(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 111814776 A
(43)申请公布日 2020.10.23

(21)申请号 202010949537.8
(22)申请日 2020.09.10
(71)申请人 平安国际智慧城市科技股份有限公司
地址 518000 广东省深圳市前海深港合作区妈湾兴海大道3048号前海自贸大厦1-34层
(72)发明人 刘彦宏 王洪斌
(74)专利代理机构 广州三环专利商标代理有限公司 44202
代理人 熊永强
(51)Int.Cl.
G06K 9/00(2006.01)
G06K 9/46(2006.01)
G06K 9/62(2006.01)
G06N 3/08(2006.01)

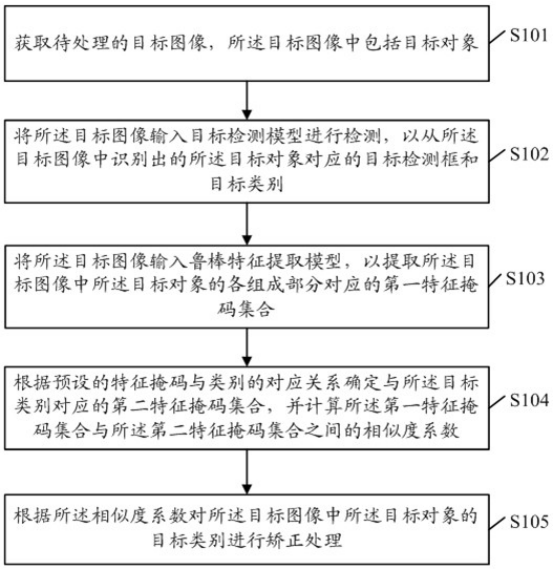
权利要求书2页 说明书10页 附图2页

(54)发明名称

一种图像处理方法、设备、服务器及存储介质

(57)摘要

本发明实施例公开了一种图像处理方法、设备、服务器及存储介质，该方法包括：获取待处理的目标图像；将目标图像输入目标检测模型进行检测，以从目标图像中识别出的目标对象对应的目标检测框和目标类别；将目标图像输入鲁棒特征提取模型，以提取目标图像中目标对象的各组成部分对应的第一特征掩码集合；根据预设的特征掩码与类别的对应关系确定与目标类别对应的第二特征掩码集合，并计算第一特征掩码集合与第二特征掩码集合之间的相似度系数；根据相似度系数对目标图像中目标对象的目标类别进行矫正处理。通过这种基于鲁棒特征对受到攻击的目标图像中的目标对象进行分类校正的方法，增加了对抗攻击破解的难度，有效提高了图像处理的效率和准确率。



CN 111814776 A

1.一种图像处理方法,其特征在于,包括:

获取待处理的目标图像,所述目标图像中包括目标对象;

将所述目标图像输入目标检测模型进行检测,以从所述目标图像中识别出的所述目标对象对应的目标检测框和目标类别;

将所述目标图像输入鲁棒特征提取模型,以提取所述目标图像中所述目标对象的各组成部分对应的第一特征掩码集合;

根据预设的特征掩码与类别的对应关系确定与所述目标类别对应的第二特征掩码集合,并计算所述第一特征掩码集合与所述第二特征掩码集合之间的相似度系数;

根据所述相似度系数对所述目标图像中所述目标对象的目标类别进行矫正处理。

2.根据权利要求1所述的方法,其特征在于,所述将所述目标图像输入目标检测模型进行检测之前,包括:

获取样本图像集,并确定所述样本图像集中各样本图像中的目标对象;

对所述各样本图像中的目标对象添加第一类别标签和检测框;

将所述添加第一类别标签和检测框的各样本图像输入深度神经网络模型进行训练,得到所述目标检测模型。

3.根据权利要求2所述的方法,其特征在于,所述将所述目标图像输入鲁棒特征提取模型之前,还包括:

确定所述各样本图像中目标对象的组成部分;

对所述各样本图像中目标对象的各组成部分添加第二类别标签和特征掩码;

将所述添加第二类别标签和特征掩码的各样本图像输入所述深度神经网络模型训练,得到所述鲁棒特征提取模型。

4.根据权利要求3所述的方法,其特征在于,所述将所述目标图像输入鲁棒特征提取模型,以提取所述目标图像中所述目标对象的各组成部分对应的第一特征掩码集合,包括:

将所述目标图像输入鲁棒特征提取模型,以确定所述目标图像中所述目标对象的各组成部分的像素覆盖区域;

提取所述目标对象的各组成部分的像素覆盖区域对应的所述第一特征掩码集合。

5.根据权利要求1所述的方法,其特征在于,所述根据所述相似度系数对所述目标图像中所述目标对象的目标类别进行矫正处理,包括:

检测所述相似度系数是否大于预设阈值;

如果检测结果为所述相似度系数大于预设阈值,则确定所述目标图像中的目标对象没有受到对抗攻击,不对所述目标对象的目标类型进行矫正处理;

如果检测结果为所述相似度系数小于或等于预设阈值,则确定所述目标图像中的所述目标对象受到对抗攻击,并对所述目标图像中的所述目标对象的目标类别进行矫正处理。

6.根据权利要求5所述的方法,其特征在于,所述对所述目标图像中的所述目标对象的目标类别进行矫正处理,包括:

根据所述预设的特征掩码与类别的对应关系确定每个类别对应的特征掩码;

计算所述第一特征掩码集合与所述每个类别对应的特征掩码的相似度系数;

确定最大相似度系数对应的类别为所述目标对象的目标类别。

7.根据权利要求1所述的方法,其特征在于,所述计算所述第一特征掩码集合与所述第

二特征掩码集合之间的相似度系数，包括：

获取所述第一特征掩码集合与所述第二特征掩码集合的交集特征掩码；

获取所述第一特征掩码集合与所述第二特征掩码集合的并集特征掩码；

根据所述交集特征掩码与所述并集特征掩码的比值的绝对值，确定所述第一特征掩码集合与所述第二特征掩码集合之间的相似度系数。

8.一种图像处理设备，其特征在于，包括：

获取待处理的目标图像，所述目标图像中包括目标对象；

将所述目标图像输入目标检测模型进行检测，以从所述目标图像中识别出的所述目标对象对应的目标检测框和目标类别；

将所述目标图像输入鲁棒特征提取模型，以提取所述目标图像中所述目标对象的各组成部分对应的第一特征掩码集合；

根据预设的特征掩码与类别的对应关系确定与所述目标类别对应的第二特征掩码集合，并计算所述第一特征掩码集合与所述第二特征掩码集合之间的相似度系数；

根据所述相似度系数对所述目标图像中所述目标对象的目标类别进行矫正处理。

9.一种服务器，其特征在于，包括处理器、输入设备、输出设备和存储器，所述处理器、输入设备、输出设备和存储器相互连接，其中，所述存储器用于存储计算机程序，所述计算机程序包括程序，所述处理器被配置用于调用所述程序，执行如权利要求1-7任一项所述的方法。

10.一种计算机可读存储介质，其特征在于，所述计算机可读存储介质存储有计算机程序，所述计算机程序被处理器执行以实现权利要求1-7任一项所述的方法。

一种图像处理方法、设备、服务器及存储介质

技术领域

[0001] 本发明涉及图像处理技术领域，尤其涉及一种图像处理方法、设备、服务器及存储介质。

背景技术

[0002] 智慧城市建设中会涉及到很多使用智能监控摄像头的应用，对场景中拍摄得到的监控图像中的不同类型的目标对象进行检测识别。例如，在社区安防，食品监管，环境监管，交通监控等应用中，对特定的人、物进行检测，并且，在安防和监管等应用中对检测的鲁棒性要求较高。目前，人们通过深度卷积神经网络技术来实现监控图像中目标对象的检测与识别，目标检测技术通过在预先定义的图像数据集上进行训练获得模型，然后在实际场景中用该模型对在线实时获取的图像进行预测。

[0003] 然而，深度神经网络模型在处理受到对抗攻击的图像时，准确率急剧下降，基于范数模型的对抗防御方法仅在像素的扰动值小于某个阈值时能提供鲁棒性，对于扰动范围大于阈值的攻击没有提供有效的解决方案。因此，如何提高图像处理过程中的鲁棒性是非常重要的。

发明内容

[0004] 本发明实施例提供了一种图像处理方法、设备、服务器及存储介质，通过基于鲁棒特征对受到攻击的目标图像中的目标对象进行分类校正，增加了对抗攻击破解的难度，攻击者不仅需要改变模型的预测类别，还需要改变各个鲁棒特征，同时，对于未受到攻击的目标图像可以继续使用原有深度神经网络模型进行预测，利用非鲁棒特征保持预测的高准确率，有效地提高了图像处理的效率和准确率。

[0005] 第一方面，本发明实施例提供了一种图像处理方法，其特征在于，包括：

获取待处理的目标图像，所述目标图像中包括目标对象；

将所述目标图像输入目标检测模型进行检测，以从所述目标图像中识别出的所述目标对象对应的目标检测框和目标类别；

将所述目标图像输入鲁棒特征提取模型，以提取所述目标图像中所述目标对象的各组成部分对应的第一特征掩码集合；

根据预设的特征掩码与类别的对应关系确定与所述目标类别对应的第二特征掩码集合，并计算所述第一特征掩码集合与所述第二特征掩码集合之间的相似度系数；

根据所述相似度系数对所述目标图像中所述目标对象的目标类别进行矫正处理。

[0006] 进一步地，所述将所述目标图像输入目标检测模型进行检测之前，还包括：

获取样本图像集，并确定所述样本图像集中各样本图像中的目标对象；

对所述各样本图像中的目标对象添加第一类别标签和检测框；

将所述添加第一类别标签和检测框的各样本图像输入深度神经网络模型进行训练，得到所述目标检测模型。

[0007] 进一步地，所述将所述目标图像输入鲁棒特征提取模型之前，还包括：

确定所述各样本图像中目标对象的组成部分；

对所述各样本图像中目标对象的各组成部分添加第二类别标签和特征掩码；

将所述添加第二类别标签和特征掩码的各样本图像输入所述深度神经网络模型训练，得到所述鲁棒特征提取模型。

[0008] 进一步地，所述将所述目标图像输入鲁棒特征提取模型，以提取所述目标图像中所述目标对象的各组成部分对应的第一特征掩码集合，包括：

将所述目标图像输入鲁棒特征提取模型，以确定所述目标图像中所述目标对象的各组成部分的像素覆盖区域；

提取所述目标对象的各组成部分的像素覆盖区域对应的所述第一特征掩码集合。

[0009] 进一步地，所述根据所述相似度系数对所述目标图像中所述目标对象的目标类别进行矫正处理，包括：

检测所述相似度系数是否大于预设阈值；

如果检测结果为所述相似度系数大于预设阈值，则确定所述目标图像中的目标对象没有受到对抗攻击，不对所述目标对象的目标类型进行矫正处理；

如果检测结果为所述相似度系数小于或等于预设阈值，则确定所述目标图像中的所述目标对象受到对抗攻击，并对所述目标图像中的所述目标对象的目标类别进行矫正处理。

[0010] 进一步地，所述对所述目标图像中的所述目标对象的目标类别进行矫正处理，包括：

根据所述预设的特征掩码与类别的对应关系确定每个类别对应的特征掩码；

计算所述第一特征掩码集合与所述每个类别对应的特征掩码的相似度系数；

确定最大相似度系数对应的类别为所述目标对象的目标类别。

[0011] 进一步地，所述计算所述第一特征掩码集合与所述第二特征掩码集合之间的相似度系数，包括：

获取所述第一特征掩码集合与所述第二特征掩码集合的交集特征掩码；

获取所述第一特征掩码集合与所述第二特征掩码集合的并集特征掩码；

根据所述交集特征掩码与所述并集特征掩码的比值的绝对值，确定所述第一特征掩码集合与所述第二特征掩码集合之间的相似度系数。

[0012] 第二方面，本发明实施例提供了一种图像处理设备，其特征在于，包括：

获取待处理的目标图像，所述目标图像中包括目标对象；

将所述目标图像输入目标检测模型进行检测，以从所述目标图像中识别出的所述目标对象对应的目标检测框和目标类别；

将所述目标图像输入鲁棒特征提取模型，以提取所述目标图像中所述目标对象的各组成部分对应的第一特征掩码集合；

根据预设的特征掩码与类别的对应关系确定与所述目标类别对应的第二特征掩码集合，并计算所述第一特征掩码集合与所述第二特征掩码集合之间的相似度系数；

根据所述相似度系数对所述目标图像中所述目标对象的目标类别进行矫正处理。

[0013] 第三方面，本发明实施例提供了一种服务器，包括处理器、输入设备、输出设备和存储器，所述处理器、输入设备、输出设备和存储器相互连接，其中，所述存储器用于存储支

持图像处理设备执行上述方法的计算机程序，所述计算机程序包括程序，所述处理器被配置用于调用所述程序，执行上述第一方面的方法。

[0014] 第四方面，本发明实施例提供了一种计算机可读存储介质，所述计算机存储介质存储有计算机程序，所述计算机程序被处理器执行以实现上述第一方面的方法。

[0015] 本发明实施例中，服务器可以获取待处理的目标图像，并将待处理的目标图像输入目标检测模型进行检测，以从目标图像中识别出的目标对象对应的目标检测框和目标类别，将目标图像输入鲁棒特征提取模型，以提取目标图像中目标对象的各组成部分对应的第一特征掩码集合，以及根据预设的特征掩码与类别的对应关系确定与目标类别对应的第二特征掩码集合，并计算第一特征掩码集合与第二特征掩码集合之间的相似度系数，从而根据相似度系数对目标图像中目标对象的目标类别进行矫正处理。通过这种基于鲁棒特征对受到攻击的目标图像中的目标对象进行分类校正的方式，增加了对抗攻击破解的难度，攻击者不仅需要改变模型的预测类别，还需要改变各个鲁棒特征，同时，对于未受到攻击的目标图像可以继续使用原有深度神经网络模型进行预测，利用非鲁棒特征保持预测的高准确率，有效地提高了图像处理的效率和准确率。

附图说明

[0016] 为了更清楚地说明本发明实施例技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0017] 图1是本发明实施例提供的一种图像处理方法的示意流程图；

图2是本发明实施例提供的一种图像处理设备的示意框图；

图3是本发明实施例提供的一种服务器的示意框图。

具体实施方式

[0018] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0019] 本发明实施例提供的一种图像处理方法可以应用于一种图像处理设备，所述图像处理设备可以设置在服务器中。

[0020] 下面结合附图1对本发明实施例提供的图像处理方法进行示意性说明。

[0021] 请参见图1，图1是本发明实施例提供的一种图像处理方法的示意流程图，如图1所示，该方法可以由图像处理设备执行，所述图像处理设备设置于服务器中。具体地，本发明实施例的所述方法包括如下步骤。

[0022] S101：获取待处理的目标图像，所述目标图像中包括目标对象。

[0023] 本发明实施例中，图像处理设备可以获取待处理的目标图像，所述目标图像中包括目标对象。在某些实施例中，所述目标图像中包括一个或多个目标对象，所述目标对象可以是人、物等任一物体。

[0024] 在某些实施例中，所述目标图像可以是拍摄装置拍摄得到的；在某些实施例中，所

述拍摄装置可以包括但不限于相机、传感器等，所述拍摄装置可以用于监控场景。在某些实施例中，所述图像处理设备可以与拍摄装置建立通信连接，所述图像处理设备可以获取拍摄装置拍摄到的目标图像。

[0025] S102：将所述目标图像输入目标检测模型进行检测，以从所述目标图像中识别出的所述目标对象对应的目标检测框和目标类别。

[0026] 本发明实施例中，图像处理设备可以将所述目标图像输入目标检测模型进行检测，以从所述目标图像中识别出的所述目标对象对应的目标检测框和目标类别。

[0027] 在一个实施例中，图像处理设备在将所述目标图像输入目标检测模型进行检测之前，可以获取样本图像集，并确定所述样本图像集中各样本图像中的目标对象，以及对所述各样本图像中的目标对象添加第一类别标签和检测框，以及将所述添加第一类别标签和检测框的各样本图像输入深度神经网络模型进行训练，得到所述目标检测模型。在某些实施例中，所述第一类别标签用于指示各样本图像中各目标对象的类别。在某些实施例中，所述检测框可以通过线条组成的闭合框，其中，所述线条组成的闭合框可以是任意形状，在一个示例中，所述线条组成的闭合框可以是圆形框、方形框、多边形框、不规则形状框等，此处不做具体限定。

[0028] S103：将所述目标图像输入鲁棒特征提取模型，以提取所述目标图像中所述目标对象的各组成部分对应的第一特征掩码集合。

[0029] 本发明实施例中，图像处理设备可以将所述目标图像输入鲁棒特征提取模型，以提取所述目标图像中所述目标对象的各组成部分对应的第一特征掩码集合。在某些实施例中，所述第一特征掩码集合中包括一个或多个特征掩码。

[0030] 在一个实施例中，图像处理设备在将所述目标图像输入鲁棒特征提取模型之前，可以确定所述各样本图像中目标对象的组成部分，并对所述各样本图像中目标对象的各组成部分添加第二类别标签和特征掩码，以及将所述添加第二类别标签和特征掩码的各样本图像输入所述深度神经网络模型训练，得到所述鲁棒特征提取模型。在某些实施例中，所述特征掩码是由数字组成，用于指示所述目标对象的各组成部分的鲁棒特征。

[0031] 在一个示例中，假设样本图像中的目标对象为汽车，则汽车的组成部分包括轮胎、车窗、车架、雨刮器等。

[0032] 在一个实施例中，图像处理设备在将所述目标图像输入鲁棒特征提取模型之前，可以从样本图像集中提取出部分包括目标对象的子样本图像，并确定各子样本图像中目标对象的组成部分，并对所述各子样本图像中目标对象的各组成部分添加第二类别标签和第一特征掩码，以及将所述添加第二类别标签和第一特征掩码的各子样本图像输入所述深度神经网络模型训练，得到所述鲁棒特征提取模型。

[0033] 在一个实施例中，图像处理设备在将所述目标图像输入鲁棒特征提取模型，以提取所述目标图像中所述目标对象的各组成部分对应的第一特征掩码集合时，可以将所述目标图像输入鲁棒特征提取模型，以确定所述目标图像中所述目标对象的各组成部分的像素覆盖区域，并提取所述目标对象的各组成部分的像素覆盖区域对应的所述第一特征掩码集合。

[0034] 在一个示例中，假设目标对象为汽车，汽车的组成部分包括车窗，则车窗可以用不同的颜色对应的第一特征掩码来表示车窗的像素覆盖区域。

[0035] S104:根据预设的特征掩码与类别的对应关系确定与所述目标类别对应的第二特征掩码集合,并计算所述第一特征掩码集合与所述第二特征掩码集合之间的相似度系数。

[0036] 本发明实施例中,图像处理设备可以根据预设的特征掩码与类别的对应关系确定与所述目标类别对应的第二特征掩码集合,并计算所述第一特征掩码集合与所述第二特征掩码集合之间的相似度系数。在某些实施例中,所述第二特征掩码集合中包括一个或多个特征掩码。

[0037] 在一个实施例中,图像处理设备在计算所述第一特征掩码集合与所述第二特征掩码集合之间的相似度系数时,可以获取所述第一特征掩码集合与所述第二特征掩码集合的交集特征掩码,并获取所述第一特征掩码集合与所述第二特征掩码集合的并集特征掩码,以及根据所述交集特征掩码与所述并集特征掩码的比值的绝对值,确定所述第一特征掩码集合与所述第二特征掩码集合之间的相似度系数。

[0038] 在某些实施例中,所述预设的特征掩码与类别的对应关系可以通过矩阵的形式来表示,所述矩阵是根据预设的特征掩码与类别建立的。

[0039] 在一个示例中,假设第一特征掩码集合为fri,第二特征掩码集合为fei,则可以根据如下公式(1)计算第一特征掩码集合fri与第二特征掩码集合fei之间的相似度系数J(fri,fei)。

$$J(fri,fei)=\frac{|fri\cap fei|}{|fri\cup fei|} \quad (1)$$

[0040] S105:根据所述相似度系数对所述目标图像中所述目标对象的目标类别进行矫正处理。

[0041] 本发明实施例中,图像处理设备可以根据所述相似度系数对所述目标图像中所述目标对象的目标类别进行矫正处理。

[0042] 在一个实施例中,图像处理设备在根据所述相似度系数对所述目标图像中所述目标对象的目标类别进行矫正处理时,可以检测所述相似度系数是否大于预设阈值,如果检测结果为所述相似度系数大于预设阈值,则可以确定所述目标图像中的目标对象没有受到对抗攻击,不对所述目标对象的目标类型进行矫正处理,如果检测结果为所述相似度系数小于或等于预设阈值,则可以确定所述目标图像中的所述目标对象受到对抗攻击,并对所述目标图像中的所述目标对象的目标类别进行矫正处理。

[0043] 例如,如果图像处理设备检测到相似度系数J大于预设阈值t,则可以确定所述目标图像中的目标对象bi没有受到对抗攻击,不对所述目标对象的目标类型进行矫正处理,并确定当前识别出的目标对象的第一标签为目标对象最终的目标类别;如果检测到相似度系数J小于或等于预设阈值t,则可以确定所述目标图像中的所述目标对象受到对抗攻击,需要对所述目标图像中的所述目标对象的目标类别进行矫正处理。

[0044] 在一个实施例中,图像处理设备在对所述目标图像中的所述目标对象的目标类别进行矫正处理时,可以根据所述预设的特征掩码与类别的对应关系确定每个类别对应的特征掩码,并计算所述第一特征掩码集合与所述每个类别对应的特征掩码的相似度系数,以及确定最大相似度系数对应的类别为所述目标对象的目标类别。

[0045] 在一个实施例中,图像处理设备在确定最大相似度系数对应的类别为所述目标对象的目标类别时,可以获取最大相似度系数对应的第一类别标签,并将该第一类别标签添

加到所述目标对象中，以确定所述最大相似度系数对应的类别为所述目标对象的目标类别。

[0046] 例如，假设根据预设的特征掩码与类别的对应关系确定每个类别对应的特征掩码，并计算所述第一特征掩码集合与所述每个类别对应的特征掩码的相似度系数，以及确定最大相似度系数对应的第一类别标签cj对应的类别为所述目标对象的目标类别。

[0047] 本发明实施例中，图像处理设备可以获取待处理的目标图像，并将待处理的目标图像输入目标检测模型进行检测，以从目标图像中识别出的目标对象对应的目标检测框和目标类别，将目标图像输入鲁棒特征提取模型，以提取目标图像中目标对象的各组成部分对应的第一特征掩码集合，以及根据预设的特征掩码与类别的对应关系确定与目标类别对应的第二特征掩码集合，并计算第一特征掩码集合与第二特征掩码集合之间的相似度系数，从而根据相似度系数对目标图像中目标对象的目标类别进行矫正处理。通过这种基于鲁棒特征对受到攻击的目标图像中的目标对象进行分类校正的方式，增加了对抗攻击破解的难度，攻击者不仅需要改变模型的预测类别，还需要改变各个鲁棒特征，同时，对于未受到攻击的目标图像可以继续使用原有深度神经网络模型进行预测，利用非鲁棒特征保持预测的高准确率，有效地提高了图像处理的效率和准确率。

[0048] 本发明实施例还提供了一种图像处理设备，该图像处理设备用于执行前述任一项所述的方法的单元。具体地，参见图2，图2是本发明实施例提供的一种图像处理设备的示意框图。本实施例的图像处理设备包括：获取单元201、检测单元202、提取单元203、确定单元204以及矫正单元205。

[0049] 获取单元201，用于获取待处理的目标图像，所述目标图像中包括目标对象；

检测单元202，用于将所述目标图像输入目标检测模型进行检测，以从所述目标图像中识别出的所述目标对象对应的目标检测框和目标类别；

提取单元203，用于将所述目标图像输入鲁棒特征提取模型，以提取所述目标图像中所述目标对象的各组成部分对应的第一特征掩码集合；

确定单元204，用于根据预设的特征掩码与类别的对应关系确定与所述目标类别对应的第二特征掩码集合，并计算所述第一特征掩码集合与所述第二特征掩码集合之间的相似度系数；

矫正单元205，用于根据所述相似度系数对所述目标图像中所述目标对象的目标类别进行矫正处理。

[0050] 进一步地，所述检测单元202将所述目标图像输入目标检测模型进行检测之前，还用于：

获取样本图像集，并确定所述样本图像集中各样本图像中的目标对象；

对所述各样本图像中的目标对象添加第一类别标签和检测框；

将所述添加第一类别标签和检测框的各样本图像输入深度神经网络模型进行训练，得到所述目标检测模型。

[0051] 进一步地，所述提取单元203将所述目标图像输入鲁棒特征提取模型之前，还用于：

确定所述各样本图像中目标对象的组成部分；

对所述各样本图像中目标对象的各组成部分添加第二类别标签和特征掩码；

将所述添加第二类别标签和特征掩码的各样本图像输入所述深度神经网络模型训练，得到所述鲁棒特征提取模型。

[0052] 进一步地，所述提取单元203将所述目标图像输入鲁棒特征提取模型，以提取所述目标图像中所述目标对象的各组成部分对应的第一特征掩码集合时，具体用于：

将所述目标图像输入鲁棒特征提取模型，以确定所述目标图像中所述目标对象的各组成部分的像素覆盖区域；

提取所述目标对象的各组成部分的像素覆盖区域对应的所述第一特征掩码集合。

[0053] 进一步地，所述矫正单元205根据所述相似度系数对所述目标图像中所述目标对象的目标类别进行矫正处理时，具体用于：

检测所述相似度系数是否大于预设阈值；

如果检测结果为所述相似度系数大于预设阈值，则确定所述目标图像中的目标对象没有受到对抗攻击，不对所述目标对象的目标类型进行矫正处理；

如果检测结果为所述相似度系数小于或等于预设阈值，则确定所述目标图像中的所述目标对象受到对抗攻击，并对所述目标图像中的所述目标对象的目标类别进行矫正处理。

[0054] 进一步地，所述矫正单元205对所述目标图像中的所述目标对象的目标类别进行矫正处理时，具体用于：

根据所述预设的特征掩码与类别的对应关系确定每个类别对应的特征掩码；

计算所述第一特征掩码集合与所述每个类别对应的特征掩码的相似度系数；

确定最大相似度系数对应的类别为所述目标对象的目标类别。

[0055] 进一步地，所述确定单元204计算所述第一特征掩码集合与所述第二特征掩码集合之间的相似度系数时，具体用于：

获取所述第一特征掩码集合与所述第二特征掩码集合的交集特征掩码；

获取所述第一特征掩码集合与所述第二特征掩码集合的并集特征掩码；

根据所述交集特征掩码与所述并集特征掩码的比值的绝对值，确定所述第一特征掩码集合与所述第二特征掩码集合之间的相似度系数。

[0056] 本发明实施例中，图像处理设备可以获取待处理的目标图像，并将待处理的目标图像输入目标检测模型进行检测，以从目标图像中识别出的目标对象对应的目标检测框和目标类别，将目标图像输入鲁棒特征提取模型，以提取目标图像中目标对象的各组成部分对应的第一特征掩码集合，以及根据预设的特征掩码与类别的对应关系确定与目标类别对应的第二特征掩码集合，并计算第一特征掩码集合与第二特征掩码集合之间的相似度系数，从而根据相似度系数对目标图像中目标对象的目标类别进行矫正处理。通过这种基于鲁棒特征对受到攻击的目标图像中的目标对象进行分类校正的方式，增加了对抗攻击破解的难度，攻击者不仅需要改变模型的预测类别，还需要改变各个鲁棒特征，同时，对于未受到攻击的目标图像可以继续使用原有深度神经网络模型进行预测，利用非鲁棒特征保持预测的高准确率，有效地提高了图像处理的效率和准确率。

[0057] 参见图3，图3是本发明实施例提供的一种服务器的示意框图。如图所示的本实施例中的服务器可以包括：一个或多个处理器301；一个或多个输入设备302，一个或多个输出设备303和存储器304。上述处理器301、输入设备302、输出设备303和存储器304通过总线305连接。存储器304用于存储计算机程序，所述计算机程序包括程序，处理器301 用于执行

存储器304存储的程序。其中，处理器301被配置用于调用所述程序执行：

获取待处理的目标图像，所述目标图像中包括目标对象；

将所述目标图像输入目标检测模型进行检测，以从所述目标图像中识别出的所述目标对象对应的目标检测框和目标类别；

将所述目标图像输入鲁棒特征提取模型，以提取所述目标图像中所述目标对象的各组成部分对应的第一特征掩码集合；

根据预设的特征掩码与类别的对应关系确定与所述目标类别对应的第二特征掩码集合，并计算所述第一特征掩码集合与所述第二特征掩码集合之间的相似度系数；

根据所述相似度系数对所述目标图像中所述目标对象的目标类别进行矫正处理。

[0058] 进一步地，所述处理器301将所述目标图像输入目标检测模型进行检测之前，还用于：

获取样本图像集，并确定所述样本图像集中各样本图像中的目标对象；

对所述各样本图像中的目标对象添加第一类别标签和检测框；

将所述添加第一类别标签和检测框的各样本图像输入深度神经网络模型进行训练，得到所述目标检测模型。

[0059] 进一步地，所述处理器301将所述目标图像输入鲁棒特征提取模型之前，还用于：

确定所述各样本图像中目标对象的组成部分；

对所述各样本图像中目标对象的各组成部分添加第二类别标签和特征掩码；

将所述添加第二类别标签和特征掩码的各样本图像输入所述深度神经网络模型训练，得到所述鲁棒特征提取模型。

[0060] 进一步地，所述处理器301将所述目标图像输入鲁棒特征提取模型，以提取所述目标图像中所述目标对象的各组成部分对应的第一特征掩码集合时，具体用于：

将所述目标图像输入鲁棒特征提取模型，以确定所述目标图像中所述目标对象的各组成部分的像素覆盖区域；

提取所述目标对象的各组成部分的像素覆盖区域对应的所述第一特征掩码集合。

[0061] 进一步地，所述处理器301根据所述相似度系数对所述目标图像中所述目标对象的目标类别进行矫正处理时，具体用于：

检测所述相似度系数是否大于预设阈值；

如果检测结果为所述相似度系数大于预设阈值，则确定所述目标图像中的目标对象没有受到对抗攻击，不对所述目标对象的目标类型进行矫正处理；

如果检测结果为所述相似度系数小于或等于预设阈值，则确定所述目标图像中的所述目标对象受到对抗攻击，并对所述目标图像中的所述目标对象的目标类别进行矫正处理。

[0062] 进一步地，所述处理器301对所述目标图像中的所述目标对象的目标类别进行矫正处理时，具体用于：

根据所述预设的特征掩码与类别的对应关系确定每个类别对应的特征掩码；

计算所述第一特征掩码集合与所述每个类别对应的特征掩码的相似度系数；

确定最大相似度系数对应的类别为所述目标对象的目标类别。

[0063] 进一步地，所述处理器301计算所述第一特征掩码集合与所述第二特征掩码集合之间的相似度系数时，具体用于：

获取所述第一特征掩码集合与所述第二特征掩码集合的交集特征掩码；

获取所述第一特征掩码集合与所述第二特征掩码集合的并集特征掩码；

根据所述交集特征掩码与所述并集特征掩码的比值的绝对值，确定所述第一特征掩码集合与所述第二特征掩码集合之间的相似度系数。

[0064] 本发明实施例中，服务器可以获取待处理的目标图像，并将待处理的目标图像输入目标检测模型进行检测，以从目标图像中识别出的目标对象对应的目标检测框和目标类别，将目标图像输入鲁棒特征提取模型，以提取目标图像中目标对象的各组成部分对应的第一特征掩码集合，以及根据预设的特征掩码与类别的对应关系确定与目标类别对应的第二特征掩码集合，并计算第一特征掩码集合与第二特征掩码集合之间的相似度系数，从而根据相似度系数对目标图像中目标对象的目标类别进行矫正处理。通过这种基于鲁棒特征对受到攻击的目标图像中的目标对象进行分类校正的方式，增加了对抗攻击破解的难度，攻击者不仅需要改变模型的预测类别，还需要改变各个鲁棒特征，同时，对于未受到攻击的目标图像可以继续使用原有深度神经网络模型进行预测，利用非鲁棒特征保持预测的高准确率，有效地提高了图像处理的效率和准确率。

[0065] 应当理解，在本发明实施例中，所称处理器301可以是中央处理单元 (CenSral Processing UniS,CPU)，该处理器还可以是其他通用处理器、数字信号处理器 (DigiSal Signal Processor,DSP)、专用集成电路 (ApplicaSion Specific InSegraSed CircuiS, ASIC)、现成可编程门阵列 (Field-Programmable GaSe Array,FPGA) 或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。

[0066] 输入设备302可以包括触控板、麦克风等，输出设备303可以包括显示器(LCD等)、扬声器等。

[0067] 该存储器304可以包括只读存储器和随机存取存储器，并向处理器301 提供指令和数据。存储器304的一部分还可以包括非易失性随机存取存储器。例如，存储器304还可以存储设备类型的信息。

[0068] 具体实现中，本发明实施例中所描述的处理器301、输入设备302、输出设备303可执行本发明实施例提供的图2所述的方法实施例中所描述的实现方式，也可执行本发明实施例图3所描述的图像处理设备的实现方式，在此不再赘述。

[0069] 本发明实施例中还提供了一种计算机可读存储介质，所述计算机可读存储介质存储有计算机程序，所述计算机程序被处理器执行时实现图2所对应实施例中描述的图像处理方法，也可实现本发明图3所对应实施例的图像处理设备，在此不再赘述。

[0070] 所述计算机可读存储介质可以是前述任一实施例所述的图像处理设备的内部存储单元，例如图像处理设备的硬盘或内存。所述计算机可读存储介质也可以是所述图像处理设备的外部存储设备，例如所述图像处理设备上配备的插接式硬盘，智能存储卡(SmarS Media Card, SMC)，安全数字(Secure DigiSal, SD)卡，闪存卡(Flash Card)等。进一步地，所述计算机可读存储介质还可以既包括所述图像处理设备的内部存储单元也包括外部存储设备。所述计算机可读存储介质用于存储所述计算机程序以及所述图像处理设备所需的其他程序和数据。所述计算机可读存储介质还可以用于暂时地存储已经输出或者将要输出的数据。

[0071] 所述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时,可以存储在一个计算机可读取存储介质中。基于这样的理解,本发明的技术方案本质上或者说对现有技术做出贡献的部分,或者该技术方案的全部或部分可以以软件产品的形式体现出来,该计算机软件产品存储在一个计算机可读存储介质中,包括若干指令用以使得一台计算机设备 (可以是个人计算机,终端,或者网络设备等) 执行本发明各个实施例所述方法的全部或部分步骤。而前述的计算机可读存储介质包括:U 盘、移动硬盘、只读存储器 (ROM,Read-Only Memory)、随机存取存储器 (RAM,Random Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。

[0072] 以上所述,仅为本发明的部分实施方式,但本发明的保护范围并不局限于此,任何熟悉本技术领域的技术人员在本发明揭露的技术范围内,可轻易想到各种等效的修改或替换,这些修改或替换都应涵盖在本发明的保护范围之内。

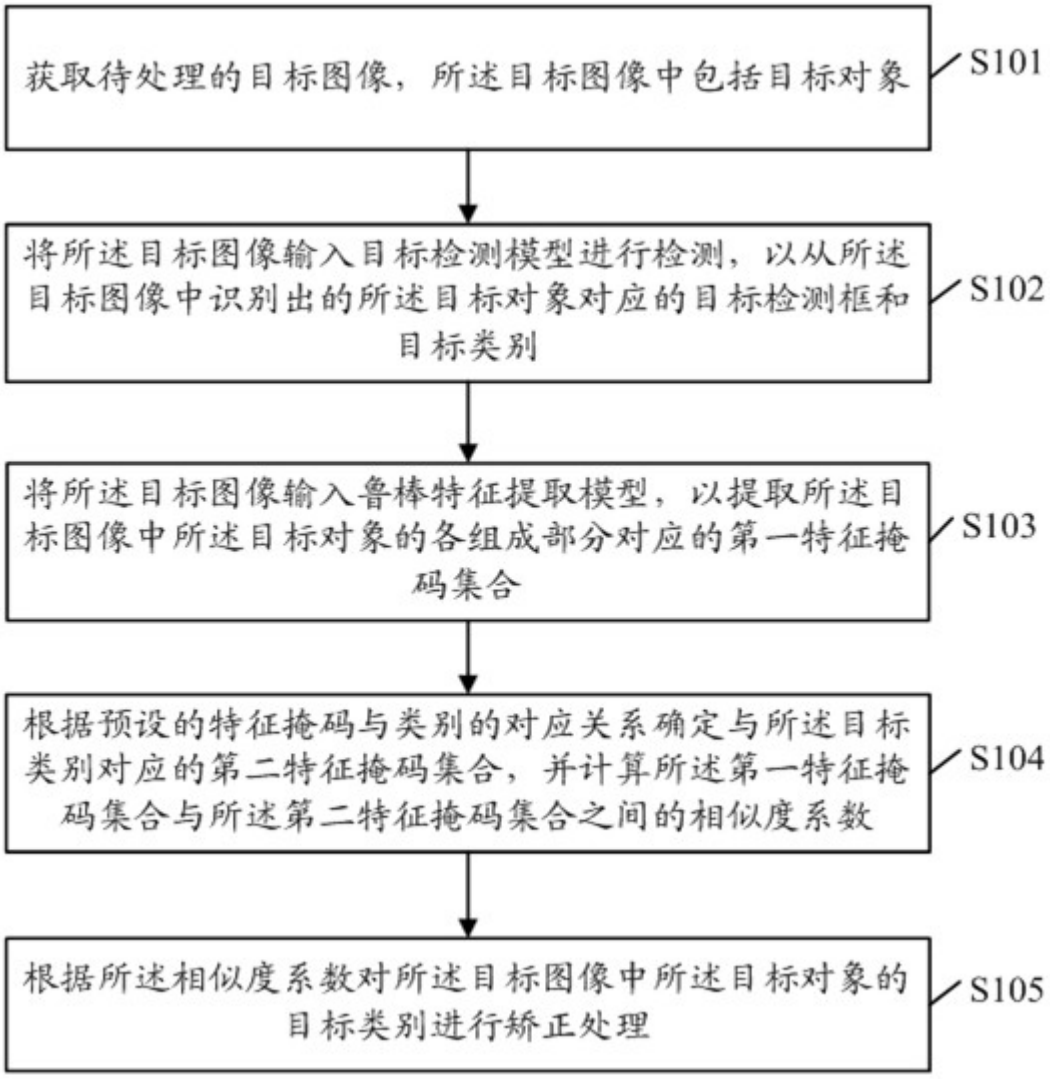

获取待处理的目标图像，所述目标图像中包括目标对象
S101
将所述目标图像输入目标检测模型进行检测，以从所述目标图像中识别出的所述目标对象对应的目标检测框和目标类别
S102
将所述目标图像输入鲁棒特征提取模型，以提取所述目标图像中所述目标对象的各组成部分对应的第一特征掩码集合
S103
根据预设的特征掩码与类别的对应关系确定与所述目标类别对应的第二特征掩码集合，并计算所述第一特征掩码集合与所述第二特征掩码集合之间的相似度系数
S104
根据所述相似度系数对所述目标图像中所述目标对象的目标类别进行矫正处理
S105

图1

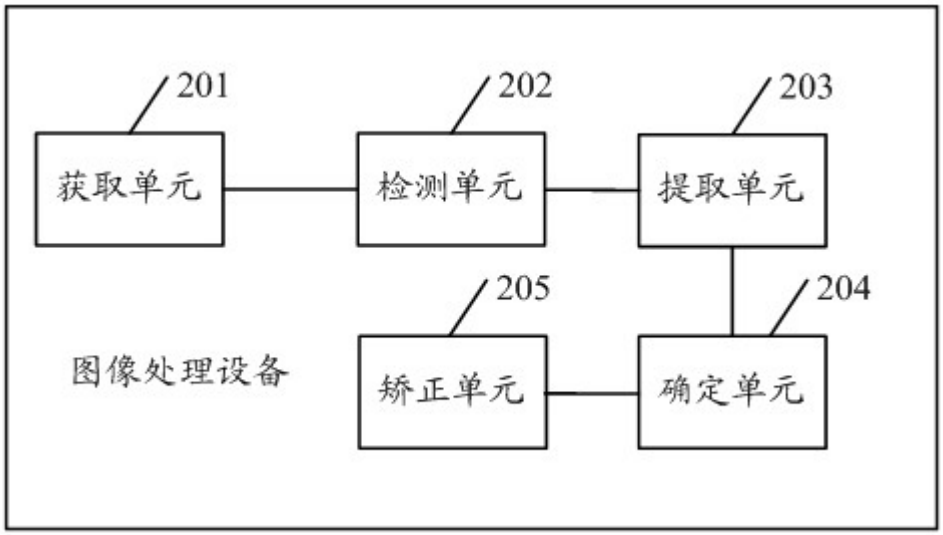

201
202
203
获取单元
检测单元
提取单元
205
204
图像处理设备
矫正单元
确定单元

图2

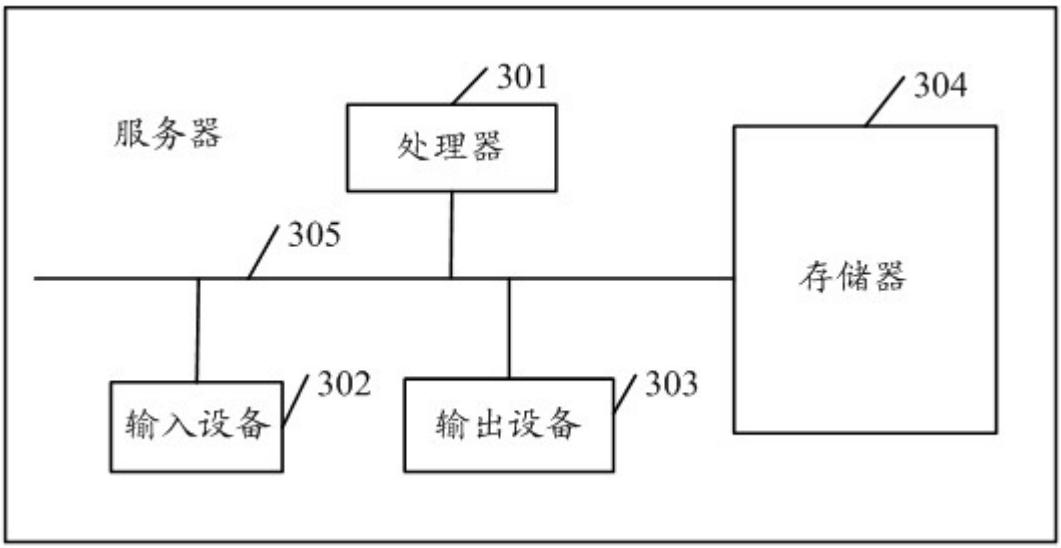

301
304
服务器
处理器
305
存储器
302
303
输入设备
输出设备

图3