专利申请技术交底书

发明人（定稿前需要再确认）：\*\*\*

撰写人及其联系方式(电话/邮箱/微信): \*\*\*

|  |  |  |
| --- | --- | --- |
| **发明名称** | | 一种证件防伪造及伪造来源区分解决方案 |
| **所属技术领域**  (要求保护的技术方案所属的技术领域) | | 计算机视觉，防伪技术，信息安全 |
| **关键词** | | 证件防伪造，证件来源区分，深度学习 |
| **背景技术**  背景技术部分应当写明对发明或者实用新型的理解、检索、审查有用的背景技术，并且引证反映这些背景技术的文件。尤其要引证包含发明或者实用新型专利申请最接近的现有技术文件。此外，还要客观地指出背景技术中存在的问题和缺点，但是，仅限于涉及由发明或者实用新型的技术方案所解决的问题和缺点。在可能的情况下，说明存在这种问题和缺点的原因以及解决这些问题时曾经遇到的困难。 | | 证件防伪是防伪技术领域的重要问题。现有的证件防伪方法常常需要其他身份信息辅助进行防伪识别，如指纹，OID编码等，还可能需要借助于特殊的硬件设备。专利CN101833652A公开了一种基于指纹识别的身份核实系统，增加指纹识别技术提高证件防伪功能，同时辨别证件真伪及持有人真伪。专利CN106384145A公开了一种利用OID编码的证件防伪系统和方法，涉及在证件表面标记含有OID编码的二维码，通过含有识别防伪功能的应用软件的智能终端进行识别真假的利用OID编码的证件。专利CN205230086公开了一种身份证明识别系统，包括证件扫描模块、识别模块和控制处理模块，同时需要进行指纹识别核对。  证件防伪技术在生活中的很多领域都有重要应用，特别是在互联网金融领域，证件防伪技术能够有效保护开户人账户安全。然而进行证件伪造信息的建模是很复杂的。一方面，伪造的信息获取比较有限，如在互联网领域，伪造信息仅来自于图片或视频文件，且无法根据持有人的额外信息进行辨别。另一方面，根据证件伪造来源的不同，其特征也不相同，特征的复杂性意味着建模的难度更大。现有的证件防伪方法需要借助很多额外信息或借助特殊的硬件设备，随着互联网金融的发展，亟需掌握更方便、高效的证件防伪造技术。 |
| **发明的详细内容** | **此项专利申请所要解决的技术问题**  （针对现有技术中存在的缺陷和不足,用正面的、尽可能简洁的语言客观而有根据地反映发明或者实用新型要解决的技术问题，也可以进一步说明其效果，但是描述语言不得采用广告式的宣传用语） | 1. 利用深度学习框架解决证件防伪造问题。可以通过深度神经网络的强大描述能力进行建模，识别并区分正常的证件和伪造的证件。 2. 在证件防伪造的同时进行伪造信息来源的区分，如可将来源区分为：正常拍摄、复印件、PS、翻拍等。 3. 我们提出的在深度学习框架下的证件防伪造及来源区分解决方案在进行伪造的证件来源区分的同时，能够抵御伪造攻击的情况。 |
| **此项专利申请的技术方案简介**（进行概括，简要描述核心发明点。） | 1. 此算法进行证件防伪造及来源区分，可分为以下四个步骤进行，首先获取待检测证件图片或视频，进行预处理。之后，将待检测图片输入深度神经网络，得到网络输出的类别向量。第三步，分析输出的类别向量，得到是否为伪造证件的结果。若为伪造证件，第四步，由输出的类别向量进一步得到伪造信息的来源。 2. 利用此算法可以同时获得是否为伪造证件及伪造信息的来源。利用统一的深度神经网络解决以上两个问题，节省计算时间。 3. 该算法所述深度神经网络可位于终端设备中，解决移动端APP所需的证件防伪需求，也可位于服务器中，解决更大信息量的证件伪造信息检测需求。 4. 该算法所述的证件防伪造深度神经网络可以及时进行迭代更新，能够迅速应对新出现的伪造情况进行防伪检测。 |
| **此项专利申请的具体详细的一种或多种实施方式**（如有附图，请结合附图详细说明，并请区分哪些步骤或部件是实现方案所必不可少的，哪些步骤或部件是可选的以及可替换的方案有哪些） | 本发明的流程如图1所示    获取待检测证件图片或视频，预处理    利用深度神经网络检测待检测图片中是否存在伪造信息，对待检测图片进行证件防伪检测    输出是否为伪造证件的判定结果    若为伪造证件，输出伪造信息来源  图 1  一，获取待检测图片或视频  本发明的输入来自于用户提供的图片或现场拍摄的视频文件。根据输入文件类型不同，在进行后续的操作之前需要统一数据输入接口文件类型。针对图片类型文件仅进行必要的图像预处理操作，等待后续输入网络；针对视频类型文件，需要通过选帧操作，将选帧获取的图片进行图像预处理操作，等待后续输入网络。选帧操作具体用于从部分视频中选取至少一张图像作为待检测图像，要求选取的图像质量较高，最后检测该至少一张待检测图像中是否存在伪造信息。其中图像质量可以通过以下任意一项或多项标准衡量：证件是否位于图像中心、证件边缘是否被完整包括进图像内、证件表面所占图像面积比例高低、图像清晰度的高低、曝光度高低等，本发明实施例中选取的质量较高的图像可以是：证件位于图像中心、证件边缘被完整包括进图像内、证件占图像比例约1/2-3/4、图像清晰度较高、曝光度较高。  具体获取待检测文件流程如图2所示。    获取待检测证件图片或视频文件    是否为图片类型文件    视频文件选帧操作  获得图片类型文件  图 2  二，证件防伪检测及来源区分  输入：已获取的待检测图片文件。  输出：网络输出的类别向量。  在证件防伪检测的实现中，利用深度学习网络进行伪造信息特征建模和伪造信息来源区分。其中伪造信息来源包括复印件、PS、翻拍等。其中伪造信息的综合特征包括且不限于以下任意多项：局部二值模式（LBP）特征、稀疏编码的柱状图（HSC）特征、颜色（RGB）特征、全景图（LARGE）特征、证件区域（SMALL）特征、证件细节（TINY）特征。具体应用中，可以根据可能出现的伪造证件信息对该提取的综合特征包括的特征项进行更新。  其中，通过LBP特征，可以突出待检测图像中的边缘信息；通过HSC特征，可以更明显的反映待检测图像中的反光与模糊信息；通过RGB特征，可以更明显的区分真实拍摄的证件与证件复印件信息；LARGE特征是全图特征，基于LARGE特征，可以提取到待检测图像中最明显的伪造线索（hack）；证件区域（SMALL）是待检测图像中证件区域若干倍大小（例如1.5倍大小）的区域切图，包含证件、证件与背景切合的部分，基于SMALL特征，可以提取到反光、翻拍设备屏幕摩尔纹的边缘等伪造线索；证件细节图（TINY）是取证件大小的区域切图，包含证件，基于TINY特征，可以提取到图像PS（photoshop编辑）、翻拍屏幕摩尔纹、反光等伪造线索。上述各项特征中包含的伪造证件的伪造线索，可以预先通过训练深度神经网络模型，被深度神经网络学习到，之后任何包含这些伪造线索的图像输入深度神经网络后均会被检测出来，就可以判断为伪造证件图像，否则为真实证件图像。  由上述伪造特征训练好的深度神经网络对至少一张待检测图像分别进行综合特征提取。深度神经网络基于提取的综合特征中是否包含多个类别的伪造证件信息中的任意一项伪造信息，检测待检测图像是否伪造证件图像，得到待检测图像是否为伪造证件图像的证件防伪检测结果。  若所有的待检测图像中均不存在任何伪造信息，待检测视频通过证件防伪检测。否则，若任一待检测图像中存在多个类别伪造证件信息中的任意一项或多项伪造信息，待检测视频或图像未通过证件防伪检测。  若待检测视频或图像未通过证件防伪检测，则根据深度神经网络输出的类别向量，进一步输出伪造信息来源，主要为以下几项：复印件、PS、翻拍。  现有技术中，进行证件防伪造检测的方法一旦确定后就不容易更新了，难以应对新出现的伪造情况。本发明基于深度神经网络来进行证件防伪检测，当出现新的伪造样例时，可以及时通过新出现的伪造线索对深度神经网络进行训练，很容易在后端进行微调式的训练，及时更新深度神经网络，使深度神经网络及时学习到各种新出现的伪造线索、及时上线，从而能够迅速应对新出现的伪造情况进行防伪检测。  上述流程如图3所示。    待检测图片或视频文件  伪造信息特征  预处理      利用深度学习网络进行伪造信息特征建模    获得至少一张待检测图像    获得证件防伪造信息检测深度神经网络模型    利用新获得的伪造信息更新深度神经网络模型  输入已训练的深度神经网络模型进行防伪造信息结果预测    否  未通过证件防伪检测  所有的待检测图像中均不存在任何伪造信息    输出伪造信息来源  是    待检测视频通过证件防伪检测  图 3  三，业务平台证件防伪检测流程  在业务平台需要证件信息时首先进行证件防伪造检测，在待检测视频或图片通过证件防伪检测时，从待检测视频或图片中提取证件号码，证件照片中的图像作为注册用户的身份信息。  具体流程描述如下：业务平台可在接收到登录或验证请求时，获取待检测证件视频或图像，经过选帧操作及预处理操作后，通过已训练的深度神经网络提取待检测图像特征，检测待检测图像中是否存在伪造信息，对待检测图像进行证件防伪造检测，并向业务平台反馈证件防伪检测结果。若检测结果显示不存在伪造信息，则进行证件识别及信息提取，与库中信息进行比对验证信息正确性，若信息正确，则登录请求通过，对请求登录的用户发送的业务请求进行处理。若检测结果显示存在伪造信息，则登录请求不通过，并可有选择性的返回伪造信息来源，用于进一步的区分。 |
| **附图说明** |  |
| **此项专利申请的发明点与以往技术相比的不同点** | |  |  |  |  | | --- | --- | --- | --- | |  | 发明点 | 现有技术 | 现有技术 | | 步骤1 | 本方法利用深度学习实现通用的证件防伪造解决方案，并可及时迭代更新。 | 现有技术常依赖于额外的用户信息，技术通用性不足。 |  | | 步骤2 | 本方法可以同时区分伪造信息来源。 | 现有技术主要进行防伪，未进行来源区分。 |  | | 步骤3 | 本方法包含终端实现和服务器端实现，且无需复杂的硬件支持。 | 现有基础常依赖于特殊硬件。 |  | | 步骤4 | 本方法通过深度神经网络实现证件防伪，使利用深度学习进行防伪技术的探索成为可能。 | 传统深度学习框架主要用来进行图片分类，不能直接用于处理伪造信息。 |  | |  |  |  |  | |
| **此项专利申请与以往技术相比的有益效果** | 1. 利用深度学习框架进行证件伪造特征建模。 2. 利用深度神经网络，使得对伪造信息的分辨更为准确，能够更好的区分真实身份信息和伪造身份信息。 3. 在实现证件防伪造的功能的同时进行伪造信息来源的区分，有助于防伪技术的进一步有目的的提升，并且可以将伪造信息来源作为额外的伪造类别标签，提供给业务端口使用。 |
|  |  |
| **用户使用场景** （用户是怎样利用本方案的核心发明点来解决他们遇到的实际问题的?讲使用本技术的故事，并把核心技术应用在故事中。） | | 1. 在需要证件识别的场景中，可以利用本算法对证件是否为伪造证件进行区分。 2. 可以利用本算法对证件伪造来源的预测结果区分伪造信息类别。 3. 可以利用本算法帮助改善证件识别效果。 |
| **此专利申请在哪些产品中会被应用** | | 证件防伪，证件来源区分 |
| **如何检测此项专利申请在实际产品中被使用** | | 1. 产品中是否采用了深度神经网络进行证件伪造特征建模，利用深度神经网络进行真实信息和伪造信息区分。 2. 产品中是否利用相似的网络结构，在进行伪造信息区分的同时给出伪造信息来源。ㄌ |
| **补充材料**  （例如：技术术语的解释，相应申请的论文原文，或者，有助于方案理解的其他资料） | | 无 |