(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 113034433 B
(45)授权公告日 2024.01.02

(21)申请号 202110048821.2

(22)申请日 2021.01.14

(65)同一申请的已公布的文献号
申请公布号 CN 113034433 A

(43)申请公布日 2021.06.25

(73)专利权人 腾讯科技(深圳)有限公司
地址 518057 广东省深圳市南山区高新区科技中一路腾讯大厦35层

(72)发明人 胡一凡

(74)专利代理机构 广州三环专利商标代理有限公司 44202
专利代理师 熊永强 杜维

(51)Int.Cl.
G06T 7/00(2017.01)
G06V 20/40(2022.01)
G06V 10/80(2022.01)
G06N 3/08(2023.01)
G06V 10/82(2022.01)
G06N 3/0464(2023.01)

(56)对比文件
CN 109359502 A,2019.02.19
CN 110472531 A,2019.11.19
CN 111324874 A,2020.06.23
CN 111859018 A,2020.10.30
CN 112200136 A,2021.01.08
US 2008240579 A1,2008.10.02
US 2019130172 A1,2019.05.02

审查员 李淑

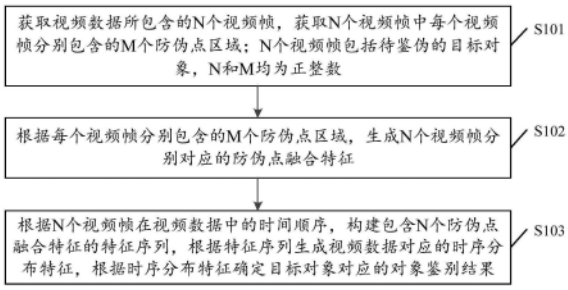
权利要求书4页 说明书26页 附图12页

(54)发明名称

数据鉴伪方法、装置、设备以及介质

(57)摘要

本申请实施例提供了一种数据鉴伪方法、装置、设备以及介质,该方法涉及人工智能技术,可以应用于身份证件鉴别场景中,该方法包括:获取视频数据所包含的N个视频帧,获取N个视频帧中每个视频帧分别包含的M个防伪点区域;N个视频帧包括待鉴伪的目标对象,N和M均为正整数;根据每个视频帧分别包含的M个防伪点区域,生成N个视频帧分别对应的防伪点融合特征;根据N个视频帧在视频数据中的时间顺序,构建包含N个防伪点融合特征的特征序列,根据特征序列生成视频数据对应的时序分布特征,根据时序分布特征确定目标对象对应的对象鉴别结果。采用本申请实施例,可以提高目标对象的鉴别准确度。



CN 113034433 B

1.一种数据鉴伪方法,其特征在于,包括:

获取视频数据所包含的N个视频帧,获取所述N个视频帧中每个视频帧分别包含的M个防伪点区域;所述N个视频帧包括待鉴伪的目标对象,N和M均为正整数;

获取所述N个视频帧中的视频帧T_i,在所述视频帧T_i的M个防伪点区域中获取防伪点区域R_j,在对象鉴别模型中获取与所述防伪点区域R_j相匹配的目标卷积神经网络;所述对象鉴别模型包括所述M个防伪点区域分别对应的卷积神经网络,i为小于或等于N的正整数,j为小于或等于M的正整数;

将所述防伪点区域R_j输入至所述目标卷积神经网络,根据所述目标卷积神经网络中的卷积层,对所述防伪点区域R_j进行卷积处理,得到所述防伪点区域R_j对应的防伪点分类特征;

获取M个防伪点区域分别对应的防伪点分类特征,将M个防伪点分类特征进行合并,得到所述视频帧T_i对应的防伪点融合特征,获取所述N个视频帧分别对应的防伪点融合特征;

根据所述N个视频帧在所述视频数据中的时间顺序,构建包含N个防伪点融合特征的特征序列,将所述特征序列中的N个防伪点融合特征依次输入至所述对象鉴别模型中的时序分类网络,在所述时序分类网络中获取所述N个防伪点融合特征之间的时序分布特征;

将所述时序分布特征输入至所述对象鉴别模型中的全连接层,通过所述全连接层输出目标特征向量,根据所述目标特征向量确定所述目标对象对应的对象鉴别结果;所述目标特征向量包括合法评估值和伪造评估值。

2.根据权利要求1所述的方法,其特征在于,所述获取视频数据所包含的N个视频帧,获取所述N个视频帧中每个视频帧分别包含的M个防伪点区域,包括:

获取摄像设备采集的视频数据,对所述视频数据进行分帧处理,得到视频帧序列;

根据间隔时间信息在所述视频帧序列中获取所述N个视频帧,获取所述N个视频帧中的视频帧T_i;i为小于或等于N的正整数;

获取所述视频数据中的所述目标对象对应的对象类型,获取与所述对象类型相关联的防伪点信息;

根据所述防伪点信息对所述视频帧T_i进行分割,得到所述视频帧T_i中的M个防伪点区域。

3.根据权利要求1所述的方法,其特征在于,所述通过所述全连接层输出目标特征向量,根据所述目标特征向量确定所述目标对象对应的对象鉴别结果,包括:

根据所述全连接层,将所述时序分布特征转换为目标特征向量;

若所述合法评估值大于所述伪造评估值,则确定所述目标对象对应的对象鉴别结果为合法鉴别结果;

若所述合法评估值小于所述伪造评估值,则确定所述目标对象对应的对象鉴别结果为伪造鉴别结果。

4.根据权利要求1所述的方法,其特征在于,所述视频数据为目标用户在业务机构办理开户业务时所提供的身份证视频数据,所述目标对象为身份证件;

所述方法还包括:

若所述身份证件的对象鉴别结果为合法鉴别结果,则在所述业务机构中继续执行针对所述目标用户的所述开户业务;

若所述身份证件的对象鉴别结果为伪造鉴别结果,则确定所述目标用户在所述业务机构中的开户业务办理结果为开户失败结果;所述开户失败结果用于指示所述目标用户提供新的身份证视频数据。

5.一种数据鉴伪方法,其特征在于,包括:

获取样本视频数据所包含的N个样本视频帧,获取所述N个样本视频帧中每个样本视频帧分别包含的M个样本防伪点区域;所述N个样本视频帧包括样本对象,所述样本视频数据携带针对所述样本对象的标签信息,N和M均为正整数;

将所述每个样本视频帧分别包含的M个样本防伪点区域输入至初始鉴别模型中各自对应的初始卷积神经网络,通过初始卷积神经网络输出每个样本防伪点区域分别对应的样本防伪点分类特征,将每个样本视频帧所包含的M个样本防伪点区域对应的样本防伪点分类特征进行合并,得到所述N个样本视频帧分别对应的样本防伪点融合特征;所述初始鉴别模型包括M个样本防伪点区域分别对应的初始卷积神经网络;

根据所述N个样本视频帧在所述样本视频数据中的时间顺序,将N个样本防伪点融合特征依次输入至所述初始鉴别模型中的初始时序分类网络;

在所述初始时序分类网络中获取所述N个样本防伪点融合特征之间的样本时序分布特征,将所述样本时序分布特征输入至所述初始鉴别模型中的全连接层,通过所述初始鉴别模型中的全连接层的输出结果,确定所述样本对象对应的样本鉴别结果;所述初始鉴别模型中的全连接层的输出结果包括合法评估值和伪造评估值;

根据所述标签信息、所述样本鉴别结果以及所述N个样本防伪点融合特征,对所述初始鉴别模型的网络参数进行修正,将包含修正后的网络参数的初始鉴别模型确定为对象鉴别模型;所述对象鉴别模型用于识别视频数据所包含的目标对象对应的对象鉴别结果。

6.根据权利要求5所述的方法,其特征在于,所述获取样本视频数据所包含的N个样本视频帧,包括:

将所述样本视频数据划分为N个样本视频片段,分别对每个样本视频片段进行分帧处理,得到所述每个样本视频片段分别对应的样本视频帧序列;

分别在N个样本视频帧序列中随机选取样本视频帧,得到所述样本视频数据中的所述N个样本视频帧。

7.根据权利要求5所述的方法,其特征在于,所述初始鉴别模型中的初始卷积神经网络包括第一卷积神经网络和第二卷积神经网络;所述标签信息包括第一防伪点标签、第二防伪点标签以及真伪标签;所述M个样本防伪点区域包括第一样本区域和第二样本区域,所述样本防伪点融合特征包括所述第一卷积神经网络输出的针对所述第一样本区域的第一样本防伪点分类特征,以及所述第二卷积神经网络输出的针对所述第二样本区域的第二样本防伪点分类特征;

所述根据所述标签信息、所述样本鉴别结果以及所述N个样本防伪点融合特征,对所述初始鉴别模型的网络参数进行修正,将包含修正后的网络参数的初始鉴别模型确定为对象鉴别模型,包括:

根据所述第一防伪点标签与所述第一样本防伪点分类特征之间的误差,生成所述第一卷积神经网络对应的第一损失参数;

根据所述第二防伪点标签与所述第二样本防伪点分类特征之间的误差,生成所述第二

卷积神经网络对应的第二损失函数；

根据所述真伪标签与所述样本鉴别结果之间的误差，生成所述初始时序分类网络对应的第三损失函数；

根据所述第一损失参数、所述第二损失函数以及所述第三损失函数，生成所述初始鉴别模型对应的目标损失函数；

根据所述目标损失函数对所述初始鉴别模型的网络参数进行修正，将包含修正后的网络参数的初始鉴别模型确定为对象鉴别模型。

8.根据权利要求7所述的方法，其特征在于，所述根据所述目标损失函数对所述初始鉴别模型的网络参数进行修正，将包含修正后的网络参数的初始鉴别模型确定为对象鉴别模型，包括：

根据所述目标损失函数对所述第一卷积神经网络和所述初始时序分类网络的网络参数进行修正，并暂停对所述第二卷积神经网络的网络参数进行修正；

当所述目标损失函数在连续p次训练中均达到第一最小值时，根据所述目标损失函数对修正后的初始时序分类网络的网络参数，以及所述第二卷积神经网络的网络参数进行修正，并暂停对修正后的第一卷积神经网络的网络参数进行修正；p为正整数；

当所述目标损失函数在连续q次训练中达到第二最小值时，将所述初始鉴别模型在最后一次训练中的网络参数确定为目标网络参数，将包含所述目标网络参数的初始鉴别模型确定为对象鉴别模型；q为正整数。

9.一种数据鉴伪装置，其特征在于，包括：

防伪点区域获取模块，用于获取视频数据所包含的N个视频帧，获取所述N个视频帧中每个视频帧分别包含的M个防伪点区域；所述N个视频帧包括待鉴伪的目标对象，N和M均为正整数；

融合特征生成模块，用于获取所述N个视频帧中的视频帧T_i，在所述视频帧T_i的M个防伪点区域中获取防伪点区域R_j，在对象鉴别模型中获取与所述防伪点区域R_j相匹配的目标卷积神经网络；所述对象鉴别模型包括所述M个防伪点区域分别对应的卷积神经网络，i为小于或等于N的正整数，j为小于或等于M的正整数；

所述融合特征生成模块，还用于将所述防伪点区域R_j输入至所述目标卷积神经网络，根据所述目标卷积神经网络中的卷积层，对所述防伪点区域R_j进行卷积处理，得到所述防伪点区域R_j对应的防伪点分类特征；

所述融合特征生成模块，还用于获取M个防伪点区域分别对应的防伪点分类特征，将M个防伪点分类特征进行合并，得到所述视频帧T_i对应的防伪点融合特征，获取所述N个视频帧分别对应的防伪点融合特征；

鉴别结果获取模块，用于根据所述N个视频帧在所述视频数据中的时间顺序，构建包含N个防伪点融合特征的特征序列，将所述特征序列中的N个防伪点融合特征依次输入至所述对象鉴别模型中的时序分类网络，在所述时序分类网络中获取所述N个防伪点融合特征之间的时序分布特征；

鉴别结果获取模块，还用于将所述时序分布特征输入至所述对象鉴别模型中的全连接层，通过所述全连接层输出目标特征向量，根据所述目标特征向量确定所述目标对象对应的对象鉴别结果；所述目标特征向量包括合法评估值和伪造评估值。

10.一种数据鉴伪装置,其特征在于,包括:

样本区域获取模块,用于获取样本视频数据所包含的N个样本视频帧,获取所述N个样本视频帧中每个样本视频帧分别包含的M个样本防伪点区域;所述N个样本视频帧包括样本对象,所述样本视频数据携带针对所述样本对象的标签信息,N和M均为正整数;

样本融合特征生成模块,用于将所述每个样本视频帧分别包含的M个样本防伪点区域输入至初始鉴别模型中各自对应的初始卷积神经网络,通过初始卷积神经网络输出每个样本防伪点区域分别对应的样本防伪点分类特征,将每个样本视频帧所包含的M个样本防伪点区域对应的样本防伪点分类特征进行合并,得到所述N个样本视频帧分别对应的样本防伪点融合特征;所述初始鉴别模型包括M个样本防伪点区域分别对应的初始卷积神经网络;

样本融合特征输入模块,用于根据所述N个样本视频帧在所述样本视频数据中的时间顺序,将N个样本防伪点融合特征依次输入至所述初始鉴别模型中的初始时序分类网络;

样本鉴别结果获取模块,用于在所述初始时序分类网络中获取所述N个样本防伪点融合特征之间的样本时序分布特征,将所述样本时序分布特征输入至所述初始鉴别模型中的全连接层,通过所述初始鉴别模型中的全连接层的输出结果,确定所述样本对象对应的样本鉴别结果;所述初始鉴别模型中的全连接层的输出结果包括合法评估值和伪造评估值;

网络参数修正模块,用于根据所述标签信息、所述样本鉴别结果以及所述N个样本防伪点融合特征,对所述初始鉴别模型的网络参数进行修正,将包含修正后的网络参数的初始鉴别模型确定为对象鉴别模型;所述对象鉴别模型用于识别视频数据所包含的目标对象对应的对象鉴别结果。

11.一种计算机设备,其特征在于,包括存储器和处理器;

所述存储器与所述处理器相连,所述存储器用于存储计算机程序,所述处理器用于调用所述计算机程序,以使得所述计算机设备执行权利要求1至4任一项所述的方法,或者执行权利要求5至8任一项所述的方法。

12.一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中存储有计算机程序,所述计算机程序适于由处理器加载并执行,以使得具有所述处理器的计算机设备执行权利要求1至4任一项所述的方法,或者执行权利要求5至8任一项所述的方法。

数据鉴伪方法、装置、设备以及介质

技术领域

[0001] 本申请涉及互联网技术领域,尤其涉及一种数据鉴伪方法、装置、设备以及介质。

背景技术

[0002] 随着社会发展技术的进步,伪造物品的情形也随之增加,如伪造各种类型的证件、伪造钞票、伪造古玩物件的情形时有发生,如何鉴别物品的真实性成为一个普遍的社会难题。

[0003] 现有的证件鉴伪技术中,可以采集证件的图像数据(如证件的扫描件、照片等),获取图像数据中所包含的证件特征(如人脸特征、证件编号特征以及证件特定标识特征等),通过对证件特征进行识别,确定证件的真实性。然而,证件中的有些特征可能需要在不同视觉角度或不同光线下才能显示,由于采集到的图像数据可能是一个角度下所拍摄的照片,因此通过该图像数据无法获取到证件的全部特征,容易造成证件的鉴别结果出现偏差,进而导致证件的鉴别准确度过低。

发明内容

[0004] 本申请实施例提供一种数据鉴伪方法、装置、设备以及介质,可以提高目标对象的鉴别准确度。

[0005] 本申请实施例一方面提供了一种数据鉴伪方法,包括:

[0006] 获取视频数据所包含的N个视频帧,获取N个视频帧中每个视频帧分别包含的M个防伪点区域;N个视频帧包括待鉴伪的目标对象,N和M均为正整数;

[0007] 根据每个视频帧分别包含的M个防伪点区域,生成N个视频帧分别对应的防伪点融合特征;

[0008] 根据N个视频帧在视频数据中的时间顺序,构建包含N个防伪点融合特征的特征序列,根据特征序列生成视频数据对应的时序分布特征,根据时序分布特征确定目标对象对应的对象鉴别结果。

[0009] 本申请实施例一方面提供了一种数据鉴伪方法,包括:

[0010] 获取样本视频数据所包含的N个样本视频帧,获取N个样本视频帧中每个样本视频帧分别包含的M个样本防伪点区域;N个样本视频帧包括样本对象,样本视频数据携带针对样本对象的标签信息,N和M均为正整数;

[0011] 将每个样本视频帧分别包含的M个样本防伪点区域输入至初始鉴别模型中的初始卷积神经网络,通过初始卷积神经网络,生成N个样本视频帧分别对应的样本防伪点融合特征;

[0012] 根据N个样本视频帧在样本视频数据中的时间顺序,将N个样本防伪点融合特征依次输入至初始鉴别模型中的初始时序分类网络;

[0013] 通过初始时序分类网络,生成样本视频数据对应的样本时序分布特征,根据样本时序分布特征确定样本对象对应的样本鉴别结果;

[0014] 根据标签信息、样本鉴别结果以及N个样本防伪点融合特征,对初始鉴别模型的网络参数进行修正,将包含修正后的网络参数的初始鉴别模型确定为对象鉴别模型;对象鉴别模型用于识别视频数据所包含的目标对象对应的对象鉴别结果。

[0015] 本申请实施例一方面提供了一种数据鉴伪装置,包括:

[0016] 防伪点区域获取模块,用于获取视频数据所包含的N个视频帧,获取N个视频帧中每个视频帧分别包含的M个防伪点区域;N个视频帧包括待鉴伪的目标对象,N和M均为正整数;

[0017] 融合特征生成模块,用于根据每个视频帧分别包含的M个防伪点区域,生成N个视频帧分别对应的防伪点融合特征;

[0018] 鉴别结果获取模块,用于根据N个视频帧在视频数据中的时间顺序,构建包含N个防伪点融合特征的特征序列,根据特征序列生成视频数据对应的时序分布特征,根据时序分布特征确定目标对象对应的对象鉴别结果。

[0019] 其中,防伪点区域获取模块包括:

[0020] 视频分帧处理单元,用于获取摄像设备采集的视频数据,对视频数据进行分帧处理,得到视频帧序列;

[0021] 视频帧选取单元,用于根据间隔时间信息在视频帧序列中获取N个视频帧,获取N个视频帧中的视频帧T_i;i为小于或等于N的正整数;

[0022] 防伪点信息获取单元,用于获取视频数据中的目标对象对应的对象类型,获取与对象类型相关联的防伪点信息;

[0023] 视频帧分割单元,用于根据防伪点信息对视频帧T_i进行分割,得到视频帧 T_i中的M个防伪点区域。

[0024] 其中,融合特征生成模块包括:

[0025] 网络匹配单元,用于获取N个视频帧中的视频帧T_i,在视频帧T_i的M个防伪点区域中获取防伪点区域R_j,在对象鉴别模型中获取与防伪点区域R_j相匹配的目标卷积神经网络;对象鉴别模型包括M个防伪点区域分别对应的卷积神经网络,i为小于或等于N的正整数,j为小于或等于M的正整数;

[0026] 卷积处理单元,用于将防伪点区域R_j输入至目标卷积神经网络,根据目标卷积神经网络中的卷积层,对防伪点区域R_j进行卷积处理,得到防伪点区域R_j对应的防伪点分类特征;

[0027] 特征合并单元,用于获取M个防伪点区域分别对应的防伪点分类特征,将 M个防伪点分类特征进行合并,得到视频帧T_i对应的防伪点融合特征。

[0028] 其中,鉴别结果获取模块包括:

[0029] 时序分布特征获取单元,用于将特征序列中的N个防伪点融合特征依次输入至对象鉴别模型中的时序分类网络,在时序分类网络中获取N个防伪点融合特征之间的时序分布特征;

[0030] 结果输出单元,用于将时序分布特征输入至对象鉴别模型中的全连接层,通过全连接层输出目标特征向量,根据目标特征向量确定目标对象对应的对象鉴别结果。

[0031] 其中,结果输出单元可以包括:

[0032] 特征转换子单元,用于根据全连接层,将时序分布特征转换为目标特征向量;目标

特征向量包括合法评估值和伪造评估值；

[0033] 比较子单元，用于若合法评估值大于伪造评估值，则确定目标对象对应的对象鉴别结果为合法鉴别结果；

[0034] 上述比较单元，还用于若合法评估值小于伪造评估值，则确定目标对象对应的对象鉴别结果为伪造鉴别结果。

[0035] 其中，视频数据为目标用户在业务机构办理开户业务时所提供的身份证视频数据，目标对象为身份证件；

[0036] 该装置还包括：

[0037] 业务执行模块，用于若身份证件的对象鉴别结果为合法鉴别结果，则在业务机构中继续执行针对目标用户的开户业务；

[0038] 业务办理失败提示模块，用于若身份证件的对象鉴别结果为伪造鉴别结果，则确定目标用户在业务机构中的开户业务办理结果为开户失败结果；开户失败结果用于指示目标用户提供新的身份证视频数据。

[0039] 本申请实施例一方面提供了一种数据鉴伪装置，包括：

[0040] 样本区域获取模块，用于获取样本视频数据所包含的N个样本视频帧，获取N个样本视频帧中每个样本视频帧分别包含的M个样本防伪点区域；N个样本视频帧包括样本对象，样本视频数据携带针对样本对象的标签信息，N和M 均为正整数；

[0041] 样本融合特征生成模块，用于将每个样本视频帧分别包含的M个样本防伪点区域输入至初始鉴别模型中的初始卷积神经网络，通过初始卷积神经网络，生成N个样本视频帧分别对应的样本防伪点融合特征；

[0042] 样本融合特征输入模块，用于根据N个样本视频帧在样本视频数据中的时间顺序，将N个样本防伪点融合特征依次输入至初始鉴别模型中的初始时序分类网络；

[0043] 样本鉴别结果获取模块，用于通过初始时序分类网络，生成样本视频数据对应的样本时序分布特征，根据样本时序分布特征确定样本对象对应的样本鉴别结果；

[0044] 网络参数修正模块，用于根据标签信息、样本鉴别结果以及N个样本防伪点融合特征，对初始鉴别模型的网络参数进行修正，将包含修正后的网络参数的初始鉴别模型确定为对象鉴别模型；对象鉴别模型用于识别视频数据所包含的目标对象对应的对象鉴别结果。

[0045] 其中，样本区域获取模块包括：

[0046] 样本视频分帧处理单元，用于将样本视频数据划分为N个样本视频片段，分别对每个样本视频片段进行分帧处理，得到每个样本视频片段分别对应的样本视频帧序列；

[0047] 样本视频帧选取单元，用于分别在N个样本视频帧序列中随机选取样本视频帧，得到样本视频数据中的N个样本视频帧。

[0048] 其中，初始卷积神经网络包括第一卷积神经网络和第二卷积神经网络；标签信息包括第一防伪点标签、第二防伪点标签以及真伪标签；M个样本防伪点区域包括第一样本区域和第二样本区域，样本防伪点融合特征包括第一卷积神经网络输出的针对第一样本区域的第一样本防伪点分类特征，以及第二卷积神经网络输出的针对第二样本区域的第二样本防伪点分类特征；

[0049] 网络参数修正模块包括：

[0050] 第一损失函数生成单元,用于根据第一防伪点标签与第一样本防伪点分类特征之间的误差,生成第一卷积神经网络对应的第一损失参数;

[0051] 第二损失函数生成单元,用于根据第二防伪点标签与第二样本防伪点分类特征之间的误差,生成第二卷积神经网络对应的第二损失函数;

[0052] 第三损失函数生成单元,用于根据真伪标签与样本鉴别结果之间的误差,生成初始时序分类网络对应的第三损失函数;

[0053] 目标损失函数生成单元,用于根据第一损失参数、第二损失函数以及第三损失函数,生成初始对象鉴别模型对应的目标损失函数;

[0054] 参数修正单元,用于根据目标损失函数对初始鉴别模型的网络参数进行修正,将包含修正后的网络参数的初始鉴别模型确定为对象鉴别模型。

[0055] 其中,参数修正单元包括:

[0056] 第一修正子单元,用于根据目标损失函数对第一卷积神经网络和初始时序分类网络的网络参数进行修正,并暂停对第二卷积神经网络的网络参数进行修正;

[0057] 第二修正子单元,用于当目标损失函数在连续p次训练中均达到第一最小值时,根据目标损失函数对修正后的初始时序分类网络的网络参数,以及第二卷积神经网络的网络参数进行修正,并暂停对修正后的第一卷积神经网络的网络参数进行修正;p为正整数;

[0058] 目标网络参数确定子单元,用于当目标损失函数在连续q次训练中达到第二最小值时,将初始鉴别模型在最后一次训练中的网络参数确定为目标网络参数,将包含目标网络参数的初始鉴别模型确定为对象鉴别模型;q为正整数。

[0059] 本申请实施例一方面提供了一种计算机设备,包括存储器和处理器,存储器与处理器相连,存储器用于存储计算机程序,处理器用于调用计算机程序,以使得该计算机设备执行本申请实施例中上述一方面提供的方法。

[0060] 本申请实施例一方面提供了一种计算机可读存储介质,计算机可读存储介质中存储有计算机程序,计算机程序适于由处理器加载并执行,以使得具有处理器的计算机设备执行本申请实施例中上述一方面提供的方法。

[0061] 根据本申请的一个方面,提供了一种计算机程序产品或计算机程序,该计算机程序产品或计算机程序包括计算机指令,该计算机指令存储在计算机可读存储介质中。计算机设备的处理器从计算机可读存储介质读取该计算机指令,处理器执行该计算机指令,使得该计算机设备执行上述一方面提供的方法。

[0062] 本申请实施例可以获取包含待鉴伪的目标对象的视频数据,获取视频数据的N个视频帧中每个视频帧分别包含的M个防伪点区域,N和M为正整数,进而可以根据每个视频帧分别包含的M个防伪点区域,生成N个视频帧分别对应的防伪点融合特征;根据N个视频帧在视频数据中的时间顺序,构建包含N 个防伪点融合特征的特征序列,根据特征序列可以生成视频数据对应的时序分布特征,对时序分布特征进行分类,可以得到视频数据中所包含的目标对象对应的对象鉴别结果。可见,通过获取目标对象对应的视频数据,可以从视频数据中获取不同防伪点在相同视频帧中的特征信息,也可以获取相同防伪点在不同视频帧中的特征信息,通过将相同视频帧中不同防伪点的特征信息进行融合,以得到每个视频帧对应的防伪点融合特征,进而可以获取每个视频帧所对应的防伪点融合特征之间的时序分布特征,该时序分布特征可以用于表征该目标对象在不同视觉角度下的特征信息,可以提高

目标对象的鉴别准确度。

附图说明

[0063] 为了更清楚地说明本申请实施例或现有技术中的技术方案,下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图仅仅是本申请的一些实施例,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。

[0064] 图1是本申请实施例提供的一种网络架构的结构示意图;

[0065] 图2是本申请实施例提供的一种数据鉴伪场景示意图;

[0066] 图3是本申请实施例提供的一种身份证件的防伪点示意图;

[0067] 图4是本申请实施例提供的一种数据鉴伪方法的流程示意图;

[0068] 图5是本申请实施例提供的一种在视频帧中获取防伪点区域的示意图;

[0069] 图6是本申请实施例提供的一种业务办理中对身份证件进行鉴伪的示意图;

[0070] 图7是本申请实施例提供的一种数据鉴伪方法的流程示意图;

[0071] 图8是本申请实施例提供的一种训练初始鉴别模型的示意图;

[0072] 图9是本申请实施例提供的一种数据鉴伪装置的结构示意图;

[0073] 图10是本申请实施例提供的一种数据鉴伪装置的结构示意图;

[0074] 图11是本申请实施例提供的一种计算机设备的结构示意图;

[0075] 图12是本申请实施例提供的一种计算机设备的结构示意图。

具体实施方式

[0076] 下面将结合本申请实施例中的附图,对本申请实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例仅仅是本申请一部分实施例,而不是全部的实施例。基于本申请中的实施例,本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例,都属于本申请保护的范围。

[0077] 本申请实施例涉及人工智能(Artificial Intelligence,AI)技术。人工智能是利用数字计算机或者数字计算机控制的机器模拟、延伸和扩展人的智能,感知环境、获取知识并使用知识获得最佳结果的理论、方法、技术及应用系统。换句话说,人工智能是计算机科学的一个综合技术,它企图了解智能的实质,并生产出一种新的能以人类智能相似的方式做出反应的智能机器。人工智能也就是研究各种智能机器的设计原理与实现方法,使机器具有感知、推理与决策的功能。

[0078] 人工智能技术是一门综合学科,涉及领域广泛,既有硬件层面的技术也有软件层面的技术。人工智能基础技术一般包括如传感器、专用人工智能芯片、云计算、分布式存储、大数据处理技术、操作/交互系统、机电一体化等技术。人工智能软件技术主要包括计算机视觉技术、语音处理技术、自然语言处理技术以及机器学习/深度学习等几大方向。本申请实施例具体涉及人工智能技术下属的计算机视觉技术(Computer Vision,CV)。

[0079] 计算机视觉是一门研究如何使机器“看”的科学,更进一步的说,就是指用摄影机和电脑代替人眼对目标进行识别、跟踪和测量等机器视觉,并进一步做图形处理,使电脑处理成为更适合人眼观察或传送给仪器检测的图像。作为一个科学学科,计算机视觉研究相

关的理论和技术,试图建立能够从图像或者多维数据中获取信息的人工智能系统。计算机视觉技术通常包括图像处理、图像识别、图像语义理解、图像检索、OCR、视频处理、视频语义理解、视频内容/行为识别、三维物体重建、3D技术、虚拟现实、增强现实、同步定位与地图构建等技术,还包括常见的人脸识别、指纹识别等生物特征识别技术。本申请实施例具体涉及计算机视觉技术中的视频内容识别。

[0080] 请参见图1,图1是本申请实施例提供的一种网络架构的结构示意图。如图 1所示,该网络架构可以包括服务器10d和用户终端集群,该用户终端集群可以包括一个或者多个用户终端,这里不对用户终端的数量进行限制。如图1所示,该用户终端集群可以具体包括用户终端10a、用户终端10b以及用户终端10c等。其中,服务器10d可以是独立的物理服务器,也可以是多个物理服务器构成的服务器集群或者分布式系统,还可以是提供云服务、云数据库、云计算、云函数、云存储、网络服务、云通信、中间件服务、域名服务、安全服务、CDN、以及大数据和人工智能平台等基础云计算服务的云服务器。用户终端10a、用户终端10b以及用户终端10c等均可以包括:智能手机、平板电脑、笔记本电脑、掌上电脑、移动互联网设备(mobile internet device,MID)、可穿戴设备(例如智能手表、智能手环等)以及智能电视等具有视频数据处理功能的智能终端。如图1所示,用户终端10a、用户终端10b以及用户终端10c等可以分别与服务器10d进行网络连接,以便于每个用户终端均可以通过该网络连接与服务器10d 之间进行数据交互。

[0081] 在数据鉴伪场景中,以图1所示的用户终端10a为例,用户终端10a可以获取包含目标对象的视频数据,该视频数据可以为采用摄像设备采集的针对目标对象的视频数据。为了鉴别视频数据中所包含的目标对象的真实性,用户终端 10a可以从视频数据中抽取N个视频帧,其中,N为正整数,如N可以为1,2, 3……,本申请实施例对N的数值不做限定;进而可以根据目标对象的防伪点信息(此处的防伪点信息可以是已知的,如目标对象为身份证件时,权威机构可以为身份证件提供一些官方的防伪点),对N个视频帧中的每个视频帧均进行分割和区域剪裁,获取每个视频帧所包含的M个防伪点区域(每个视频帧中,一个防伪点提取一个防伪点区域),其中,M为正整数,如M可以为1,2,3……, M的数值与目标对象的类型相关联,不同类型的目标对象具有不同数量的防伪点。用户终端10a可以从每个视频帧所包含的M个防伪点区域中获取对应的防伪点分类特征,将每个视频帧获取的M个防伪点区域的防伪点分类特征进行合并,得到N个视频帧分别对应的防伪点融合特征;根据N个视频帧在视频数据中的时间顺序,构建包含N个防伪点融合特征的特征序列,根据特征序列可以生成视频数据对应的时序分布特征,进而可以根据时序分布特征确定目标对象对应的对象鉴别结果。本申请实施例可以采集包含目标对象的视频数据,通过对视频数据中的目标对象进行识别分类,生成的时序分布特征更能表达目标对象的细节特征,根据时序分布特征所确定的对象鉴别结果,可以提高目标对象的鉴别准确度。

[0082] 请一并参见图2,图2是本申请实施例提供的一种数据鉴伪场景示意图。用户需要在银行办理开户业务时,可以通过银行提供的线上电子技术办理开户业务,即足不出户就可以在银行完成开户业务。例如,线上电子技术可以为通过电子程序认识客户(electronic Know your customer,eKYC),eKYC是虚拟银行开户中的核心技术;对于虚拟银行线上开户业务来说,认识客户的技术难度比普通线下认识客户要高很多,其中,身份证件鉴伪过程是eKYC整体流程中的重要环节,其中身份证件可以包括不同国家或地区的身份证件。当用户

使用身份证件办理虚拟银行开户业务时,可以通过身份证件的本身特质对其进行鉴伪,进而根据鉴别结果可以判断办理开户业务的用户所提供的身份证件是否经过仿冒或篡改。如图2所示,用户在虚拟银行申请开户的过程中,可以使用摄像设备采集一段包含身份证件的视频数据20a,该用户所使用的用户终端可以获取摄像设备采集的视频数据20a,并将该视频数据20a传输至虚拟银行的后台服务器。其中,摄像设备可以是用户所使用的用户终端中的内部摄像组件(如用户终端自带的照相机),或者为与用户终端具有通信连接的外接摄像设备;视频数据20a可以是指从不同角度和不同光线下所采集的视频数据。

[0083] 后台服务器在接收到用户终端传输的视频数据20a后,可以对视频数据20a 进行分帧处理,得到该视频数据20a对应的视频帧序列,可以从视频序列中选取N个视频帧,如视频帧T1、视频帧T2、视频帧T3、……、视频帧TN,其中, N为正整数。后台服务器可以对N个视频帧中的每个视频帧进行分割处理,获取每个视频帧分别对应的防伪点融合特征,根据N个视频帧分别对应的防伪点融合特征可以确定视频数据20a中所包含的身份证件的鉴别结果。N个视频帧所对应的防伪点融合特征的获取过程是相同的,下面以视频帧T1为例,对防伪点融合特征的获取过程进行描述。

[0084] 如图2所示,后台服务器可以根据身份证件的防伪点信息,对视频帧T1进行分割处理,从视频帧T1中剪裁出M个防伪点区域,其中,M为正整数,M 的具体取值与身份证件的防伪点数量相关联,如身份证件的防伪点数量为2时,此时的M可以为2,一个防伪点区域可以包括一个防伪点,当然,当身份证件的多个防伪点位于相同区域时,一个防伪点区域也可以包括多个防伪点。如图2 所示,当用户的身份证件包括M个防伪点时,可以对视频帧T1进行分割和剪裁,获取视频帧T1所包含的M个防伪点区域,其中,M个防伪点区域可以有重叠内容。例如,在视频帧T1中获取到防伪点区域20b、防伪点区域20c、防伪点区域20d等M个防伪点区域。

[0085] 后台服务器可以获取针对身份证件的鉴别模型,该鉴别模型可以至少包括 M个卷积神经网络(Convolutional Neural Networks,CNN)和时序分类网络,即鉴别模型所包含的卷积神经网络的数量可以大于或等于身份证件中所包含的防伪点数量,该鉴别模型可以用于鉴别不同类型身份证件的真实性。例如,第一类身份证件的防伪点数量为4个,第二类身份证件的防伪点在第一类身份证件的基础上增加了2个防伪点,为了可以准确地鉴别第一类身份证件和第二类身份证件的真实性,该鉴别模型可以包括6个卷积神经网络和一个时序分类网络。

[0086] 后台服务器可以在鉴别模型中获取M个防伪点区域中每个防伪点区域分别对应卷积神经网络,如与防伪点区域20b相匹配的卷积神经网络为:卷积神经网络20e,与防伪点区域20c相匹配的卷积神经网络为:卷积神经网络20f,与防伪点区域20d相匹配的卷积神经网络为:卷积神经网络20g。将防伪点区域 20b输入卷积神经网络20e中,通过卷积神经网络20e可以获取防伪点区域20b 对应的防伪点分类特征1;将防伪点区域20c输入卷积神经网络20f中,通过卷积神经网络20f可以获取防伪点区域20c对应的防伪点分类特征2;将防伪点区域20d输入卷积神经网络20g中,通过卷积神经网络g获取防伪点区域20d对应的防伪点分类特征3;依次类推,后台服务器可以获取M个防伪点区域分别对应的防伪点分类特征。将M个防伪点区域分别对应的防伪点分类特征进行合并,得到视频帧T1对应的防伪点融合特征20h。基于上述获取防伪点融合特征 20h的过程,后台服务器可以获取N个视频帧分别对

应的防伪点融合特征,即获取与视频数据20a相关联的N个防伪点融合特征。

[0087] 进一步地,可以根据N个视频帧在视频数据20a中的时间顺序,将N个防伪点融合特征依次输入时序分类网络20i中,该时序分类网络20i可以为长短期记忆网络(Long Short Term Memory Networks,LSTM),σ和tanh可以表示为不同激活函数;在时序分类网络20i中,前一个视频帧的输出结果可以与下一个视频帧的防伪点融合特征一起输入至时序分类网络20j,如视频帧T1在时序分类网络20j中的输出结果可以与视频帧T2对应的防伪点融合特征共同输入时序分类网络20j中;进而可以通过时序分类网络20i获取N个防伪点融合特征之间的时序分布特征,根据时序分布特征可以确定视频数据20a中所包含的身份证件对应的证件鉴别结果。当证件鉴别结果为合法鉴别结果时,可以确定该用户所提供的身份证件为合法证件,进而为该用户继续执行开户流程;当证件鉴别结果为伪造鉴别结果时,可以确定该用户所提供的身份证件为伪造证件,为该用户取消开户流程,提醒用户重新提供新的身份证件所对应的视频数据,再次触发虚拟银行的开户流程。本申请实施例中,通过包含M个卷积神经网络和时序分类网络20j的鉴别模型,对视频数据20a所包含的身份证件进行鉴别,可以提高身份证件的鉴别准确度。

[0088] 需要说明的是,用户身份证件的防伪点信息是公开的,如一代身份证件的公开防伪点(即权威机构提供的官方防伪点)包括9个,请一并参见图3,图3 是本申请实施例提供的一种身份证件的防伪点示意图。如图3所示,一代身份证的公开防伪点可以包括:一代身份证的正面携带光学变色油墨,即身份证件中的插卡方向图标不同角度下可以看到不同的颜色;一代身份证的正面携带扭索图案;一代身份证的正面和反面均携带微缩文字印刷;一代身份证的正面具有渐淡色的背景;一代身份证携带紫外线照射点;一代身份证具有彩虹印刷;一代身份证的正面携带动感印刷,即一定角度下可以看到身份证的正面具有“H”字符,从不同角度可以看到身份证的正面具有“K”字符;一代身份证携带浮雕;一代身份证在不同角度看具有多重激光影像,如在不同角度下看到的字符清晰度是不一样的。可选的,在本申请实施例中,除了采用权威机构公开的官方防伪点对身份证件进行鉴伪之外,还可以增加一些用于鉴伪的非官方防伪点,如身份证所包含的数学特征、身份证件的特定区域等非官方防伪点,在对身份证件进行鉴伪时,引入更多的防伪点,可以提高身份证件的鉴别准确率。

[0089] 请参见图4,图4是本申请实施例提供的一种数据鉴伪方法的流程示意图。可以理解地,该数据处理方法可以由计算机设备执行,该计算机设备可以为用户终端,或者为服务器,或者为用户终端和服务器组成的系统,或者为一个计算机程序应用(包括程序代码),这里不做具体限定。如图4所示,该数据鉴伪方法可以包括以下步骤:

[0090] 步骤S101,获取视频数据所包含的N个视频帧,获取N个视频帧中每个视频帧分别包含的M个防伪点区域;N个视频帧包括待鉴伪的目标对象,N和M 均为正整数。

[0091] 具体的,在针对目标对象的鉴伪场景中,目标对象本身可以包含静态防伪点和动态防伪点,其中,静态防伪点可以是指目标对象中的细致网格和背景纹路等信息,通常可以通过高像素对焦完好的摄像设备对目标对象进行拍摄,所获得的拍摄照片可以捕捉到目标对象中的静态防伪点;动态防伪点可以是指目标对象中可以根据不同角度或者不同光线进行变换的防伪点,通过摄像设备所拍摄的单张照片通常无法捕捉到目标对象中的动态防伪点。如图3所示,扭索图案、缩微文字印刷、渐淡色的背景、浮雕等防伪点可以称为静态防伪

点,不同角度的光学变色油墨、不同角度的动感印刷以及不同角度的多重激光影像等防伪点可以称为动态防伪点。本申请实施例中,目标对象可以包括但不限于:不同类型的证件(如不同区域的居民身份证件、护照、军官证等用于表征居民身份的其他证件)、钞票(如人民币)、古玩物件(如古董书画、古董瓷器等)。不同的目标对象具有不同的静态防伪点和动态防伪点,为方便描述,下面将静态防伪点和动态防伪点统称为防伪点。

[0092] 为了更准确地捕捉到目标对象所包含的防伪点,计算机设备可以采用摄像设备采集目标对象对应的视频数据(如上述图2所对应实施例中的视频数据20a),在视频数据中获取N个视频帧,根据目标对象所包含的防伪点信息,对N个视频帧中的每个视频帧均进行分割处理,从每个视频帧中获取M个防伪点区域,该M个防伪点区域均可以输入对象鉴别模型中。其中,N和M均为正整数,N 可以预先进行人为设置,如N可以为1,2,3……;M的取值与目标对象所包含的防伪点数量相关联,M可以是指目标对象在鉴伪过程中所使用的防伪点数量,目标对象在鉴伪过程中所使用的防伪点可以包括目标对象对应的全部公开防伪点,或者可以包括目标对象对应的全部公开防伪点和一部分非公开的防伪点(即仅在本申请实施例中用于鉴别目标对象的防伪点),或者可以包括目标对象对应的部分公开防伪点和部分非公开的防伪点,本申请实施例中,可以根据实际需求确定鉴伪过程中所使用的防伪点。用于采集视频数据的摄像设备可以为计算机设备中内接的摄像组件(如计算机设备自带的照相机),或者为与计算机设备具有通信连接的外接摄像设备,外接摄像设备采集到目标对象对应的视频数据后,可以将采集到的视频数据传输至计算机设备。

[0093] 其中,从视频数据中获取N个视频帧的过程可以包括:计算机设备可以对摄像设备所采集的视频数据进行分帧处理,得到该视频数据对应的视频帧序列,进而可以根据间隔时间信息在视频帧序列中,从头到尾获取N个视频帧;计算机设备可以获取视频数据中的目标对象所对应的对象类型,并获取与对象类型相关联的防伪点信息;对于N个视频帧中的视频帧T_i,计算机设备可以根据防伪点信息对视频帧T_i进行分割,得到视频帧T_i中的M个防伪点区域。其中,i 为小于或等于N的正整数,即i的最小取值为1,最大取值为N,上述防伪点信息可以为防伪点在目标对象中的位置区域和目标对象中的防伪点数量等信息。视频帧序列所包含的每个视频帧的时长可以默认是相同的,由于相邻视频帧中所包含的特征信息是相似的,因此计算机设备可以根据间隔时间信息从视频帧序列中均匀获取N个视频帧,如视频帧序列所包含的视频帧的数量为50,N取值为10,则在视频帧序列中每5个视频帧抽取一个视频帧。若计算机设备获取到目标对象所对应的防伪点信息为:防伪点1位于目标对象的位置1,防伪点2 位于目标对象的位置2,防伪点3位于目标对象的位置3,则根据位置1、位置 2以及位置3,对视频帧T_i进行分割,获取视频帧T_i中防伪点1对应的防伪点区域1、防伪点2对应的防伪点区域2以及防伪点3对应的防伪点区域3。

[0094] 请一并参见图5,图5是本申请实施例提供的一种在视频帧中获取防伪点区域的示意图。如图5所示,假设N取值为30,计算机设备可以获取包含目标对象的视频数据30a,通过对视频数据30a进行分帧处理,得到该视频数据30a对应的视频帧序列30b,如视频数据30a可以划分为180个视频帧,此时的视频帧序列30b可以包括180个视频帧,分别表示为视频帧T1,视频帧T2,……,视频帧T180。计算机设备可以从视频帧序列30b中从头到尾均匀获取30个视频帧,即从视频帧序列30b所包含的180个视频帧中,每6个视频帧选取一个视频帧,如从视频帧T1至视频帧T6中选取视频帧T1,从视频帧T7至视频帧T12中选取视频帧T7,……,

从视频帧T175至视频帧T180中选取视频帧T175,以获取30个视频帧。可选的,计算机设备还可以从视频帧T1至视频帧T6中任意选取一个视频帧,从选中的视频帧开始,每6个视频帧选取一个视频帧,以获取 30个视频帧。例如,可以从视频帧T1至视频帧T6中选取视频帧T2,从视频帧 T7至视频帧T12中选取视频帧T8,……,从视频帧T175至视频帧T180中选取视频帧T176。

[0095] 进一步地,计算机设备可以对30个视频帧中的每个视频帧均进行分割处理,下面以30个视频帧中的视频帧T1为例,根据目标对象对应的防伪点信息对视频帧T1进行分割。如图5所示,目标对象对应的防伪点信息包括防伪点1、防伪点2、防伪点3以及防伪点4,根据防伪点1、防伪点2、防伪点3以及防伪点4分别在视频帧T1中的位置,对该视频帧T1进行分割,得到包含防伪点1 的区域1、包含防伪点2的区域2、包含防伪点3的区域3以及包含防伪点4的区域4,其中,区域1、区域2、区域3以及区域4均可以作为视频帧T1中的防伪点区域,此时的M为4。

[0096] 步骤S102,根据每个视频帧分别包含的M个防伪点区域,生成N个视频帧分别对应的防伪点融合特征。

[0097] 具体的,计算机设备可以获取对象鉴别模型,该对象鉴别模型可以用于识别视频数据所包含的目标对象的真实性,将每个视频帧分别包含的M个防伪点区域输入对象鉴别模型的卷积神经网络中,通过卷积神经网络输出每个防伪点区域中的防伪点分类特征,将每个视频帧分别对应的M个防伪点分类特征进行合并,得到N个视频帧分别对应的防伪点融合特征。其中,对象鉴别模型可以包括至少M个卷积神经网络和时序分类网络,每个卷积神经网络均可以看成一个网络分支,卷积神经网络可以用于提取防伪点区域中的防伪点分类特征,时序分类网络可以用于对N个视频帧分别对应的防伪点融合特征进行处理,获取 N个防伪点融合特征之间的时序分布特征,以确定视频数据所包含的目标对象对应的对象鉴别结果。需要说明的是,对象鉴别模型中所包含的卷积神经网络之间是相互独立的,各卷积神经网络可以具有相同的网络结构,也可以具有不同的网络结构,但是各卷积神经网络之间的网络参数肯定是不一样的。

[0098] 其中,卷积神经网络包括但不限于:AlexNet模型(一种卷积神经网络模型)、VGG模型(一种深度卷积神经网络模型)、GooLeNet模型(一种深度卷积神经网络模型)、ResNet模型(一种残差网络模型)、DenseNet模型(一种稠密连接网络模型)、MobileNet模型(一种轻量的卷积神经网络)、NasNet模型(一种用于识别图像的卷积神经网络模型),当然,卷积神经网络还可以为两个或两个以上的模型的组合,或者为对上述模型进行结构调整后的新模型(例如,本申请实施例中所使用的卷积神经网络可以为NasNet-Mobile网络,该NasNet-Mobile网络是NasNet模型削减参数后所得到的新模型);时序分类网络包括但不限于:循环神经网络(Rerrent Neural Network,RNN)、长短期记忆网络(Long Short Term Memory Networks,LSTM)、门控循环单元(Gated Recurrent Units,GRU)、时序卷积神经网络(Temporal Convolutional Network, TCN)。

[0099] 下面以N个视频帧中的视频帧T_i为例,对于视频帧T_i所包含的M个防伪点区域中的任意一个防伪点区域R_j,可以在对象鉴别模型所包含的所有卷积神经网络分支中获取与该防伪点区域R_j相匹配的目标卷积神经网络(该对象鉴别模型可以包括用于识别不同防伪点的卷积神经网络),j为小于或等于M的正整数,即j的最小取值为1,最大取值为M;计算机设

备可以将防伪点区域R_j输入至目标卷积神经网络,根据目标卷积神经网络中的卷积层,对防伪点区域R_j进行卷积处理,得到防伪点区域R_j对应的防伪点分类特征;通过对象鉴别模型中与M个防伪点区域分别匹配的卷积神经网络,可以获取M个防伪点区域分别对应的防伪点分类特征,将视频帧T_i对应的M个防伪点分类特征进行合并,得到视频帧T_i对应的防伪点融合特征。换言之,计算机设备可以将M个防伪点区域分别输入至各自对应的卷积神经网络,在各自对应的卷积神经网络中对M个防伪点区域进行并行处理,获取每个防伪点区域中的防伪点分类特征;计算机设备可以采用上述方式,获取N个视频帧分别对应的防伪点融合特征。

[0100] 举例来说,假设N为30,M为3(防伪点的数量为3),视频帧T_i中的i 可以取值为1,2,……,30,防伪点区域R_j中的j可以取值为1,2,3。对于 30个视频帧中的视频帧T_1(i=1),计算机设备可以从视频帧T_1中获取防伪点区域R_1、防伪点区域R_2、防伪点区域R_3,从对象鉴别模型中分别确定与防伪点区域R_1相匹配的卷积神经网络1,与防伪点区域R_2相匹配的卷积神经网络2以及与防伪点区域R_3相匹配的卷积神经网络3。计算机设备可以将防伪点区域R_1输入卷积神经网络1中,通过卷积神经网络1可以获取防伪点区域R_1对应的防伪点分类特征1;将防伪点区域R_2输入卷积神经网络2中,通过卷积神经网络2 可以获取防伪点区域R_2对应的防伪点分类特征2;将防伪点区域R_3输入卷积神经网络3中,通过卷积神经网络3可以获取防伪点区域R_3对应的防伪点分类特征3,将防伪点分类特征1、防伪点分类特征2以及防伪点分类特征3进行合并,可以得到视频帧T_1对应的防伪点融合特征。

[0101] 其中,各卷积神经网络中可以包括一个或者多个卷积层,每个卷积层均可以对输入数据进行卷积处理,以卷积神经网络1中的任意一个卷积层为例,对防伪点区域R_1的卷积处理过程进行描述。每个卷积层可以对应一个或多个卷积核(kernel,也可以称为滤波器,或者称为感受野),卷积处理可以是指卷积核与防伪点区域R_1对应的输入矩阵进行矩阵乘法运算,卷积运算后的输出图像特征的行数H_{out}和列数W_{out}是由输入矩阵的大小、卷积核的大小、步长(stride) 以及边界填充(padding)共同决定的,即$H_{out}=(H_{in}-H_{kerner}+2*padding)/stride+1$, $W_{out}=(W_{in}-W_{kerner}+2*padding)/stride+1$。$H_{in}$,$H_{kerner}$分别表示输出图像特征的行数和卷积核的行数;$W_{in}$,$W_{kerner}$分别表示输入矩阵的列数和卷积核的列数。当卷积神经网络1中仅包含一个卷积层时,该卷积层输出的图像特征可以作为防伪点分类特征1;当卷积神经网络1包括多个卷积层时,前一个卷积层的输出图像特征可以作为后一个卷积层的输入,最后一个卷积层输出的图像特征可以作为防伪点分类特征1。可选的,卷积神经网络1还可以包括池化层、归一化层以及全连接层等,该卷积神经网络1中最后一个网络层的输出结果可以称为防伪点分类特征1。

[0102] 其中,计算机设备对防伪点分类特征1、防伪点分类特征2以及防伪点分类特征3的合并过程可以为拼接过程,如防伪点分类特征1表示为[0.1,0.2,0.1, 0.6],防伪点分类特征2表示为[0.2,0.05,0.25,0.5],防伪点分类特征3表示为[0.15,0.15,0,0.7],此时视频帧T_1对应的防伪点融合特征可以表示为[0.1, 0.2,0.1,0.6,0.2,0.05,0.25,0.5,0.15,0.15,0,0.7]。30个视频帧所对应的防伪点分类特征的合并顺序是相同的,如视频帧T_1对应的防伪点融合特征是按照防伪点A所对应的防伪点分类特征1、伪点B所对应的防伪点分类特征2 以及伪点C所对应的防伪点分类特征3的顺序进行合并的,则其余视频帧对应的防伪点融合特征同样需要按照防伪点A、防伪点B以及防伪点C所对应的防伪点分类特征的顺序

进行合并。

[0103] 基于与上述视频帧T_1相同的处理过程,计算机设备可以得到30个视频帧分别对应的防伪点融合特征。30个视频帧中每个视频帧均可以包含3个防伪点区域,每个视频帧均与上述卷积神经网络1、卷积神经网络2以及卷积神经网络3 相关联。

[0104] 步骤S103,根据N个视频帧在视频数据中的时间顺序,构建包含N个防伪点融合特征的特征序列,根据特征序列生成视频数据对应的时序分布特征,根据时序分布特征确定目标对象对应的对象鉴别结果。

[0105] 具体的,计算机设备可以按照N个视频帧在视频数据中的时间顺序,即N 个视频帧在视频帧序列中的排列顺序,构建包含N个防伪点融合特征的特征序列,将特征序列中的N个防伪点融合特征依次输入至对象鉴别模型中的时序分类网络,在时序分类网络中可以获取N个防伪点融合特征之间的时序分布特征;将时序分布特征输入至对象鉴别模型中的全连接层,通过全连接层可以输出目标特征向量,根据目标特征向量确定目标对象对应的对象鉴别结果。通过对象鉴别模型中的各卷积神经网络输出视频帧T_1所包含的M个防伪点区域分别对应的防伪点分类特征后,可以将M个防伪点分类特征合并为视频帧T_1对应的防伪点融合特征x1,进而将防伪点融合特征x1输入至对象鉴别模型中的时序分类网络,在时序分类网络中对防伪点融合特征x1进行处理;与此同时,对象鉴别模型中的各卷积神经网络可以对视频帧T_2所包含的M个防伪点区域进行特征提取,获取视频帧T_2所包含的M个防伪点区域分别对应的防伪点分类特征,将视频帧 T_2所对应的M个防伪点分类特征合并为视频帧T_2的防伪点融合特征x2,进而可以将防伪点融合特征x2输入至时序分类网络,在时序分类网络中对防伪点融合特征x2进行处理;以此类推,N个视频帧所对应的防伪点融合特征依次输入至时序分类网络,通过时序分类网络可以获取N个防伪点融合特征之间的时序分布特征。

[0106] 其中,下面以时序分布网络是LSTM网络(LSTM网络的结构如上述图2 所对应实施例中的时序分类网络20i所示)为例,对特征序列的处理过程进行描述。首先对特征序列所包含的N个防伪点融合特征进行正向编码,计算机设备初始化隐藏状态向量h10,在t11时刻,将特征序列中位于首位的防伪点融合特征x1、隐藏状态向量h10输入LSTM网络,根据公式(1)计算t11时刻的隐藏状态向量h11,公式(1)表示如下:

[0107] $$i_t=\sigma(W_{xi}x_t+W_{hi}h_{t-1}+W_{ci}c_{t-1}+b_i) \quad (1)$$

[0108] $$f_t=\sigma(W_{xf}x_t+W_{hf}h_{t-1}+W_{cf}c_{t-1}+b_f)$$

[0109] $$c_t=f_tc_{t-1}+i_t\tanh(W_{xc}x_t+W_{hc}h_{t-1}+b_c)$$

[0110] $$o_t=\sigma(W_{xo}x_t+W_{ho}h_{t-1}+W_{co}c_t+b_o)$$

[0111] $$h_t=o_t\tanh(c_t)$$

[0112] 其中,σ(.)表示为激活函数,i,f,o分别表示为LSTM网络中的输入门、遗忘门、输出门。所有的W用于表示两门之间的权重矩阵。在特征序列的编码过程中,整个LSTM网络中的参数是共享的,即在计算每一个时刻的隐藏状态向量时,上述参数都不变。

[0113] 在t12时刻,将特征序列中位于第二位的防伪点融合特征x2、t11时刻的隐藏状态向量h11输入LSTM网络,根据公式(1)再计算t12时刻的隐藏状态向量h12;在t13时刻,同样根据公式(1)计算t13时刻的隐藏状态向量h13。换言之,t时刻的隐藏状态向量ht是由t-1时刻的隐藏状态向量h(t-1)和t时刻的防伪点融合特征xt决定的,不断地迭代,直至最后一次

迭代得到隐藏状态向量h1N,将隐藏状态向量h11、h12、...、h1N组合为正向编码矩阵,正向编码矩阵的尺寸可以表示为:N×L,其中N表示防伪点融合特征的数量,L表示每个防伪点融合特征正向编码后的隐藏状态向量的维数。

[0114] 进一步地,还可以对特征序列所包含的N个防伪点融合特征进行反向编码,计算机设备可以初始化隐藏状态向量h20,在t21时刻,将特征序列中位于末位的防伪点融合特征xN、隐藏状态向量h20输入LSTM网络,根据公式(1)计算t21时刻的隐藏状态向量h21;在t22时刻,将特征序列中位于倒数第二位的防伪点融合特征x(N-1)、t21时刻的隐藏状态向量h21输入LSTM网络,根据公式(1)计算t22时刻的隐藏状态向量h22。和正向循码相同,t时刻的隐藏状态向量ht是由t-1时刻的隐藏状态向量h(t-1)和t时刻的防伪点融合特征x(N+1-t) 决定的,不断地迭代,直至最后一次迭代得到隐藏状态向量h2N,将隐藏状态向量h21、h22、...、h2N组合为反向编码矩阵。反向编码矩阵的尺寸可以表示为:N×L,其中N表示防伪点融合特征的数量,L表示每个防伪点融合特征反向编码后的隐藏状态向量的维数。

[0115] 正向编码和反向循环编码的过程除了输入防伪点融合特征的顺序不同(正向编码是从前往后输入,反向编码是从后往前输入),其余的过程都相同,这是为了保证即使特征序列中包含的防伪点融合特征非常多,防伪点融合特征的时序信息也不会随着序列而消减。

[0116] 计算机设备将正向编码矩阵与反向编码矩阵拼接为隐藏状态矩阵,可以知道隐藏状态矩阵的尺寸为N×2L,此时的隐藏状态矩阵可以确定为视频数据对应的时序分布特征。

[0117] 进一步地,将时序分布特征输入对象鉴别模型的全连接层中,通过全连接层可以将时序分布特征转换为目标特征向量,目标特征向量可以包括合法评估值和伪造评估值两个数值;若合法评估值大于伪造评估值,则可以确定目标对象对应的对象鉴别结果为合法鉴别结果,即视频数据所包含的目标对象为合法对象;若合法评估值小于伪造评估值,则可以确定目标对象对应的对象鉴别结果为伪造鉴别结果,即视频数据所包含的目标对象为伪造对象。换言之,该目标特征向量可以是一个维度为2的向量,该目标特征向量可以用于表示目标对象的二分类结果(合法鉴别结果和伪造鉴别结果),如目标特征向量表示为[a,b],a用于表示伪造评估值,b用于表示合法评估值,当a>b时,表示目标对象为伪造对象,当a<b时,表示目标对象为合法对象。

[0118] 可选的,本申请实施例中的对象鉴别模型可以应用在业务机构(例如,银行等金融机构)的业务办理(例如,用户开户等业务)中,此时的视频数据可以为目标用户在业务机构办理开户业务时所提供的身份证视频数据,该视频数据种所包含的目标对象为身份证件;若计算机设备通过对象鉴别模型确定身份证件的对象鉴别结果为合法鉴别结果,则在业务机构中继续执行针对目标用户的开户业务;若计算机设备通过对象鉴别模型确定身份证件的对象鉴别结果为伪造鉴别结果,则可以确定目标用户在业务机构中的开户业务办理结果为开户失败结果,即目标用户所提供的身份证件为伪造证件,该目标用户可能为非法用户,该开户失败结果可以用于指示目标用户提供新的身份证视频数据,即该目标用户需要重新提供新的身份证件来证明其身份是合法的。本申请实施例中的对象鉴别模型可以用于区分防伪点的动态变化,因此该对象鉴别模型可以应用在不同类型身份证件的高仿鉴伪场景中,还可以应用在任意具有动态防伪点的证件鉴伪场景中进行高仿假证识别;当然,该对象鉴别模型还可以应用在低仿证件的识别中(如证件的复印,打印,翻拍等),低仿证件(如复

印、打印以及翻拍的证件)视频中的防伪点不会改变亮度或颜色,而真正的证件会改变亮度或颜色,因此通过防伪点的颜色或亮度变化,可以识别低仿证件。

[0119] 请一并参见图6,图6是本申请实施例提供的一种业务办理中对身份证件进行鉴伪的示意图。如图6所示,用户小A可以在所使用的终端设备40a中对银行应用执行触发操作,终端设备40a可以响应针对银行应用的触发操作,在终端设备40a中显示银行应用的主页,用户小A可以在银行应用的主页中触发开户办理选项,终端设备40a可以响应针对开户办理选项的触发操作,在银行应用所对应客户端中显示开户业务办理页面,该业务办理页面可以包括用户个人信息输入框,如用户姓名输入框、用户性别输入框、用户联系方式输入框、证件类型输入框以及证件视频数据上传控件等。用户小A可以在用户姓名输入框中输入“小A”,在用户性别输入框中输入“男”,在用户联系方式输入框中输入“13xxxxxx21”,在证件类型输入框中输入“一代身份证”等信息。对于开户办理业务中所需要的证件视频,若终端设备40a中存在用户小A所对应身份证件40c的视频数据,则用户小A可以通过开户办理页面中的“上传”功能控件,将终端设备40a所存储的视频数据上传至银行应用所对应的客户端;若终端设备40a中不存在用户小A所对应身份证件40c的视频数据,则用户小A 可以触发开户办理页面中的功能控件40b,实时拍摄身份证件40c的视频数据。用户小A可以按照开户办理页面中的提示信息“证件视频需要包括证件的正面和反面,需要从不同角度拍摄视频”拍摄自己的身份证件40c,拍摄完成后,用户小A可以触发控件40d,将实时拍摄到的视频数据上传至银行应用所对应的客户端。当然,用户小A若不满意拍摄的视频数据,可以取消拍摄的视频数据,对身份证件40c进行重新拍摄。

[0120] 用户小A将拍摄的视频数据上传至银行应用所对应的客户端后,该银行应用的客户端可以对用户小A上传的视频数据进行初步检验(如检验用户小A拍摄的视频是否包含身份证件40c的正面和反面,视频数据是否是从不同角度拍摄的),若视频数据初步检验合格,则可以在开户办理页面中显示初步检验合格的视频数据40e,并在开户办理页面中显示提示信息“拍摄视频符合要求”;若视频数据初步检验不合格,则可以在开户办理页面中显示提示信息“拍摄视频不符合要求,请重新拍摄视频数据”。

[0121] 进一步地,对于初步检验合格的视频数据40e,银行应用的客户端可以将用户小A拍摄的视频数据40e传输至银行应用的后台服务器,后台服务器可以对视频数据40e所包含的身份证件40c进行鉴伪,其中,鉴伪过程可以参见上述图4所对应实施例中对步骤S101-步骤S103的描述,这里不再进行赘述。若后台服务器通过对视频数据40e中的身份证件40c进行鉴伪,确定身份证件40c为合法证件,则可以继续在银行应用中为用户办理开户业务;若后台服务器通过对视频数据40e中的身份证件40c进行鉴伪,确定身份证件40c为伪造证件,则可以将鉴别结果(伪造证件)传输给银行应用所对应的客户端,在银行应用的客户端中可以显示提示信息40f(“视频所包含的身份证件为伪造证件,请重新提供新的身份证件,否则开户办理失败”),如用户小A可以在规定时间内(如半个小时,此时可以在开户办理页面中显示视频上传倒计时)重新上传包含新的身份证件的视频数据,并由银行应用的后台服务器对新的身份证件进行鉴伪;若用户小A在规定时间内未重新上传包含新的身份证件的视频数据,则可以确定用户小A此次开户办理业务失败,结束用户小A的开户办理业务。

[0122] 可选的,本申请实施例中的对象鉴别模型可以应用在钞票鉴伪场景中,计算机设备获取到钞票对应的视频数据后,可以将该视频数据输入对象鉴别模型中,通过该对象鉴

别模型得到钞票的鉴别结果,根据鉴别结果确定该钞票的真实性。可选的,该对象鉴别模型可以封装在验钞机中,该验钞机可以对钞票进行扫描,获取钞票的视频数据,进而采用验钞机中封装的对象鉴别模型,对钞票进行鉴伪,以鉴别钞票的真实性,可以提高钞票的鉴别准确度。

[0123] 可选的,本申请实施例中的对象模型还可以应用在古董鉴伪场景中,对于爱好古董的用户,在购买古董物件时,往往需要请相关的古董鉴别专家来鉴定古董的真实性;而将对象鉴别模型应用在古董鉴伪场景后,该用户只需拍摄一段包含古董的视频数据,并将该视频数据上传至古董鉴别应用中,通过对象鉴别模型对上传至古董鉴别应用的视频数据进行处理,输出古董的鉴别结果,用户可以根据古董的鉴别结果确定古董的真实性,无需请古董鉴别专家进行人工鉴伪,可以提高古董的鉴伪效率。

[0124] 本申请实施例中,通过获取目标对象对应的视频数据,可以从视频数据中获取不同防伪点在相同视频帧中的特征信息,也可以获取相同防伪点在不同视频帧中的特征信息,通过将相同视频帧中不同防伪点的特征信息进行融合,以得到每个视频帧对应的防伪点融合特征,进而可以获取每个视频帧所对应的防伪点融合特征之间的时序分布特征,该时序分布特征可以用于表征该目标对象在不同视觉角度下的特征信息,可以提高目标对象的鉴别准确度;使用的对象鉴别模型中可以包含分别用于识别每个防伪点的卷积神经网络,卷积神经网络可以对每个帧视频帧所包含的M个防伪点区域进行并行处理,即每个卷积神经网络均可以进行独立工作,互不影响,进而可以将各卷积神经网络所输出的结果进行融合,并输入至时序分类网络中,通过时序分类网络可以输出视频数据对应的对象鉴别结果,可以提高视频数据的识别效率。

[0125] 可以理解的是,采用对象鉴别模型对视频数据中的目标对象进行鉴伪之前,还需要对对象鉴伪模型进行训练,以确保对象鉴别模型针对目标对象的鉴别准确率。下面通过图7和图8对对象鉴别模型的训练过程进行具体描述。

[0126] 请参见图7,图7是本申请实施例提供的一种数据鉴伪方法的流程示意图。可以理解地,该数据处理方法可以由计算机设备执行,该计算机设备可以为用户终端,或者为服务器,或者为用户终端和服务器组成的系统,或者为一个计算机程序应用(包括程序代码),这里不做具体限定。如图7所示,该数据鉴伪方法可以包括以下步骤:

[0127] 步骤S201,获取样本视频数据所包含的N个样本视频帧,获取N个样本视频帧中每个样本视频帧分别包含的M个样本防伪点区域;N个样本视频帧包括样本对象,样本视频数据携带针对样本对象的标签信息,N和M均为正整数。

[0128] 具体的,将训练阶段中的对象鉴别模型称为初始鉴别模型(即未完成训练的对象鉴别模型),用于训练初始鉴别模型的样本视频数据可以是指包含不同类型证件的视频数据,或者包含钞票的视频数据,或者包含古董玩物的视频数据等,即样本视频数据所包含的样本对象可以包括不同类型证件、钞票以及古董万物等携带防伪点的对象,本申请对样本视频数据所包含的样本对象的类型不做具体限定,为方便描述,本申请实施例均以样本对象是身份证件为例,对初始鉴别模型的训练过程进行描述。

[0129] 通过摄像设备可以采集真实身份证件的视频数据和伪造身份证件的视频数据,进而可以采用人工标注或者标注工具自动标注的方式,对采集到的每个视频数据标注标签信息,该标签信息可以包括视频数据所包含的身份证件的真伪标签,以及身份证件中每个防

伪点分别对应的防伪点标签。换言之,视频数据除了携带真伪标签之外,对身份证件的每个防伪点(尤其是动态防伪点)均进行细致标注,得到每个防伪点分别对应的防伪点标签,将携带真伪标签和防伪点标签的视频数据确定为样本视频数据。例如,用于训练初始鉴别模型的样本视频数据可以包括一代身份证件的视频数据和二代身份证件的视频数据,一代身份证件包括“HK”防伪点、人脸防伪点以及数字防伪点等防伪点,“HK”防伪点对应的防伪点标签可以包括但不限于:“H”标签、“K”标签、分不清标签,人脸防伪点对应的防伪点标签可以包括但不限于:五官可见标签、五官不可见标签,数字防伪点对应的防伪点标签可以包括但不限于:清晰标签、模糊标签、看不见标签。二代身份证件包括三角区域防伪点、全息图防伪点以及人脸防伪点等防伪点,三角区域防伪点对应的防伪点标签包括但不限于:看不到标签、模糊标签、清晰标签、指纹装标签,全息图防伪点对应的防伪点标签包括但不限于:彩色标签、红黄色标签、无色标签,人脸防伪点对应的防伪点标签可以包括但不限于:清晰标签、模糊标签。

[0130] 可选的,为了增加样本视频数据的数据量,可以采取平移旋转、随机加白噪声等增强方法,对样本视频数据进行增广,例如,对样本视频数据1进行平移旋转,将平移旋转后的样本视频数据1确定为新的样本视频数据3;或者对样本视频数据2随机加白噪声,将加白噪声后的样本视频数据2确定为新的样本视频数据4等。

[0131] 可选的,计算机设备还可以将每个样本视频数据平均划分为N个样本视频片段,分别对每个样本视频片段进行分帧处理,得到每个样本视频片段分别对应的样本视频帧序列,进而可以分别在N个样本视频帧序列中随机选取样本视频帧,得到样本视频数据中的N个样本视频帧,此时的N个样本视频帧可以作为训练初始鉴别模型的视频序列,N为正整数,本申请实施例中的N可以预先进行人为设置。例如,将样本视频数据平均划分为3个样本视频片段(此时N 的取值为3),对N个样本视频片段进行分帧处理,得到每个样本视频片段分别对应样本视频帧序列,样本视频片段1对应的样本视频序列1包括视频帧1、视频帧2、视频帧3,样本视频片段2对应的样本视频序列2包括视频帧4、视频帧5、视频帧6,样本视频片段3对应的样本视频序列3包括视频帧7、视频帧8、视频帧9。计算机设备可以分别从样本视频序列1、样本视频序列2以及样本视频序列3中随机选取一个视频帧,将随机选取的3个视频帧作为训练初始鉴别模型的样本视频帧,如视频帧1、视频帧4、视频帧7可以作为训练初始鉴别模型的样本视频帧,视频帧1、视频帧5、视频帧8同样可以作为训练初始鉴别模型的样本视频帧等。

[0132] 对于N个样本视频帧中的任一样本视频帧,计算机设备均可以根据样本对象对应的防伪点信息,对每个样本视频帧进行分割,获取每个样本视频帧分别包含的M个样本防伪点区域。其中,上述防伪点信息可以为防伪点在样本对象中的位置区域和样本对象中的防伪点数量等信息;M个样本防伪点区域的获取过程可以参见上述图4所对应实施例的步骤S101中,对M个防伪点区域的获取过程的描述,这里不再进行赘述。

[0133] 步骤S202,将每个样本视频帧分别包含的M个样本防伪点区域输入至初始鉴别模型中的初始卷积神经网络,通过初始卷积神经网络,生成N个样本视频帧分别对应的样本防伪点融合特征。

[0134] 具体的,计算机设备可以获取还未进行训练的初始鉴别模型,此时的初始鉴别模型可以是指对网络参数进行初始化处理后的鉴别模型,将每个样本视频帧分别包含的M个

样本防伪点区域输入至初始鉴别模型中的初始卷积神经网络,通过初始卷积神经网络对输入的样本防伪点区域进行卷积处理,可以生成N个样本视频帧分别对应的样本防伪点融合特征。需要说明的是,初始鉴别模型可以包括M个或以上的初始卷积神经网络,一个防伪点可以对应一个初始卷积神经网络,即包含同一个防伪点的样本防伪点区域均可以输入至同一个初始卷积神经网络中,对于一个样本视频帧所包含的M个样本防伪点区域,该M个样本防伪点区域可以分别输入至各自对应的初始卷积神经网络,通过初始卷积神经网络输出每个样本防伪点区域分别对应的样本防伪点分类特征,将M个样本防伪点分类特征进行合并,得到每个样本视频帧对应的样本防伪点融合特征。其中,样本防伪点融合特征的生成过程可以参见上述图4所对应实施例的步骤 S102中,对防伪点融合特征的生成过程的描述,这里不再进行赘述。

[0135] 步骤S203,根据N个样本视频帧在样本视频数据中的时间顺序,将N个样本防伪点融合特征依次输入至初始鉴别模型中的初始时序分类网络。

[0136] 具体的,计算机设备在获取到N个样本视频帧分别对应的样本防伪点融合特征后,可以根据N个样本视频帧在样本视频数据中的时间顺序,将N个样本防伪点融合特征依次输入至初始鉴别模型中的初始时序分类网络。

[0137] 本申请实施例中,为方便描述,下面均以初始卷积神经网络是NasNet-Mobile 网络,初始时序分类网络是LSTM为例,对初始鉴别模型的训练过程进行描述。

[0138] 步骤S204,通过初始时序分类网络,生成样本视频数据对应的样本时序分布特征,根据样本时序分布特征确定样本对象对应的样本鉴别结果。

[0139] 具体的,计算机设备可以在初始时序分类网络中可以获取N个样本防伪点融合特征之间的样本时序分布特征,将样本时序分布特征输入至初始鉴别模型中的全连接层,通过该全连接层可以确定样本对象对应的样本鉴别结果。其中,在初始时序分类网络中对N个样本防伪点融合特征的处理过程(可以理解为确定样本鉴别结果的过程),可以参见上述图4所对应实施例的步骤S103中对N 个防伪点融合特征的处理过程(可以理解为对象鉴别结果的确定过程),这里不再进行赘述。

[0140] 步骤S205,根据标签信息、样本鉴别结果以及N个样本防伪点融合特征,对初始鉴别模型的网络参数进行修正,将包含修正后的网络参数的初始鉴别模型确定为对象鉴别模型;对象鉴别模型用于识别视频数据所包含的目标对象对应的对象鉴别结果。

[0141] 具体的,计算机设备可以根据样本视频数据的真伪标签与样本鉴别结果之间的映射关系,以及N个样本防伪点融合特征与防伪点标签之间的映射关系,对初始鉴别模型进行训练。初始鉴别模型可以包括一个或者多个卷积神经网络,初始鉴别模型所包含的初始卷积神经网络的数量可以根据实际需求进行设置,本申请实施例对初始卷积神经网络的数量不做限定。计算机设备可以根据真伪标签和样本鉴别结果构建初始时序分类网络的损失函数,根据样本视频数据所包含的防伪点标签和样本防伪点分类特征构建各初始卷积神经网络的损失函数,进而可以根据各初始卷积神经网络的损失函数和初始时序分类网络的损失函数构建整个初始鉴别模型从端到端的损失函数。

[0142] 例如,初始鉴别模型可以包括初始卷积神经网络1、初始卷积神经网络 2、……、初始卷积神经网络M;初始卷积神经网络1可以输出样本防伪点区域 1对应的样本防伪点分类特征1,该样本防伪点区域1对应于防伪点标签1,初始卷积神经网络2可以输出样本防伪点

区域2对应的样本防伪点分类特征2,该样本防伪点区域2对应于防伪点标签2,……,初始卷积神经网络M可以输出样本防伪点区域M对应的样本防伪点分类特征M,该样本防伪点区域M对应于防伪点标签M;计算机设备可以根据防伪点标签1和样本防伪点分类特征1构建初始卷积神经网络1的损失函数1,根据防伪点标签2和样本防伪点分类特征 2构建初始卷积神经网络2的损失函数2,……,根据防伪点标签M和样本防伪点分类特征M构建初始卷积神经网络M的损失函数M;进而可以根据损失函数 1、损失函数2、……、损失函数M以及初始时序分类网络的损失函数构建整个初始鉴别模型从端到端的损失函数,其中,整个初始鉴别模型从端到端的损失函数可以使用交叉熵(Cross Entropy,CE)损失表示:$Loss=a*(Loss_{CNN1}+Loss_{CNN2}+\cdots+Loss_{CNNM})+Loss_{LSTM}$,其中,a为参数,Loss表示整个初始鉴别模型从端到端的损失函数,$Loss_{CNN1}$表示初始卷积神经网络1的损失函数,……,$Loss_{CNNM}$表示初始卷积神经网络M的损失函数,$Loss_{LSTM}$表示初始时序分类网络(此处默认初始时序分类网络为LSTM)的损失函数。

[0143] 计算机设备可以根据整个初始鉴别模型的损失函数对初始鉴别模型的网络参数进行训练,在训练阶段可以采用轮流训练的方式对初始鉴别模型中的初始卷积神经网络和初始时序分类网络进行训练,如冻结初始卷积神经网络2至初始卷积神经网络M的网络参数,训练初始卷积神经网络1和初始时序分类网络的网络参数;当整个初始鉴别模型的损失函数值在连续p(p的取值的可以预先进行设置,如p取值为10)次训练中均达到最小值时,可以冻结初始卷积神经网络1、初始卷积神经网络3、……、初始卷积神经网络M的网络参数,训练初始卷积神经网络2和初始时序分类网络的网络参数;以此类推,可以冻结初始卷积神经网络1、……、初始卷积神经网络M-1的网络参数,训练初始卷积神经网络M和初始时序分类网络的网络参数,如此循环往复,直至目标函数在连续M*p次训练中均达到最小值,停止训练,保存此时的网络参数,将此时的初始鉴别模型确定为对象鉴别模型。

[0144] 为方便描述,下面以初始鉴别模型包括第一卷积神经网络和第二卷积神经网络两个初始卷积神经网络为例,对初始鉴别模型网络参数的训练过程进行详细描述。此时每个样本视频数据所携带的标签信息可以包括第一防伪点标签、第二防伪点标签以及真伪标签;M个样本防伪点区域可以包括第一样本区域和第二样本区域,样本防伪点融合特征可以包括第一卷积神经网络输出的针对第一样本区域的第一样本防伪点分类特征,以及第二卷积神经网络输出的针对第二样本区域的第二样本防伪点分类特征;进而可以根据第一防伪点标签与第一样本防伪点分类特征之间的误差,生成第一卷积神经网络对应的第一损失参数,根据第二防伪点标签与第二样本防伪点分类特征之间的误差,生成第二卷积神经网络对应的第二损失函数,根据真伪标签与样本鉴别结果之间的误差,生成初始时序分类网络对应的第三损失函数;进而可以根据第一损失参数、第二损失函数以及第三损失函数,生成初始对象鉴别模型对应的目标损失函数(即整个初始鉴别模型从端到端的损失函数);计算机设备可以根据目标损失函数对整个初始鉴别模型的网络参数进行修正,将包含修正后的网络参数的初始鉴别模型确定为对象鉴别模型,通过不断迭代对目标损失函数进行优化处理,在目标函数达到最小值时获得最优的网络参数,将包含最优的网络参数的初始鉴别模型确定为对象鉴别模型。

[0145] 进一步地,整个初始鉴别模型的训练逻辑可以描述如下:计算机设备可以根据目标损失函数对第一卷积神经网络和初始时序分类网络的网络参数进行修正,并暂停对第二

卷积神经网络的网络参数进行修正;当目标损失函数在连续p 次训练中均达到第一最小值时,根据目标损失函数对修正后的初始时序分类网络的网络参数,以及第二卷积神经网络的网络参数进行修正,并暂停对修正后的第一卷积神经网络的网络参数进行修正,其中,p为预先设置的正整数,如p 可以为1,2,……;当目标损失函数在连续q次训练中达到第二最小值时,将初始鉴别模型在最后一次训练中的网络参数确定为目标网络参数,将包含目标网络参数的初始鉴别模型确定为对象鉴别模型,其中,q为预先设置的正整数,如q可以为1,2,……;q与p可以相同,也可以不相同,本申请对此不做限定。可选的,当目标损失函数在连续q次训练中达到第二最小值(本申请实施例中的第一最小值和第二最小值为不同的数值)时,可以再次根据目标损失函数对第一卷积神经网络和初始时序分类网络的网络参数进行修正,并暂停对第二卷积神经网络的网络参数进行修正,如此循环往复,若不管是训练第一卷积神经网络和初始时序分类网络的网络参数,还是训练第二卷积神经网络和初始时序分类网络的网络参数,目标损失函数的损失值均不再下降,即均处于最小值,则可以停止训练,保存此时的网络参数,将此时的初始鉴别模型确定为对象鉴别模型。

[0146] 请一并参见图8,图8是本申请实施例提供的一种训练初始鉴别模型的示意图,如图8所示,视频帧50a和视频帧50b可以是指同一个样本视频数据所包含的样本视频帧,视频帧50c和视频帧50d可以是指同一个样本视频数据所包含的样本视频帧。对初始鉴别模型(包括卷积神经网络1、卷积神经网络2、初始时序分类网络以及全连接层等)的网络参数进行初始化处理,随后可以冻结卷积神经网络2的网络参数,对卷积神经网络1、初始时序分类网络以及全连接层的网络参数进行训练,当连续p个epoch(完整训练所有样本视频数据的次数) 的目标损失函数的损失值达到最小值时,可以冻结卷积神经网络1的网络参数,对卷积神经网络2、初始时序分类网络以及全连接层的网络参数进行训练,当连续p个epoch的目标损失函数的损失值达到最小值时,可以重复上述训练过程,直至2p个epoch的目标损失函数的损失值达到最小值,可以停止训练,此时的初始鉴别模型可以确定为对象鉴别模型。

[0147] 在初始鉴别模型训练完成后,为了验证训练完成的对象鉴别模型的有效性,可以使用不同的样本数据集进行实验,如可以使用样本数据集1和样本数据集2 进行实验,其中,样本数据集1可以包括685个一代真实身份证件的视频和130 个一代高仿伪造身份证件的视频,样本数据集2可以包括279个二代真实身份证件的视频和135个二代高仿伪造身份证件的视频。通过在样本数据集1和样本数据集2中进行实验,训练完成的对象鉴别模型测试的假证通过率(false acceptance rate,FAR)和真证拒绝率(false rejection rate,FRR)均小于5%,比用于识别单个图像数据的模型以及用于识别多个图像数据的模型的效果均有大幅度提升;另外,对象鉴别模型的计算时间很快,在CPU(Central Processing Unit/Processor,中央处理单元)上的处理时间在20秒以内,GPU(Graphics Processing Unit,图形处理器)上的处理时间在5秒以内,可以满足用户的实际使用要求。

[0148] 对于本申请实施例中的初始鉴别模型,输入该初始鉴别模型的防伪点数量可以自由选择,无论是一个防伪点,或者是两个防伪点,或者是是个防伪点,均可以适用于上述初始鉴别模型,并且对于不同证件的防伪点也可进行类似处理;其次,该初始鉴别模型的初始时序分类网络可以融合不同防伪点在同一视频帧的所有防伪点信息进行处理,可以有效探索不同防伪点在视频帧中的组合,并获取N个样本视频帧在时序分布上的防伪点进行分类;通过轮流训练的方式对出时间别模型的网络参数进行训练,可以节省计算机设备的大量显

存,从而能加载更多样本视频数据,提升batchnorm(在初始鉴别模型的训练过程中所使用的加速神经网络训练,加速收敛速度及稳定性的算法)的有效性,使训练更快更鲁棒;其次,对每个防伪点进行分开训练可以加快网络收敛,不容易出现开始训练时不同防伪点不能同步收敛的问题,并且轮流训练的方式可以让单个防伪点和最终的鉴别结果都达到最优,不仅可以提高对象鉴别模型的适用性,还可以提高对象鉴别模型的鉴别准确度。

[0149] 请参见图9,图9是本申请实施例提供的一种数据鉴伪装置的结构示意图。数据鉴伪装置可以是运行于计算机设备中的一个计算机程序(包括程序代码),该装置可以用于执行图4所对应实施例提供的方法中的相应步骤。如图9所示,数据鉴伪装置1可以包括:防伪点区域获取模块11,融合特征生成模块12,鉴别结果获取模块13;

[0150] 防伪点区域获取模块11,用于获取视频数据所包含的N个视频帧,获取N 个视频帧中每个视频帧分别包含的M个防伪点区域;N个视频帧包括待鉴伪的目标对象,N和M均为正整数;

[0151] 融合特征生成模块12,用于根据每个视频帧分别包含的M个防伪点区域,生成N个视频帧分别对应的防伪点融合特征;

[0152] 鉴别结果获取模块13,用于根据N个视频帧在视频数据中的时间顺序,构建包含N个防伪点融合特征的特征序列,根据特征序列生成视频数据对应的时序分布特征,根据时序分布特征确定目标对象对应的对象鉴别结果。

[0153] 其中,防伪点区域获取模块11,融合特征生成模块12,鉴别结果获取模块 13的具体功能实现方式可以参见上述图4所对应实施例中的步骤S101-步骤 S103,这里不再进行赘述。

[0154] 在一些可行的实施方式中,防伪点区域获取模块11可以包括:视频分帧处理单元111,视频帧选取单元112,防伪点信息获取单元113,视频帧分割单元 114;

[0155] 视频分帧处理单元111,用于获取摄像设备采集的视频数据,对视频数据进行分帧处理,得到视频帧序列;

[0156] 视频帧选取单元112,用于根据间隔时间信息在视频帧序列中获取N个视频帧,获取N个视频帧中的视频帧T_i;i为小于或等于N的正整数;

[0157] 防伪点信息获取单元113,用于获取视频数据中的目标对象对应的对象类型,获取与对象类型相关联的防伪点信息;

[0158] 视频帧分割单元114,用于根据防伪点信息对视频帧T_i进行分割,得到视频帧T_i中的M个防伪点区域。

[0159] 其中,视频分帧处理单元111,视频帧选取单元112,防伪点信息获取单元113,视频帧分割单元114的具体功能实现方式可以参见上述图4所对应实施例中的步骤S101,这里不再进行赘述。

[0160] 在一些可行的实施方式中,融合特征生成模块12可以包括:网络匹配单元 121,卷积处理单元122,特征合并单元123;

[0161] 网络匹配单元121,用于获取N个视频帧中的视频帧T_i,在视频帧T_i的M 个防伪点区域中获取防伪点区域R_j,在对象鉴别模型中获取与防伪点区域R_j相匹配的目标卷积神经网络;对象鉴别模型包括M个防伪点区域分别对应的卷积神经网络,i为小于或等于N的正整数,j为小于或等于M的正整数;

[0162] 卷积处理单元122,用于将防伪点区域R_j输入至目标卷积神经网络,根据目标卷积神经网络中的卷积层,对防伪点区域R_j进行卷积处理,得到防伪点区域R_j对应的防伪点分类特征;

[0163] 特征合并单元123,用于获取M个防伪点区域分别对应的防伪点分类特征,将M个防伪点分类特征进行合并,得到视频帧T_i对应的防伪点融合特征。

[0164] 其中,网络匹配单元121,卷积处理单元122,特征合并单元123的具体功能实现方式可以参见上述图4所对应实施例中的步骤S102,这里不再进行赘述。

[0165] 在一些可行的实施方式中,鉴别结果获取模块13可以包括:时序分布特征获取单元131,结果输出单元132;

[0166] 时序分布特征获取单元131,用于将特征序列中的N个防伪点融合特征依次输入至对象鉴别模型中的时序分类网络,在时序分类网络中获取N个防伪点融合特征之间的时序分布特征;

[0167] 结果输出单元132,用于将时序分布特征输入至对象鉴别模型中的全连接层,通过全连接层输出目标特征向量,根据目标特征向量确定目标对象对应的对象鉴别结果。

[0168] 其中,在一些可行的实施方式中,结果输出单元132可以包括:特征转换子单元1321,比较子单元1322;

[0169] 特征转换子单元1321,用于根据全连接层,将时序分布特征转换为目标特征向量;目标特征向量包括合法评估值和伪造评估值;

[0170] 比较子单元1322,用于若合法评估值大于伪造评估值,则确定目标对象对应的对象鉴别结果为合法鉴别结果;

[0171] 上述比较单元1322,还用于若合法评估值小于伪造评估值,则确定目标对象对应的对象鉴别结果为伪造鉴别结果。

[0172] 其中,时序分布特征获取单元131,结果输出单元132的具体功能实现方式可以参见上述图4所对应实施例中的步骤S103,这里不再进行赘述。

[0173] 在一些可行的实施方式中,视频数据为目标用户在业务机构办理开户业务时所提供的身份证视频数据,目标对象为身份证件;

[0174] 该数据鉴伪装置1还可以包括:业务执行模块14,业务办理失败提示模块 15;

[0175] 业务执行模块14,用于若身份证件的对象鉴别结果为合法鉴别结果,则在业务机构中继续执行针对目标用户的开户业务;

[0176] 业务办理失败提示模块15,用于若身份证件的对象鉴别结果为伪造鉴别结果,则确定目标用户在业务机构中的开户业务办理结果为开户失败结果;开户失败结果用于指示目标用户提供新的身份证视频数据。

[0177] 其中,业务执行模块14,业务办理失败提示模块15的具体功能实现方式可以参见上述图4所对应实施例中的步骤S103,这里不再进行赘述。

[0178] 本申请实施例中,通过获取目标对象对应的视频数据,可以从视频数据中获取不同防伪点在相同视频帧中的特征信息,也可以获取相同防伪点在不同视频帧中的特征信息,通过将相同视频帧中不同防伪点的特征信息进行融合,以得到每个视频帧对应的防伪点融合特征,进而可以获取每个视频帧所对应的防伪点融合特征之间的时序分布特征,该时序分布特征可以用于表征该目标对象在不同视觉角度下的特征信息,可以提高目标对象

的鉴别准确度;使用的对象鉴别模型中可以包含分别用于识别每个防伪点的卷积神经网络,卷积神经网络可以对每个帧视频帧所包含的M个防伪点区域进行并行处理,即每个卷积神经网络均可以进行独立工作,互不影响,进而可以将各卷积神经网络所输出的结果进行融合,并输入至时序分类网络中,通过时序分类网络可以输出视频数据对应的对象鉴别结果,可以提高视频数据的识别效率。

[0179] 请参见图10,图10是本申请实施例提供的一种数据鉴伪装置的结构示意图。数据鉴伪装置可以是运行于计算机设备中的一个计算机程序(包括程序代码),该数据鉴伪装置可以用于执行图7所对应实施例提供的方法中的相应步骤。如图10所示,数据鉴伪装置2可以包括:样本区域获取模块21,样本融合特征生成模块22,样本融合特征输入模块23,样本鉴别结果获取模块24,网络参数修正模块25;

[0180] 样本区域获取模块21,用于获取样本视频数据所包含的N个样本视频帧,获取N个样本视频帧中每个样本视频帧分别包含的M个样本防伪点区域;N个样本视频帧包括样本对象,样本视频数据携带针对样本对象的标签信息,N和 M均为正整数;

[0181] 样本融合特征生成模块22,用于将每个样本视频帧分别包含的M个样本防伪点区域输入至初始鉴别模型中的初始卷积神经网络,通过初始卷积神经网络,生成N个样本视频帧分别对应的样本防伪点融合特征;

[0182] 样本融合特征输入模块23,用于根据N个样本视频帧在样本视频数据中的时间顺序,将N个样本防伪点融合特征依次输入至初始鉴别模型中的初始时序分类网络;

[0183] 样本鉴别结果获取模块24,用于通过初始时序分类网络,生成样本视频数据对应的样本时序分布特征,根据样本时序分布特征确定样本对象对应的样本鉴别结果;

[0184] 网络参数修正模块25,用于根据标签信息、样本鉴别结果以及N个样本防伪点融合特征,对初始鉴别模型的网络参数进行修正,将包含修正后的网络参数的初始鉴别模型确定为对象鉴别模型;对象鉴别模型用于识别视频数据所包含的目标对象对应的对象鉴别结果。

[0185] 其中,样本区域获取模块21,样本融合特征生成模块22,样本融合特征输入模块23,样本鉴别结果获取模块24,网络参数修正模块25的具体功能实现方式可以参见上述图7所对应实施例中的步骤S201-步骤S205,这里不再进行赘述。

[0186] 在一些可行的实施方式中,样本区域获取模块21可以包括:样本视频分帧处理单元211,样本视频帧选取单元212;

[0187] 样本视频分帧处理单元211,用于将样本视频数据划分为N个样本视频片段,分别对每个样本视频片段进行分帧处理,得到每个样本视频片段分别对应的样本视频帧序列;

[0188] 样本视频帧选取单元212,用于分别在N个样本视频帧序列中随机选取样本视频帧,得到样本视频数据中的N个样本视频帧。

[0189] 其中,样本视频分帧处理单元211,样本视频帧选取单元212的具体功能实现方式可以参见上述图7所对应实施例中的步骤S201,这里不再进行赘述。

[0190] 在一些可行的实施方式中,初始卷积神经网络包括第一卷积神经网络和第二卷积神经网络;标签信息包括第一防伪点标签、第二防伪点标签以及真伪标签;M个样本防伪点区域包括第一样本区域和第二样本区域,样本防伪点融合特征包括第一卷积神经网络输出的针对第一样本区域的第一样本防伪点分类特征,以及第二卷积神经网络输出的针对第二

样本区域的第二样本防伪点分类特征；

[0191] 网络参数修正模块25可以包括：第一损失函数生成单元251，第二损失函数生成单元252，第三损失函数生成单元253，目标损失函数生成单元254，参数修正单元255；

[0192] 第一损失函数生成单元251，用于根据第一防伪点标签与第一样本防伪点分类特征之间的误差，生成第一卷积神经网络对应的第一损失参数；

[0193] 第二损失函数生成单元252，用于根据第二防伪点标签与第二样本防伪点分类特征之间的误差，生成第二卷积神经网络对应的第二损失函数；

[0194] 第三损失函数生成单元253，用于根据真伪标签与样本鉴别结果之间的误差，生成初始时序分类网络对应的第三损失函数；

[0195] 目标损失函数生成单元254，用于根据第一损失参数、第二损失函数以及第三损失函数，生成初始对象鉴别模型对应的目标损失函数；

[0196] 参数修正单元255，用于根据目标损失函数对初始鉴别模型的网络参数进行修正，将包含修正后的网络参数的初始鉴别模型确定为对象鉴别模型。

[0197] 其中，第一损失函数生成单元251，第二损失函数生成单元252，第三损失函数生成单元253，目标损失函数生成单元254，参数修正单元255的具体功能实现方式可以参见上述图7所对应实施例中的步骤S205，这里不再进行赘述。

[0198] 参数修正单元255包括：第一修正子单元2551，第二修正子单元2552，目标网络参数确定子单元2553；

[0199] 第一修正子单元2551，用于根据目标损失函数对第一卷积神经网络和初始时序分类网络的网络参数进行修正，并暂停对第二卷积神经网络的网络参数进行修正；

[0200] 第二修正子单元2552，用于当目标损失函数在连续p次训练中均达到第一最小值时，根据目标损失函数对修正后的初始时序分类网络的网络参数，以及第二卷积神经网络的网络参数进行修正，并暂停对修正后的第一卷积神经网络的网络参数进行修正；p为正整数；

[0201] 目标网络参数确定子单元2553，用于当目标损失函数在连续q次训练中达到第二最小值时，将初始鉴别模型在最后一次训练中的网络参数确定为目标网络参数，将包含目标网络参数的初始鉴别模型确定为对象鉴别模型；q为正整数。

[0202] 其中，第一修正子单元2551，第二修正子单元2552，目标网络参数确定子单元2553的具体功能实现方式可以参见上述图7所对应实施例中的步骤S205，这里不再进行赘述。

[0203] 本申请实施例中，对于训练初始鉴别模型的样本视频数据，不仅可以携带真伪标签(如合法标签和伪造标签)，还可以携带每个防伪点分别对应的防伪点标签(如防伪点1对应的标签可以包括清晰、模糊以及看不见等标签等)，采用携带真伪标签和防伪点标签的样本视频数据训练初始鉴别模型，使得训练完成的对象鉴别模型可以从视频数据中提取更具鉴别力的特征，进而提高视频数据中针对目标对象的鉴别准确度；在训练初始鉴别模型时，可以采用轮流训练的方式(可以理解为轮流训练初始鉴别模型中针对不同防伪点的卷积神经网络)进行训练，可以节省计算机设备的显存资源，对每个防伪点分别对应的卷积神经网络进行独立训练，可以解决不同防伪点很难同步收敛的问题，进而可以加快网络收敛的速度，从而提高初始鉴别模型的训练效率；采用训练完成的鉴别模型对视频数据所包含的目标对象进行鉴别时，以确保目标对象对应的每个防伪点的识别结果均是最优结果，金额如

可以提高目标对象的鉴别准确度。

[0204] 请参见图11,图11是本申请实施例提供的一种计算机设备的结构示意图。如图11所示,该计算机设备1000可以包括:处理器1001,网络接口1004和存储器1005,此外,上述计算机设备1000还可以包括:用户接口1003,和至少一个通信总线1002。其中,通信总线1002用于实现这些组件之间的连接通信。其中,用户接口1003可以包括显示屏(Display)、键盘(Keyboard),可选用户接口1003还可以包括标准的有线接口、无线接口。可选的,网络接口1004 可以包括标准的有线接口、无线接口(如WI-FI接口)。存储器1005可以是高速RAM存储器,也可以是非不稳定的存储器(non-volatile memory),例如至少一个磁盘存储器。可选的,存储器1005还可以是至少一个位于远离前述处理器1001的存储装置。如图11所示,作为一种计算机可读存储介质的存储器1005 中可以包括操作系统、网络通信模块、用户接口模块以及设备控制应用程序。

[0205] 在如图11所示的计算机设备1000中,网络接口1004可提供网络通讯功能;而用户接口1003主要用于为用户提供输入的接口;而处理器1001可以用于调用存储器1005中存储的设备控制应用程序,以实现:

[0206] 获取视频数据所包含的N个视频帧,获取N个视频帧中每个视频帧分别包含的M个防伪点区域;N个视频帧包括待鉴伪的目标对象,N和M均为正整数;

[0207] 根据每个视频帧分别包含的M个防伪点区域,生成N个视频帧分别对应的防伪点融合特征;

[0208] 根据N个视频帧在视频数据中的时间顺序,构建包含N个防伪点融合特征的特征序列,根据特征序列生成视频数据对应的时序分布特征,根据时序分布特征确定目标对象对应的对象鉴别结果。

[0209] 应当理解,本申请实施例中所描述的计算机设备1000可执行前文图4所对应实施例中对数据鉴伪方法的描述,也可执行前文图9所对应实施例中对数据鉴伪装置1的描述,在此不再赘述。另外,对采用相同方法的有益效果描述,也不再进行赘述。

[0210] 请参见图12,图12是本申请实施例提供的一种计算机设备的结构示意图。如图12所示,该计算机设备2000可以包括:处理器2001,网络接口2004和存储器2005,此外,上述计算机设备2000还可以包括:用户接口2003,和至少一个通信总线2002。其中,通信总线2002用于实现这些组件之间的连接通信。其中,用户接口2003可以包括显示屏(Display)、键盘(Keyboard),可选用户接口2003还可以包括标准的有线接口、无线接口。网络接口2004可选的可以包括标准的有线接口、无线接口(如WI-FI接口)。存储器2005可以是高速 RAM存储器,也可以是非不稳定的存储器(non-volatile memory),例如至少一个磁盘存储器。存储器2005可选的还可以是至少一个位于远离前述处理器 2001的存储装置。如图12所示,作为一种计算机可读存储介质的存储器2005 中可以包括操作系统、网络通信模块、用户接口模块以及设备控制应用程序。

[0211] 在如图12所示的计算机设备2000中,网络接口2004可提供网络通讯功能;而用户接口2003主要用于为用户提供输入的接口;而处理器2001可以用于调用存储器2005中存储的设备控制应用程序,以实现:

[0212] 获取样本视频数据所包含的N个样本视频帧,获取N个样本视频帧中每个样本视频帧分别包含的M个样本防伪点区域;N个样本视频帧包括样本对象,样本视频数据携带针对

样本对象的标签信息,N和M均为正整数;

[0213] 将每个样本视频帧分别包含的M个样本防伪点区域输入至初始鉴别模型中的初始卷积神经网络,通过初始卷积神经网络,生成N个样本视频帧分别对应的样本防伪点融合特征;

[0214] 根据N个样本视频帧在样本视频数据中的时间顺序,将N个样本防伪点融合特征依次输入至初始鉴别模型中的初始时序分类网络;

[0215] 通过初始时序分类网络,生成样本视频数据对应的样本时序分布特征,根据样本时序分布特征确定样本对象对应的样本鉴别结果;

[0216] 根据标签信息、样本鉴别结果以及N个样本防伪点融合特征,对初始鉴别模型的网络参数进行修正,将包含修正后的网络参数的初始鉴别模型确定为对象鉴别模型;对象鉴别模型用于识别视频数据所包含的目标对象对应的对象鉴别结果。

[0217] 应当理解,本申请实施例中所描述的计算机设备2000可执行前文图9所对应实施例中对数据鉴伪方法的描述,也可执行前文图10所对应实施例中对数据鉴伪装置2的描述,在此不再赘述。另外,对采用相同方法的有益效果描述,也不再进行赘述。

[0218] 此外,这里需要指出的是:本申请实施例还提供了一种计算机可读存储介质,且计算机可读存储介质中存储有前文提及的数据鉴伪装置1和数据鉴伪装置2所执行的计算机程序,且计算机程序包括程序指令,当处理器执行程序指令时,能够执行前文图4和图9任一项所对应实施例中对数据鉴伪方法的描述,因此,这里将不再进行赘述。另外,对采用相同方法的有益效果描述,也不再进行赘述。对于本申请所涉及的计算机可读存储介质实施例中未披露的技术细节,请参照本申请方法实施例的描述。作为示例,程序指令可被部署在一个计算设备上执行,或者在位于一个地点的多个计算设备上执行,又或者,在分布在多个地点且通过通信网络互连的多个计算设备上执行,分布在多个地点且通过通信网络互连的多个计算设备可以组成区块链系统。

[0219] 此外,需要说明的是:本申请实施例还提供了一种计算机程序产品或计算机程序,该计算机程序产品或者计算机程序可以包括计算机指令,该计算机指令可以存储在计算机可读存储介质中。计算机设备的处理器从计算机可读存储介质读取该计算机指令,处理器可以执行该计算机指令,使得该计算机设备执行前文图4和图9任一项所对应实施例中对数据鉴伪方法的描述,因此,这里将不再进行赘述。另外,对采用相同方法的有益效果描述,也不再进行赘述。对于本申请所涉及的计算机程序产品或者计算机程序实施例中未披露的技术细节,请参照本申请方法实施例的描述。

[0220] 需要说明的是,对于前述的各个方法实施例,为了简单描述,故将其都表述为一系列的动作组合,但是本领域技术人员应该知悉,本申请并不受所描述的动作顺序的限制,因为依据本申请,某一些步骤可以采用其他顺序或者同时进行。其次,本领域技术人员也应该知悉,说明书中所描述的实施例均属于优选实施例,所涉及的动作和模块并不一定是本申请所必须的。

[0221] 本申请实施例方法中的步骤可以根据实际需要进行顺序调整、合并和删减。

[0222] 本申请实施例装置中的模块可以根据实际需要进行合并、划分和删减。

[0223] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程,是可以通过计算机程序来指令相关的硬件来完成,计算机程序可存储于一计算机可读取存储介质

中,该程序在执行时,可包括如上述各方法的实施例的流程。其中,存储介质可为磁碟、光盘、只读存储器(Read-Only Memory,ROM)或随机存储器(Random Access Memory,RAM)等。

[0224] 以上所揭露的仅为本申请较佳实施例而已,当然不能以此来限定本申请之权利范围,因此依本申请权利要求所作的等同变化,仍属本申请所涵盖的范围。

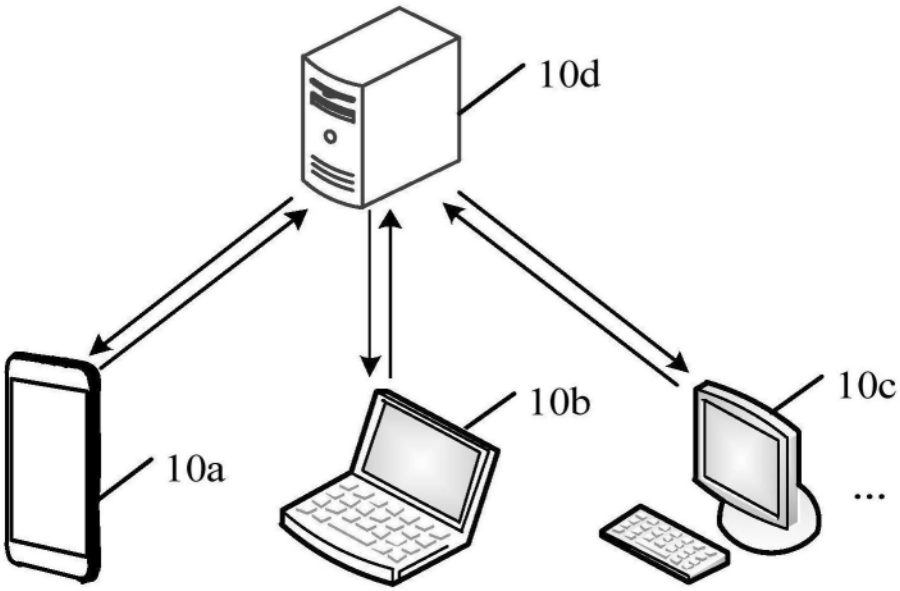


图1

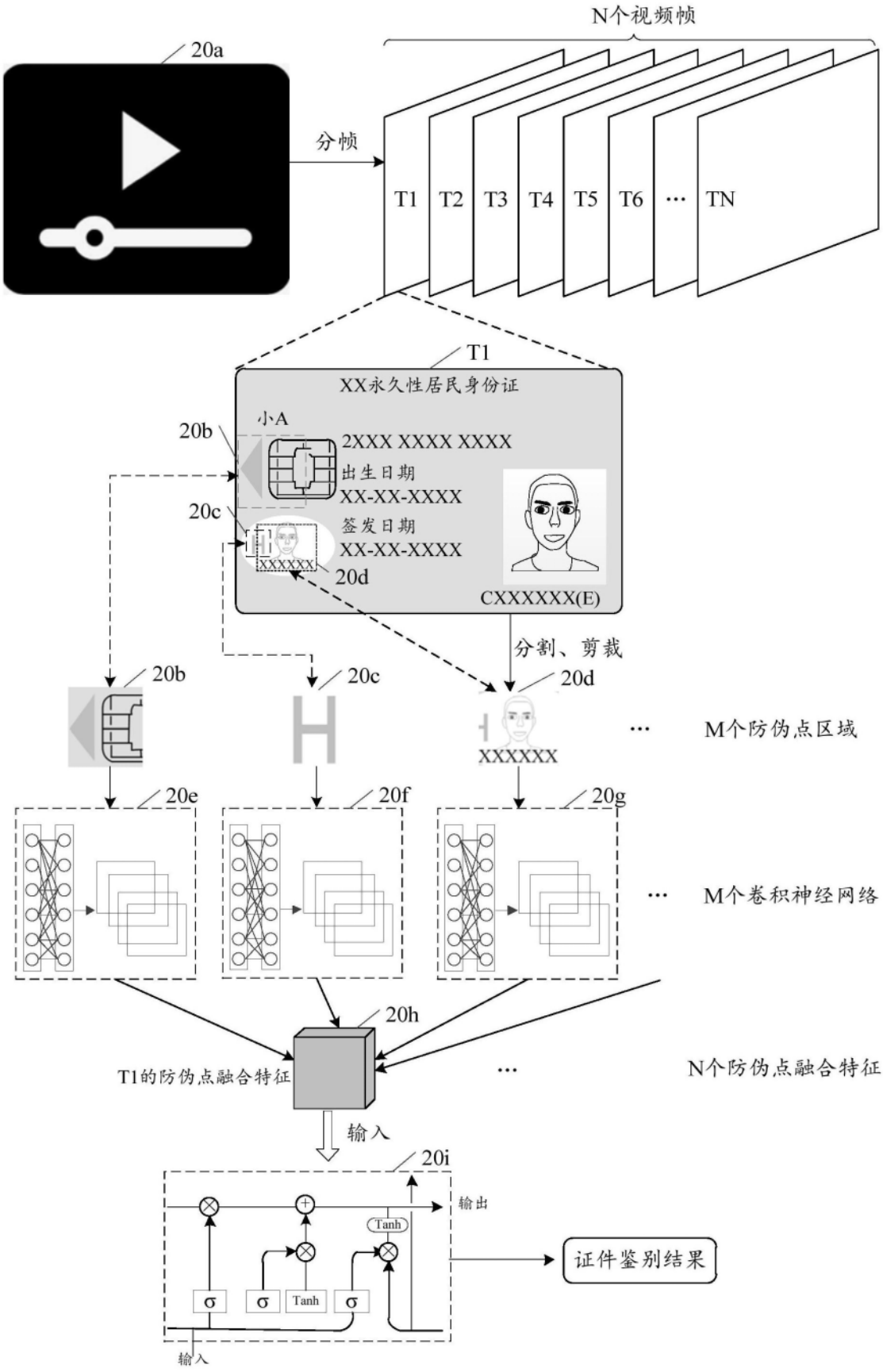

N个视频帧
20a
分帧
T1 T2 T3 T4 T5 T6 … TN
T1
XX永久性居民身份证
小A
20b
2XXX XXXX XXXX
出生日期
XX-XX-XXXX
20c
签发日期
XX-XX-XXXX
XXXXXX
20d
CXXXXXX(E)
分割、剪裁
20b
20c
20d
XXXXXX
… M个防伪点区域
20e
20f
20g
… M个卷积神经网络
20h
T1的防伪点融合特征
… N个防伪点融合特征
输入
20i
输出
Tanh
σ
σ
Tanh
σ
输入
证件鉴别结果

图2

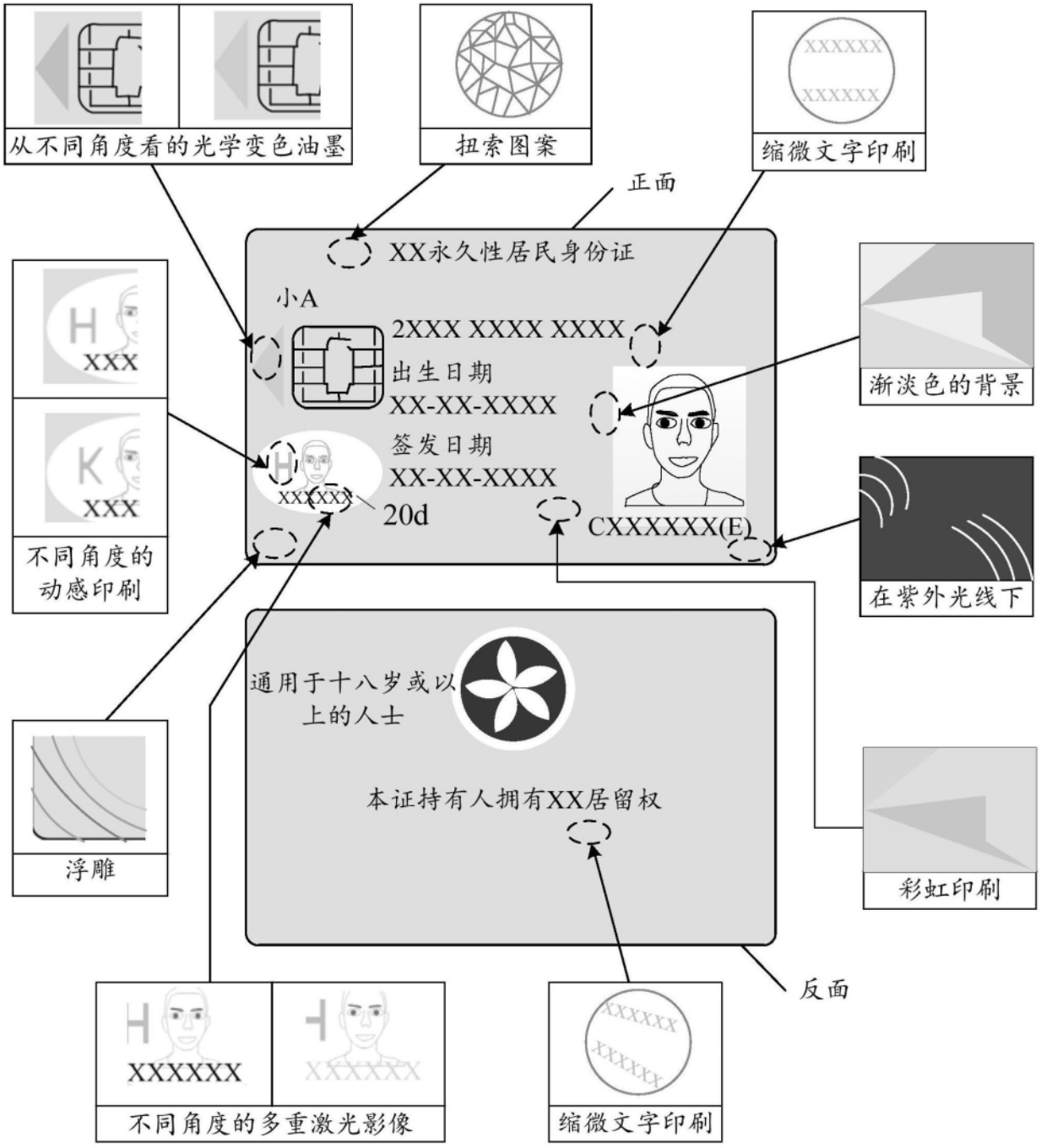

从不同角度看的光学变色油墨
扭索图案
缩微文字印刷
正面
XX永久性居民身份证
小A
2XXX XXXX XXXX
出生日期
XX-XX-XXXX
签发日期
XX-XX-XXXX
20d
CXXXXXX(E)
渐淡色的背景
在紫外光线下
不同角度的动感印刷
通用于十八岁或以上的人士
本证持有人拥有XX居留权
浮雕
彩虹印刷
反面
不同角度的多重激光影像
缩微文字印刷

图3

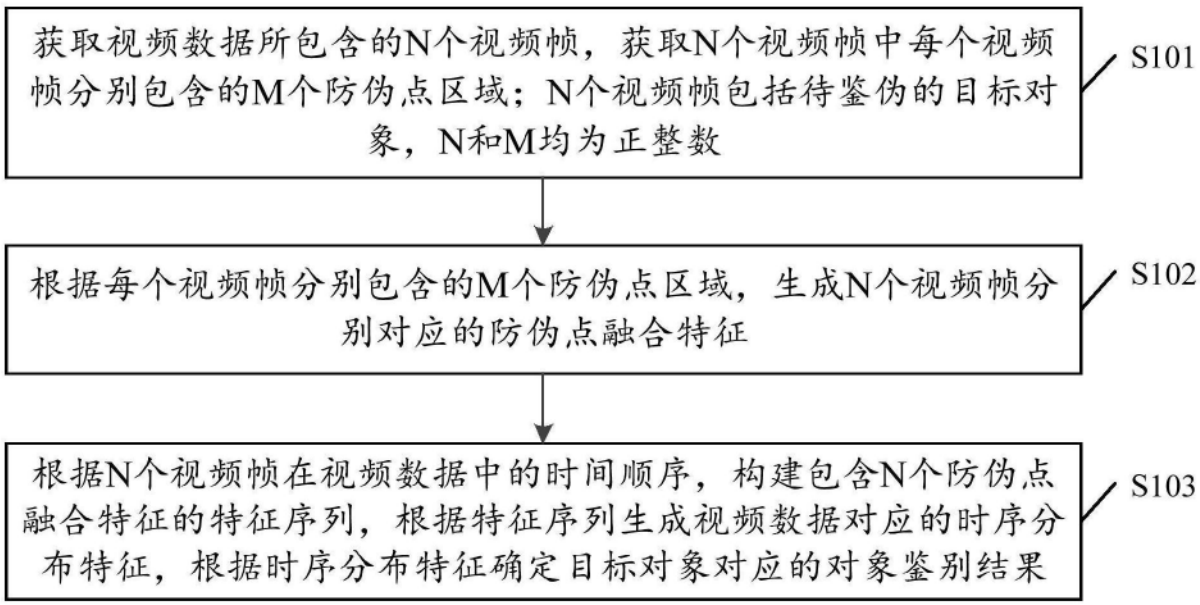

获取视频数据所包含的N个视频帧，获取N个视频帧中每个视频帧分别包含的M个防伪点区域；N个视频帧包括待鉴伪的目标对象，N和M均为正整数
S101
根据每个视频帧分别包含的M个防伪点区域，生成N个视频帧分别对应的防伪点融合特征
S102
根据N个视频帧在视频数据中的时间顺序，构建包含N个防伪点融合特征的特征序列，根据特征序列生成视频数据对应的时序分布特征，根据时序分布特征确定目标对象对应的对象鉴别结果
S103

图4

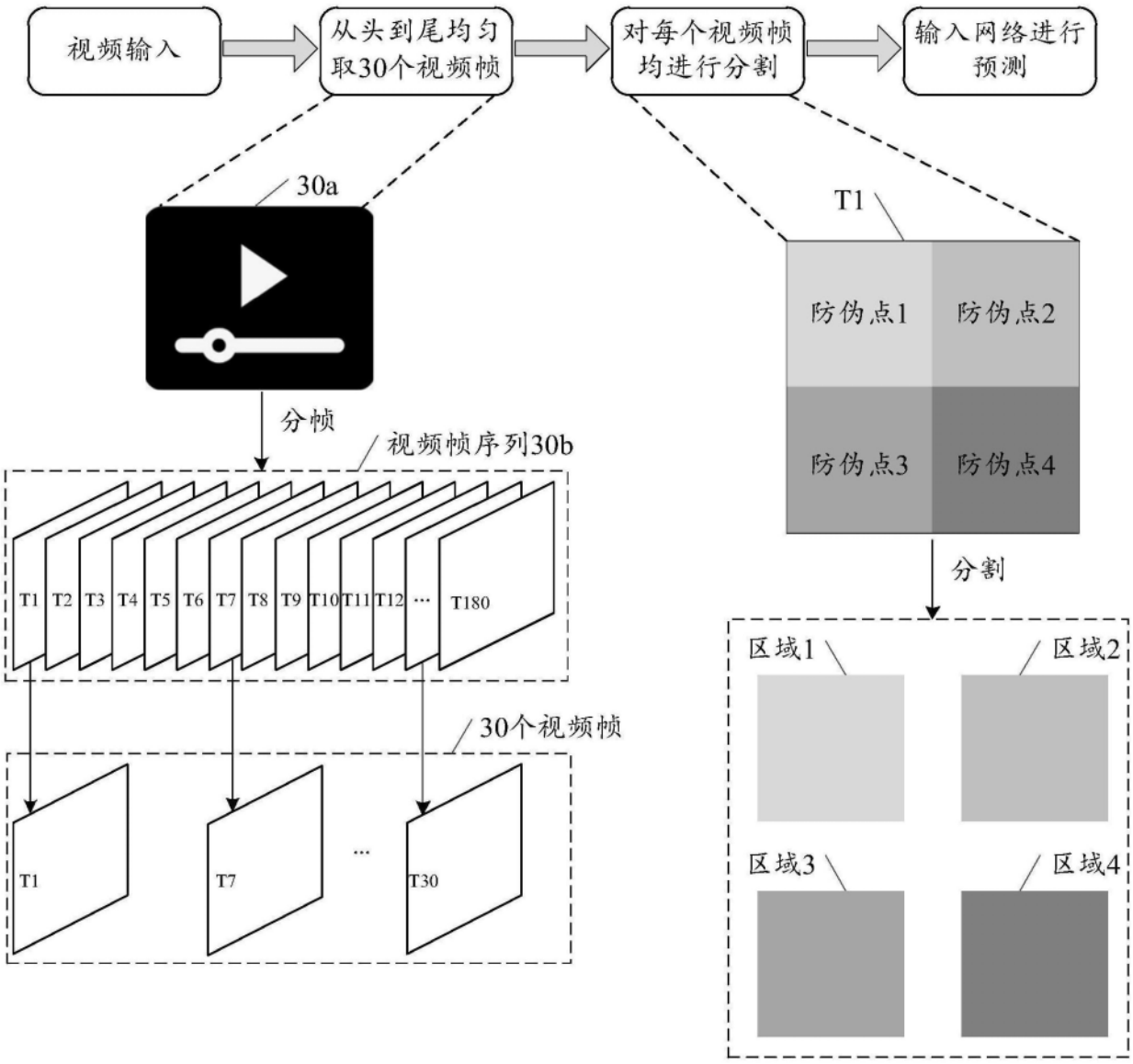

视频输入
从头到尾均匀取30个视频帧
对每个视频帧均进行分割
输入网络进行预测
30a
分帧
视频帧序列30b
T1 T2 T3 T4 T5 T6 T7 T8 T9 T10 T11 T12 ··· T180
30个视频帧
T1
T7
...
T30
T1
防伪点1
防伪点2
防伪点3
防伪点4
分割
区域1
区域2
区域3
区域4

图5

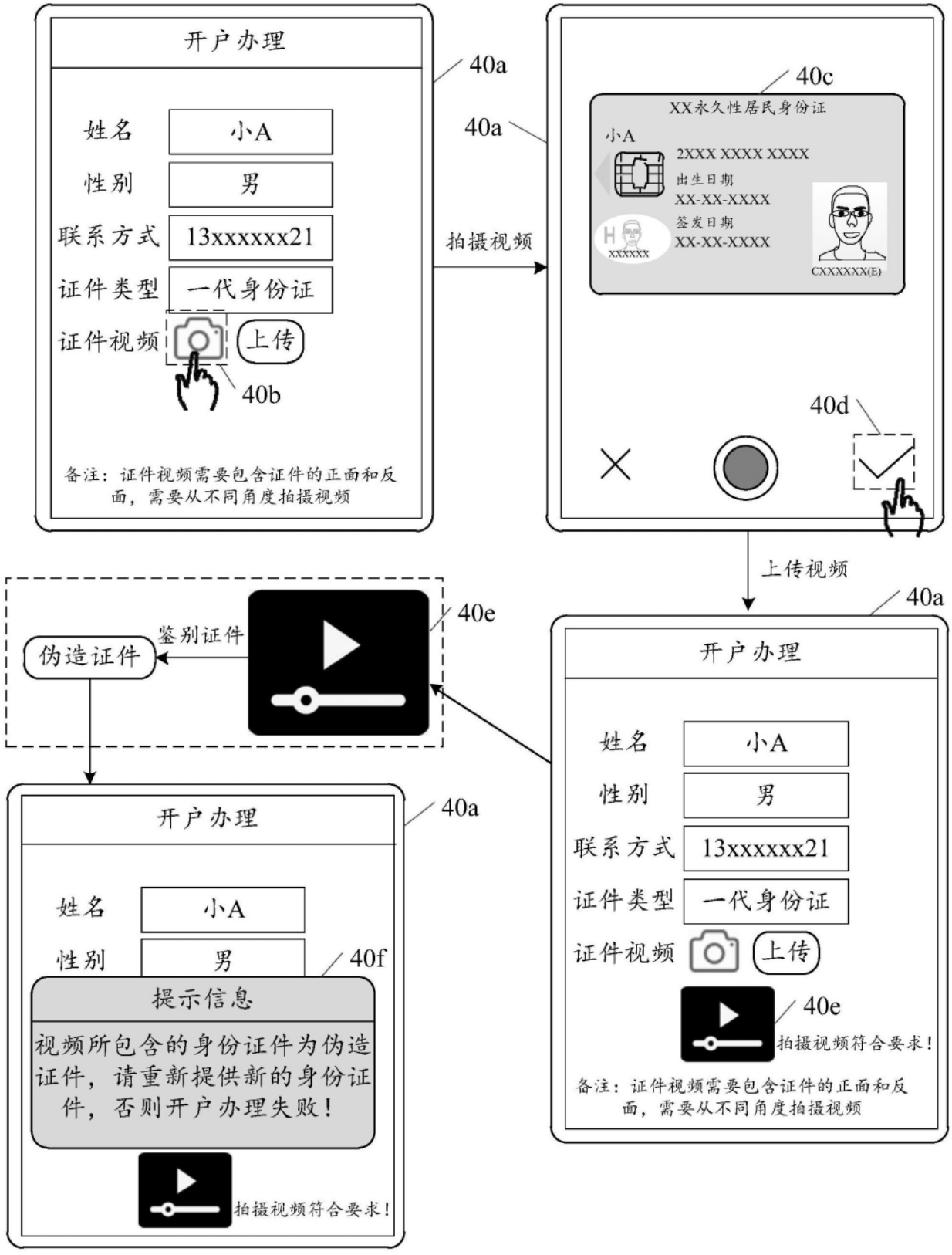

开户办理
姓名
小A
性别
男
联系方式
13xxxxxx21
证件类型
一代身份证
证件视频
上传
40a
40b
备注：证件视频需要包含证件的正面和反面，需要从不同角度拍摄视频
拍摄视频
40c
XX永久性居民身份证
小A
2XXX XXXX XXXX
出生日期
XX-XX-XXXX
签发日期
XX-XX-XXXX
CXXXXXX(E)
40d
上传视频
伪造证件
鉴别证件
40e
提示信息
视频所包含的身份证件为伪造证件，请重新提供新的身份证件，否则开户办理失败！
40f
拍摄视频符合要求！

图6

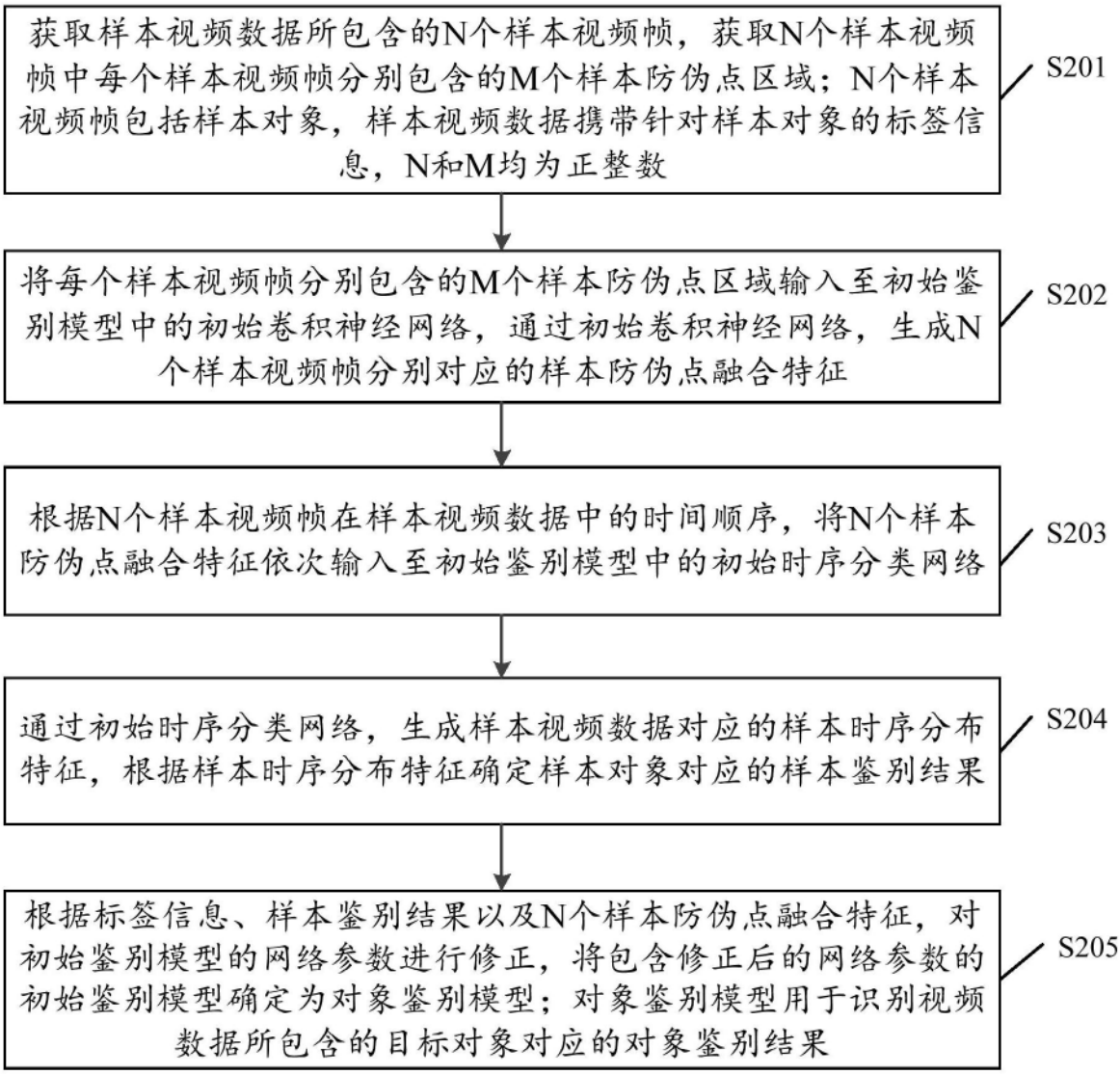

获取样本视频数据所包含的N个样本视频帧，获取N个样本视频帧中每个样本视频帧分别包含的M个样本防伪点区域；N个样本视频帧包括样本对象，样本视频数据携带针对样本对象的标签信息，N和M均为正整数
S201
将每个样本视频帧分别包含的M个样本防伪点区域输入至初始鉴别模型中的初始卷积神经网络，通过初始卷积神经网络，生成N个样本视频帧分别对应的样本防伪点融合特征
S202
根据N个样本视频帧在样本视频数据中的时间顺序，将N个样本防伪点融合特征依次输入至初始鉴别模型中的初始时序分类网络
S203
通过初始时序分类网络，生成样本视频数据对应的样本时序分布特征，根据样本时序分布特征确定样本对象对应的样本鉴别结果
S204
根据标签信息、样本鉴别结果以及N个样本防伪点融合特征，对初始鉴别模型的网络参数进行修正，将包含修正后的网络参数的初始鉴别模型确定为对象鉴别模型；对象鉴别模型用于识别视频数据所包含的目标对象对应的对象鉴别结果
S205

图7

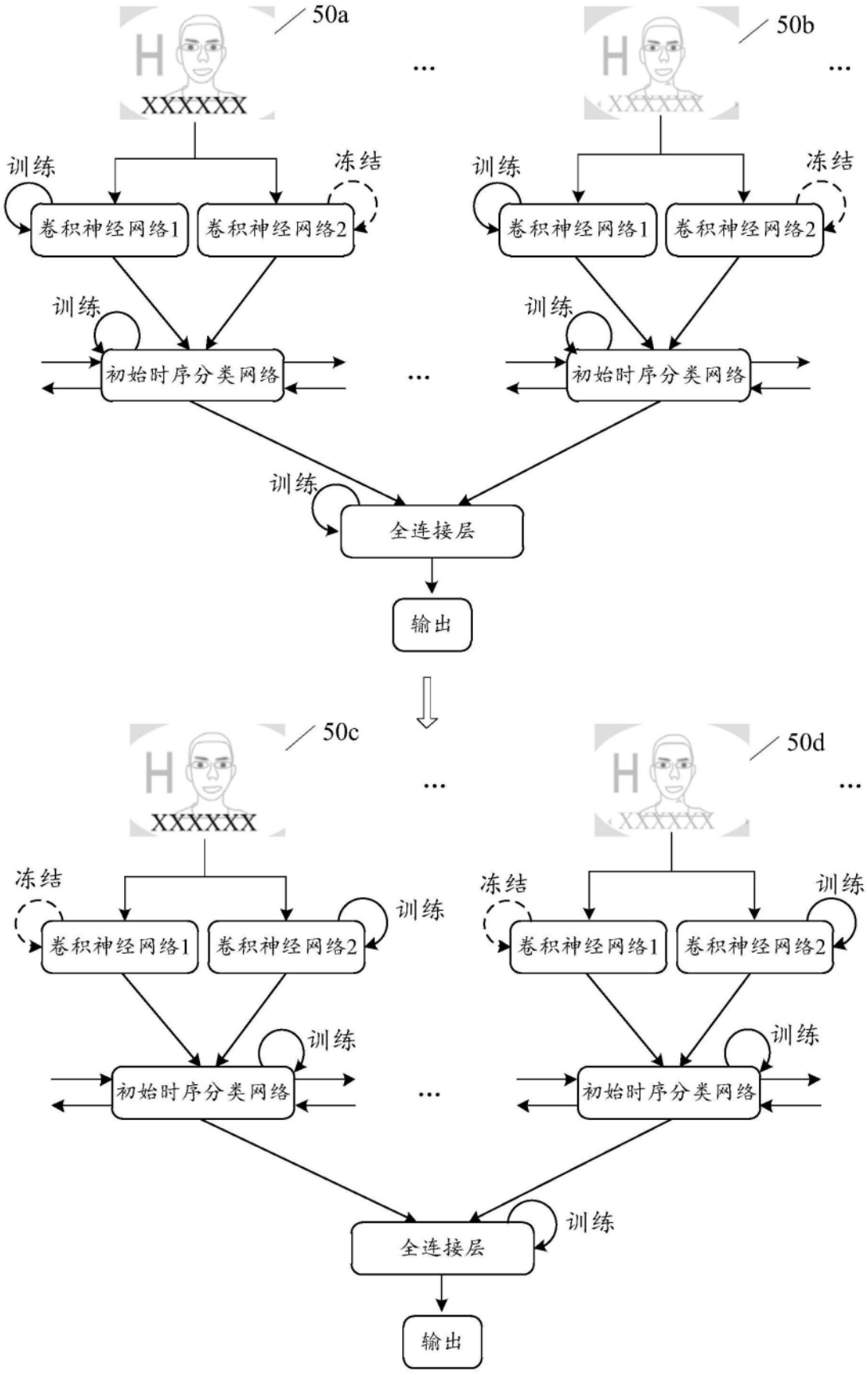

50a
50b
XXXXXX
训练
冻结
卷积神经网络1
卷积神经网络2
初始时序分类网络
全连接层
输出
50c
50d

图8

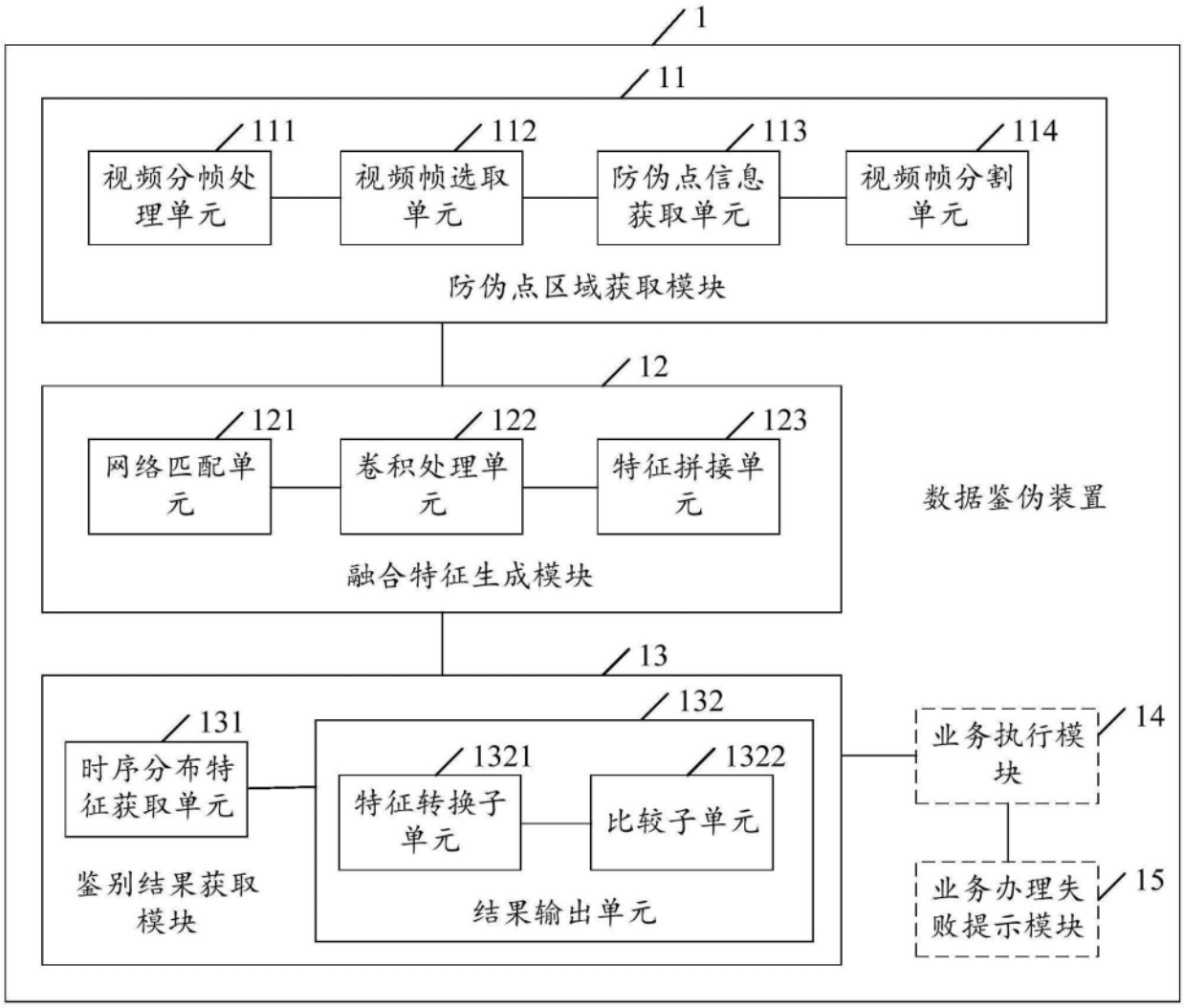

1
11
111
视频分帧处理单元
112
视频帧选取单元
113
防伪点信息获取单元
114
视频帧分割单元
防伪点区域获取模块
12
121
网络匹配单元
122
卷积处理单元
123
特征拼接单元
融合特征生成模块
数据鉴伪装置
13
131
时序分布特征获取单元
鉴别结果获取模块
132
1321
特征转换子单元
1322
比较子单元
结果输出单元
14
业务执行模块
15
业务办理失败提示模块

图9

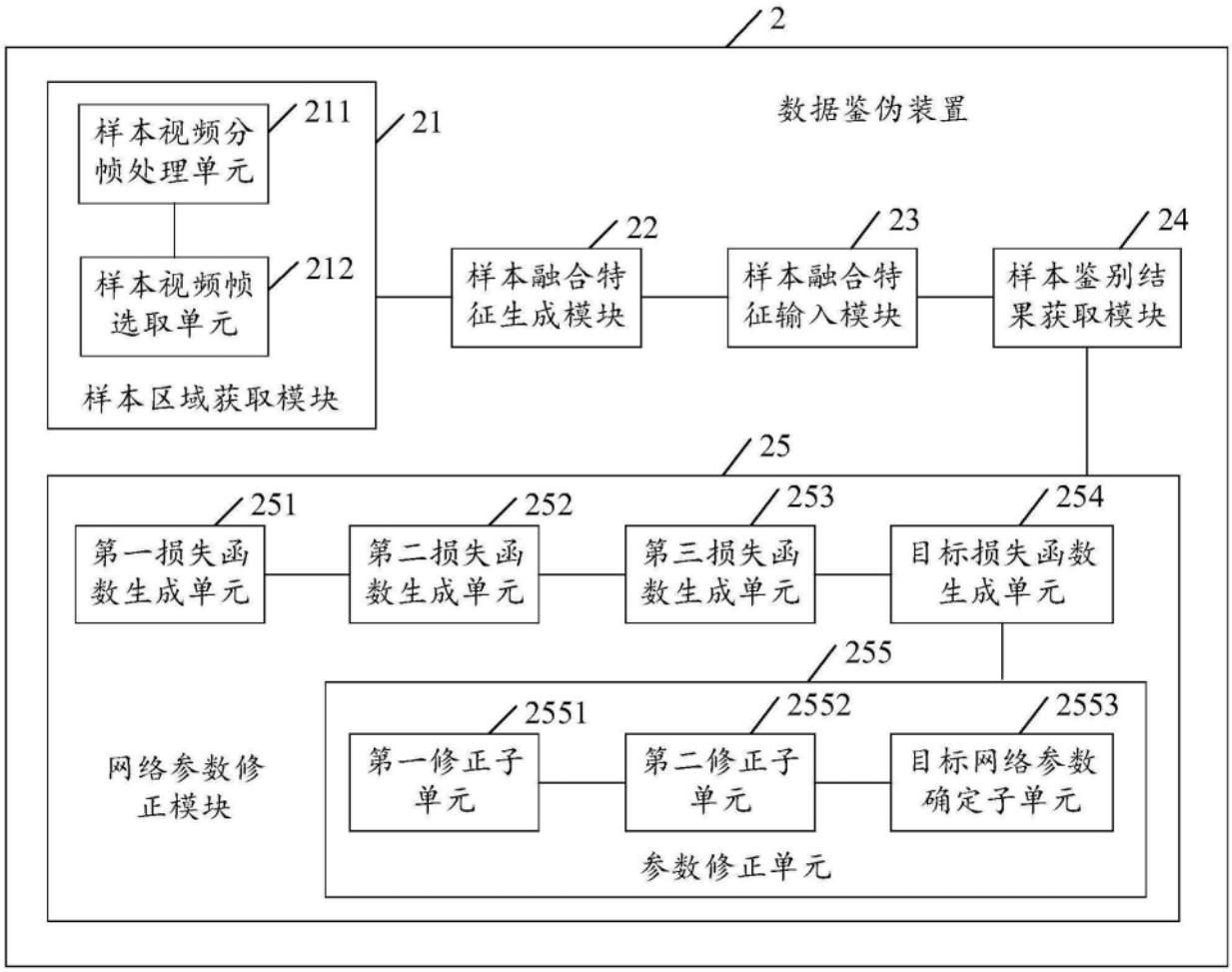

2
数据鉴伪装置
样本视频分帧处理单元
211
21
样本视频帧选取单元
212
样本区域获取模块
22
样本融合特征生成模块
23
样本融合特征输入模块
24
样本鉴别结果获取模块
25
251
第一损失函数生成单元
252
第二损失函数生成单元
253
第三损失函数生成单元
254
目标损失函数生成单元
255
2551
第一修正子单元
2552
第二修正子单元
2553
目标网络参数确定子单元
参数修正单元
网络参数修正模块

图10

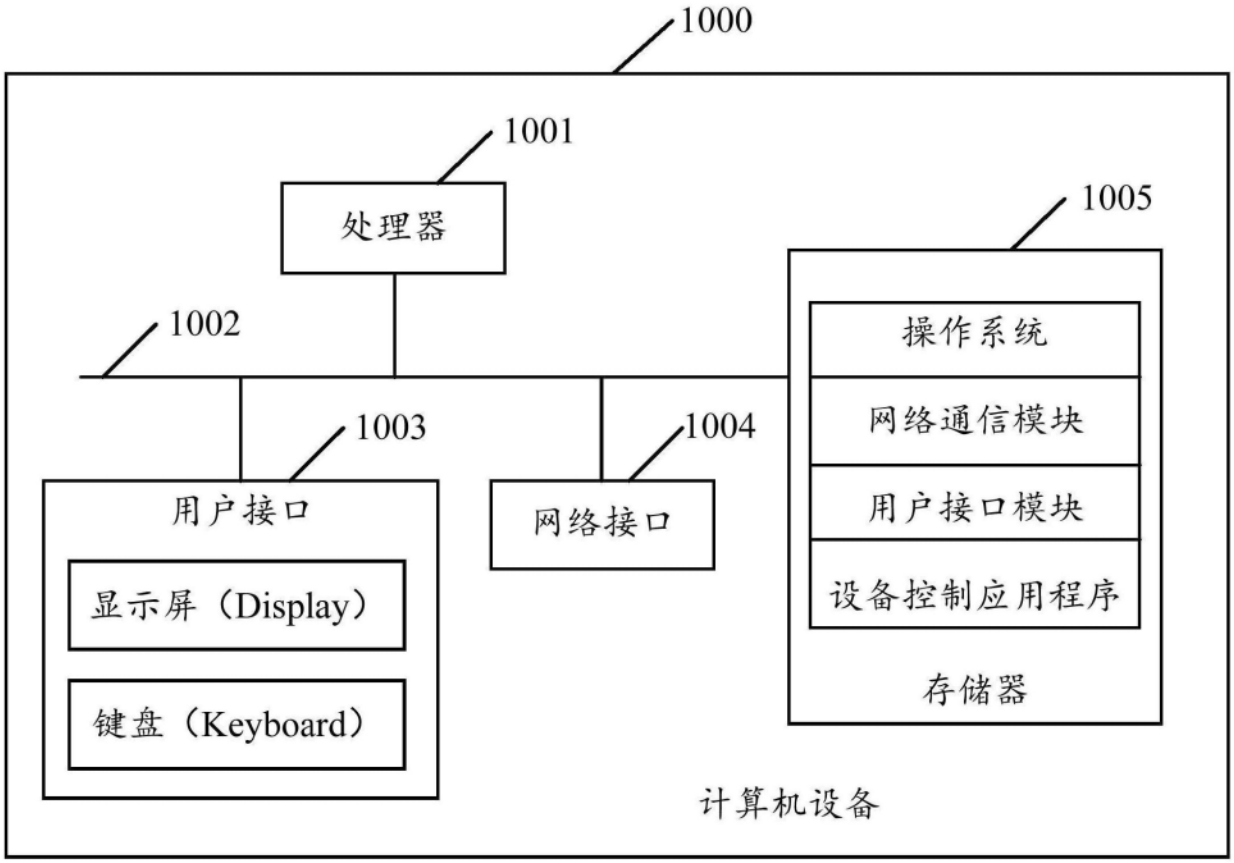

1000
1001
处理器
1005
1002
操作系统
网络通信模块
用户接口模块
设备控制应用程序
存储器
1003
1004
用户接口
网络接口
显示屏（Display）
键盘（Keyboard）
计算机设备

图11

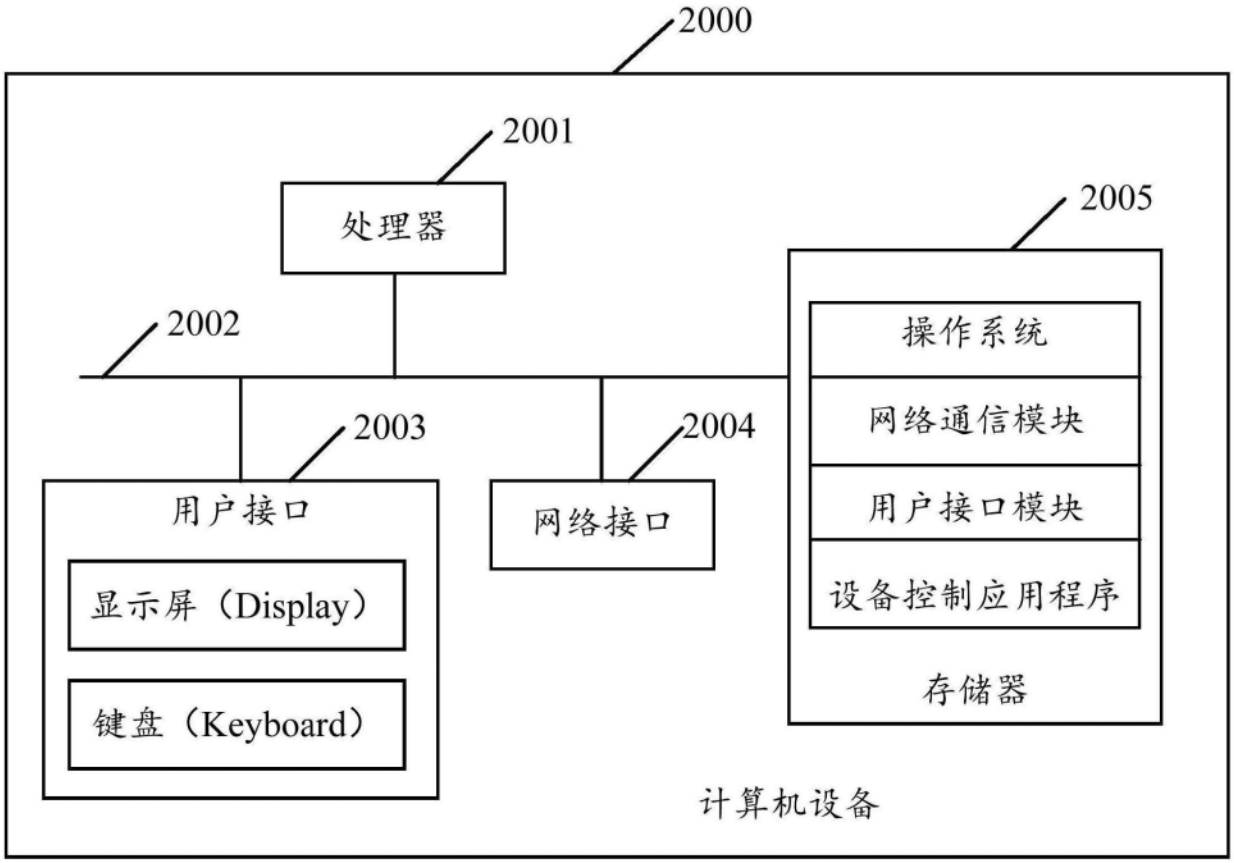

2000
2001
处理器
2005
2002
操作系统
网络通信模块
用户接口模块
设备控制应用程序
存储器
2003
2004
用户接口
网络接口
显示屏（Display）
键盘（Keyboard）
计算机设备

图12