(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 110473135 A
(43)申请公布日 2019.11.19

(21)申请号 201910701385.7

(22)申请日 2019.07.31

(71)申请人 哈尔滨工业大学(深圳)
地址 518055 广东省深圳市南山区桃源街道深圳大学城哈尔滨工业大学校区

(72)发明人 廖清 丁烨

(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 颜希文 麦小婵

(51)Int.Cl.
G06T 1/00(2006.01)

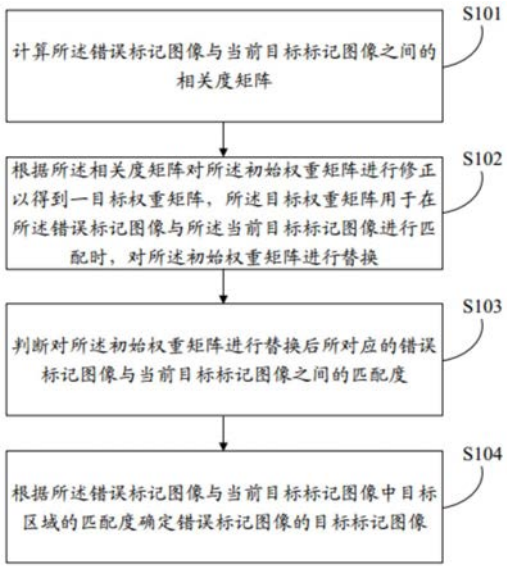
权利要求书2页 说明书9页 附图2页

(54)发明名称

图像处理方法、系统、可读存储介质及智能设备

(57)摘要

本发明公开了一种图像处理方法、系统、可读存储介质及智能设备，所述方法包括：获取一目标标记图像，通过对抗生成网络模型对所述目标标记图像进行干扰，以得到至少一干扰图像；通过收敛模型对所述干扰图像进行收敛，将收敛合格的干扰图像作为对抗样本，并将所述对抗样本覆盖于目标标记图像上；对进行对抗样本覆盖的目标标记图像进行图像识别，以得到错误标记图像，每个用户所得到的错误标记图片均不相同；根据所述错误标记图像与当前目标标记图像中目标区域的匹配度确定错误标记图像的目标标记图像。本发明能够解决现有水印易被识别和易被干扰这的问题，提高了用户图像隐私体验的满意度，满足了实际应用需求。



CN 110473135 A

1.一种图像处理方法,其特征在于,所述方法包括如下步骤:

获取一目标标记图像,通过对抗生成网络模型对所述目标标记图像进行干扰,以得到至少一干扰图像;

通过收敛模型对所述干扰图像进行收敛,将收敛合格的干扰图像作为对抗样本,并将所述对抗样本覆盖于目标标记图像上;

对进行对抗样本覆盖的目标标记图像进行图像识别,以得到错误标记图像,每个用户所得到的错误标记图片均不相同;

根据所述错误标记图像与当前目标标记图像中目标区域的匹配度确定错误标记图像的目标标记图像。

2.根据权利要求1所述的图像处理方法,其特征在于,获取一目标标记图像,通过对抗生成网络模型对所述目标标记图像进行干扰,以得到至少一干扰图像的步骤包括:

获取原图像的图像信息,并根据所述图像信息对原图像进行离散化处理,从而将该原图像划分为若干可识别区域;

通过图像识别模型对所述原图像的若干可识别区域进行标记,以得到所述目标标记图像,该目标标记图像携带有可识别区域的正确标签;

通过对抗生成网络模型对所述目标标记图像进干扰,以得到对应的干扰图像,该干扰图像携带有可识别区域的错误标签。

3.根据权利要求2所述的图像处理方法,其特征在于,通过图像识别模型对所述原图像的若干可识别区域进行标记,以得到所述目标标记图像的步骤包括:

对所述原图像的若干可识别区域进行抽取与分解形成标记因子;

根据所述标记因子进行机器算法学习后得可识别区域的正确标签。

4.根据权利要求3所述的图像处理方法,其特征在于,根据所述标记因子进行机器算法学习后得可识别区域的正确标签的计算公式为:

$$Y_n = \phi() = V_k \times (\sum_{i=1}^{n} W_i \times X_i + B_k)$$

其中,Φ()为激活函数,V_k为调节系数,W_i为初始权重,X_i为标记因子,B_k为偏移累加量。

5.根据权利要求1所述的图像处理方法,其特征在于,所述错误标记图像对应有一初始权重矩阵,根据所述错误标记图像与当前目标标记图像中目标区域的匹配度确定错误标记图像的目标标记图像的步骤包括:

计算所述错误标记图像与当前目标标记图像之间的相关度矩阵;

根据所述相关度矩阵对所述初始权重矩阵进行修正以得到一目标权重矩阵,所述目标权重矩阵用于在所述错误标记图像与所述当前目标标记图像进行匹配时,对所述初始权重矩阵进行替换;

判断对所述初始权重矩阵进行替换后所对应的错误标记图像与当前目标标记图像之间的匹配度;

当所述错误标记图像与当前目标标记图像之间的匹配度大于预设匹配值时,则将所述当前目标标记图像作为所述错误标记图像的目标标记图像。

6.根据权利要求5所述的图像处理方法,其特征在于,所述预设匹配值的取值范围为93%～98%。

7.根据权利要求5所述的图像处理方法，其特征在于，判断对所述初始权重矩阵进行替换后所对应的错误标记图像与当前目标标记图像之间的匹配度的步骤之后所述方法还包括：

当所述错误标记图像与当前目标标记图像之间的匹配度小于预设匹配值时，判断所述错误标记图像是否携带当前目标标记图像的关联标识；

若是，则根据所述关联标识查询关联匹配库，并将所述关联匹配库与所述错误标记图像进行匹配，以得到关联数据，根据所述关联数据确定所述错误标记图像的目标标记图像；

若否，则发出报警提示。

8.一种图像处理系统，其特征在于，所述系统包括：

获取模块，用于获取一目标标记图像，通过对抗生成网络模型对所述目标标记图像进行干扰，以得到至少一干扰图像；

收敛模块，用于通过收敛模型对所述干扰图像进行收敛，将收敛合格的干扰图像作为对抗样本，并将所述对抗样本覆盖于目标标记图像上；

识别模块，用于对进行对抗样本覆盖的目标标记图像进行图像识别，以得到错误标记图像，每个用户所得到的错误标记图片均不相同；

确定模块，用于根据所述错误标记图像与当前目标标记图像中目标区域的匹配度确定错误标记图像的目标标记图像。

9.一种可读存储介质，其上存储有计算机程序，其特征在于，该程序被处理器执行时实现如权利要求1－7任意一项所述的图像处理方法。

10.一种智能设备，包括存储器、处理器以及存储在存储器上并可在处理器上运行的计算机程序，其特征在于，所述处理器执行所述程序时实现上述权利要求1－7任意一项所述的图像处理方法。

图像处理方法、系统、可读存储介质及智能设备

技术领域

[0001] 本发明涉及数字信息安全技术领域，特别是涉及一种图像处理方法、系统、可读存储介质及智能设备。

背景技术

[0002] 随着摄影及图像处理技术的不断发展，增强现实技术也逐渐成熟，增强现实技术是通过实时地计算摄影机影像的位置及角度并加上相应图像的技术，以实现在拍摄得到的图片上把虚拟物体渲染在现实世界并进行互动的一种高科技技术，被广泛运用在生活当中，同时图像资产也应用而生。

[0003] 与内容不敏感的图像资产(如新闻照片等)不同，对于内容敏感的图像资产，如私人照片、漫画作品、秘密文件等，因为版权拥有者通常不愿或需收费才可以私密公开给指定的被授权人，其版权侵权者通常不会于公开图像时透露自己的身份，因此侦测和识别此类侵权者是一个亟待解决的问题。为了侦测和识别此类侵权者，现有技术通常会在图片上加上针对不同被授权人的多样性水印，即对于不同的被授权人，其收到的图片上所附带的水印均不相同。当发现未授权被公开的侵权图片时，通过提取图片上的水印，即可侦测到对应侵权者的身份，并就此提出诉讼或赔偿。

[0004] 然而，现有技术通常面临着水印易被识别和易被干扰这两个问题。如果水印人眼可以识别，那么会一定程度影响用户对于图片的观感。例如在图片的关键位置添加一个二维码，那么用户在观看图片时由于会观看到二维码覆盖于图片的关键位置上，用户体验会严重下降。此外，由于无法正确提取水印，则会导致侦测和识别侵权者身份的过程失效，因此无法就此提出诉讼或赔偿。

发明内容

[0005] 为了解决上述问题，本发明的目的是提供一种能够提高图片水印安全性，具有防篡改功能的图像处理方法、系统、可读存储介质。

[0006] 根据本发明提供的图像处理方法包括：

[0007] 获取一目标标记图像，通过对抗生成网络模型对所述目标标记图像进行干扰，以得到至少一干扰图像；

[0008] 通过收敛模型对所述干扰图像进行收敛，将收敛合格的干扰图像作为对抗样本，并将所述对抗样本覆盖于目标标记图像上；

[0009] 对进行对抗样本覆盖的目标标记图像进行图像识别，以得到错误标记图像，每个用户所得到的错误标记图片均不相同；

[0010] 根据所述错误标记图像与当前目标标记图像中目标区域的匹配度确定错误标记图像的目标标记图像。

[0011] 根据本发明提供的图像处理方法，首先获取一目标标记图像，通过对抗生成网络模型对所述目标标记图像进行干扰，以得到至少一干扰图像；通过收敛模型对所述干扰图

像进行收敛，将收敛合格的干扰图像作为对抗样本，并将所述对抗样本覆盖于目标标记图像上；对进行对抗样本覆盖的目标标记图像进行图像识别，以得到错误标记图像，每个用户所得到的错误标记图片均不相同；根据所述错误标记图像与当前目标标记图像中目标区域的匹配度确定错误标记图像的目标标记图像。本发明提供的图像处理方法，通过对每个用户制造不同的水印，由于生成的水印人眼无法识别，不会影响用户对图片的观感，且在不确定所使用图像识别模型的类型时算法也无法识别，因此无法定位可识别区域。即使可识别区域被定位，由于添加的水印为特定区域针对性的对抗训练结果，算法很难识别其中附加的信息，此外由于对抗样本的特点和多可识别区域的设计，即使图片污损，其水印仍可被识别及匹配，可以准确匹配侵权用户。

[0012] 另外，根据本发明上述的图像处理方法，还可以具有如下附加的技术特征：

[0013] 进一步地，获取一目标标记图像，通过对抗生成网络模型对所述目标标记图像进行干扰，以得到至少一干扰图像的步骤包括：

[0014] 获取原图像的图像信息，并根据所述图像信息对原图像进行离散化处理，从而将该原图像划分为若干可识别区域；

[0015] 通过图像识别模型对所述原图像的若干可识别区域进行标记，以得到所述目标标记图像，该目标标记图像携带有可识别区域的正确标签；

[0016] 通过对抗生成网络模型对所述目标标记图像进干扰，以得到对应的干扰图像，该干扰图像携带有可识别区域的错误标签。

[0017] 进一步地，通过图像识别模型对所述原图像的若干可识别区域进行标记，以得到所述目标标记图像的步骤包括：

[0018] 对所述原图像的若干可识别区域进行抽取与分解形成标记因子；

[0019] 根据所述标记因子进行机器算法学习后得可识别区域的正确标签。

[0020] 进一步地，根据所述标记因子进行机器算法学习后得可识别区域的正确标签的计算公式为：

[0021] $$Y_n = \phi() = V_k \times (\sum_{i=1}^{n} W_i \times X_i + B_k)$$

[0022] 其中，Φ（）为激活函数，V_k为调节系数，W_i为初始权重，X_i为标记因子，B_k为偏移累加量。

[0023] 进一步地，所述错误标记图像对应有一初始权重矩阵，根据所述错误标记图像与当前目标标记图像中目标区域的匹配度确定错误标记图像的目标标记图像的步骤包括：

[0024] 计算所述错误标记图像与当前目标标记图像之间的相关度矩阵；

[0025] 根据所述相关度矩阵对所述初始权重矩阵进行修正以得到一目标权重矩阵，所述目标权重矩阵用于在所述错误标记图像与所述当前目标标记图像进行匹配时，对所述初始权重矩阵进行替换；

[0026] 判断对所述初始权重矩阵进行替换后所对应的错误标记图像与当前目标标记图像之间的匹配度；

[0027] 当所述错误标记图像与当前目标标记图像之间的匹配度大于预设匹配值时，则将所述当前目标标记图像作为所述错误标记图像的目标标记图像。

[0028] 进一步地，所述预设匹配值的取值范围为93％～98％。

[0029] 进一步地，判断对所述初始权重矩阵进行替换后所对应的错误标记图像与当前目

标标记图像之间的匹配度的步骤之后所述方法还包括：

[0030] 当所述错误标记图像与当前目标标记图像之间的匹配度小于预设匹配值时，判断所述错误标记图像是否携带当前目标标记图像的关联标识；

[0031] 若是，则根据所述关联标识查询关联匹配库，并将所述关联匹配库与所述错误标记图像进行匹配，以得到关联数据，根据所述关联数据确定所述错误标记图像的目标标记图像；

[0032] 若否，则发出报警提示。

[0033] 本发明的另一实施例提出一种图像处理系统，解决现有水印易被识别和易被干扰这的问题，提高了用户图像隐私体验的满意度。

[0034] 根据本发明实施例的图像处理系统，包括：

[0035] 确定模块，用于根据访问周期内当前源地址的空间访问量确定当前源地址是否为冷源地址；

[0036] 判断模块，用于当所述当前源地址为冷源地址时，判断所述当前源地址在第一访问位置的数据块的引用计数是否小于预设值；

[0037] 删除模块，用于将所述当前源地址删除；

[0038] 迁移模块，用于将所述当前源地址移动至第二访问位置并进行保存，所述当前源地址在第二访问位置的数据块的引用计数大于第一访问位置。

[0039] 本发明的另一个实施例还提出一种存储介质，其上存储有计算机程序，该程序被处理器执行时实现上述方法的步骤。

[0040] 本发明的另一个实施例还提出一种智能设备，包括存储器、处理器以及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述程序时实现上述方法的步骤。

[0041] 本发明的附加方面和优点将在下面的描述中部分给出，部分将从下面的描述中变得明显，或通过本发明的实施例了解到。

附图说明

[0042] 图1是本发明第一实施例提出的图像处理方法的流程图；

[0043] 图2是图1中步骤S101的具体流程图；

[0044] 图3是图1中步骤S104的具体流程图；

[0045] 图4是本发明第二实施例提出的图像处理系统的结构框图。

具体实施方式

[0046] 为使本发明实施例的目的、技术方案和优点更加清楚，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。

[0047] 请参阅图1，本发明第一实施例提出的一种图像处理方法，其中，包括步骤S101～S104：

[0048] 步骤S101，获取一目标标记图像，通过对抗生成网络模型对所述目标标记图像进

行干扰，以得到至少一干扰图像。

[0049] 本实施例中，以图像处理设备为例进行说明，但需要了解的是，本发明实施例并不限于此，本发明实施例的方法可以应用在任何智能设备中，即任何可进行图像处理的电子设备中。具体的，现有技术中，通常会在图片上加上针对不同被授权人的多样性水印，即对于不同的被授权人，其收到的图片上所附带的水印均不相同。当发现未授权被公开的侵权图片时，通过提取图片上的水印，即可侦测到对应侵权者的身份，并就此提出诉讼或赔偿，然而却面临着水印易被识别和易被干扰的。因此，如果水印人眼可以识别，那么会一定程度影响用户对于图片的观感，如果水印容易被去除或干扰，那么当侵权图片被公开时，由于无法正确提取水印，则会导致侦测和识别侵权者身份的过程失效，因此无法就此提出诉讼或赔偿。

[0050] 本实施例中，当接收到一目标图像获取指令时；则获取目标标记图像，通过对抗生成网络模型对所述目标标记图像进行干扰，以得到至少一干扰图像，从而使未被授权的用户对图像进行公开时，能够追溯其身份，以提出诉讼或赔偿，此外还可使未授权的用户并不能正确识别该图像的图像信息，提高了图像的安全性。

[0051] 请参阅图2，获取一目标标记图像，通过对抗生成网络模型对所述目标标记图像进行干扰，以得到至少一干扰图像的方法包括如下步骤：

[0052] 步骤S1011，获取原图像的图像信息，并根据所述图像信息对原图像进行离散化处理，从而将该原图像划分为若干可识别区域。

[0053] 步骤S1012，通过图像识别模型对所述原图像的若干可识别区域进行标记，以得到所述目标标记图像，该目标标记图像携带有可识别区域的正确标签。

[0054] 具体的，对所述原图像的若干可识别区域进行抽取与分解形成标记因子；根据所述标记因子进行机器算法学习后得可识别区域的正确标签。

[0055] 根据所述标记因子进行机器算法学习后得可识别区域的正确标签的计算公式为：

[0056] $$Y_n = \phi() = V_k \times (\sum_{i=1}^{n} W_i \times X_i + B_k)$$

[0057] 其中，φ()为激活函数，V_k为调节系数，W_i为初始权重，X_i为标记因子，B_k为偏移累加量。

[0058] 如上所述，通过输入原图像的图像信息，经过数据标准化与抽取分解，获得原图像的标记因子X_i，配置对应的初始权重W_i，进行求和与B_k偏移累加，通过V_k系数调节，激活函数φ()，输出可识别区域的正确标签。

[0059] 步骤S1013，通过对抗生成网络模型对所述目标标记图像进干扰，以得到对应的干扰图像，该干扰图像携带有可识别区域的错误标签。

[0060] 如上所述，通过对原图形进行离散化处理，从而将该原图像划分为若干可识别区域，并非随机选择、固定位置、整张图片、或电子信息，以便于用户根据对可识别区域的识别结果确定对应的目标标记图像，每张图片可以支持m^n个用户，其中m为图片可识别区域的数量，n为图像识别模型可识别的标记数量，且各可识别区域的大小可以一致，也可以不一致；通过图像识别模型(如YOLOv3)对所述原图像的若干可识别区域进行标记，以得到所述目标标记图像，其中该目标标记图像携带有可识别区域的正确标签，该正确标签覆盖于整个原始图像，如可识别区域1被识别为标签a、可识别区域2被识别为标签b、可识别区域3被识别为标签c。

[0061] 进一步地，通过对抗生成网络模型对所述目标标记图像进干扰，以得到对应的干扰图像，该干扰图像携带有可识别区域的错误标签，可以理解的，错误标签是由识别错误而产生的，该识别错误被称为差异值(loss)，通过制定不同的训练目标，对抗生成网络模型可以生成不同的干扰图像，并产生不同的差异值，直至收敛并得到稳定的识别错误。例如，当对抗生成网络通过指定的收敛模型(如BP-Gradient)收敛时，其产生的干扰图像可以使得图像识别模型准确稳定的将可识别区域1错误的识别为标签x、可识别区域2错误的识别为标签y、可识别区域3错误的识别为标签z。

[0062] 步骤S102，通过收敛模型对所述干扰图像进行收敛，将收敛合格的干扰图像作为对抗样本，并将所述对抗样本覆盖于目标标记图像上。

[0063] 如上所述，当对抗生成网络通过指定的收敛模型(如BP-Gradient)收敛时，所产生的干扰图像被称为对抗样本，将所述对抗样本覆盖于当前目标标记图像上，以便于对当前目标标记图像进行标记，即使图片污损，其水印仍可被识别及匹配，可以准确匹配侵权用户。由于对抗样本的生成特点，其通常为像素扰动，而像素扰动对于人眼来说难以识别，且通过不同的识别错误，其序列和位置可以嵌入不同的用户识别信息。例如：用户A得到的图像是经过将可识别区域1、2、3分别错误的识别为x、y、z的对抗样本所覆盖后的图像；用户B得到的图像是经过将可识别区域1、2、3分别错误的识别为i、j、k的对抗样本所覆盖后的图像。则用户A和用户B所得到的图片分别携带了可标示其身份的不同信息，从而可寻找图片的所有者。

[0064] 步骤S103，对进行对抗样本覆盖的目标标记图像进行图像识别，以得到错误标记图像，其中，每个用户所得到的错误标记图片均不相同。

[0065] 具体的，图像识别模型对对抗样本覆盖后的原始图像进行图像识别，可以得到该图像可识别区域的所对应的目标错误标签，可识别区域1被识别为标签x、可识别区域2被识别为标签y、可识别区域3被识别为标签z，其“错误标签”特指由指定图像识别模型所标记的与其在原始图像中所标记的标签不符的标签。由于每个用户所得到的错误标记图片均不相同，从而可追溯该图片的所有者。

[0066] 步骤S104，根据所述错误标记图像与当前目标标记图像中目标区域的匹配度确定错误标记图像的目标标记图像。

[0067] 请参阅图3，所述错误标记图像对应有一初始权重矩阵，根据所述错误标记图像与当前目标标记图像中目标区域的匹配度确定错误标记图像的目标标记图像的步骤包括：

[0068] 步骤S1041，计算所述错误标记图像与当前目标标记图像之间的相关度矩阵。

[0069] 步骤S1042，根据所述相关度矩阵对所述初始权重矩阵进行修正以得到一目标权重矩阵，所述目标权重矩阵用于在所述错误标记图像与所述当前目标标记图像进行匹配时，对所述初始权重矩阵进行替换。

[0070] 步骤S1043，判断对所述初始权重矩阵进行替换后所对应的错误标记图像与当前目标标记图像之间的匹配度。

[0071] 步骤S1044，当所述错误标记图像与当前目标标记图像之间的匹配度大于预设匹配值时，则将所述当前目标标记图像作为所述错误标记图像的目标标记图像。所述预设匹配值的取值范围为93%～98%。

[0072] 如上所述，在将错误标记图像与当前目标标记图像进行匹配比较时，先计算所述

错误标记图像与当前目标标记图像之间的相关度矩阵M(i,j)，根据得到的相关度矩阵M(i,j)对所述初始权重矩阵进行修正以得到一目标权重矩阵K'(i,j)，在确定了目标权重矩阵K'(i,j)之后，判断对所述初始权重矩阵K(i,j)进行替换后所对应的错误标记图像与当前目标标记图像之间的匹配度。由于该相关度矩阵对应的相关度值存在大小差异，直接反应了错误标记图像与当前目标标记图像之间的匹配程度，因此可以根据该相关度矩阵M(i,j)的值，对初始权重矩阵K(i,j)进行修正得到目标权重矩阵K'(i,j)。在进行实际匹配时，将原来的初始权重矩阵替换为目标权重矩阵K'(i,j)，以使得替换后的目标权重矩阵K'(i,j)的值与上述的相关度矩阵的值更为吻合，从而提高相互匹配时对应的匹配精度。当所述错误标记图像与当前目标标记图像之间的匹配度大于预设匹配值93％～98％时，则将所述当前目标标记图像作为所述错误标记图像的目标标记图像。

[0073] 在此还需要说明的是，判断对所述初始权重矩阵进行替换后所对应的错误标记图像与当前目标标记图像之间的匹配度的步骤之后所述方法还包括：当所述错误标记图像与当前目标标记图像之间的匹配度小于预设匹配值时，判断所述错误标记图像是否携带当前目标标记图像的关联标识；若是，则根据所述关联标识查询关联匹配库，并将所述关联匹配库与所述错误标记图像进行匹配，以得到关联数据，根据所述关联数据确定所述错误标记图像的目标标记图像；若否，则发出报警提示。

[0074] 如上所述，通过判断所述错误标记图像是否携带当前目标标记图像的关联标识，当所述错误标记图像携带当前目标标记图像的关联标识时，则根据所述关联标识查询关联匹配库，并将所述关联匹配库与所述错误标记图像进行匹配，以得到关联数据，从而实现根据所述关联数据确定所述错误标记图像的目标标记图像，便于用户通过多方平台进行图像信息的验证，此外通过报警信息的提示，以便于用户及时维护自己的权益，且具有一定的威慑作用。

[0075] 作为一个具体的实施例，由于不同的错误标记信息对应着不同的用户，例如，图像A经过图像识别模型对对抗样本覆盖后的原始图像进行图像识别得到的标签为x、y、z；而图像B经过图像识别模型对对抗样本覆盖后的原始图像进行图像识别得到的标签为i、j、k。则可通过数据库匹配得知图像A属于用户A、图像B属于用户B。另外，由于信息序列可以嵌入一定的抗干扰特性，即使图片污损导致图像识别模型无法正确识别部分可识别区域的标签，其结果仍然可以匹配对应的用户。例如，即使图像A经过图像识别模型对对抗样本覆盖后的原始图像进行图像识别得到的标签为x、y，而可识别区域3并未被正确识别，由于x、y与i、j、k相比，前者与用户A的标签x、y、z更近似，仍可断定图片A属于用户A。

[0076] 根据本发明提供的图像处理方法，首先获取一目标标记图像，通过对抗生成网络模型对所述目标标记图像进行干扰，以得到至少一干扰图像；通过收敛模型对所述干扰图像进行收敛，将收敛合格的干扰图像作为对抗样本，并将所述对抗样本覆盖于目标标记图像上；对进行对抗样本覆盖的目标标记图像进行图像识别，以得到错误标记图像，每个用户所得到的错误标记图片均不相同；根据所述错误标记图像与当前目标标记图像中目标区域的匹配度确定错误标记图像的目标标记图像。本发明提供的图像处理方法，通过对每个用户制造不同的水印，由于生成的水印人眼无法识别，不会影响用户对图片的观感，且在不确定所使用图像识别模型的类型时算法也无法识别，因此无法定位可识别区域。即使可识别区域被定位，由于添加的水印为特定区域针对性的对抗训练结果，算法很难识别其中附加

的信息，此外由于对抗样本的特点和多可识别区域的设计，即使图片污损，其水印仍可被识别及匹配，可以准确匹配侵权用户。

[0077] 请参阅图4，基于同一发明构思，本发明第二实施例提供的图像处理系统，包括：

[0078] 获取模块10，用于获取一目标标记图像，通过对抗生成网络模型对所述目标标记图像进行干扰，以得到至少一干扰图像。

[0079] 本实施例中，所述获取模块10包括：

[0080] 获取单元11，用于获取原图像的图像信息，并根据所述图像信息对原图像进行离散化处理，从而将该原图像划分为若干可识别区域。

[0081] 标记单元12，用于通过图像识别模型对所述原图像的若干可识别区域进行标记，以得到所述目标标记图像，该目标标记图像携带有可识别区域的正确标签。

[0082] 具体的，对所述原图像的若干可识别区域进行抽取与分解形成标记因子；根据所述标记因子进行机器算法学习后得可识别区域的正确标签。

[0083] 根据所述标记因子进行机器算法学习后得可识别区域的正确标签的计算公式为：

[0084] $$Y_n = \phi() = V_k \times (\sum_{i=1}^{n} W_i \times X_i + B_k)$$

[0085] 其中，φ（）为激活函数，V_k为调节系数，W_i为初始权重，X_i为标记因子，B_k为偏移累加量。

[0086] 干扰单元13，用于通过对抗生成网络模型对所述目标标记图像进干扰，以得到对应的干扰图像，该干扰图像携带有可识别区域的错误标签。

[0087] 收敛模块20，用于通过收敛模型对所述干扰图像进行收敛，将收敛合格的干扰图像作为对抗样本，并将所述对抗样本覆盖于目标标记图像上。

[0088] 识别模块30，用于对进行对抗样本覆盖的目标标记图像进行图像识别，以得到错误标记图像，每个用户所得到的错误标记图片均不相同。

[0089] 确定模块40，用于根据所述错误标记图像与当前目标标记图像中目标区域的匹配度确定错误标记图像的目标标记图像。

[0090] 本实施例中，所述确定模块40包括：

[0091] 计算单元41，用于计算所述错误标记图像与当前目标标记图像之间的相关度矩阵。

[0092] 修正单元42，用于根据所述相关度矩阵对所述初始权重矩阵进行修正以得到一目标权重矩阵，所述目标权重矩阵用于在所述错误标记图像与所述当前目标标记图像进行匹配时，对所述初始权重矩阵进行替换。

[0093] 判断单元43，用于判断对所述初始权重矩阵进行替换后所对应的错误标记图像与当前目标标记图像之间的匹配度。

[0094] 确定单元44，用于当所述错误标记图像与当前目标标记图像之间的匹配度大于预设匹配值时，则将所述当前目标标记图像作为所述错误标记图像的目标标记图像。所述预设匹配值的取值范围为93％～98％。

[0095] 所述判断单元43，还用于当所述错误标记图像与当前目标标记图像之间的匹配度小于预设匹配值时，判断所述错误标记图像是否携带当前目标标记图像的关联标识；若是，则根据所述关联标识查询关联匹配库，并将所述关联匹配库与所述错误标记图像进行匹配，以得到关联数据，根据所述关联数据确定所述错误标记图像的目标标记图像；若否，则

发出报警提示。

[0096] 根据本发明提供的图像处理系统，首先获取一目标标记图像，通过对抗生成网络模型对所述目标标记图像进行干扰，以得到至少一干扰图像；通过收敛模型对所述干扰图像进行收敛，将收敛合格的干扰图像作为对抗样本，并将所述对抗样本覆盖于目标标记图像上；对进行对抗样本覆盖的目标标记图像进行图像识别，以得到错误标记图像，每个用户所得到的错误标记图片均不相同；根据所述错误标记图像与当前目标标记图像中目标区域的匹配度确定错误标记图像的目标标记图像。本发明提供的图像处理方法，通过对每个用户制造不同的水印，由于生成的水印人眼无法识别，不会影响用户对图片的观感，且在不确定所使用图像识别模型的类型时算法也无法识别，因此无法定位可识别区域。即使可识别区域被定位，由于添加的水印为特定区域针对性的对抗训练结果，算法很难识别其中附加的信息，此外由于对抗样本的特点和多可识别区域的设计，即使图片污损，其水印仍可被识别及匹配，可以准确匹配侵权用户。

[0097] 本发明实施例提出的图像处理系统的技术特征和技术效果与本发明实施例提出的方法相同，在此不予赘述。

[0098] 此外，本发明的实施例还提出一种存储介质，其上存储有计算机程序，该程序被处理器执行时实现上述方法的步骤。

[0099] 此外，本发明的实施例还提出一种智能设备，包括存储器、处理器以及存储在存储器上并可在处理器上运行的计算机程序，其中，所述处理器执行所述程序时实现上述方法的步骤。

[0100] 在流程图中表示或在此以其他方式描述的逻辑和/或步骤，例如，可以被认为是用于实现逻辑功能的可执行指令的定序列表，可以具体实现在任何计算机可读介质中，以供指令执行系统、装置或设备(如基于计算机的系统、包括处理器的系统或其他可以从指令执行系统、装置或设备取指令并执行指令的系统)使用，或结合这些指令执行系统、装置或设备而使用。就本说明书而言，“计算机可读介质”可以是任何可以包含、存储、通信、传播或传输程序以供指令执行系统、装置或设备或结合这些指令执行系统、装置或设备而使用的装置。

[0101] 计算机可读介质的更具体的示例(非穷尽性列表)包括以下：具有一个或多个布线的电连接部(电子装置)，便携式计算机盘盒(磁装置)，随机存取存储器(RAM)，只读存储器(ROM)，可擦除可编辑只读存储器(EPROM或闪速存储器)，光纤装置，以及便携式光盘只读存储器(CDROM)。另外，计算机可读介质甚至可以是可在其上打印所述程序的纸或其他合适的介质，因为可以例如通过对纸或其他介质进行光学扫描，接着进行编辑、解译或必要时以其他合适方式进行处理来以电子方式获得所述程序，然后将其存储在计算机存储器中。

[0102] 应当理解，本发明的各部分可以用硬件、软件、固件或它们的组合来实现。在上述实施方式中，多个步骤或方法可以用存储在存储器中且由合适的指令执行系统执行的软件或固件来实现。例如，如果用硬件来实现，和在另一实施方式中一样，可用本领域公知的下列技术中的任一项或他们的组合来实现：具有用于对数据信号实现逻辑功能的逻辑门电路的离散逻辑电路，具有合适的组合逻辑门电路的专用集成电路，可编程门阵列(PGA)，现场可编程门阵列(FPGA)等。

[0103] 在本说明书的描述中，参考术语“一个实施例”、“一些实施例”、“示例”、“具体示

例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本发明的至少一个实施例或示例中。在本说明书中，对上述术语的示意性表述不一定指的是相同的实施例或示例。而且，描述的具体特征、结构、材料或者特点可以在任何的一个或多个实施例或示例中以合适的方式结合。

[0104] 尽管已经示出和描述了本发明的实施例，本领域的普通技术人员可以理解：在不脱离本发明的原理和宗旨的情况下可以对这些实施例进行多种变化、修改、替换和变型，本发明的范围由权利要求及其等同物限定。

[0105] 最后应说明的是：以上所述实施例，仅为本发明的具体实施方式，用以说明本发明的技术方案，而非对其限制，本发明的保护范围并不局限于此，尽管参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：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，其依然可以对前述实施例所记载的技术方案进行修改或可轻易想到变化，或者对其中部分技术特征进行等同替换；而这些修改、变化或者替换，并不使相应技术方案的本质脱离本发明实施例技术方案的精神和范围，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应以所述权利要求的保护范围为准。

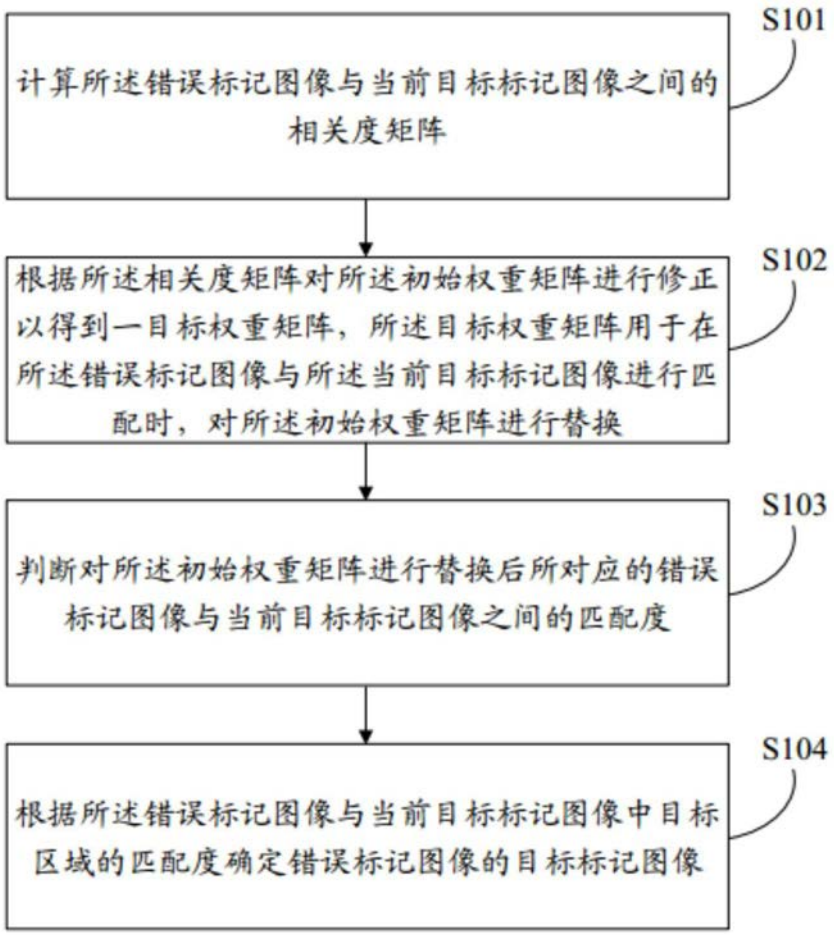

S101
计算所述错误标记图像与当前目标标记图像之间的相关度矩阵
S102
根据所述相关度矩阵对所述初始权重矩阵进行修正以得到一目标权重矩阵，所述目标权重矩阵用于在所述错误标记图像与所述当前目标标记图像进行匹配时，对所述初始权重矩阵进行替换
S103
判断对所述初始权重矩阵进行替换后所对应的错误标记图像与当前目标标记图像之间的匹配度
S104
根据所述错误标记图像与当前目标标记图像中目标区域的匹配度确定错误标记图像的目标标记图像

图1

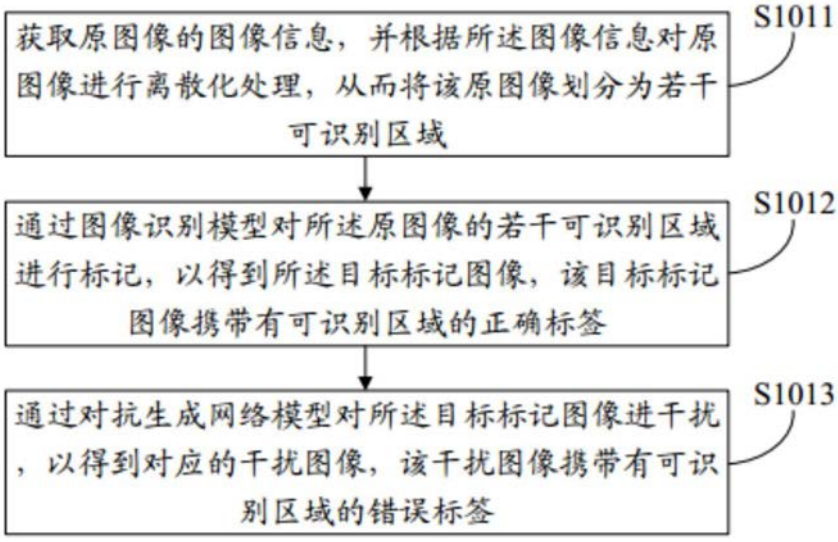

S1011
获取原图像的图像信息，并根据所述图像信息对原图像进行离散化处理，从而将该原图像划分为若干可识别区域
S1012
通过图像识别模型对所述原图像的若干可识别区域进行标记，以得到所述目标标记图像，该目标标记图像携带有可识别区域的正确标签
S1013
通过对抗生成网络模型对所述目标标记图像进干扰，以得到对应的干扰图像，该干扰图像携带有可识别区域的错误标签

图2

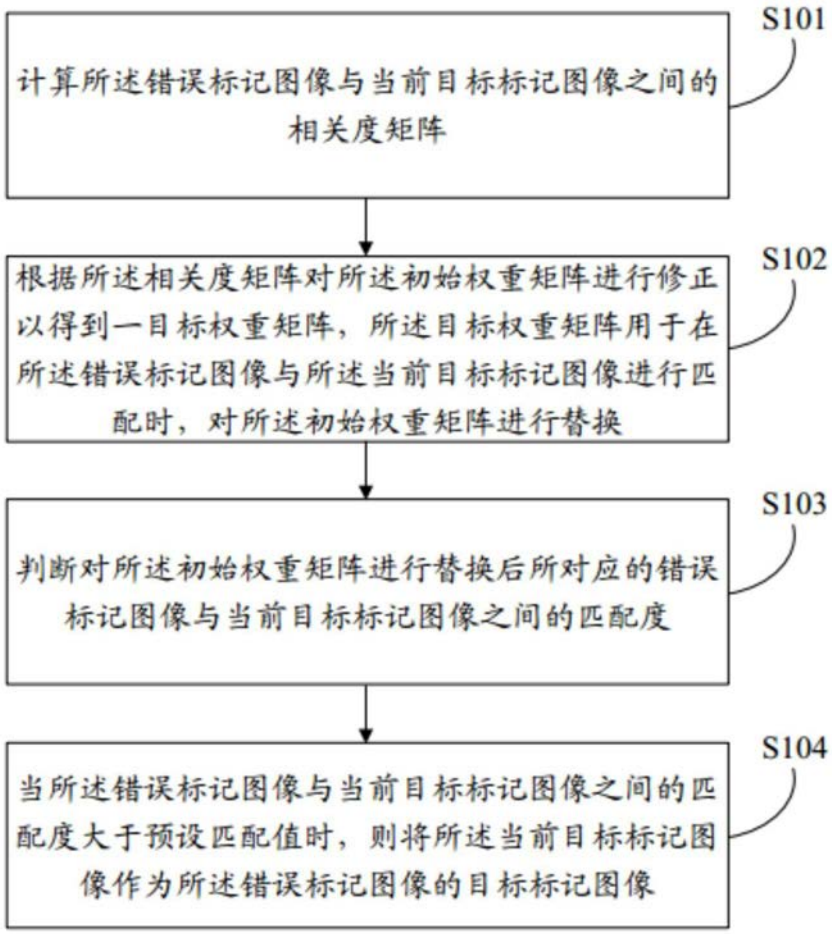

S101
计算所述错误标记图像与当前目标标记图像之间的相关度矩阵
S102
根据所述相关度矩阵对所述初始权重矩阵进行修正以得到一目标权重矩阵，所述目标权重矩阵用于在所述错误标记图像与所述当前目标标记图像进行匹配时，对所述初始权重矩阵进行替换
S103
判断对所述初始权重矩阵进行替换后所对应的错误标记图像与当前目标标记图像之间的匹配度
S104
当所述错误标记图像与当前目标标记图像之间的匹配度大于预设匹配值时，则将所述当前目标标记图像作为所述错误标记图像的目标标记图像

图3

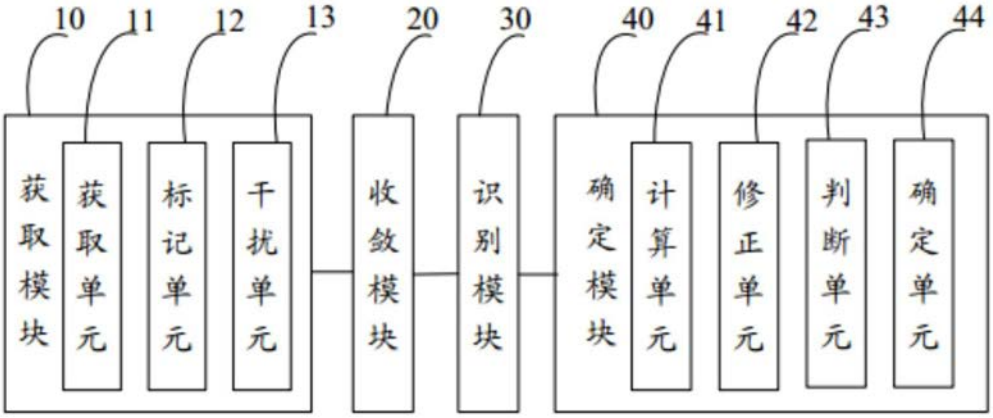

10
11
12
13
20
30
40
41
42
43
44
获取模块
获取单元
标记单元
干扰单元
收敛模块
识别模块
确定模块
计算单元
修正单元
判断单元
确定单元

图4