(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 107729847 B
(45)授权公告日 2020.08.04

(21)申请号 201710985755.5

(22)申请日 2017.10.20

(65)同一申请的已公布的文献号
申请公布号 CN 107729847 A

(43)申请公布日 2018.02.23

(73)专利权人 阿里巴巴集团控股有限公司
地址 英属开曼群岛大开曼资本大厦一座四层847号邮箱

(72)发明人 郑丹丹 徐崴 李亮

(74)专利代理机构 北京博思佳知识产权代理有限公司 11415
代理人 林祥

(51)Int.Cl.
G06K 9/00(2006.01)
G06K 9/18(2006.01)
G06K 9/62(2006.01)

(56)对比文件
CN 102713930 A,2012.10.03
CN 107071281 A,2017.08.18
CN 103257801 A,2013.08.21
CN 103745474 A,2014.04.23
US 2015227946 A1,2015.08.13
黄伟杰.无人机智能化视频监控嵌入式系统.《中国优秀硕士学位论文全文数据库》.中国学术期刊(光盘版)电子杂志社,2014,C031-71.

审查员 王文武

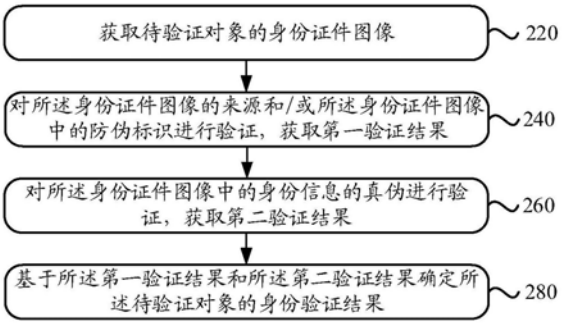
权利要求书4页 说明书17页 附图3页

(54)发明名称

一种证件验证、身份验证方法和装置

(57)摘要

本申请公开了一种证件验证、身份验证方法和装置。方法包括:获取待验证对象的身份证件图像;对所述身份证件图像的来源和/或所述身份证件图像中的防伪标识进行验证,获取第一验证结果;对所述身份证件图像中的身份信息的真伪进行验证,获取第二验证结果;基于所述第一验证结果和所述第二验证结果确定所述待验证对象的身份验证结果。



CN 107729847 B

1.一种证件验证方法,包括:

获取待验证身份证件的证件图像;

对所述证件图像中的防伪标识和所述证件图像的来源进行验证,获取第一验证结果;

基于所述第一验证结果确定所述待验证证件的验证结果;

所述对所述证件图像的来源进行验证包括:

将所述证件图像的背景区域与预先采集的第一背景图像进行对比,确定重叠度,并基于所述重叠度验证证件图像的来源;

所述确定重叠度包括:

基于采集身份证件图像时陀螺仪的第一位置信息和采集所述第一背景图像时陀螺仪的第二位置信息,对两者的角度进行调整,以对比同一陀螺仪位置信息下的所述背景区域与第一背景图像,获取重叠度。

2.根据权利要求1所述的方法,对所述证件图像中的防伪标识进行验证,获取第一验证结果包括:

确定与所述证件图像的类型对应的证件中的防伪标识;

基于确定的防伪标识验证所述证件图像中的防伪标识,获取第一验证结果,所述第一验证结果用于表示所述证件图像中存在对应的防伪标识的概率。

3.根据权利要求2所述的方法,所述防伪标识包括:水印文字、微缩文字、底纹线条、凹版印刷、偏色、防伪暗记、字体中的至少一个。

4.根据权利要求1所述的方法,对所述证件图像的来源进行验证,获取第一验证结果包括:

对所述证件图像的图像数据进行分析,确定第一验证结果,所述第一验证结果用于表示所述证件图像来源于实体证件的概率。

5.根据权利要求4所述的方法,所述对所述证件图像的图像数据进行分析包括:

对所述证件图像中的单帧图像的图像数据进行图像识别处理;

或者,

对所述证件图像中的至少两类图像的图像数据进行差值处理,获取图像差值;将所述图像差值作为预建立分类模型的输入,所述分类模型用于基于输入的图像差值输出第一验证结果。

6.根据权利要求1所述的方法,对所述证件图像的来源和所述证件图像中的防伪标识进行验证,获取第一验证结果包括:

确定与所述证件图像的类型对应的证件中的防伪标识;

基于确定的防伪标识验证所述证件图像中的防伪标识,并根据验证结果确定所述证件图像通过验证的概率;

对所述证件图像的图像数据进行分析,确定所述证件图像来源于实体证件的概率;

基于所述证件图像通过验证的概率和来源于实体证件的概率确定第一验证结果。

7.一种身份验证方法,包括:

获取待验证对象的身份证件图像;

基于权利要求1-6任一项,获取所述身份证件图像对应的身份证件的第一验证结果;对所述身份证件图像中的身份信息的真伪进行验证,获取第二验证结果;

基于所述第一验证结果和所述第二验证结果确定所述待验证对象的身份验证结果。

8.根据权利要求7所述的方法，所述获取待验证对象的身份证件图像包括：

现场采集待验证对象的身份证件图像。

9.根据权利要求7所述的方法，所述获取待验证对象的身份证件图像包括：

获取在先采集的待验证对象的身份证件图像。

10.根据权利要求7所述的方法，所述对所述身份证件图像中的身份信息的真伪进行验证，获取第二验证结果包括：

对所述身份证件图像中的身份信息进行联网核查，并根据联网核查的结果确定所述身份信息的真伪。

11.根据权利要求10所述的方法，所述对所述身份证件图像中的身份信息进行联网核查包括：

分别对所述身份信息中的文字信息和证脸图像进行联网核查。

12.根据权利要求11所述的方法，对所述身份信息中的证脸图像进行联网核查之前，还包括：

现场采集持证人的人脸图像；

其中，对所述身份信息中的证脸图像进行联网核查，包括：

将所述证脸图像、所述持证人的人脸图像和联网核查获取的人脸图像进行交叉验证。

13.根据权利要求12所述的方法，在确定所述身份信息的真伪之前，还包括：

基于所述持证人的人脸图像进行活体检测，获取活体检测结果；

其中，确定所述身份信息的真伪包括：

基于所述联网核查的结果和所述活体检测结果确定所述身份信息的真伪。

14.根据权利要求7-13任一项所述的方法，基于所述第一验证结果和所述第二验证结果确定所述待验证对象的身份验证结果包括：

若所述第二验证结果为未通过，则确定所述身份验证结果为未通过；

或者，

若所述第二验证结果为通过，则基于所述第一验证结果确定所述身份验证结果是否为通过。

15.根据权利要求7-13任一项所述的方法，基于所述第一验证结果和所述第二验证结果确定所述待验证对象的身份验证结果包括：

若所述第二验证结果为通过，则基于第一验证结果确定所述身份验证结果为通过的概率。

16.一种身份验证装置，包括：

获取单元，用于获取待验证身份证件的证件图像；

第一验证单元，用于对所述证件图像中的防伪标识和所述证件图像的来源进行验证，获取第一验证结果；

确定单元，用于基于所述第一验证结果确定所述待验证证件的验证结果；

所述对所述证件图像的来源进行验证包括：

将所述证件图像的背景区域与预先采集的第一背景图像进行对比，确定重叠度，并基于所述重叠度验证证件图像的来源；

所述确定重叠度包括：

基于采集身份证件图像时陀螺仪的第一位置信息和采集所述第一背景图像时陀螺仪的第二位置信息，对两者的角度进行调整，以对比同一陀螺仪位置信息下的所述背景区域与第一背景图像，获取重叠度。

17.根据权利要求16所述的装置，所述第一验证单元，用于确定与所述证件图像的类型对应的证件中的防伪标识；

基于确定的防伪标识验证所述证件图像中的防伪标识，获取第一验证结果，所述第一验证结果用于表示所述证件图像中存在对应的防伪标识的概率。

18.根据权利要求17所述的装置，所述防伪标识包括：水印文字、微缩文字、底纹线条、凹版印刷、偏色、防伪暗记、字体中的至少一个。

19.根据权利要求16所述的装置，所述第一验证单元，用于对所述证件图像的图像数据进行分析，确定第一验证结果，所述第一验证结果用于表示所述证件图像来源于实体证件的概率。

20.根据权利要求19所述的装置，所述第一验证单元，用于对所述证件图像中的单帧图像的图像数据进行图像识别处理；或者，对所述身份证件图像中的至少两类图像的图像数据进行差值处理，获取图像差值；将所述图像差值作为预建立分类模型的输入，所述分类模型用于基于输入的图像差值输出第一验证结果。

21.根据权利要求16所述的装置，所述第一验证单元，用于确定与所述证件图像的类型对应的证件中的防伪标识；基于确定的防伪标识验证所述证件图像中的防伪标识，并根据验证结果确定所述证件图像通过验证的概率；对所述证件图像的图像数据进行分析，确定所述证件图像来源于实体证件的概率；基于所述证件图像通过验证的概率和来源于实体证件的概率确定第一验证结果。

22.一种身份验证装置，包括：权利要求16-21任一项所述的第一验证单元，以及

获取单元，用于获取待验证对象的身份证件图像；

第二验证单元，用于对所述身份证件图像中的身份信息的真伪进行验证，获取第二验证结果；

确定单元，用于基于所述第一验证单元获得的第一验证结果和所述第二验证结果确定所述待验证对象的身份验证结果。

23.根据权利要求22所述的装置，所述获取单元，用于现场采集所述待验证对象的身份证件图像。

24.根据权利要求22所述的装置，所述获取单元，用于获取在先采集的所述待验证对象的身份证件图像。

25.根据权利要求22所述的装置，所述第二验证单元，用于对所述身份证件图像中的身份信息进行联网核查，并根据联网核查的结果确定所述身份信息的真伪。

26.根据权利要求25所述的装置，所述第二验证单元，用于分别对所述身份信息中的文字信息和证脸图像进行联网核查。

27.根据权利要求26所述的装置，还包括：采集单元；

所述采集单元，用于现场采集持证人的人脸图像；

所述第二验证单元，用于将所述证脸图像、所述持证人的人脸图像和联网核查获取的

人脸图像进行交叉验证。

28.根据权利要求27所述的装置，所述第二验证单元，还用于基于所述持证人的人脸图像进行活体检测，获取活体检测结果；基于所述联网核查的结果和所述活体检测结果确定所述身份信息的真伪。

29.根据权利要求22-28任一项所述的装置，所述确定单元，用于若所述第二验证结果为未通过，则确定所述身份验证结果为未通过；或者，若所述第二验证结果为通过，则基于所述第一验证结果确定所述身份验证结果是否为通过。

30.根据权利要求22-28任一项所述的装置，所述确定单元，用于若所述第二验证结果为通过，则基于第一验证结果确定所述身份验证结果为通过的概率。

31.一种身份验证装置，包括：

处理器；以及

被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器执行以下操作：

获取待验证身份证件的证件图像；

对所述证件图像中的防伪标识和所述证件图像的来源进行验证，获取第一验证结果；

基于所述第一验证结果确定所述待验证证件的验证结果；

所述对所述证件图像的来源进行验证包括：

将所述证件图像的背景区域与预先采集的第一背景图像进行对比，确定重叠度，并基于所述重叠度验证证件图像的来源；

所述确定重叠度包括：

基于采集身份证件图像时陀螺仪的第一位置信息和采集所述第一背景图像时陀螺仪的第二位置信息，对两者的角度进行调整，以对比同一陀螺仪位置信息下的所述背景区域与第一背景图像，获取重叠度。

32.一种身份验证装置，包括：

处理器；以及

被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器执行以下操作：

获取待验证对象的身份证件图像；

对所述身份证件图像的来源和所述身份证件图像中的防伪标识进行验证，获取第一验证结果；

对所述身份证件图像中的身份信息的真伪进行验证，获取第二验证结果；

基于所述第一验证结果和所述第二验证结果确定所述待验证对象的身份验证结果；

所述对所述身份证件图像的来源进行验证包括：

将所述身份证件图像的背景区域与预先采集的第一背景图像进行对比，确定重叠度，并基于所述重叠度验证证件图像的来源；

所述确定重叠度包括：

基于采集所述身份证件图像时陀螺仪的第一位置信息和采集所述第一背景图像时陀螺仪的第二位置信息，对两者的角度进行调整，以对比同一陀螺仪位置信息下的所述背景区域与第一背景图像，获取重叠度。

一种证件验证、身份验证方法和装置

技术领域

[0001] 本申请涉及互联网技术领域，尤其涉及一种证件验证、身份验证方法和装置。

背景技术

[0002] 互联网时代，许多事情都越来越便利，用户只需在终端设备上进行操作即可办理所需的业务。但是，由于部分业务被要求很高的安全等级，需要对用户填写的信息和提供的证明文件的真实性、完整性、合规性进行认真审查，以避免被不法分子所乘。因此，必须线下通过特定业务办理系统办理相关业务。

[0003] 例如：由于存在太多证件伪造、翻拍的情况。因此，一般会要求用户提供身份证件给柜台人员，由柜台人员用专业授权机器读取身份证芯片，进行联网核查。

[0004] 虽然，现有技术方案能在一定程度上解决证件伪造、翻拍的问题，但依然无法满足线上办理相关业务的需求，因此，需要更加可靠的方案。

发明内容

[0005] 本说明书实施例提供一种证件验证、身份验证方法和装置，用于解决现有技术提供地身份验证方案无法满足线上办理相关业务所需安全等级的问题。

[0006] 本说明书实施例提供一种证件验证方法，包括：

[0007] 获取待验证证件的证件图像；

[0008] 对所述证件图像中的防伪标识和/或所述证件图像的来源进行验证，获取第一验证结果；

[0009] 基于所述第一验证结果确定所述待验证证件的验证结果。

[0010] 可选的，对所述证件图像中的防伪标识进行验证，获取第一验证结果包括：

[0011] 确定与所述证件图像的类型对应的证件中的防伪标识；

[0012] 基于确定的防伪标识验证所述证件图像中的防伪标识，获取第一验证结果，所述第一验证结果用于表示所述证件图像中存在对应的防伪标识的概率。

[0013] 可选的，所述防伪标识包括：水印文字、微缩文字、底纹线条、凹版印刷、偏色、防伪暗记、字体中的至少一个。

[0014] 可选的，对所述证件图像的来源进行验证，获取第一验证结果包括：

[0015] 对所述证件图像的图像数据进行分析，确定第一验证结果，所述第一验证结果用于表示所述证件图像来源于实体证件的概率。

[0016] 可选的，所述对所述证件图像的图像数据进行分析包括：

[0017] 对所述证件图像中的单帧图像的图像数据进行图像识别处理；

[0018] 或者，

[0019] 对所述证件图像中的至少两类图像的图像数据进行差值处理，获取图像差值；将所述图像差值作为预建立分类模型的输入，所述分类模型用于基于输入的图像差值输出第一验证结果。

[0020] 可选的，对所述证件图像的来源和所述证件图像中的防伪标识进行验证，获取第一验证结果包括：

[0021] 确定与所述证件图像的类型对应的证件中的防伪标识；

[0022] 基于确定的防伪标识验证所述证件图像中的防伪标识，并根据验证结果确定所述证件图像通过验证的概率；

[0023] 对所述证件图像的图像数据进行分析，确定所述证件图像来源于实体证件的概率；

[0024] 基于所述证件图像通过验证的概率和来源于实体证件的概率确定第一验证结果。

[0025] 本说明书实施例还提供一种身份验证方法，包括：

[0026] 获取待验证对象的身份证件图像；

[0027] 基于上述证件验证方法，获取所述身份证件图像对应的身份证件的第一验证结果；对所述身份证件图像中的身份信息的真伪进行验证，获取第二验证结果；

[0028] 基于所述第一验证结果和所述第二验证结果确定所述待验证对象的身份验证结果。

[0029] 可选的，所述获取待验证对象的身份证件图像包括：

[0030] 现场采集待验证对象的身份证件图像。

[0031] 可选的，所述获取待验证对象的身份证件图像包括：

[0032] 获取在先采集的待验证对象的身份证件图像。

[0033] 可选的，所述对所述身份证件图像中的身份信息的真伪进行验证，获取第二验证结果包括：

[0034] 对所述身份证件图像中的身份信息进行联网核查，并根据联网核查的结果确定所述身份信息的真伪。

[0035] 可选的，所述对所述身份证件图像中的身份信息进行联网核查包括：

[0036] 分别对所述身份信息中的文字信息和证脸图像进行联网核查。

[0037] 可选的，对所述身份信息中的证脸图像进行联网核查之前，还包括：

[0038] 现场采集持证人的人脸图像；

[0039] 其中，对所述身份信息中的证脸图像进行联网核查，包括：

[0040] 将所述证脸图像、所述持证人的人脸图像和联网核查获取的人脸图像进行交叉验证。

[0041] 可选的，在确定所述身份信息的真伪之前，还包括：

[0042] 基于所述持证人的人脸图像进行活体检测，获取活体检测结果；

[0043] 其中，确定所述身份信息的真伪包括：

[0044] 基于所述联网核查的结果和所述活体检测结果确定所述身份信息的真伪。

[0045] 可选的，基于所述第一验证结果和所述第二验证结果确定所述待验证对象的身份验证结果包括：

[0046] 若所述第二验证结果为未通过，则确定所述身份验证结果为未通过；

[0047] 或者，

[0048] 若所述第二验证结果为通过，则基于所述第一验证结果确定所述身份验证结果是否为通过。

[0049] 可选的，基于所述第一验证结果和所述第二验证结果确定所述待验证对象的身份验证结果包括：

[0050] 若所述第二验证结果为通过，则基于第一验证结果确定所述身份验证结果为通过的概率。

[0051] 本说明书实施例还提供一种身份验证装置，包括：

[0052] 获取单元，用于获取待验证证件的证件图像；

[0053] 第一验证单元，用于对所述证件图像中的防伪标识和/或所述证件图像的来源进行验证，获取第一验证结果；

[0054] 确定单元，用于基于所述第一验证结果确定所述待验证证件的验证结果。

[0055] 可选的，所述第一验证单元，用于确定与所述证件图像的类型对应的证件中的防伪标识；

[0056] 基于确定的防伪标识验证所述证件图像中的防伪标识，获取第一验证结果，所述第一验证结果用于表示所述证件图像中存在对应的防伪标识的概率。

[0057] 可选的，所述防伪标识包括：水印文字、微缩文字、底纹线条、凹版印刷、偏色、防伪暗记、字体中的至少一个。

[0058] 可选的，所述第一验证单元，用于对所述证件图像的图像数据进行分析，确定第一验证结果，所述第一验证结果用于表示所述证件图像来源于实体证件的概率。

[0059] 可选的，所述第一验证单元，用于对所述证件图像中的单帧图像的图像数据进行图像识别处理；或者，对所述身份证件图像中的至少两类图像的图像数据进行差值处理，获取图像差值；将所述图像差值作为预建立分类模型的输入，所述分类模型用于基于输入的图像差值输出第一验证结果。

[0060] 可选的，所述第一验证单元，用于确定与所述证件图像的类型对应的证件中的防伪标识；基于确定的防伪标识验证所述证件图像中的防伪标识，并根据验证结果确定所述证件图像通过验证的概率；对所述证件图像的图像数据进行分析，确定所述证件图像来源于实体证件的概率；基于所述证件图像通过验证的概率和来源于实体证件的概率确定第一验证结果。

[0061] 本说明书实施例还提供一种身份验证装置，包括：上述的第一验证单元，以及

[0062] 获取单元，用于获取待验证对象的身份证件图像；

[0063] 第二验证单元，用于对所述身份证件图像中的身份信息的真伪进行验证，获取第二验证结果；

[0064] 确定单元，用于基于所述第一验证单元获得的第一验证结果和所述第二验证结果确定所述待验证对象的身份验证结果。

[0065] 可选的，所述获取单元，用于现场采集所述待验证对象的身份证件图像。

[0066] 可选的，所述获取单元，用于获取在先采集的所述待验证对象的身份证件图像。

[0067] 可选的，所述第二验证单元，用于对所述身份证件图像中的身份信息进行联网核查，并根据联网核查的结果确定所述身份信息的真伪。

[0068] 可选的，所述第二验证单元，用于分别对所述身份信息中的文字信息和证脸图像进行联网核查。

[0069] 可选的，还包括：采集单元；

[0070] 所述采集单元，用于现场采集持证人的人脸图像；

[0071] 所述第二验证单元，用于将所述证脸图像、所述持证人的人脸图像和联网核查获取的人脸图像进行交叉验证。

[0072] 可选的，所述第二验证单元，还用于基于所述持证人的人脸图像进行活体检测，获取活体检测结果；基于所述联网核查的结果和所述活体检测结果确定所述身份信息的真伪。

[0073] 可选的，所述确定单元，用于若所述第二验证结果为未通过，则确定所述身份验证结果为未通过；或者，若所述第二验证结果为通过，则基于所述第一验证结果确定所述身份验证结果是否为通过。

[0074] 可选的，所述确定单元，用于若所述第二验证结果为通过，则基于第一验证结果确定所述身份验证结果为通过的概率。

[0075] 本说明书实施例还提供一种身份验证装置，包括：

[0076] 处理器；以及

[0077] 被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器执行以下操作：

[0078] 获取待验证证件的证件图像；

[0079] 对所述证件图像的来源和/或所述证件图像中的防伪标识进行验证，获取第一验证结果；

[0080] 基于所述第一验证结果确定所述待验证证件的验证结果。

[0081] 本说明书实施例还提供一种身份验证装置，包括：

[0082] 处理器；以及

[0083] 被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器执行以下操作：

[0084] 获取待验证对象的身份证件图像；

[0085] 对所述身份证件图像的来源和/或所述身份证件图像中的防伪标识进行验证，获取第一验证结果；

[0086] 对所述身份证件图像中的身份信息的真伪进行验证，获取第二验证结果；

[0087] 基于所述第一验证结果和所述第二验证结果确定所述待验证对象的身份验证结果。

[0088] 本说明书实施例采用的上述至少一个技术方案能够达到以下有益效果：

[0089] 本说明书实施例通过对身份证件图像的真伪以及身份证件图像中身份信息的真伪进行验证，与现有技术中使用专业授权机器实现身份验证的方案相比，能在不使用专业授权机器的前提下有效解决证件内容伪造、翻拍证件等情况，进而为线上办理相关业务提供满足所需安全等级的身份验证能力。

附图说明

[0090] 此处所说明的附图用来提供对本申请的进一步理解，构成本申请的一部分，本申请的示意性实施例及其说明用于解释本申请，并不构成对本申请的不当限定。在附图中：

[0091] 图1为本说明书实施例的应用场景图；

[0092] 图2为本说明书实施例1提供的身份验证方法的流程示意图；

[0093] 图3为本说明书实施例2提供的身份验证方法的流程示意图；

[0094] 图4为本说明书实施例3提供的身份验证装置的结构示意图；

[0095] 图5为本说明书实施例4提供的身份验证装置的结构示意图；

[0096] 图6为本说明书实施例5提供的电子设备的结构示意图。

具体实施方式

[0097] 为使本申请的目的、技术方案和优点更加清楚，下面将结合本申请具体实施例及相应的附图对本申请技术方案进行清楚、完整地描述。显然，所描述的实施例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，都属于本申请保护的范围。

[0098] 参见图1，该图示出了本说明书实施例的一种示例性应用场景。该场景中，用户在办理相关业务时，可以通过终端设备13中的应用程序(Application，app)填写相关信息，并在满足预设条件时，采集身份证件图像，并上传至业务授权系统的设备12和/或设备11，由设备12和/或设备11针对身份证件图像进行验证，并基于验证结果响应用户办理的业务。这里的相关业务可以是各种在线办理的业务，比如，远程开户。对应的，身份证件图像可以为用户身份证的图像。

[0099] 本说明书实施例的另一种示例性应用场景可以为：

[0100] 用户通过终端设备向授权系统的客户端展示身份证件图像，或者，用户向授权系统的客户端展示身份证件，由客户端采集身份证件的图像。然后，客户端将身份证件图像上传至授权系统的服务器，由服务器进行验证，并向客户端返回验证结果，由客户端基于验证结果确定是否授权用户。

[0101] 其中，此过程可发生在用户过安检、登录需授权平台等过程中。另外，办理业务的用户与身份证件对应的用户是否需要一致具体视业务办理方的规定而定。

[0102] 本说明书实施例的应用场景除上述例示出的两种外，还可以是各种其他场景，在此不做特别限定，只要在技术上能够应用到本说明书提供到的方案均可使用。下面结合附图，详细说明本申请各实施例提供的技术方案。

[0103] 实施例1

[0104] 图2为本说明书实施例1提供的身份验证方法的流程示意图，参见图2，该方法可以具体包括如下步骤：

[0105] 步骤220、获取待验证对象的身份证件图像；

[0106] 其中，身份证件图像可以为拍摄身份证件获取的图像，身份证件可以为：身份证、临时身份证、学历证、驾照等可以证明待验证对象身份的证件，身份证件中记载有待验证对象的身份信息，例如：姓名、身份证号、学籍号等等。

[0107] 需要说明的是，步骤220的一种实现方式可以为：现场采集待验证对象的的身份证件图像。此处的“现场”为需要验证身份的“现场”，其可以是验证身份办理业务的现场，例如：在办理开户业务时，采集待验证对象的身份证的图像的现场；也可以不是办理业务的现场，例如：在过安检时，采集待验证对象的相关证件的图像的现场。

[0108] 结合图1，不难理解的是，“现场采集身份证件图像”的方式可以具体为：

[0109] 用户自主打开拍摄界面，或者，基于用户的操作，授权系统调用终端设备的摄像头以开启拍摄界面，然后，拍摄待验证对象的身份证件获取身份证件图像。

[0110] 步骤220的另一种实现方式可以为：获取在先采集的待验证对象的身份证件图像。此处的“在先”用于区别步骤220的上一种实现方式中的“现场”，本实现方式可举例为：将之前拍摄的身份证件图像存储在预定位置，当需要进行身份验证时，基于存储地址获取对应的身份证件图像。

[0111] 步骤240、对所述身份证件图像的来源和/或所述身份证件图像中的防伪标识进行验证，获取第一验证结果；

[0112] 本步骤中的身份证件图像的来源可以为多种来源，比如，拍摄于实体的身份证件、ps后/未ps的证件照片、证件的复印件、屏幕翻拍、预定的拍摄场景等等。防伪标识为是能粘贴、印刷、热转移在标的物表面，或标的物包装上，或标的物附属物(如商品挂牌、名片以及防伪证卡)上，具有防伪作用的标识。例如：身份证上的防伪标识包括：国徽、证件名称、长城图案、证件的签发机关和有效期及彩色花纹等等。

[0113] 需要说明的是，对于不同的业务，由于其所需安全等级不同，可选择性的设置合法来源和防伪标识的完整度。对于安全等级要求比较高的业务而言，例如：远程开户。需满足条件：身份证件图像的来源是实体的身份证件和具备完整的防伪标识，或者满足该条件的概率达到一定的阈值。而对于安全等级要求比较低的业务而言，满足的条件可适当放宽。

[0114] 下面以“远程开户”为例对步骤240的实现进行示例性说明：首先，对步骤240中验证身份证件图像的来源的实现方式进行示例说明，包括：验证身份证件图像是否来源于实体证件、验证身份证件图像是否与现场采集的图像来源于同一拍摄环境；然后，基于验证身份证件图像的来源的实现方式，此处列举五种实现方式。本领域技术人员在此基础上可以扩展出其他的实现方式，这些方式均在本申请的保护范围之内：

[0115] 第一种实现方式：

[0116] 这种实现方式可以适用于对安全等级要求较高的场合，比如，要求身份证件图像具备完整的防伪标识，或者满足该条件的概率达到一定的阈值。具体可以为：

[0117] 确定与所述身份证件图像的类型对应的身份证件中的防伪标识；基于确定的防伪标识验证所述身份证件图像中的防伪标识，并根据验证结果确定第一验证结果，所述第一验证结果用于表示所述身份证件图像通过验证的概率。其中，防伪标识包括：水印文字、微缩文字、底纹线条、凹版印刷、偏色、防伪暗记、字体中的至少一个。

[0118] 需要说明的是，不同类型的身份证件对应有不同的防伪标识，例如：身份证、护照、驾驶证均有与之对应的防伪标记。相应地，可基于用户在办理业务的过程中选择的证件类型确定采集的身份证件图像的类型，或者，对采集的身份证件图像进行图像识别处理，以确定身份证件图像的类型。

[0119] 另外，不难理解的是，可通过训练分类模型的方式，将身份证件图像中的防伪标识作为分类模型的输入，或者，将身份证件图像作为分类模型的输入，分类模型输出身份证件图像通过防伪标识验证的概率。其中，扫描身份证件图像以获取防伪标识的方式可举例为：采用透光检查识别水印文字等。

[0120] 第二种实现方式可以为：

[0121] 这种实现方式对前提条件要求是身份证件图像的来源是实体身份证件，或者满足

该条件的概率达到一定的阈值。具体可以由下面两种方案实现：

[0122] 第一种方案(身份证件图像至少为一张)：

[0123] 首先，对所述身份证件图像进行第一次验证，以确定所述身份证件图像来源于屏幕翻拍的概率；其次，对所述身份证件图像进行第二次验证，以确定所述身份证件图像来源于复印件的概率；最后，基于所述身份证件图像来源于屏幕翻拍的概率和来源于复印件的概率确定所述身份证件图像来源于实体证件的概率。其中，第一次验证和第二次验证的顺序此处不做限定，可并行也可串行。

[0124] 第一种方案中，第一次验证具体可以按照如下方式进行：

[0125] 基于预定特定特征，对所述身份证件图像中的证件区域特征检测，以结合屏幕摩尔纹分类模型对比正常身份证件图像和屏幕翻拍的身份证件图像在证件区域之间的差异性；其中，特定特征可举例为：屏幕摩尔纹、证件水印、印刷反光等特征。以及，基于预定特定特征，对所述身份证件图像的边框进行特征检测，以结合屏幕边框分类模型对比正常身份证件图像和屏幕翻拍的身份证件图像的边框之间的差异性，例如：屏幕翻拍的身份证件图像通过有黑边框。其中，特定特征可举例为：屏幕摩尔纹、证件水印、印刷反光等特征。所述证件区域为所述身份证件图像对应的身份证件的区域。

[0126] 第一种方案中，第二次验证具体可以按照如下方式进行：

[0127] 基于黑白复印件和/或彩色复印件对应的像素级特征，对所述身份证件图像的图像数据进行特征检测。具体实现方式可以是基于黑白复印件分类DNN模型检测所述身份证件图像中对应的像素级特征，确定所述身份证件图像为黑白复印件的概率。基于彩色复印件分类DNN模型检测所述身份证件图像中对应的像素级特征，确定所述身份证件图像为彩色复印件的概率。

[0128] 经过上述第一次验证和第二次验证之后，再基于屏幕摩尔纹分类模型、屏幕框分类模型、黑白复印件分类DNN模型和彩色复印件分类DNN模型输出的结果中的至少一个确定身份证件图像的来源是真实的实体身份证件的概率。

[0129] 第二种方案：

[0130] 对所述身份证件图像的图像数据进行分析，确定第一验证结果，所述第一验证结果用于表示所述身份证件图像来源于实体证件的概率。具体可以为：

[0131] 对所述身份证件图像中的单帧图像的图像数据进行图像识别处理，验证身份证件图像中是否存在像素级别的特定特征，然后，基于身份证件图像中特定特征的存在情况确定第一验证结果。也可以将图像数据作为分类模型的输入，获取分类模型输出的第一验证结果。特定特征可举例为：屏幕摩尔纹、证件水印、印刷反光等。

[0132] 或者，

[0133] 至少有两类身份证件图像，对所述身份证件图像中的至少两类图像的图像数据进行差值处理，获取图像差值；将所述图像差值作为预建立分类模型的输入，所述分类模型用于基于输入的图像差值输出第一验证结果；其中，所述至少两类图像可以为不同拍摄条件下采集的两类图像，例如：自然条件下采集的一类图像和闪光灯下采集的一类图像，或者，不同曝光度下采集的图像。进一步地，差值处理的对象可以为自然条件下采集的图像与闪光灯下采集的图像。

[0134] 第三种实现方式可以为：

[0135] 这种实现方式对前提条件要求是身份证件图像的来源是真实的实体身份证件和具备完整的防伪标识，或者，满足该条件的概率达到一定的阈值。

[0136] 其实现过程与第一种和第二种实现方式相似，故，相似之处此处不再赘述。另外，第三种实现方式还包括：基于所述身份证件图像通过验证的概率和来源于实体证件的概率确定第一验证结果，即确定身份证件图像对应的待验证对象的身份证件的可信度。

[0137] 第四种实现方式可以为：

[0138] 这种实现方式可以适用于对安全等级要求较高的场合，比如，要求是身份证件图像与第一背景图像来源于同一拍摄场景，或者，满足该条件的概率达到一定的阈值。其中，安全等级要求与需要拍摄的身份证件图像相关，例如，要求越高，需要拍摄的身份证件图像越多且需要与第一背景图像来源于同一拍摄场景的身份证件图像也越多。具体可以为：

[0139] 在执行步骤220之前，预先采集一张或多张背景图像(下述简称为第一背景图像)，然后，将身份证件图像与第一背景图像进行对比，确定两者之间的重叠度。

[0140] 不难理解的是，若两者之间的重叠度大于一定阈值，则确定两者是在同一拍摄场景下完成的；而且，对比的方式可以为身份证件图像与单张背景图像之间的对比，也可以为将背景图像组合长一张背景图像后与身份证件图像进行对比。

[0141] 其中，确定两者是否在同一拍摄场景下的方案可以包括：将所述背景区域的图像中的背景区域与第一背景图像进行对比，获取所述身份证件图像与所述第一背景图像之间的重叠度；根据所述重叠度确定所述第一验证结果，所述第一验证结果用于表示所述身份证件图像与所述第一背景图像来源于同一拍摄场景的概率。所述背景区域为所述身份证件图像中身份证件所占区域之外的区域。

[0142] 为进一步提高第四种实现方式的验证效果和效率，可基于采集所述身份证件图像时陀螺仪的第一位置信息和采集所述第一背景图像时所述陀螺仪的第二位置信息，对两者的角度进行调整，以对比同一陀螺仪位置信息下的背景区域第一背景图像，获取重叠度，并基于重叠度确定两者拍摄于同一拍摄场景的概率。

[0143] 举例如下：在启动采集身份证件的图像之前，在陀螺仪处于第二位置信息时拍摄第一背景图像，例如：桌子及其周边的图像。然后，在陀螺仪处于第一位置信息下，采集身份证件的图像。然后，分离身份证件图像中的证件区域和背景区域，并基于陀螺仪的位置信息对比背景区域与第一背景图像，获取重叠度。其中，证件区域为份证件图像中身份证件所占区域。

[0144] 第五种实现方式可以为：

[0145] 这种实现方式可以适用于对安全等级要求较高的场合，比如，要求证件的材质为真是证件的材质，或者，满足该条件的概率达到一定的阈值。具体可以为：

[0146] 基于至少两类图像的图像数据获取的图像差值确定证件的材质，进而对比该证件的材质与对应类型的真实证件的材质，并基于对比结果确定该证件为真实证件的概率，作为第一验证结果。

[0147] 不难理解的是，不同类型的证件可能由不同的材质制作而成，而证件材质不同，会在不同拍摄条件下出现较大的差异性。由此，可将两类图像的图像差值输入至训练好的分类模型中，得到分类模型输出的第一验证结果。

[0148] 不难理解的是，上述几种可行的实现方式可基于待办理业务及其对应要求的安全

等级而合理选择，或者，合理交叉设置，此处不再赘述。

[0149] 步骤260、对所述身份证件图像中的身份信息的真伪进行验证，获取第二验证结果；

[0150] 需要说明的是，步骤260的一种实现方式可以为：

[0151] 对所述身份证件图像中的身份信息进行联网核查，并根据联网核查的结果确定所述身份信息的真伪。

[0152] 其中，联网核查的具体方式可以为：联网核查的公民身份信息系统以人民银行现有的内网和网间互联平台为基础，向公安部的信息共享系统转发人民银行用户以及通过帐户系统、征信系统、反洗钱系统各自的前置系统发出的核查请求；接受并转发商业银行用户以及通过其综合业务系统通过其前置系统发出的核查请求；接受并转发公安部信息共享系统的核查结果。

[0153] 另外，联网核查的对象可以包括：身份信息中的文字信息和证脸图像。文字信息可以为基于光学字符识别(Optical Character Recognition，OCR)识别获取的证件ID、姓名等信息，证脸图像为识别出的头像。

[0154] 步骤280、基于所述第一验证结果和所述第二验证结果确定所述待验证对象的身份验证结果。

[0155] 需要说明的是，基于步骤240和步骤260获取的第一验证结果和第二验证结果，本步骤的一种实现方式可以为：

[0156] 若第二验证结果为未通过，则确定所述身份验证结果为未通过；

[0157] 或者，

[0158] 若第二验证结果为通过，则基于所述第一验证结果确定所述身份验证结果是否为通过。具体可以为：当第一验证结果对应的通过的概率低于预定阈值时，则确定所述身份验证结果为未通过；当第一验证结果对应的通过的概率高于预定阈值时确定所述身份验证结果为通过。

[0159] 本步骤的另一种实现方式可以为：

[0160] 若所述第二验证结果为通过，则基于第一验证结果确定所述身份验证结果为通过/未通过的概率。

[0161] 对于步骤280的两种实现方式，由于上述每一个步骤都可能存在图像拍摄角度、拍摄质量等问题，导致整个流程不是一个顺序执行的过程，因此，本实施例提供一个决策引擎，以一定规则来评估整个验证的结果。举例如下：

[0162] 由于第一验证结果的影响因素可包括：身份证件图像通过防伪标识验证的概率、身份证件图像来源于实体证件的概率、身份证图像和现场图像来源于同一场景的概率中一个或多个，因此，在确定第一验证结果对应的概率时，可基于需求、经验等条件，对参与确定第一验证结果的影响因素设置对应的权重，并基于对应权重和概率确定第一验证结果对应的概率。例如：参与确定第一验证结果的影响因素身份证件图像通过防伪标识验证的概率、身份证件图像来源于实体证件的概率、身份证图像和现场图像来源于同一场景的概率分别为60％、70％、80％，设置的权重分别对应为30％、30％、40％，则最后计算出的第一验证结果对应的概率为71％。

[0163] 另外，为了提升证件真实性检测的速度和效率，上述对所述身份证件图像的来源

进行验证，对所述身份证件图像中的防伪标识进行验证，以及验证所述身份证件图像中的身份信息的真伪可以是并行实现的。

[0164] 不难理解的是，本发明实施例可选择性地仅执行步骤220-步骤240，以完成证件验证的过程，例如：

[0165] 获取待验证证件的证件图像；

[0166] 对所述证件图像的来源和/或所述证件图像中的防伪标识进行验证，获取第一验证结果；

[0167] 基于所述第一验证结果确定所述待验证证件的验证结果。

[0168] 或者，

[0169] 获取待验证证件的至少一张证件图像；

[0170] 对所述证件图像进行验证，以确定所述证件图像来源于屏幕翻拍的概率；

[0171] 根据所述证件图像来源于屏幕翻拍的概率获取所述待验证证件的验证结果。

[0172] 或者，

[0173] 对所述证件图像进行验证，以确定所述证件图像来源于复印件的概率；

[0174] 根据所述证件图像来源于复印件的概率获取所述待验证证件的验证结果。

[0175] 或者，

[0176] 对所述证件图像进行验证，以确定所述证件图像来源于屏幕翻拍的概率和来源于复印件的概率；

[0177] 基于所述证件图像来源于屏幕翻拍的概率和来源于复印件的概率获取所述待验证证件的验证结果。

[0178] 或者，

[0179] 获取待验证证件的证件图像；

[0180] 验证所述证件图像与现场预采集的第一背景图像是否来源于同一拍摄场景，获取所述待验证证件的验证结果。

[0181] 由于证件验证的过程与上述步骤220和步骤240中的相关描述相似，故，此处不再赘述。另外，基于实际需要，上述各个并列的证件验证方案可以相互交叉组合，例如：“防伪标识”+“是否来源于同一拍摄场景”的组合。

[0182] 可见，本发明实施例通过对身份证件图像的来源、防伪标识以及身份信息进行验证，能在不使用专业授权机器的前提下有效解决证件内容伪造、翻拍证件等情况，进而为线上办理相关业务提供满足所需安全等级的身份验证能力。

[0183] 实施例2

[0184] 图3为本说明书实施例2提供的身份验证方法的流程示意图，参见图3，本实施例在实施例1的基础上，还可以具体包括如下步骤：

[0185] 步骤320、现场采集持证人的人脸图像；

[0186] 需要说明的是，步骤320的一种实现方式可以为：

[0187] 在使用后置摄像头“现场采集身份证件图像”的同时或之后，使用前置摄像头采集“持证人的人脸图像”。

[0188] 另一种实现方式可以为：

[0189] 在第一验证结果的通过验证的概率达到预定阈值时，调用摄像头采集“持证人的

人脸图像”。

[0190] 又一种实现方式可以为：

[0191] 在将身份证件图像中的文字信息进行联网核查并得出文字信息为真的核查结果后，调用摄像头采集“持证人的人脸图像”。

[0192] 步骤340、基于所述持证人的人脸图像进行活体检测，获取活体检测结果；

[0193] 需要说明的是，基于步骤320采集的单帧图像或者多次图像进行活体检测，以确定持证人是否为活体。活体检测可举例为：眨眼判别、嘴部张合判别、视差分析方法等。由于活体检测为较为成熟的技术，故，此处不再赘述。

[0194] 步骤360、将所述证脸图像、所述持证人的人脸图像和联网核查获取的人脸图像进行交叉验证，获得证脸图像联网核查的结果；

[0195] 步骤360的一种实现方式可以为：

[0196] 将身份证件图像中的证脸图像与联网核查获取的人脸图像进行验证，得到第三验证结果；将证脸图像与现场采集的人脸图像进行对比，得到第四验证结果；基于第三验证结果和第四验证结果确定联网核查的结果。

[0197] 步骤380、基于所述证脸图像联网核查的结果和所述活体检测结果，结合文字信息的联网核查结果确定所述身份信息的真伪，获取第二验证结果。

[0198] 不难理解的是，基于实施例中的决策引擎，依据文字信息、证脸图像联网核查的结果和所述活体检测结果，结合一定的规则评估整个联网核查的核查结果。此处的规则可举例为：为核查的结果、活体检测的结果设置权重等。

[0199] 另外，本实施例中，在步骤320使用前置摄像头采集人脸图像的同时，后置摄像头将继续采集一张或多张(简称为第二背景图像)。相应地，为进一步地提高验证身份证件图像与背景图像是否来源于同一拍摄场景的精度，可基于采集所述身份证件图像、所述第一背景图像和所述第二背景图像时陀螺仪对应的位置信息，对比所述身份证件图像、所述第一背景图像和所述第二背景图像，确定第一验证结果；其中，所述第一验证结果用于表示所述身份证件图像、所述第一背景图像和所述第二背景图像来源于同一拍摄场景的概率。

[0200] 需要说明的是，本说明书实施例在实施例1的基础上，引入现场采集的持证人的人脸图像，并对人脸图像进行活体检测；然后，基于证脸图像、持证人的人脸图像和联网核查获取的人脸图像进行验证，进而基于活体检测和联网核查的结果确定身份信息的真伪。能避免持证人的身份和身份证件证明的身份不一致引起的身份被冒用的问题，进一步地的提高身份验证能力。

[0201] 需要说明的是，实施例1和2所提供方法的各步骤的执行主体均可以是同一设备，或者，该方法也由不同设备作为执行主体。比如，步骤220和步骤240的执行主体可以为设备1，步骤260的执行主体可以为设备2；又比如，步骤220的执行主体可以为设备1，步骤240和步骤260的执行主体可以为设备2；等等。

[0202] 另外，对于上述方法实施方式，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，本发明实施方式并不受所描述的动作顺序的限制，因为依据本发明实施方式，某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方式均属于优选实施方式，所涉及的动作并不一定是本发明实施方式所必须的。

[0203] 实施例3

[0204] 图4为本说明书实施例3提供的身份验证装置的结构示意图，装置包括：获取单元41、第一验证单元42、第二验证单元43和确定单元44，其中：

[0205] 获取单元41，用于获取待验证对象的身份证件图像；

[0206] 第一验证单元42，用于对所述身份证件图像的来源和/或所述身份证件图像中的防伪标识进行验证，获取第一验证结果；

[0207] 第二验证单元43，用于对所述身份证件图像中的身份信息的真伪进行验证，获取第二验证结果；

[0208] 确定单元44，用于基于所述第一验证结果和所述第二验证结果确定所述待验证对象的身份验证结果。

[0209] 下面对本实施例中的各功能模块的工作原理进行实例性说明：

[0210] 获取单元41的功能的实现方式可以为：

[0211] 现场采集待验证对象的身份证件图像。

[0212] 或者，

[0213] 获取在先采集的待验证对象的身份证件图像。

[0214] 第一验证单元42的功能的实现方式可以为：

[0215] 确定与所述身份证件图像的类型对应的身份证件中的防伪标识；基于确定的防伪标识验证所述身份证件图像中的防伪标识，并根据验证结果确定第一验证结果，所述第一验证结果用于表示所述身份证件图像通过验证的概率。

[0216] 其中，防伪标识包括：水印文字、微缩文字、底纹线条、凹版印刷、偏色、防伪暗记、字体中的至少一个。

[0217] 对所述身份证件图像进行第一次验证，以确定所述身份证件图像来源于屏幕翻拍的概率；

[0218] 对所述身份证件图像进行第二次验证，以确定所述身份证件图像来源于复印件的概率；

[0219] 基于所述身份证件图像来源于屏幕翻拍的概率和来源于复印件的概率确定所述身份证件图像来源于实体证件的概率。

[0220] 其中，第一次验证包括：

[0221] 基于预定特定特征，对所述身份证件图像中的证件区域和/或边框进行特征检测；

[0222] 其中，所述证件区域为所述身份证件图像对应的身份证件的区域。

[0223] 第二次验证包括：

[0224] 基于黑白复印件和/或彩色复印件对应的像素级特征，对所述身份证件图像的图像数据进行特征检测。

[0225] 对所述身份证件图像的图像数据进行分析，确定第一验证结果，所述第一验证结果用于表示所述身份证件图像来源于实体证件的概率。

[0226] 对所述身份证件图像中的单帧图像的图像数据进行图像识别处理；或者，对所述身份证件图像中的至少两类图像的图像数据进行差值处理，获取图像差值；将所述图像差值作为预建立分类模型的输入；其中，所述至少两类图像可以为不同拍摄条件下采集的两类图像，例如：自然条件下采集的一类图像和闪光灯下采集的一类图像、或者，不同曝光度

下采集的图像。

[0227] 确定与所述身份证件图像的类型对应的身份证件中的防伪标识;基于确定的防伪标识验证所述身份证件图像中的防伪标识,并根据验证结果确定所述身份证件图像通过验证的概率;对所述身份证件图像的图像数据进行分析,确定所述身份证件图像来源于实体证件的概率;基于所述身份证件图像通过验证的概率和来源于实体证件的概率确定第一验证结果。

[0228] 验证所述身份证件图像与现场预采集的第一背景图像是否来源于同一拍摄场景,获取第一验证结果。具体可以包括:

[0229] 将所述背景区域的图像中的背景区域与现场预采集的第一背景图像进行对比,获取所述身份证件图像与所述第一背景图像之间的重叠度;

[0230] 根据所述重叠度确定所述第一验证结果,所述第一验证结果用于表示所述身份证件图像与所述第一背景图像来源于同一拍摄场景的概率;

[0231] 其中,所述背景区域为所述身份证件图像中身份证件所占区域之外的区域。

[0232] 其中,将背景区域与现场预采集的第一背景图像进行对比包括:

[0233] 基于采集所述身份证件图像时陀螺仪的第一位置信息和采集所述第一背景图像时所述陀螺仪的第二位置信息,对比所述背景区域与所述第一背景图像。

[0234] 另外,在现场采集持证人的人脸图像时,采集第二背景图像;

[0235] 其中,所述验证所述身份证件图像与现场预采集的第一背景图像是否来源于同一拍摄场景,获取第一验证结果包括:

[0236] 基于采集所述身份证件图像、所述第一背景图像和所述第二背景图像时陀螺仪对应的位置信息,对比所述身份证件图像、所述第一背景图像和所述第二背景图像,确定第一验证结果;

[0237] 其中,所述第一验证结果用于表示所述身份证件图像、所述第一背景图像和所述第二背景图像来源于同一拍摄场景的概率。

[0238] 第二验证单元43的功能的实现方式可以为:

[0239] 对所述身份证件图像中的身份信息进行联网核查,并根据联网核查的结果确定所述身份信息的真伪。其中,可分别对所述身份信息中的文字信息和证脸图像进行联网核查。

[0240] 确定单元44的功能的实现方式可以为:

[0241] 若所述第二验证结果为未通过,则确定所述身份验证结果为未通过;或者,若所述第二验证结果为通过,则基于第一验证结果确定所述身份验证结果为通过的概率;或者,若所述第二验证结果为通过,则基于所述第一验证结果确定所述身份验证结果是否通过。

[0242] 可见,本发明实施例通过对身份证件图像的来源、防伪标识以及身份信息进行验证,能在不使用专业授权机器的前提下有效解决证件内容伪造、翻拍证件等情况,进而为线上办理相关业务提供满足所需安全等级的身份验证能力。

[0243] 实施例4

[0244] 图5为本说明书实施例4提供的身份验证装置的结构示意图,参见图5,装置包括:获取单元51、采集单元52、第一验证单元53、第二验证单元54和确定单元55,其中:

[0245] 获取单元51和第一验证单元53分别与实施例3中的获取单元41和第一验证单元42对应相似,故,此处不再对其进行赘述。

[0246] 另外，在实施例3的基础上，本实施例中：

[0247] 采集单元52，用于现场采集持证人的人脸图像；

[0248] 第二验证单元54，用于将所述证脸图像、所述持证人的人脸图像和联网核查获取的人脸图像进行交叉验证。

[0249] 第二验证单元54，还用于基于所述持证人的人脸图像进行活体检测，获取活体检测结果；基于所述联网核查的结果和所述活体检测结果确定所述身份信息的真伪。

[0250] 可见，本说明书实施例在实施例3的基础上，引入现场采集的持证人的人脸图像，并对人脸图像进行活体检测；然后，基于证脸图像、持证人的人脸图像和联网核查获取的人脸图像进行验证，进而基于活体检测和联网核查的结果确定身份信息的真伪。能避免持证人的身份和身份证件证明的身份不一致的问题，进一步地的提高身份验证能力。

[0251] 对于上述装置实施方式而言，由于其与方法实施方式基本相似，所以描述的比较简单，相关之处参见方法实施方式的部分说明即可。

[0252] 应当注意的是，在本发明的装置的各个部件中，根据其要实现的功能而对其中的部件进行了逻辑划分，但是，本发明不受限于此，可以根据需要对各个部件进行重新划分或者组合。

[0253] 实施例5

[0254] 图6为本说明书实施例5提供的一种电子设备的结构示意图，参见图6，该电子设备包括处理器、内部总线、网络接口、内存以及非易失性存储器，当然还可能包括其他业务所需要的硬件。处理器从非易失性存储器中读取对应的计算机程序到内存中然后运行，在逻辑层面上形成身份验证装置。当然，除了软件实现方式之外，本说明书并不排除其他实现方式，比如逻辑器件抑或软硬件结合的方式等等，也就是说以下处理流程的执行主体并不限定于各个逻辑单元，也可以是硬件或逻辑器件。

[0255] 网络接口、处理器和存储器可以通过总线系统相互连接。总线可以是ISA(Industry Standard Architecture，工业标准体系结构)总线、PCI(Peripheral Component Interconnect，外设部件互连标准)总线或EISA(Extended Industry Standard Architecture，扩展工业标准结构)总线等。所述总线可以分为地址总线、数据总线、控制总线等。为便于表示，图6中仅用一个双向箭头表示，但并不表示仅有一根总线或一种类型的总线。

[0256] 存储器用于存放程序。具体地，程序可以包括程序代码，所述程序代码包括计算机操作指令。存储器可以包括只读存储器和随机存取存储器，并向处理器提供指令和数据。存储器可能包含高速随机存取存储器(Random-Access Memory，RAM)，也可能还包括非易失性存储器(non-volatile memory)，例如至少1个磁盘存储器。

[0257] 处理器，用于执行所述存储器存放的程序，并具体执行：

[0258] 获取待验证证件的至少一张证件图像；

[0259] 对所述证件图像进行验证，以确定所述证件图像来源于屏幕翻拍的概率；

[0260] 根据所述证件图像来源于屏幕翻拍的概率获取所述待验证证件的验证结果。

[0261] 或者，

[0262] 获取待验证证件的至少一张证件图像；

[0263] 对所述证件图像进行验证，以确定所述证件图像来源于复印件的概率；

[0264] 根据所述证件图像来源于复印件的概率获取所述待验证证件的验证结果。

[0265] 或者，

[0266] 获取待验证证件的至少一张证件图像；

[0267] 对所述证件图像进行验证，以确定所述证件图像来源于屏幕翻拍的概率和来源于复印件的概率；

[0268] 基于所述证件图像来源于屏幕翻拍的概率和来源于复印件的概率获取所述待验证证件的验证结果。

[0269] 或者，

[0270] 获取待验证证件的证件图像；

[0271] 验证所述证件图像与现场预采集的第一背景图像是否来源于同一拍摄场景，获取所述待验证证件的验证结果。

[0272] 或者，

[0273] 获取待验证证件的证件图像；

[0274] 对所述证件图像的来源和/或所述证件图像中的防伪标识进行验证，获取第一验证结果；

[0275] 基于所述第一验证结果确定所述待验证证件的验证结果。

[0276] 或者，

[0277] 在上述几种证据验证方案的基础上，对所述身份证件图像中的身份信息的真伪进行验证，获取第二验证结果；

[0278] 基于待验证证件的验证结果和所述第二验证结果确定待验证证件对应的待验证对象的身份验证结果。

[0279] 上述如本说明书图2-5所示实施例揭示的身份验证装置或管理者(Master)节点执行的方法可以应用于处理器中，或者由处理器实现。处理器可能是一种集成电路芯片，具有信号的处理能力。在实现过程中，上述方法的各步骤可以通过处理器中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器可以是通用处理器，包括中央处理器(Central Processing Unit，CPU)、网络处理器(Network Processor，NP)等；还可以是数字信号处理器(Digital Signal Processor，DSP)、专用集成电路(Application Specific Integrated Circuit，ASIC)、现场可编程门阵列(Field－Programmable Gate 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。可以实现或者执行本说明书实施例中的公开的各方法、步骤及逻辑框图。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。结合本说明书实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器，处理器读取存储器中的信息，结合其硬件完成上述方法的步骤。

[0280] 身份验证装置还可执行图2或图3的方法，并实现管理者节点执行的方法。

[0281] 实施例6

[0282] 基于相同的发明创造，本说明书实施例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一个或多个程序，所述一个或多个程序当被包括多个应用程序的

电子设备执行时，使得所述电子设备执行实施例1和2提供的身份验证方法。

[0283] 上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下，在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外，在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理也是可以的或者可能是有利的。

[0284] 本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0285] 本发明是参照根据本发明实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0286] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0287] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0288] 在一个典型的配置中，计算设备包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。

[0289] 内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器(RAM)和/或非易失性内存等形式，如只读存储器(ROM)或闪存(flash RAM)。内存是计算机可读介质的示例。

[0290] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存(PRAM)、静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体(transitory media)，如调制的数据信号和载波。

[0291] 还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的

包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[0292] 本领域技术人员应明白，本申请的实施例可提供为方法、系统或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0293] 以上所述仅为本申请的实施例而已，并不用于限制本申请。对于本领域技术人员来说，本申请可以有各种更改和变化。凡在本申请的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本申请的权利要求范围之内。

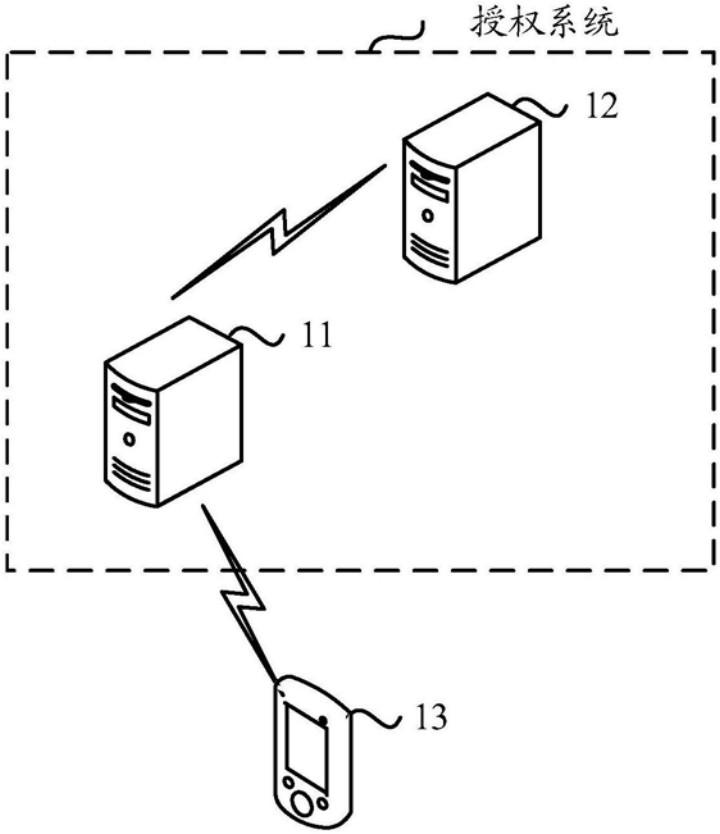

授权系统
12
11
13

图1

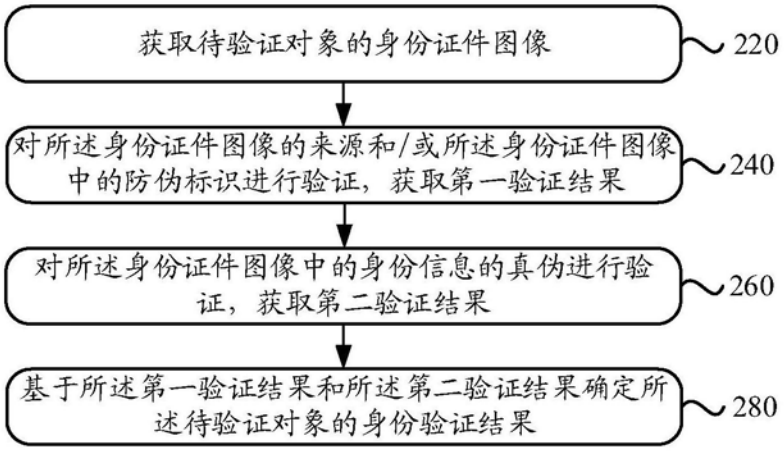

获取待验证对象的身份证件图像
220
对所述身份证件图像的来源和/或所述身份证件图像中的防伪标识进行验证，获取第一验证结果
240
对所述身份证件图像中的身份信息的真伪进行验证，获取第二验证结果
260
基于所述第一验证结果和所述第二验证结果确定所述待验证对象的身份验证结果
280

图2

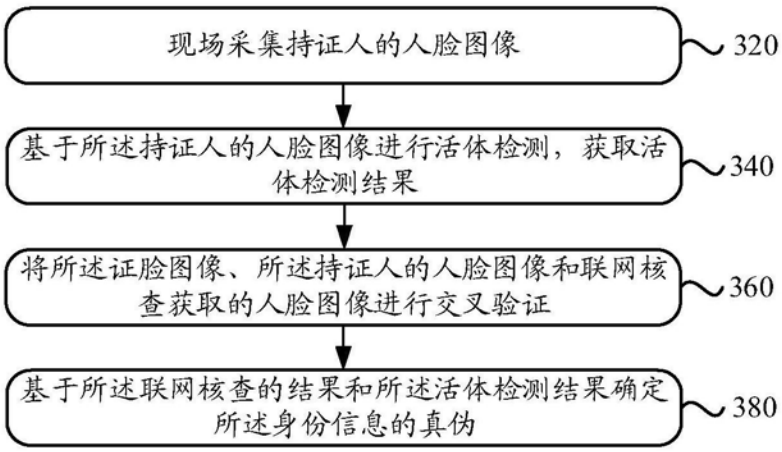

现场采集持证人的人脸图像
320
基于所述持证人的人脸图像进行活体检测，获取活体检测结果
340
将所述证脸图像、所述持证人的人脸图像和联网核查获取的人脸图像进行交叉验证
360
基于所述联网核查的结果和所述活体检测结果确定所述身份信息的真伪
380

图3

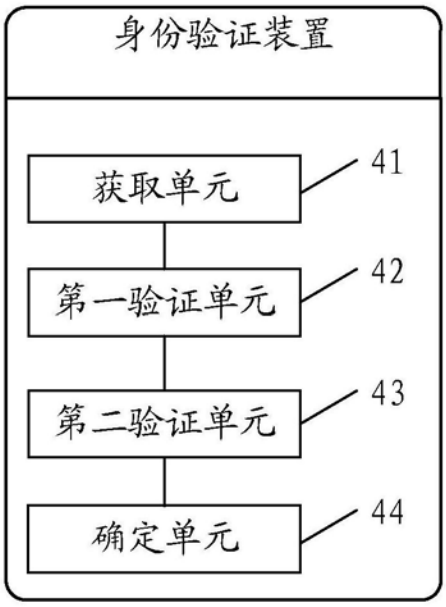

身份验证装置
获取单元
41
第一验证单元
42
第二验证单元
43
确定单元
44

图4

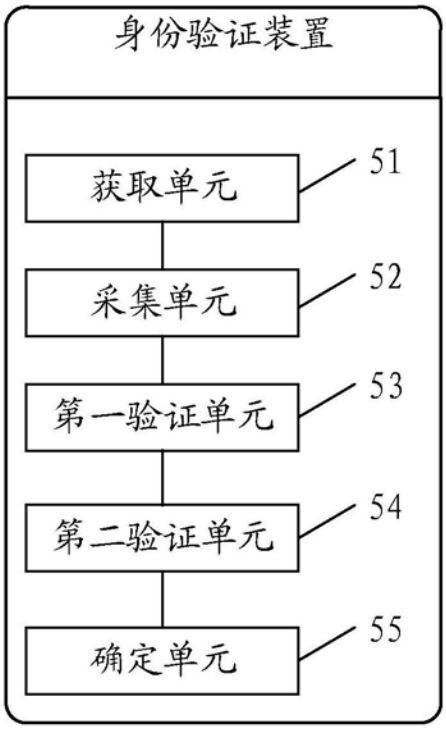

身份验证装置
获取单元
51
采集单元
52
第一验证单元
53
第二验证单元
54
确定单元
55

图5

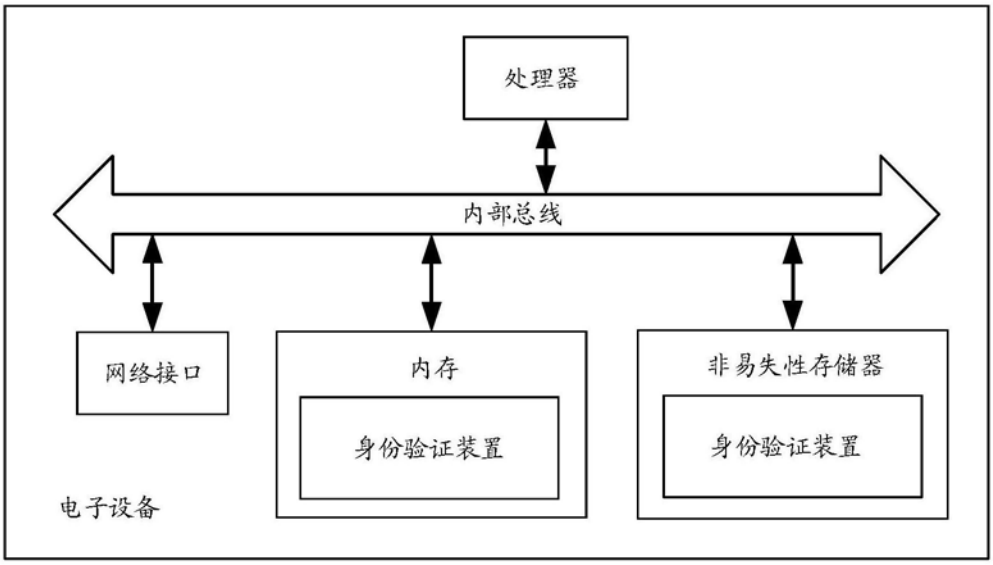

处理器
内部总线
网络接口
内存
身份验证装置
非易失性存储器
身份验证装置
电子设备

图6