的边缘、角点等这些高频信息,而可变形卷积可以自适应地改变卷积核的形状,改变感受野的范围,从而对这些信息进行更高效的处理。可变形卷积在标准卷积的每个像素点上都添加了偏移量 $\triangle p_n$ ($n=1, 2, \dots, N$),其值由另一个独立的卷积层自适应更新。令 $x(p)$ 和 $y(p)$ 分别表示输入特征图和输出特征图中位置 p 的特征,以 3×3 卷积为例,如式(4)所示:

$$y(p) = \sum_{p_n \in R} w_n \cdot x(p + p_n + \triangle p_n), \quad (4)$$

式中, w_n ($n=1, 2, \dots, 9$) 表示权重, R 为采样区域 $\{(-1, -1), (-1, 0), \dots, (0, 1), (1, 1)\}$, p_n ($n=1, 2, \dots, 9$) 为采样区域 R 中的所有采样点,由于 $\triangle p_n$ 不是整数,采用双线性插值计算 $x(p + p_n + \triangle p_n)$ 的值。本文根据每个采样点的偏移量来衡量其相应像素点的重要程度 α_n , 其值通过式(5)来计算:

$$\alpha_n = 1 - \frac{|\triangle p_{n_x}| + |\triangle p_{n_y}|}{\max(|\triangle p_{n_x}| + |\triangle p_{n_y}|)}, \quad (5)$$

式中, $\triangle p_{n_x}$ 和 $\triangle p_{n_y}$ 分别表示采样点 p_n 在 x 和 y 方向上的偏移量。

表1 本文网络结构

Tab. 1 The detailed structure of the proposed model

Structure	Layer	Input size	Output size
Preprocessing structure	Preprocessing layer	$128 \times 128 \times 1$	
	Concat		$128 \times 128 \times 2$
Deformable convolutional structure	Deformable convolution(7×7)	$128 \times 128 \times 2$	$64 \times 64 \times 96$
	BN(batch normalization)		
	Activation function (Relu)		
	Maxpooling(3×3)	$64 \times 64 \times 96$	$31 \times 31 \times 96$
Convolutional structure 1/2	ECA module		
	Conv(convolutional layer)(5×5)	$31 \times 31 \times 96 / 15 \times 15 \times 64$	$31 \times 31 \times 64 / 15 \times 15 \times 64$
	BN		
	Activation function (Relu)		
Convolutional structure 3/4	Maxpooling (3×3)	$31 \times 31 \times 64 / 15 \times 15 \times 64$	$15 \times 15 \times 64 / 7 \times 7 \times 64$
	ECA module		
	Conv($5 \times 5 / 3 \times 3$)	$7 \times 7 \times 64$	$7 \times 7 \times 64$
	BN		
Convolutional structure 5	ECA module		
	Conv(1×1)	$7 \times 7 \times 64$	$7 \times 7 \times 128$
	BN		
	Activation function(Relu)		
Classification structure	Avgpooling(3×3)	$7 \times 7 \times 128$	$3 \times 3 \times 128$
	ECA module		
	Flatten	$3 \times 3 \times 128$	1152
	Fc(fully connected layer)	1152	200
	Activation function(Relu)		
	Fc	200	200
	Softmax	200	2

最终,可变形卷积层处理后的输出特征 $y(p)$ 可以表示为:

$$y(p) = \sum_{p_n \in R} w_n \cdot x(p + p_n + \triangle p_n) \cdot \alpha_n. \quad (6)$$

2.2.3 ECA

由于预处理操作中对图像内容的抑制,使得作为输入的残差图像包含大量的冗余信息,这些信息也会参与模型的计算,对最终的预测造成影响,因此需要对卷积处理后的特征进行筛选。本文引入 ECA^[19],通过快速一维卷积获取局部跨通道交互信息,以极其轻量级的方式为特征通道高效生成通道权值,使模型能够更关注有利于最终分类的重采样特征。

3 实验结果与比较分析

3.1 实验设计

3.1.1 数据集的制作

本文实验使用 RAISE^[20]数据集作为数据来源。

RAISE 数据集是图像取证领域常用的图像数据集,该数据集包含 8 156 幅高分辨率的 TIF 格式图像,图像内容包含各种主题和场景。本文将其中的 1 400 幅分别按照 512×512 的分辨率进行切割,生成 35 000 幅 512×512 大小的子图像。除特殊说明外,该子图像集将作为本文实验中使用到的原始数据集。

3.1.2 实验环境

为了有效衡量重采样检测模型的性能,本文采用预测准确率作为评价指标。数据集中的每幅图像均会被设置一个标签,使用模型对图像的标签进行预测,正确预测的图像数量与总图像数量的比值被定义为预测准确率。所有实验都是在 Pytorch 开源神经网络框架和 NVIDIA Tesla V100-SXM2 GPU 下实现的。每个实验均进行了 30 个 epoch 的训练,1 个 epoch 是指训练集中所有数据样本所需的总迭代次数,并在每个 epoch 结束后在测试数据集上记录模型的预测准确率,训练和测试的过程是分离的。使用 Adam 优化器训练本文模型,Batch_size 设置为 64,初始学习率设置为 0.001,每 6 个 epoch 学习率下降为之前的一半。

3.2 实验结果与分析

3.2.1 未压缩重采样图像检测结果

为了尽可能地贴近现实取证场景,本小节设计了 5 组实验来评估模型性能。首先生成未经重采样操作的图像数据集,对 3.1.1 小节子数据集中每幅图像的中心区域进行 256×256 大小的裁剪。然后设计重采样因子集,由于图像尺寸均是整数,所以本小节用 5 组不同的重采样尺寸集来更多地反映范围内的重采样因子,如式(7)所示:

$$\begin{aligned} S_1: & (256, 768); \\ S_2: & (256, 384, 640, 768); \\ S_3: & (256, 320, 384, 448, 576, 640, 704, 768); \\ S_4: & (256, 288, 320, 352, 384, 416, 448, 480) \cup \\ & (544, 576, 608, 640, 672, 704, 736, 768); \\ S_5: & (256, 257, \dots, 510, 511) \cup (513, 514, \dots, \\ & 767, 768)。 \end{aligned} \quad (7)$$

每组尺寸集适用一组实验,对于各组实验的每幅图像从该组对应尺寸集 S 随机选择一个数字 m ,将这幅图像重采样到 $m \times m$ 大小的尺寸,重采样方式采用双三次插值,然后对重采样后的图像中心区域进行 256×256 大小的裁剪。共得到 6 个分别包含 35 000 幅图像的数据集,由 1 个未重采样数据集和 5 个重采样数据集组成。

本文实验对各模型均使用相同的训练数据集和测试数据集在相同的实验环境下进行对比评估。重复使用未重采样数据集分别和其余 5 个重采样数据集进行分组实验,每组实验中 60 000 幅图像用于训练,10 000 幅图像用于测试。

图 4 和表 2 显示,BAYAR^[5]和 PENG^[17]的模型对各尺寸集的重采样图像均达到了 96% 以上的预测准确率,已经具有了相当优秀的检测性能,本文模型进一步将各个尺寸集上的预测准确率提升到了 98% 以上,并且本文模型具有更快的收敛速度。

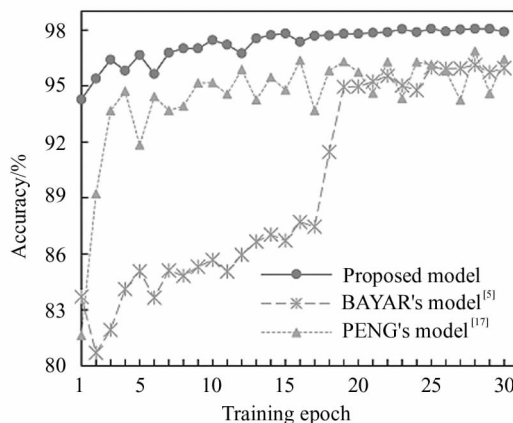


图 4 S_5 尺寸集下的预测准确率

Fig. 4 Prediction accuracy with size set of S_5

表 2 不同图像尺寸集下的预测准确率

Tab. 2 Prediction accuracy with different image size sets

Model	S_1	S_2	S_3	S_4
BAYAR's model ^[5]	97.62%	97.17%	97.32%	97.30%
PENG's model ^[17]	97.15%	97.04%	96.60%	96.54%
Proposed model	98.39%	98.18%	98.11%	98.16%

3.2.2 压缩重采样图像检测结果

前述实验显示了本文方法和现有方法对未压缩的重采样图像优秀的检测能力。然而在现实生活中,为了使图像数据便于传输,数字图像往往还会经历压缩的过程。JPEG 压缩是一种常见的有损压缩算法,其产生的块效应^[21]会对重采样特征产生严重干扰,压缩率越高,则干扰越大。

在 3.2.1 节的基础上,本小节设计了针对不同 JPEG 质量因子的重采样图像的实验。首先,对原始数据集的图像中心进行 256×256 大小的裁剪,然后用 JPEG 质量因子 $Q=50-90$ 、间隔为 10 对裁剪后得到的图像进行压缩,得到未重采样的 JPEG 图像数据集。然后采用 3.2.1 节中的 S_5 图像尺寸集对原始

图像集进行双三次插值的重采样,同样裁剪其中心 256×256 大小的区域,进行 $Q=50-90$ 、间隔为 10 的压缩,得到 JPEG 重采样图像数据集。一共得到 10 个分别包含 35 000 幅图像的数据集。每一对相同 JPEG 质量因子的正负样本数据集视为一组进行实验,其中 60 000 幅图像用于训练,10 000 幅图像用于测试。考虑双流卷积神经网络^[13]对 JPEG 重采样图像具有优秀的检测能力,实验引入此模型作为比较。如图 5 所示,与另外两种模型相比,双流卷积神经网络模型对 JPEG 压缩图像的检测具有明显优势,但本文模型的预测准确率在其基础上又有较大提升,在 JPEG 质量因子为 70 时,本文模型相比双流卷积神经网络模型的预测准确率提升了 6.40%,相比 PENG^[17]的模型提升了 16.41%。在 JPEG 质量因子为 80 时,本文模型的预测准确率相比 BAYAR^[5]的模型提升了 16.95%。

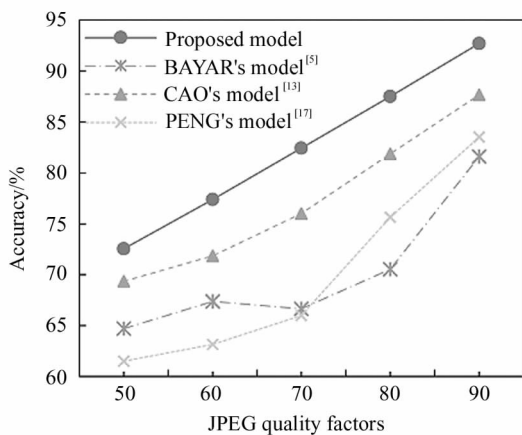


图 5 不同 JPEG 品质因子下的模型预测准确率

Fig. 5 Prediction accuracy of model with different JPEG factors

3.2.3 不同尺寸压缩重采样图像检测结果

图像尺寸对模型的性能有较大影响,因此本小节将测试不同图像尺寸下模型的检测性能。保持 JPEG 质量因子 $Q=85$,分别对原始图像和经 S_5 尺寸集双三次插值处理后的重采样图像中心区域进行 256×256 、 128×128 、 64×64 大小的裁剪,得到 3 组共 6 个分别包含 35 000 幅图像的未重采样图像数据集和重采样图像数据集。

具体结果如表 3 所示。本文模型在各尺寸图像中的检测性能均保持领先优势,其中在 256×256 、 128×128 尺寸的情况下,相比 BAYAR 和 CAO 均保持 13%和 5%左右的提高,在 64×64 图像尺寸情况下的提升幅度略有下降,但仍达到了 8.84%和 3.42%。

表 3 不同尺寸的 JPEG 重采样检测准确率

Tab. 3 Resampling detection accuracy with different sizes after JPEG compression

Model	256×256	128×128	64×64
BAYAR's model ^[5]	77.64%	72.75%	68.55%
CAO's model ^[13]	84.95%	80.21%	73.97%
PENG's model ^[17]	77.80%	—	—
Proposed model	90.63%	85.26%	77.39%

3.2.4 不同插值算法的压缩重采样图像检测结果

现实情况中重采样图像的插值算法并不固定,目前有 3 种图像重采样插值算法使用较为广泛,为了验证本文方法对其他插值算法的有效性,本小节共设计了 3 组实验。首先仍然是对原始数据集裁剪 256×256 的中心区域后做 JPEG 质量因子 $Q=85$ 的压缩处理,然后在以 S_5 尺寸集对图像进行重采样操作时,其重采样插值方法分别使用最近邻插值法、双线性插值法以及随机插值法(在最近邻插值法、双线性插值法和双三次插值法中随机)插值,对重采样后的图像裁剪 256×256 的中心区域后做 JPEG 质量因子 $Q=85$ 的压缩处理。共得到 1 个包含 35 000 幅未经重采样处理的 JPEG 图像数据集和 3 个包含 35 000 幅以不同插值算法重采样的 JPEG 图像数据集。对应分组训练,其中 60 000 幅用于训练,10 000 幅用于测试。

实验结果如表 4 所示,结合表 3 分析可知,各种模型对最近邻插值法处理的图像预测准确率均较高,而在插值算法改变时,各种模型的预测准确率变化并没有呈现出同步性,如 BAYAR 的模型在不同算法间达到了 9.34%的差距,而本文方法最大仅下降了 1.77%,但均保持在 90%左右或以上的预测准确率,说明不同模型对不同插值算法具有一定的针对性,且本文模型对不同插值算法处理的重采样图像具有较高的通用性。

表 4 不同插值算法的 JPEG 重采样检测准确率

Tab. 4 Resampling detection accuracy with different interpolation algorithms after JPEG compression

Model	Nearest	Bilinear	Random
BAYAR's model ^[5]	84.92%	75.58%	77.08%
CAO's model ^[13]	89.37%	84.85%	85.05%
PENG's model ^[17]	84.38%	78.02%	74.96%
Proposed model	91.53%	90.47%	89.76%

3.2.5 不同数据集的压缩重采样图像检测结果

为了验证本文模型的泛化能力,本小节引入 BOSSbase 数据集^[22]和 ALASKA2 数据集^[23]进行实验。其特点分别是 BOSSbase 数据集中的 BOSSbase v1.01 包含 10 000 幅 512×512 分辨率的 pgm 格式的灰度图像,ALASKA2 数据集中的 Cover 文件夹包含 75 000 幅 512×512 分辨率的 jpg 格式的彩色图像。

对其分别处理,以 256×256 的大小裁剪 BOSSbase 中 10 000 幅原始图像的中心区域,对得到的中心区域图像进行 JPEG 质量因子 $Q=85$ 的压缩,然后以 S_5 尺寸集对 10 000 幅原始图像做重采样处理,插值方式为双三次插值,裁剪重采样操作后的图像的中心 256×256 区域,以 JPEG 质量因子 $Q=85$ 对裁剪得到的中心图像进行压缩,最终得到以 BOSSbase 数据集为基础的 10 000 幅未重采样的 JPEG 图像和 10 000 幅重采样后的 JPEG 图像。将其中 16 000 幅图像(各取 8 000 幅)用于训练,其余用于测试。对 ALASKA2 数据集取其前 35 000 幅图像作为原始图像,对原始图像做 256×256 大小的中心区域裁剪,并保存为 JPEG 质量因子 $Q=85$ 的 JPEG 图像,然后对原始图像以 S_5 尺寸集做重采样处理,插值方式为双三次插值,对重采样后的图像做 256×256 中心裁剪,并保存为 JPEG 质量因子 $Q=85$ 的 JPEG 图像,得到以 ALASKA2 数据集为基础的 35 000 幅未重采样的 JPEG 图像和 35 000 幅重采样后的 JPEG 图像,60 000 幅用于训练,10 000 幅用于测试。

实验结果如表 5 所示,结合表 3 可以看出,以不同数据集为基础制作的训练数据会对模型产生一定的影响,以本文方法为例,在 BOSSbase 数据集中的预测准确率为 85.12%,而在 ALASKA2 数据集中达到 95.22%,产生差异的原因主要是各数据集中图像的数量、内容和格式等的不同,但本文模型在所使用到的 3 种数据集中的预测准确率均优于其他模型,进一步验证了本文模型的优越性。

表 5 不同数据集的 JPEG 重采样图像预测准确率

Tab. 5 Prediction accuracy of JPEG resampling images based on different datasets

Model	BOSSbase	ALASKA2
BAYAR's model ^[5]	78.39%	88.55%
CAO's model ^[13]	82.11%	94.31%
PENG's model ^[17]	79.01%	87.54%
Proposed model	85.12%	95.22%

3.3 模型架构的有效性验证

3.3.1 预处理结构的有效性

为了评估本文模型预处理层中两个滤波结构的有效性,本文首先设计了 3 种情况进行研究,即只使用 K_1 滤波器、只使用 K_2 滤波器同本文提出的完整模型进行比较。本小节使用 3.2.3 小节中图像尺寸为 128×128 的数据集进行实验,具体结果如表 6 所示。实验结果说明, K_1 和 K_2 滤波器的设置是合理的, K_1 滤波器对本文问题具有较好的检测能力,而 K_2 滤波器也起到了补充的作用。

表 6 含有不同滤波结构的模型的预测准确率

Tab. 6 Prediction accuracy of models with different filters

Model with filter	Accuracy/%
K_1	84.84
K_2	84.18
$K_1 + K_3$	84.79
$K_2 + K_3$	84.24
$K_1 + K_2 + K_3$	85.30
Proposed model	85.26

此外,本小节还添加了一个如式(8)所示的双流卷积网络^[13]中的 1×3 高通滤波器 K_3 进行对比试验。

$$K_3 = [0.5, -1, 0.5]。 \quad (8)$$

从表 6 可以看出, K_3 滤波器并不能明显提升模型性能,进一步说明盲目添加滤波器的种类并不能提高图像重采样检测模型的性能。

3.3.2 架构有效性

本小节测试本文方法中涉及架构的性能,具体设计了 3 个实验,分别是在本文模型的基础上去除预处理层的模型以及同时去除可变形卷积层和 ECA 层的模型,实验数据集与上一小节保持一致。

具体结果如表 7 所示,去除预处理层后的模型准确率降低到了 50% 左右,说明直接以重采样图像作为输入的卷积神经网络模型无法解决本文问题。此外,在去除其他结构后,相应模型的性能也发生一定程度的下降,说明本文模型结构设计的合理性。

表 7 不同结构模型的预测准确率

Tab. 7 Prediction accuracy of models with different structure

Model with different structure	Accuracy/%
Without preprocessing layer	49.77
Without deformable convolutional layer and ECA module	83.8
Proposed model	85.26

4 结 论

本文提出了一种基于卷积神经网络的重采样图

像检测模型。该模型提高了卷积神经网络对不同重采样因子的重采样特征整合提取的效率,使得对随机重采样因子的重采样图像检测性能明显提高。这是由于现有方法仅注重对预处理层的设计,但忽视了预处理后的图像作为输入发生的变化,从而没有对卷积神经网络提取特征的方式做适应性改进。

本文通过添加可变形卷积层和ECA来解决随机重采样因子重采样图像的检测问题。此方法有效的原因有3点:1)从重采样插值原理出发设计预处理层,能够较好地抑制图像内容,强调蕴含重采样特征的高频信息流;2)相比方形卷积,可变形卷积能够更好地处理这种作为输入的信息流,从而更好地对特征进行提取;3)对于信息流中仍然参与运算的冗余信息,通过ECA对其进行筛选。相比现有方法,本文方法的性能有较大提升,然而当增大JPEG压缩率或是减小图像尺寸时,模型的预测准确率随之出现了一定程度的下降。因此,如何设计出针对更高压缩率和更小分辨率的重采样图像检测模型,仍是图像取证领域的一个挑战性课题。

参考文献:

- [1] REDI J A, TAKTAK W, DUGELAY J L. Digital image forensics: a booklet for beginners[J]. *Multimedia Tools and Applications*, 2011, 51(1): 133-162.
- [2] XIONG S T, ZHANG Y J, WU F, et al. Image splicing detection based on statistical noise level analysis[J]. *Journal of Optoelectronics • Laser*, 2020, 31(2): 214-221.
熊士婷, 张玉金, 吴飞, 等. 基于统计噪声水平分析的图像拼接检测[J]. *光电子 • 激光*, 2020, 31(2): 214-221.
- [3] KANG X, STAMM M C, PENG A, et al. Robust median filtering forensics using an autoregressive model[J]. *IEEE Transactions on Information Forensics and Security*, 2013, 8(9): 1456-1468.
- [4] 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.
- [5] BAYAR B, STAMM M C. Constrained convolutional neural networks: a new approach towards general purpose image manipulation detection[J]. *IEEE Transactions on Information Forensics and Security*, 2018, 13(11): 2691-2706.
- [6] POPESCU A C, FARID H. Exposing digital forgeries by detecting traces of resampling[J]. *IEEE Transactions on Signal Processing*, 2005, 53(2): 758-767.
- [7] GALLAGHER A C. Detection of linear and cubic interpolation in JPEG compressed images[C]//The 2nd Canadian Conference on Computer and Robot Vision (CRV'05), May 9-11, 2005, British Columbia, Canada. New York: IEEE, 2005: 65-72.
- [8] CHANG C C, LIN C J. LIBSVM: a library for support vector machines[J]. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 2011, 2(3): 1-27.
- [9] FENG X, COX I J, DOERR G. Normalized energy density-based forensic detection of resampled images[J]. *IEEE Transactions on Multimedia*, 2012, 14(3): 536-545.
- [10] FAN W, WANG K, CAYRE F. General-purpose image forensics using patch likelihood under image statistical models[C]//2015 IEEE International Workshop on Information Forensics and Security (WIFS), November 16-19, 2015, Rome, Italy. New York: IEEE, 2015: 1-6.
- [11] CHEN Y, KANG X, WANG Z J, et al. Densely connected convolutional neural network for multi-purpose image forensics under anti-forensic attacks[C]//Proceedings of the 6th ACM Workshop on Information Hiding and Multimedia Security, June 20-22, 2018, New York, United States. New York: Association for Computing Machinery, 2018: 91-96.
- [12] HUANG G, LIU Z, VAN DER MAATEN L, et al. Densely connected convolutional networks[C]//2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), July 21-26, 2017, Honolulu, United States. New York: IEEE, 2017: 4700-4708.
- [13] CAO G, ZHOU A, HUANG X, et al. Resampling detection of recompressed images via dual-stream convolutional neural network[J]. *Mathematical Biosciences and Engineering*, 2019, 16(5): 5022-5040.
- [14] LIANG Y, FANG Y, LUO S, et al. Image resampling detection based on convolutional neural network[C]//2019 15th International Conference on Computational Intelligence and Security (CIS), December 13-16, Macao, China. New York: IEEE, 2019: 257-261.
- [15] DING F, WU H, ZHU G, et al. Meteor: Measurable energy map toward the estimation of resampling rate via a convolutional neural network[J]. *IEEE Transactions on Circuits and Systems for Video Technology*, 2020, 30(12): 4715-4727.
- [16] LAMBA M, MITRA K. Multi-patch aggregation models for resampling detection[C]//2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), May 4-8, 2020, Barcelona, Spain. New York: IEEE, 2020: 2967-2971.
- [17] PENG L, LIAO X, CHEN M. Resampling parameter estimation via dual-filtering based convolutional neural net-

- work[J]. *Multimedia Systems*, 2021, 27(3): 363-370.
- [18] DAI J, QI H, XIONG Y, et al. Deformable convolutional networks[C]//*Proceedings of the IEEE International Conference on Computer Vision (ICCV)*, October 22-29, 2017, Venice, Italy. New York: IEEE, 2017: 764-773.
- [19] WANG Q, WU B, ZHU P, et al. ECA-Net: Efficient channel attention for deep convolutional neural networks[C]//*2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, June 13-19, 2020, Seattle, United States. New York: IEEE, 2020: 11531-11539.
- [20] DANG-NGUYEN D T, PASQUINI C, CONOTTER V, et al. RAISE: A raw images dataset for digital image forensics[C]//*Proceedings of the 6th ACM Multimedia Systems Conference*, March 18-20, 2015, New York, United States. New York: Association for Computing Machinery, 2015: 219-224.
- [21] XIE H, ZHANG J, NI J Q. A survey of digital image operation forensics[J]. *Journal of Signal Processing*, 2021, 37(12): 2323-2337.
- 谢皓, 张健, 倪江群. 数字图像操作取证综述[J]. *信号处理*, 2021, 37(12): 2323-2337.
- [22] HOLUB V, FRIDRICH J, DENEMARK T. Universal distortion function for steganography in an arbitrary domain[J]. *EURASIP Journal on Information Security*, 2014, 2014(1): 1-13.
- [23] COGRANNE R, GIBOULOT Q, BAS P. The ALASKA steganalysis challenge: A first step towards steganalysis[C]//*Proceedings of the ACM Workshop on Information Hiding and Multimedia Security*, July 3-5, 2019, New York, United States. New York: Association for Computing Machinery, 2019: 125-137.
- 作者简介:
- 张玉金 (1982—), 男, 博士, 副教授, 硕士生导师, 主要研究方向为计算机视觉、多媒体内容安全、图像处理与模式识别。