(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 117751380 A
(43)申请公布日 2024.03.22

(21)申请号 202180100743.4
(22)申请日 2021.08.05
(85)PCT国际申请进入国家阶段日
2024.01.18
(86)PCT国际申请的申请数据
PCT/JP2021/029117 2021.08.05
(87)PCT国际申请的公布数据
WO2023/012967 JA 2023.02.09
(71)申请人 富士通株式会社
地址 日本神奈川县
(72)发明人 利纳·赛普蒂亚纳 内田秀继
松涛智明
(74)专利代理机构 北京集佳知识产权代理有限公司 11227
专利代理师 王秀辉
(51)Int.Cl.
G06T 7/00(2017.01)
G06N 3/02(2006.01)
G06F 21/32(2013.01)

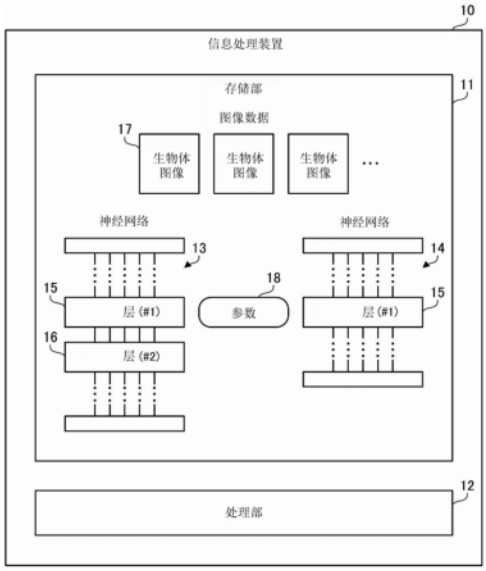
权利要求书1页 说明书11页 附图9页

(54)发明名称

生成方法、信息处理装置以及生成程序

(57)摘要

本发明削减判定的计算成本。信息处理装置(10)通过使用了分别包含人的生物体图像的多个图像数据的机器学习,计算神经网络(13)所包含的多个层各自的参数。信息处理装置(10)通过对包含层(15)且不包含层(16)的神经网络(14)中的层(15)设定对神经网络(13)的层(15)计算出的参数(18),来生成判定受理的图像数据所包含的人的生物体图像的真实性的判定模型。



CN 117751380 A

1.一种生成方法,由计算机执行如下处理:

通过使用了多个图像数据的第一机器学习,计算第一神经网络所包含的多个层各自的参数,上述多个图像数据是分别包含人的生物体图像的数据;以及

通过对包含上述多个层中的第一层且不包含上述多个层中的第二层的第二神经网络中的上述第一层设定对上述第一神经网络的上述第一层计算出的上述参数,来生成判定模型,上述判定模型用于判定受理的图像数据所包含的人的生物体图像的真实性。

2.根据权利要求1所述的生成方法,其中,

上述判定模型的生成包含执行第二机器学习,该第二机器学习是使用设定的上述参数作为初始值,更新上述第二神经网络的机器学习,

上述判定模型是更新后的上述第二神经网络。

3.根据权利要求1所述的生成方法,其中,

上述第二层是比上述第一层靠后方的层。

4.根据权利要求1所述的生成方法,其中,

上述多个层包括:包含上述第一层的多个第一层、包含上述第二层且与上述多个第一层相比位于后方的多个第二层、以及与上述多个第一层相比位于前方的多个第三层,

上述第二神经网络包含上述多个层中的上述多个第一层且不包含上述多个第二层。

5.根据权利要求4所述的生成方法,其中,

上述第二神经网络包含上述多个第三层中一部分的第三层且不包含其它的第三层。

6.根据权利要求1所述的生成方法,其中,

通过按特定的帧数分割包含多个帧的第一动态图像数据来生成上述第一机器学习所使用的上述多个图像数据,

通过从第二动态图像数据的开头提取上述特定的帧数的帧来生成上述判定模型受理的上述图像数据。

7.一种信息处理装置,具有:

存储部,存储分别包含人的生物体图像的多个图像数据;以及

处理部,通过使用了上述多个图像数据的第一机器学习,计算第一神经网络所包含的多个层各自的参数,通过对包含上述多个层中的第一层且不包含上述多个层中的第二层的第二神经网络中的上述第一层设定对上述第一神经网络的上述第一层计算出的上述参数,来生成判定模型,上述判定模型用于判定受理的图像数据所包含的人的生物体图像的真实性。

8.一种生成程序,使计算机执行如下处理:

通过使用了多个图像数据的第一机器学习,计算第一神经网络所包含的多个层各自的参数,上述多个图像数据是分别包含人的生物体图像的数据;以及

通过对包含上述多个层中的第一层且不包含上述多个层中的第二层的第二神经网络中的上述第一层设定对上述第一神经网络的上述第一层计算出的上述参数,来生成判定模型,上述判定模型用于判定受理的图像数据所包含的人的生物体图像的真实性。

生成方法、信息处理装置以及生成程序

技术领域

[0001] 本发明涉及生成方法、信息处理装置以及生成程序。

背景技术

[0002] 作为个人认证技术之一,有基于面部、指纹、静脉、虹膜等生物体信息,判定认证对象者是否为登记者本人的生物体认证。作为对生物体认证系统的安全攻击之一,有演示攻击。

[0003] 演示攻击是攻击者准备伪造了登记者的生物体信息的人造物,并通过对传感器提示人造物来冒充登记者的攻击。例如,攻击者使用智能手机等便携式拍摄装置获取登记者的生物体图像,并将显示了生物体图像的显示装置放在图像传感器上。随着拍摄元件、显示装置的高性能化,检测演示攻击的任务的难易度提高。

[0004] 因此,进行通过机器学习生成检测精度较高的模型的尝试。例如,提出了从训练用图像数据提取特征量,基于提取出的特征量,生成用于检测演示攻击的模型,并使用生成的模型检测演示攻击的异常检测系统。

[0005] 专利文献1:美国专利申请公开第2019/0057268号说明书

[0006] 但是,有通过机器学习使检测精度提高的现有技术生成层非常多的多层神经网络那样的复杂的模型的情况。复杂的模型有判定输入是否为攻击的计算成本较大,执行时间较长的情况。

发明内容

[0007] 因此,在一个方面,本发明的目的在于削减判定的计算成本。

[0008] 在一个方式中,提供计算机执行以下的处理的生成方法。通过使用了分别包含人的生物体图像的多个图像数据的第一机器学习,计算第一神经网络所包含的多个层各自的参数。通过对包含多个层中的第一层且不包含第二层的第二神经网络中的第一层设定对第一神经网络的第一层计算出的参数,来生成判定模型,上述判定模型用于判定受理的图像数据所包含的人的生物体图像的真实性。

[0009] 另外,在一个方式中,提供具有存储部和处理部的信息处理装置。另外,在一个方式中,提供使计算机执行的生成程序。

[0010] 在一个方面,削减了判定的计算成本。

[0011] 通过与表示作为本发明的例子优选的实施方式的附图相关的以下的说明,本发明的上述以及其它的目的、特征以及优点变得更加明确。

附图说明

[0012] 图1是用于说明第一实施方式的信息处理装置的图。

[0013] 图2是表示信息处理装置的硬件例的框图。

[0014] 图3是表示信息处理装置的软件例的框图。

[0015] 图4是表示训练数据用以及测试数据用的输入数据的生成例的图。

[0016] 图5是表示第一卷积神经网络的结构例的图。

[0017] 图6是表示卷积块的结构例的图。

[0018] 图7是表示第二卷积神经网络的结构例的图。

[0019] 图8是表示迁移学习中的参数的移交例的图。

[0020] 图9是表示机器学习的顺序例的流程图。

[0021] 图10是表示模型测试的顺序例的流程图。

具体实施方式

[0022] 以下,参照附图对本实施方式进行说明。

[0023] [第一实施方式]

[0024] 对第一实施方式进行说明。

[0025] 图1是用于说明第一实施方式的信息处理装置的图。

[0026] 第一实施方式的信息处理装置10通过机器学习生成用于检测针对生物体认证系统的演示攻击的判定模型。信息处理装置10也可以使用生成的判定模型检测演示攻击。信息处理装置10既可以是客户端装置也可以是服务器装置。信息处理装置10也可以称为计算机、机器学习装置或者生成装置。

[0027] 信息处理装置10具有存储部11以及处理部12。存储部11既可以是RAM(Random Access Memory:随机存取存储器)等易失性半导体存储器,也可以是HDD(Hard Disk Drive:硬盘驱动器)、闪存等非易失性存储器。处理部12例如是CPU(Central Processing Unit:中央处理器)、GPU(Graphics Processing Unit:图形处理器)、DSP(Digital Signal Processor:数字信号处理器)等处理器。但是,处理部12也可以包含ASIC(Application Specific Integrated Circuit:专用集成电路)、FPGA(Field Programmable Gate Array:现场可编程门阵列)等特定用途的电子电路。处理器例如执行存储于RAM等存储器(也可以是存储部11)的程序。处理器的集合也可以称为多处理器或者仅称为“处理器”。

[0028] 存储部11存储包含图像数据17的多个图像数据。多个图像数据分别包含人的生物体图像。生物体图像是在生物体认证时通过图像传感器读入的认证对象者的图像。例如,生物体图像是面部认证所使用的面部图像、指纹认证所使用的指纹图像等。

[0029] 但是,也可以在多个图像数据中包含不是认证对象者自身的生物体而通过将伪造物保持在图像传感器上生成的非法的图像数据。即,也可以在多个图像数据中包含相当于攻击者冒充登记者的演示攻击的图像数据。攻击者例如使用智能手机等便携式拍摄装置拍摄登记者的生物体,使该图像显示于显示装置并保持在图像传感器上。也可以对多个图像数据赋予表示是否真实的教师标签。

[0030] 处理部12使用上述的图像数据通过机器学习生成判定模型。处理部12首先生成神经网络13。神经网络13是包含层15、16的多层神经网络。神经网络13包含多个节点和将节点间连接的多个边缘。各边缘具有通过机器学习计算出值的权重作为参数。

[0031] 处理部12计算神经网络13所包含的多个层各自的参数。处理部12可以通过误差反向传播法计算参数。例如,处理部12将图像数据输入神经网络13,计算神经网络13的输出与教师标签之间的误差。处理部12从神经网络13的后方朝向前方反方向地传播误差信息,计

算误差相对于各边缘的权重的梯度,并基于梯度更新权重。

[0032] 神经网络13也可以是对输入的图像数据进行卷积运算的卷积神经网络(CNN:Convolutional Neural Network)。卷积运算例如在使被称为内核的矩阵在生物体图像之上滑动的同时反复进行积和运算。内核所包含的系数相当于上述的参数。

[0033] 神经网络13例如被生成为判定输入的图像数据是真实的还是演示攻击。神经网络13可以输出表示攻击类别的“1”和表示真实类别的“2”的任意一方。另外,输入到神经网络13的图像数据也可以是包含在不同的时刻拍摄同一物的多个帧的时间序列数据。神经网络13的输入也可以被称为张量。输入数据具有时间轴的卷积神经网络也可以称为三维卷积神经网络。

[0034] 处理部12基于神经网络13生成神经网络14。根据神经网络13生成神经网络14也被称为迁移学习。神经网络14也可以是卷积神经网络。神经网络14也可以被生成为判定输入的图像数据是真实的还是演示攻击。另外,神经网络14也可以是三维卷积神经网络。

[0035] 神经网络14包含神经网络13所包含的多个层中的层15且不包含层16。神经网络14所包含的层既可以比神经网络13少,也可以是神经网络13所包含的多个层的子集。处理部12对神经网络14的层15设定对神经网络13的层15计算出的参数18。由此,处理部12生成判定受理的图像数据所包含的人的生物体图像的真实性的判定模型。

[0036] 神经网络14也可以是判定模型。另外,处理部12也可以将通过神经网络13计算出的参数18设定为神经网络14的初始值,进一步对神经网络14执行使用了多个图像数据的机器学习。这样更新后的神经网络14也可以是判定生物体图像的真实性的判定模型。

[0037] 在神经网络13中,层15也可以与层16相比配置在前方。另外,神经网络13也可以包含分别包含多个层的前方层组(First Layers)、中央层组(Middle Layers)以及后方层组(Last Layers)。中央层组与前方层组相比配置在后方,后方层组与中央层组相比配置在后方。

[0038] 该情况下,例如层15属于中央层组,层16属于后方层组。神经网络14也可以包含属于中央层组的全部层,也可以不包含属于后方层组的任意的层。另外,神经网络14也可以包含属于前方层组的一部分的层。

[0039] 此外,处理部12也可以通过按特定的帧数分割通过图像传感器读入的动态图像,来生成分别包含连续的多个帧(例如,连续的三个帧)的多个图像数据。处理部12也可以使用根据同一动态图像生成的多个图像数据作为用于计算参数18的训练数据。另一方面,处理部12也可以通过从通过图像传感器读入的动态图像的开头提取特定的帧数的帧,来生成一个图像数据。处理部12可以在评价神经网络14的判定精度的测试时使用该图像数据,也可以在运用生物体认证系统时使用该图像数据。

[0040] 如以上说明的那样,第一实施方式的信息处理装置10通过机器学习生成根据受理的图像数据判定演示攻击命中与否的判定模型。随着拍摄装置、显示装置的高性能化,检测演示攻击的任务的难易度提高。对于这一点,通过使用生成的判定模型,能够使判定精度提高,使生物体认证系统的安全提高。

[0041] 另外,信息处理装置10通过利用机器学习计算神经网络13所包含的多个层各自的参数,并将其中的一部分的层的参数移交给神经网络14,来生成判定模型。由此,信息处理装置10能够削减判定模型的尺寸,能够削减用于判定演示攻击的有无的计算成本。另外,神

经网络14继承神经网络13的中的一部分的层的作用。因此,与从最初起生成层较少的判定模型的情况相比,能够享受层较多(深)的判定模型容易从图像数据提取本质特征这样的多层结构的优点,抑制了判定模型的精度降低。

[0042] 例如,有神经网络13的前方层组的参数被计算为具有用于从图像数据提取基本特征的基本模式信息的情况。有神经网络13的中央层组的参数被计算为具有用于从基本特征提取本质特征的本质模式信息的情况。有神经网络14的后方层组的参数被计算为具有用于进一步使本质特征抽象化的抽象模式信息的情况。但是,后方层组的参数容易受到机器学习所使用的训练数据的影响。

[0043] 因此,神经网络14通过继承某一层的参数,且不继承其后方的层的参数,能够抑制判定模型的精度降低。另外,通过神经网络14不包含后方层组,从而对训练数据的依赖性降低,判定精度提高。另外,通过神经网络14包含中央层组,从而继承基于多层结构进行学习的通用性较高的本质模式信息,而判定精度提高。另外,通过神经网络14不包含前方层组的一部分层,从而进一步了削减计算成本。

[0044] 另外,在将参数从神经网络13移交给神经网络14之后,作为迁移学习进一步更新神经网络14的参数,从而判定模型的判定精度提高。另外,由于判定模型的精度提高,而将相当于演示攻击的生物体图像错误地判定为真实的风险、将真实的生物体图像错误地判定为演示攻击的风险降低。

[0045] 另外,通过输入数据包含时间序列的多个帧,从而判定模型能够考虑如生物那样的动作、反射光的变化、环境变化等时间变化,高精度地判定演示攻击。另外,通过使用从同一动态图像分割出的多个图像数据作为训练数据,从而确保了多样并且足够的量的训练数据。另外,通过使用从动态图像的开头提取的图像数据作为测试数据,从而假定实际的生物体认证的运用适当地评价判定模型的精度。

[0046] [第二实施方式]

[0047] 接下来,对第二实施方式进行说明。

[0048] 第二实施方式的信息处理装置100通过机器学习,生成用于检测针对生物体认证系统的演示攻击的判定模型。第二实施方式的生物体认证是基于面部图像对用户进行认证的面部认证。第二实施方式的判定模型是将连续的多个帧的面部图像分类为攻击类别或者真实类别的三维卷积神经网络(3D_CNN)。

[0049] 第二实施方式的判定模型也可以组装于生物体信息登记装置。例如,生物体信息登记装置在判定模型根据登记用的面部图像检测到演示攻击的情况下,拒绝生物体信息的登记。另外,第二实施方式的判定模型也可以组装于生物体认证装置。例如,生物体认证装置在判定模型根据认证用的面部图像检测到演示攻击的情况下,与登记时的面部图像与认证时的面部图像之间的相似度无关地判定为认证失败。生物体认证系统既可以对系统管理者警告检测到演示攻击,也可以保存警告消息。第二实施方式的生物体认证系统可以利用于IC(Integrated Circuit:集成电路)认证、进出管理、无现金结算、系统登录等。

[0050] 信息处理装置100也可以进行评价生成的判定模型的精度的测试。另外,信息处理装置100也可以利用判定模型进行生物体信息登记或者生物体认证。另外,也可以由其它的信息处理装置进行判定模型的测试、生物体信息登记以及生物体认证。信息处理装置100既可以是客户端装置也可以是服务器装置。信息处理装置100也可以称为计算机、机器学习装

置或者生物体认证装置。信息处理装置100与第一实施方式的信息处理装置10对应。

[0051] 图2是表示信息处理装置的硬件例的框图。

[0052] 信息处理装置100具有与总线连接的CPU101、RAM102、HDD103、GPU104、输入接口105、介质阅读器106以及通信接口107。CPU101与第一实施方式的处理部12对应。RAM102或者HDD103与第一实施方式的存储部11对应。

[0053] CPU101是执行程序的命令的处理器。CPU101将存储于HDD103的程序以及数据的至少一部分加载到RAM102,并执行程序。信息处理装置100也可以具有多个处理器。处理器的集合也可以称为多处理器或者仅称为“处理器”。

[0054] RAM102是暂时存储由CPU101执行的程序以及在CPU101中使用于运算的数据的易失性半导体存储器。信息处理装置100也可以具有RAM以外的种类的易失性存储器。

[0055] HDD103是存储OS(Operating System:操作系统)、中间件、应用程序软件等软件的程序、以及数据的非易失性存储器。信息处理装置100也可以具有闪存、SSD(Solid State Drive:固盘)等其它的种类的非易失性存储器。

[0056] GPU104与CPU101协作地生成图像,并将图像输出到与信息处理装置100连接的显示装置111。显示装置111例如是CRT(Cathode Ray Tube:阴极射线管)显示器、液晶显示器、有机EL(Electro Luminescence:电致发光)显示器或者投影仪。此外,也可以在信息处理装置100连接打印机等其它的种类的输出设备。

[0057] 输入接口105从与信息处理装置100连接的输入设备112受理输入信号。输入设备112可以是鼠标、触摸面板或者键盘。另外,输入设备112也可以是拍摄面部图像的图像传感器。也可以后述的训练数据所使用的面部图像和测试数据所使用的面部图像的至少一方是通过输入设备112拍摄到的图像。也可以在信息处理装置100连接多个输入设备。

[0058] 介质阅读器106是读取记录于记录介质113的程序以及数据的读取装置。记录介质113例如是磁盘、光盘或者半导体存储器。在磁盘包含有软盘(FD:Flexible Disk)以及HDD。在光盘包含有CD(Compact Disc:光盘)以及DVD(Digital Versatile Disc:数字多用盘)。介质阅读器106将从记录介质113读取的程序以及数据复制到RAM102、HDD103等其它的记录介质。有通过CPU101执行读取的程序的情况。

[0059] 记录介质113也可以是便携式记录介质。记录介质113有使用于程序以及数据的分发的情况。另外,记录介质113以及HDD103也可以称为计算机能够读取的记录介质。

[0060] 通信接口107与网络114连接,并经由网络114与其它的信息处理装置进行通信。通信接口107既可以是与交换机、路由器等有线通信装置连接的有线通信接口,也可以与基站、接入点等无线通信装置连接的无线通信接口。

[0061] 图3是表示信息处理装置的软件例的框图。

[0062] 信息处理装置100具有面部图像存储部121以及模型存储部122。例如,使用RAM102或者HDD103安装这些存储部。另外,信息处理装置100具有训练数据生成部123、机器学习部124、测试数据生成部125以及攻击检测部126。例如,使用CPU101或者GPU104和程序安装这些处理部。

[0063] 面部图像存储部121存储多个动态图像。多个动态图像分别是拍摄了人的面部的面部图像,包含按时间序列排列的多个帧。动态图像的帧速率例如为30fps(frames per second:每秒帧数)或者60fps等。

[0064] 但是,在多个动态图像中包含有真实的动态图像和非法的动态图像。真实的动态图像是生物体认证用的图像传感器直接拍摄人的面部的图像。非法的动态图像是通过向生物体认证用的图像传感器提示预先由智能手机等便携式拍摄装置拍摄到的面部图像而读入的图像。非法的动态图像表示演示攻击。对多个动态图像分别赋予教师标签。教师标签是表示攻击类别的“1”或者表示真实类别的“2”。

[0065] 模型存储部122存储通过信息处理装置100生成的判定模型。如上述那样,第二实施方式的判定模型是三维卷积神经网络。该判定模型受理高度120像素、宽度120像素、3帧(H120×W120×C3)的张量作为输入数据。

[0066] 判定模型对输入的张量进行卷积运算,并输出表示攻击类别的“1”或者表示真实类别的“2”作为输入的张量所属的类别。卷积运算在使被称为内核的矩阵在张量上滑动的同时进行积和运算,生成被称为特征图的其它的张量。内核所包含的系数相当于多层神经网络所包含的节点间的边缘的权重,是通过机器学习优化的参数。判定模型是多层神经网络,通过多个层进行多次卷积运算。

[0067] 训练数据生成部123从面部图像存储部121中选择训练数据用的一个以上的动态图像,并生成训练数据。训练数据包含分别组合了输入数据和教师标签的多个记录。输入数据是输入到判定模型的张量。教师标签是判定模型的输出的正解。训练数据生成部123按每三帧分割动态图像所包含的时间序列的帧生成输入数据,并将赋予至该动态图像的教师标签与输入数据建立对应关系。

[0068] 机器学习部124使用由训练数据生成部123生成的训练数据来优化判定模型的参数。机器学习部124也可以通过误差反向传播法来优化参数。例如,机器学习部124从训练数据选择一个或者少数的记录,将张量输入到判定模型,计算判定模型的输出与教师标签之间的误差。机器学习部124从判定模型的后方朝向前方反方向地传播误差信息,计算误差相对于各边缘的权重的梯度,并基于梯度更新权重。机器学习部124在改变从训练数据中选择的记录的同时反复进行边缘的权重的更新,优化权重。

[0069] 如后述那样,机器学习部124通过迁移学习生成判定模型。机器学习部124生成某个三维卷积神经网络,这里使用优化后的参数,生成其它的三维卷积神经网络作为判定模型。后者的三维卷积神经网络是与前者的三维卷积神经网络相比层较少的紧凑的判定模型。

[0070] 测试数据生成部125从面部图像存储部121中选择测试数据用的一个以上的动态图像,生成测试数据。测试数据与训练数据相同地,包含组合了输入数据和教师标签的记录。输入数据是输入到判定模型的张量。教师标签是判定模型的输出的正解。但是,测试数据生成部125从选择的动态图像提取开头的三帧作为输入数据使用。开头的三帧以外的帧不使用于测试数据。

[0071] 攻击检测部126从模型存储部122读出判定模型。攻击检测部126使用由测试数据生成部125生成的测试数据评价判定模型的精度。攻击检测部126将测试数据所包含的输入数据输入到判定模型,计算判定模型的输出与测试数据所包含的教师标签之间的误差。攻击检测部126既可以将判定模型的精度保存于非易失性存储器,也可以显示于显示装置111,也可以发送到其它的信息处理装置。

[0072] 此外,在实际的生物体认证中,生物体认证系统通过与测试数据生成部125相同的

方法根据由图像传感器获取的动态图像生成输入数据,并通过与攻击检测部126相同的方法判定输入数据所属的类别。也可以使其它的信息处理装置具有测试数据生成部125以及攻击检测部126。

[0073] 接下来,对判定模型的结构进行说明。

[0074] 图4是表示训练数据用以及测试数据用的输入数据的生成例的图。

[0075] 如上述那样,训练数据生成部123对包含多个帧的动态图像进行分割,生成各三帧的输入数据。训练数据生成部123生成包含帧#1、#2、#3的输入数据131、包含帧#4、#5、#6的输入数据132、包含帧#7、#8、#9的输入数据133、以及包含帧#10、#11、#12的输入数据134。输入数据131、132、133、134形成训练数据中的不同的记录所包含的张量。

[0076] 另一方面,测试数据生成部125从包含多个帧的动态图像中提取前三帧生成输入数据。通常,训练数据用的动态图像与测试数据用的动态图像为不同的动态图像。测试数据生成部125生成包含帧#1、#2、#3的输入数据135。输入数据135形成测试数据中的一个记录所包含的张量。

[0077] 在生成输入数据131、132、133、134时,训练数据生成部123将动态图像归一化。训练数据生成部123通过图像识别从动态图像检查人的面部,并提取包围检查出的面部的矩形区域。训练数据生成部123将提取出的矩形区域的尺寸转换为判定模型的输入尺寸。例如,训练数据生成部123将提取出的矩形区域的尺寸转换为120×120。另外,训练数据生成部123修正各像素值将像素值的分布归一化。在生成输入数据135时,测试数据生成部125也进行相同的归一化。

[0078] 图5是表示第一卷积神经网络的结构例的图。

[0079] 如上述那样,机器学习部124生成某个三维卷积神经网络,并通过迁移学习生成其它的三维卷积神经网络。如图5所示,第一个三维卷积神经网络从开头起依次包含卷积块140、池化层141、卷积块142～149、池化层150、全连接层151以及激活层152。

[0080] 卷积块140受理H120×W120×C3的张量。卷积块140、142～149分别执行将内核应用于输入的张量生成其它的张量的卷积运算。后述卷积块140、142～149的内部结构。卷积块140、142～149的跨距例如为1。跨距是使内核在张量上滑动时的一次的移位量。在跨距为1的情况下,在各卷积块140、142～149中,张量的高度以及宽度不变化。

[0081] 池化层141、150分别执行将张量中的邻接的多个要素合成为一个要素的池化。由此,在各池化层141、150中,张量的高度以及宽度减少。池化层141、150例如将3×3或者5×5的小区域合成为一个要素。池化例如是从小区域中选择最大值的要素的最大值池化、或者计算小区域所包含的多个要素的平均的平均池化。

[0082] 全连接层151使用池化层150输出的全部的要素,计算与两个类别对应的两个数值。两个类别是表示为演示攻击的攻击类别以及表示不为演示攻击的真实类别。激活层152使用Softmax函数作为激活函数,分别将全连接层151输出的两个数值转换为0以上1以下的数值。这两个数值表示两个类别的概率。三维卷积神经网络输出与两个数值中较大的一方的数值对应的类别作为判定结果。

[0083] 三维卷积神经网络包含十个块。卷积块140相当于第一块(A1)。池化层141相当于第二块(A2)。卷积块142～149相当于第三块到第九块(A3～A9)。全连接层151相当于第十块(A10)。

[0084] 十个块中九个块大致具有以下的作用。卷积块140、池化层141以及卷积块142、143属于前方层组。卷积块144～146属于中央层组。卷积块147～149属于后方层组。

[0085] 前方层组被学习为具有用于从面部图像提取各种基本特征的基本模式信息。中央层组被学习为具有用于从通过前方层组提取出的基本特征提取面部图像的本质特征的本质模式信息。后方层组被学习为具有用于进一步使通过中央层组提取出的本质特征抽象化进行类别判定的抽象模式信息。

[0086] 通过增加三维卷积神经网络的层数,从而被夹在前方层组与后方层组之间的中央层组具有通用并且优质的本质模式信息。这是因为中央层组远离输入数据,也远离表示与教师标签的误差的误差信息,而不会较大地受到训练数据所包含的偏差、噪声的影响。但是,增加三维卷积神经网络的层数使类别判定时的计算成本增大。

[0087] 另外,有在使中央层组的参数优化的期间,产生后方层组的参数过度地适合于训练数据的过学习的情况。这是因为后方层组接近表示与教师标签的误差的误差信息,而较大地受到训练数据所包含的偏差、噪声的影响。其结果,有判定模型将基于与为了制成演示攻击的样本而使用的特定的拍摄装置不同的机型的演示攻击错误地判定为真实的风险。另外,有判定模型将真实的面部图像错误地判定为演示攻击的风险。

[0088] 因此,机器学习部124不直接使用图5的三维卷积神经网络作为判定模型,而通过迁移学习生成其它的三维卷积神经网络,并将其作为判定模型使用。

[0089] 图6是表示卷积块的结构例的图。

[0090] 卷积块140从开头起依次包含卷积层161、批归一化层162、激活层163、卷积层164、批归一化层165以及激活层166。卷积块142～149等其它的卷积块也可以具有与卷积块140相同的层结构。

[0091] 卷积层161、164分别对输入的张量执行卷积运算,生成其它的张量。批归一化层162、165分别对输入的张量执行批归一化。批归一化在属于同一小批量(Mini batch)的多个张量之间,将张量所包含的要素的分布归一化为平均0并且方差1。激活层163、166分别使用归一化线性单元(ReLU)作为激活函数,对输入的张量所包含的数值进行转换。归一化线性单元通过将负数限制为0来将各数值转换为非负数。

[0092] 这里,卷积块140将批归一化层165的输出与卷积块140的输入相加,并将相加后的张量输入到激活层166。由此,从卷积层161到批归一化层165为止的层组的参数被计算为优化与初始的输入张量的差分。这样的卷积块140也可以称为残差神经网络。此外,卷积层、批归一化层以及激活层的个数也可以各为一个。

[0093] 图7是表示第二卷积神经网络的结构例的图。

[0094] 如图7所示,通过迁移学习生成的第二个三维卷积神经网络从开头起依次包含卷积块171～174、池化层175、全连接层176以及激活层177。

[0095] 卷积块171受理H120×W120×C3的张量。卷积块171～174分别执行将内核应用于输入的张量生成其它的张量的卷积运算。池化层175执行将张量中的邻接的多个要素合成为一个要素的池化。

[0096] 全连接层176使用池化层175输出的全部的要素,计算与两个类别对应的两个数值。激活层177使用Softmax函数作为激活函数,分别将全连接层176输出的两个数值转换为0以上1以下的数值。三维卷积神经网络将与两个数值中较大的一方的数值对应的类别作为

判定结果输出。

[0097] 通过迁移学习生成的第二个三维卷积神经网络包含五个块。卷积块171相当于第一块(B1)。卷积块172相当于第二块(B2)。卷积块173相当于第三块(B3)。卷积块174相当于第四块(B4)。全连接层176相当于第五块(B5)。

[0098] 卷积块171与图5的卷积块140对应。机器学习部124复制卷积块140的参数作为卷积块171的参数的初始值。由此,能够期待卷积块171具有用于从面部图像提取基本特征的基本模式信息。

[0099] 另一方面,机器学习部124不复制前方层组所包含的卷积块142、143的参数。通过省略池化层141以及卷积块142、143,从而削减了计算成本,缩短了类别判定的执行时间。但是,第二个三维卷积神经网络也可以包含相当于卷积块142、143的卷积块。

[0100] 卷积块172～174与图5的卷积块144～146对应。机器学习部124复制卷积块144～146的参数作为卷积块172～174的参数的初始值。由此,能够期待卷积块172～174具有用于根据通过卷积块171提取出的基本特征提取本质特征的本质模式信息。

[0101] 这里,卷积块172～174各自的输入尺寸以及输出尺寸与卷积块144～146相同。另外,卷积块171的输入尺寸与卷积块140相同。另一方面,与第一个三维卷积神经网络不同,在卷积块171与卷积块172之间不存在池化层。因此,机器学习部124进行使卷积块171的输出尺寸与卷积块172的输入尺寸一致的调整。

[0102] 具体而言,机器学习部124使通过卷积块171进行的卷积运算的跨距比卷积块140大。在跨距为2的情况下,与跨距为1的情况相比,输出的张量的高度以及宽度分别成为二分之一。在跨距为3的情况下,与跨距为1的情况相比,输出的张量的高度以及宽度分别成为三分之一。

[0103] 另外,机器学习部124不复制后方层组所包含的卷积块147～149的参数。通过省略卷积块147～149,从而削减了计算成本,缩短了类别判定的执行时间。另外,通过除去对训练数据的依赖性较高的参数,从而类别判定能力通用化,判定精度提高。

[0104] 全连接层176与图5的全连接层151对应。但是,参数不从全连接层151复制到全连接层176。机器学习部124在对卷积块171～174设定了上述的初始值之后,使用训练数据,更新第二个三维卷积神经网络的参数。迁移学习所使用的训练数据既可以与第一个机器学习相同也可以不同。

[0105] 图8是表示迁移学习中的参数的移交例的图。

[0106] 卷积块140受理张量181。张量181例如具有高度120并且宽度120的尺寸。另外,卷积块140具有相当于神经网络的边缘的权重的集合的内核182。内核182例如具有高度3并且宽度3、或者高度5并且宽度5的尺寸。机器学习部124通过机器学习计算内核182的系数。卷积块140在使内核182在张量181之上滑动的同时进行积和运算,生成特征图183。该卷积运算的跨距例如为1。特征图183例如具有高度120并且宽度120的尺寸。

[0107] 例如,卷积块140进行张量181的a_{11}、a_{12}、a_{13}、a_{21}、a_{22}、a_{23}、a_{31}、a_{32}、a_{33}与内核182的k_{11}、k_{12}、k_{13}、k_{21}、k_{22}、k_{23}、k_{31}、k_{32}、k_{33}的积和运算,计算特征图183的c_{11}。另外,卷积块140进行张量181的a_{12}、a_{13}、a_{14}、a_{22}、a_{23}、a_{24}、a_{32}、a_{33}、a_{34}与内核182的k_{11}、k_{12}、k_{13}、k_{21}、k_{22}、k_{23}、k_{31}、k_{32}、k_{33}的积和运算,计算特征图183的c_{12}。

[0108] 卷积块171受理张量184。张量184的尺寸与张量181相同。另外,卷积块171具有内

核185。内核185的尺寸与内核182相同。机器学习部124将内核182复制到内核185进行迁移学习,更新内核185。卷积块171根据张量184和内核185生成特征图186。该卷积运算的跨距例如为2或者3。特征图186例如具有高度60并且宽度60、或者高度40并且宽度40的尺寸。

[0109] 例如,卷积块171进行张量184的b_{11}、b_{12}、b_{13}、b_{21}、b_{22}、b_{23}、b_{31}、b_{32}、b_{33}与内核185的k'_{11}、k'_{12}、k'_{13}、k'_{21}、k'_{22}、k'_{23}、k'_{31}、k'_{32}、k'_{33}的积和运算,计算特征图186的d_{11}。另外,卷积块171进行张量184的b_{13}、b_{14}、b_{15}、b_{23}、b_{24}、b_{25}、b_{33}、b_{34}、b_{35}与内核185的k'_{11}、k'_{12}、k'_{13}、k'_{21}、k'_{22}、k'_{23}、k'_{31}、k'_{32}、k'_{33}的积和运算,计算特征图186的d_{12}。内核185的移位量与内核182不同。

[0110] 接下来,对信息处理装置100的处理顺序进行说明。

[0111] 图9是表示机器学习的顺序例的流程图。

[0112] (S10)训练数据生成部123按每三帧分割面部的动态图像。

[0113] (S11)训练数据生成部123将各帧归一化。帧的归一化包含面部区域的提取、尺寸变更以及像素值的归一化。

[0114] (S12)训练数据生成部123将连续的三帧的输入数据与赋予至动态图像的教师标签组合,生成包含多个记录的训练数据。

[0115] (S13)机器学习部124生成包含块A1～A10的三维卷积神经网络(模型A)。

[0116] (S14)机器学习部124使用在步骤S12中生成的训练数据中的至少一部分的记录,通过机器学习优化模型A的参数。

[0117] (S15)机器学习部124与模型A不同地,生成包含块B1～B5的三维卷积神经网络(模型B)。

[0118] (S16)机器学习部124将模型A的块A1、A4、A5、A6的参数作为初始值复制到模型B的块B1～B4。

[0119] (S17)机器学习部124使用在步骤S12中生成的训练数据中的至少一部分的记录,通过机器学习优化模型B的参数。该机器学习是从在步骤S16复制的参数开始的迁移学习。

[0120] (S18)机器学习部124保存被生成的模型B作为判定模型。

[0121] 图10是表示模型测试的顺序例的流程图。

[0122] (S20)测试数据生成部125提取面部的动态图像的前三帧。

[0123] (S21)测试数据生成部125将各帧归一化。帧的归一化包含面部区域的提取、尺寸变更以及像素值的归一化。

[0124] (S22)攻击检测部126读出作为判定模型的三维卷积神经网络。攻击检测部126将包含在步骤S20中提取的三帧的面部图像的输入数据输入到判定模型。

[0125] (S23)攻击检测部126输出由判定模型判定出的类别的信息。类别是表示面部图像为演示攻击的伪造物的攻击类别、或者表示面部图像真实的真实类别。攻击检测部126既可以将判定出的类别的信息保存于非易失性存储器,也可以显示于显示装置111,也可以发送到其它的信息处理装置。

[0126] 如以上说明的那样,第二实施方式的信息处理装置100通过机器学习生成根据受理的面部图像判定演示攻击命中与否的判定模型。由此,判定精度提高而生物体认证系统的安全提高。另外,能够灵活地应对各种演示攻击方法、各种电子设备。

[0127] 另外,信息处理装置100生成较多层的神经网络,并进行复制一部分的层的参数生成层较少的神经网络的迁移学习。由此,最终的判定模型的尺寸变小,削减了用于演示攻击

的判定的计算成本,缩短了执行时间。另外,在层较多的神经网络中,容易形成用于提取面部图像的本质特征的本质模式信息。因此,最终的判定模型能够通过迁移学习享受多层结构的优点,而判定精度提高。

[0128] 另外,信息处理装置100在迁移学习时,从初始的神经网络除去后方层组。有后方层组的参数较大地依赖于训练数据的情况。由此,对训练数据的依赖度降低,对于与训练数据不同的演示攻击方法、不同的电子设备的使用,判定精度提高。另一方面,信息处理装置100在迁移学习时,从初始的神经网络复制中央层组的参数。在中央层组中,容易形成对训练数据的依赖度较低的通用的本质模式信息。由此,判定模型的判定精度提高。

[0129] 另外,信息处理装置100在迁移学习时,复制初始的神经网络所包含的前方层组中开头的块的参数。在前方层组中开头的块中,容易形成为了从面部图像提取基本特征而特别重要的基本模式信息。由此,判定模型的判定精度提高。另一方面,信息处理装置100在迁移学习时,除去前方层组所包含的其它的块。由此,最终的判定模型的尺寸减小,削减了用于演示攻击的判定的计算成本,并缩短了执行时间。

[0130] 另外,在参数的复制后,进一步进行更新层较少的神经网络的参数的机器学习,从而判定精度提高。另外,通过输入数据包含时间序列的多个帧,判定模型能够考虑如生物那样的动作、反射光的变化、环境变化等的时间变化,高精度地判定演示攻击。另外,通过按每三帧分割动态图像并使用于训练数据,能够确保多样并且足够的量的训练数据。另外,通过将动态图像的前三帧使用于测试数据,能够假定实际的生物体认证的运用适当地评价判定模型的精度。

[0131] 上述仅示出本发明的原理。并且,对于本领域技术人员来说能够进行许多的变形、变更,本发明并不限定于在上述示出并进行了说明的正确的构成以及应用例,对应的全部的变形例以及同等物视为基于附加的权利要求及其同等物的本发明的范围。

[0132] 附图标记说明

[0133] 10…信息处理装置,11…存储部,12…处理部,13、14…神经网络,15、16…层,17…图像数据,18…参数。

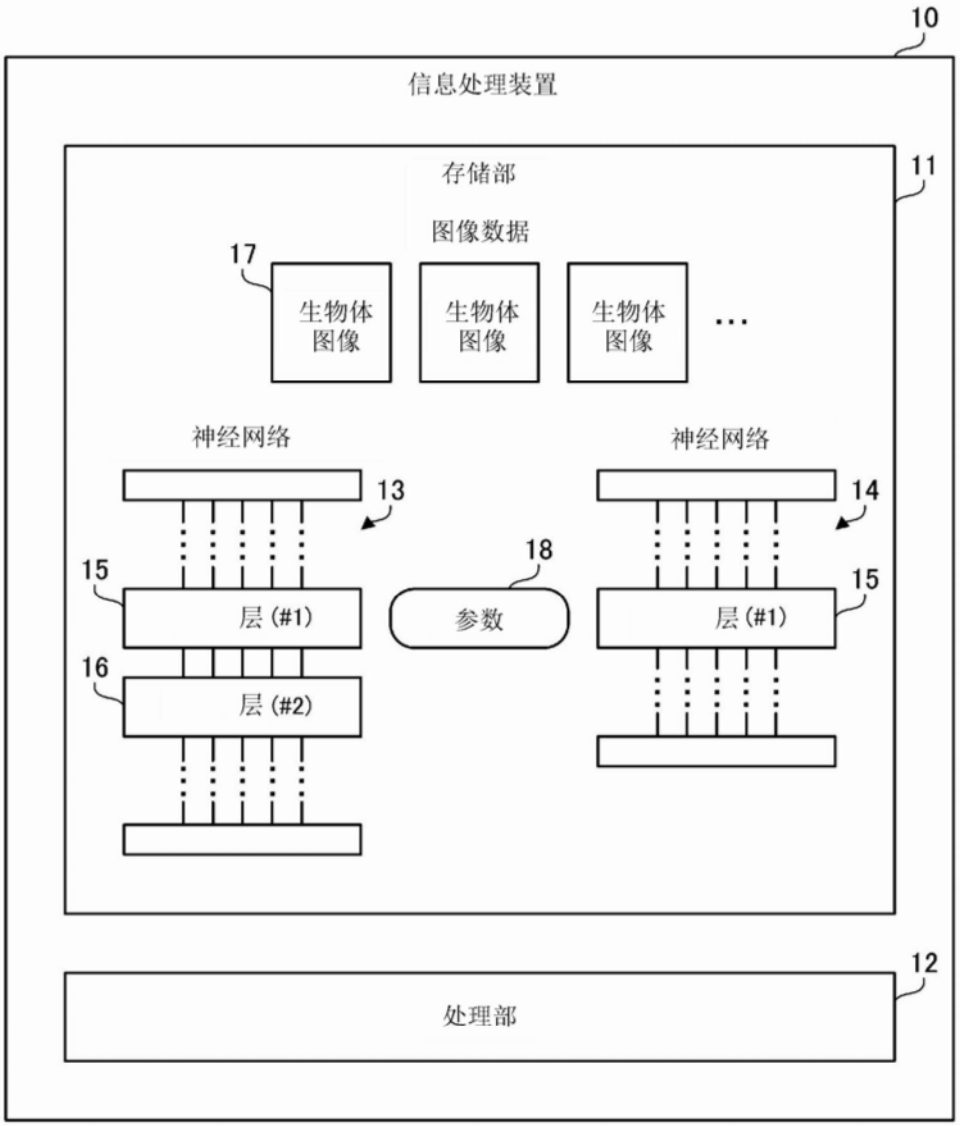

10
信息处理装置
存储部
11
图像数据
17
生物体图像
生物体图像
生物体图像
...
神经网络
神经网络
13
14
18
15
层(#1)
参数
层(#1)
15
16
层(#2)
处理部
12

图1

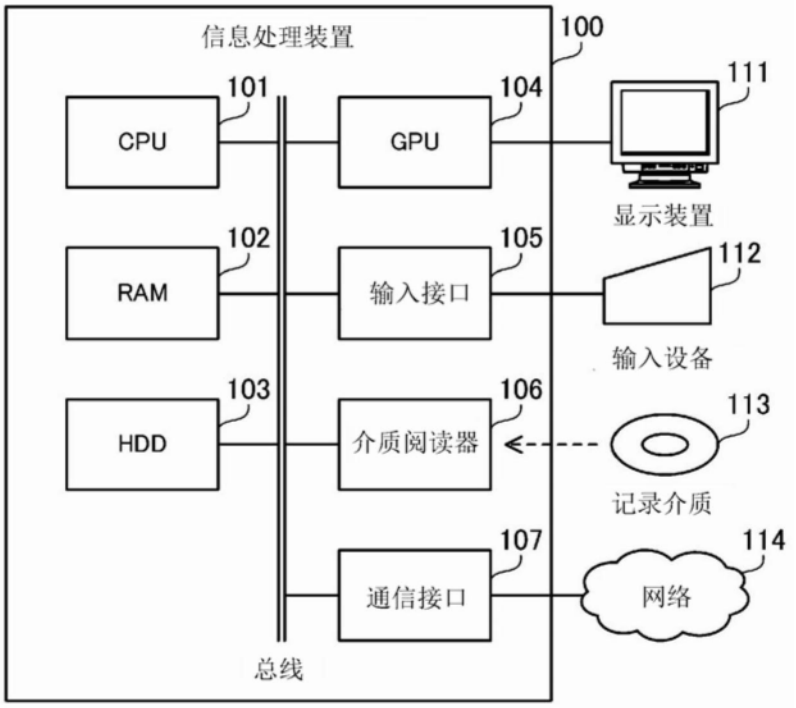

信息处理装置
100
CPU
101
GPU
104
111
显示装置
RAM
102
输入接口
105
112
输入设备
HDD
103
介质阅读器
106
113
记录介质
通信接口
107
网络
114
总线

图2

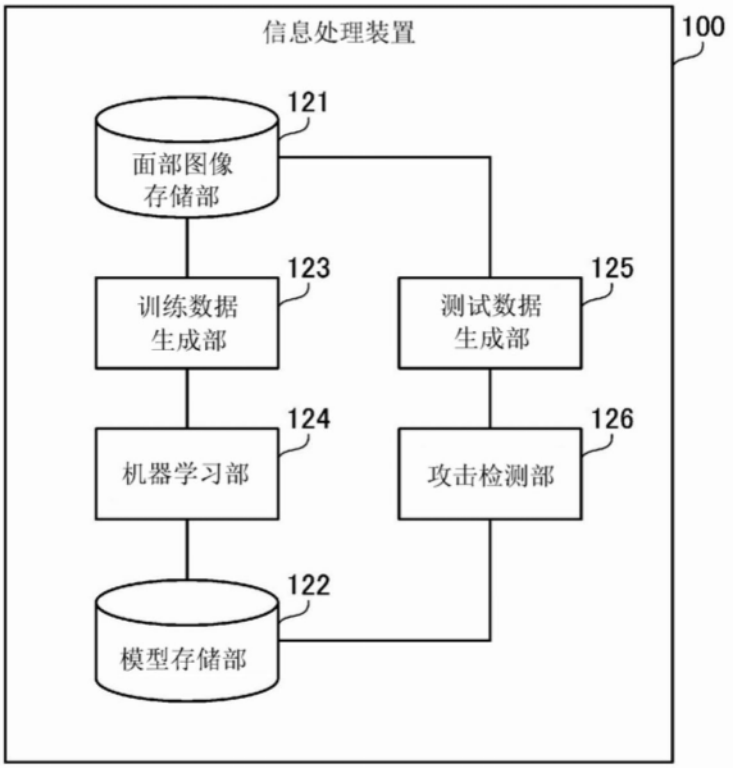

信息处理装置
100
面部图像
存储部
121
训练数据
生成部
123
测试数据
生成部
125
机器学习部
124
攻击检测部
126
模型存储部
122

图3

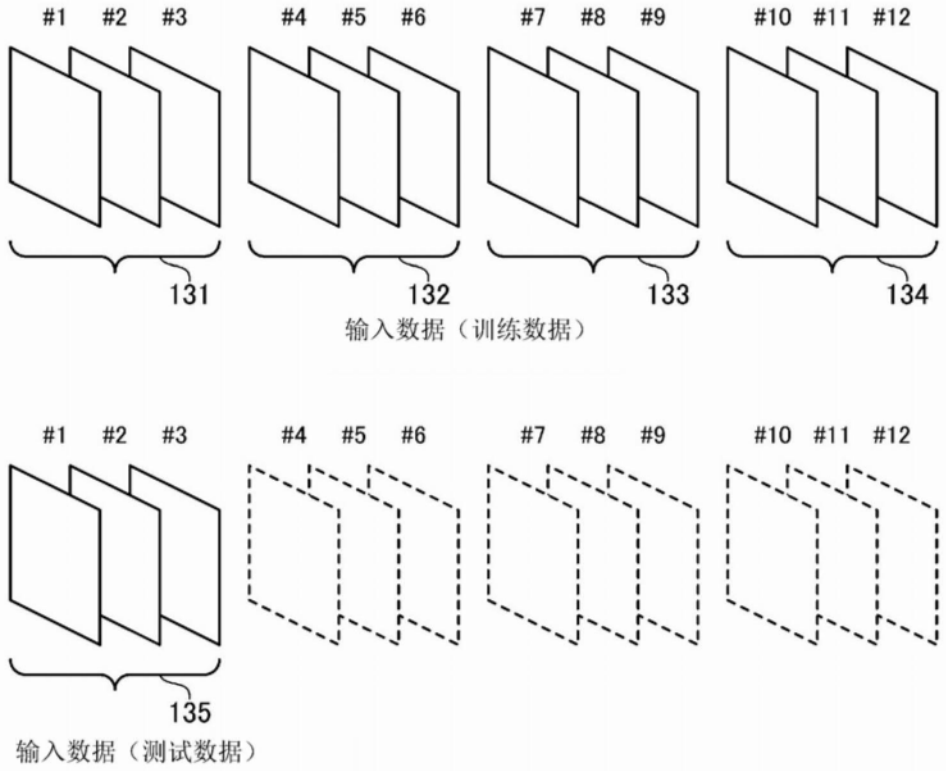

#1 #2 #3
#4 #5 #6
#7 #8 #9
#10 #11 #12
131
132
133
134
输入数据（训练数据）
#1 #2 #3
#4 #5 #6
#7 #8 #9
#10 #11 #12
135
输入数据（测试数据）

图4

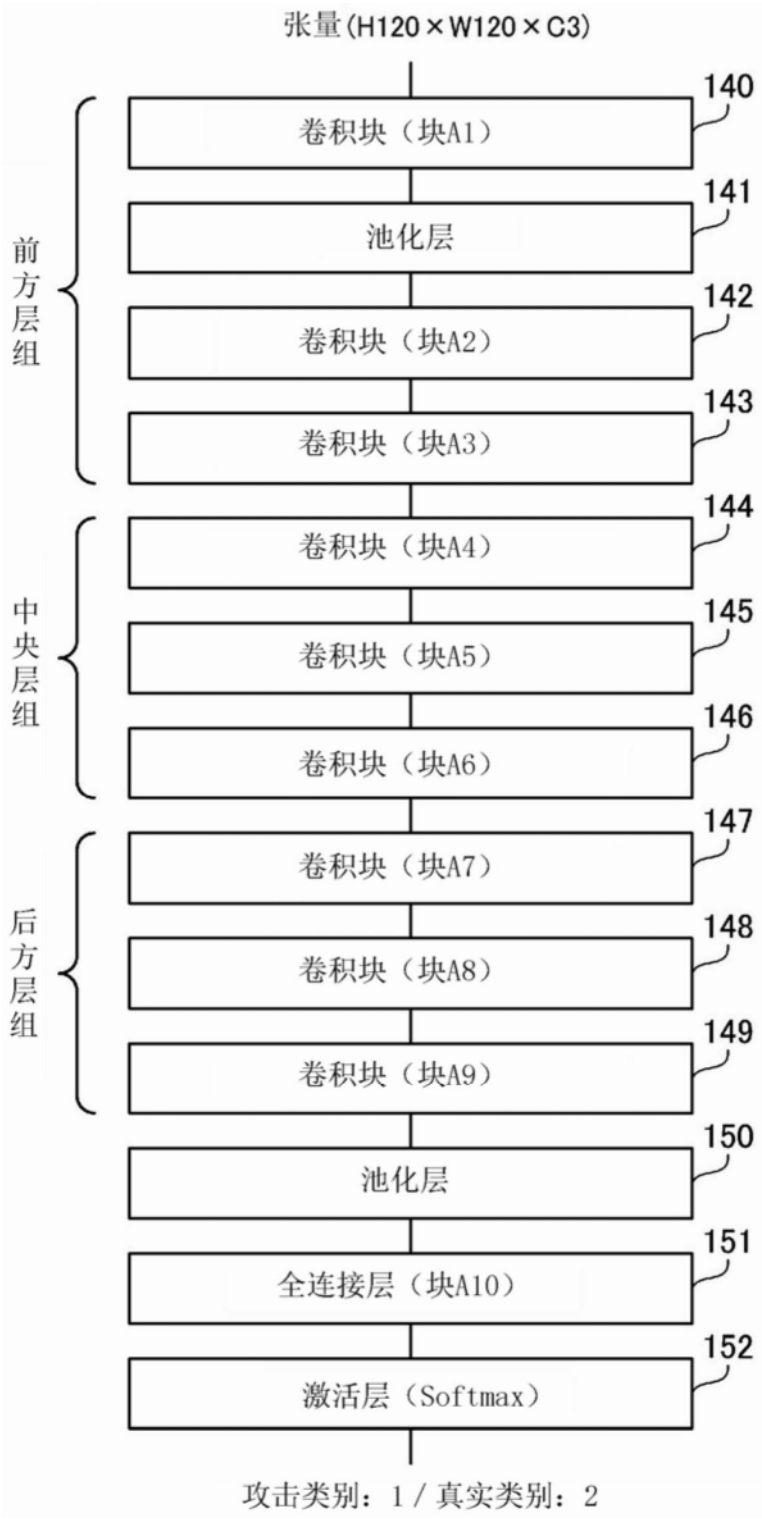

张量(H120×W120×C3)
前方层组
中央层组
后方层组
卷积块（块A1）
140
池化层
141
卷积块（块A2）
142
卷积块（块A3）
143
卷积块（块A4）
144
卷积块（块A5）
145
卷积块（块A6）
146
卷积块（块A7）
147
卷积块（块A8）
148
卷积块（块A9）
149
池化层
150
全连接层（块A10）
151
激活层（Softmax）
152
攻击类别：1 / 真实类别：2

图5

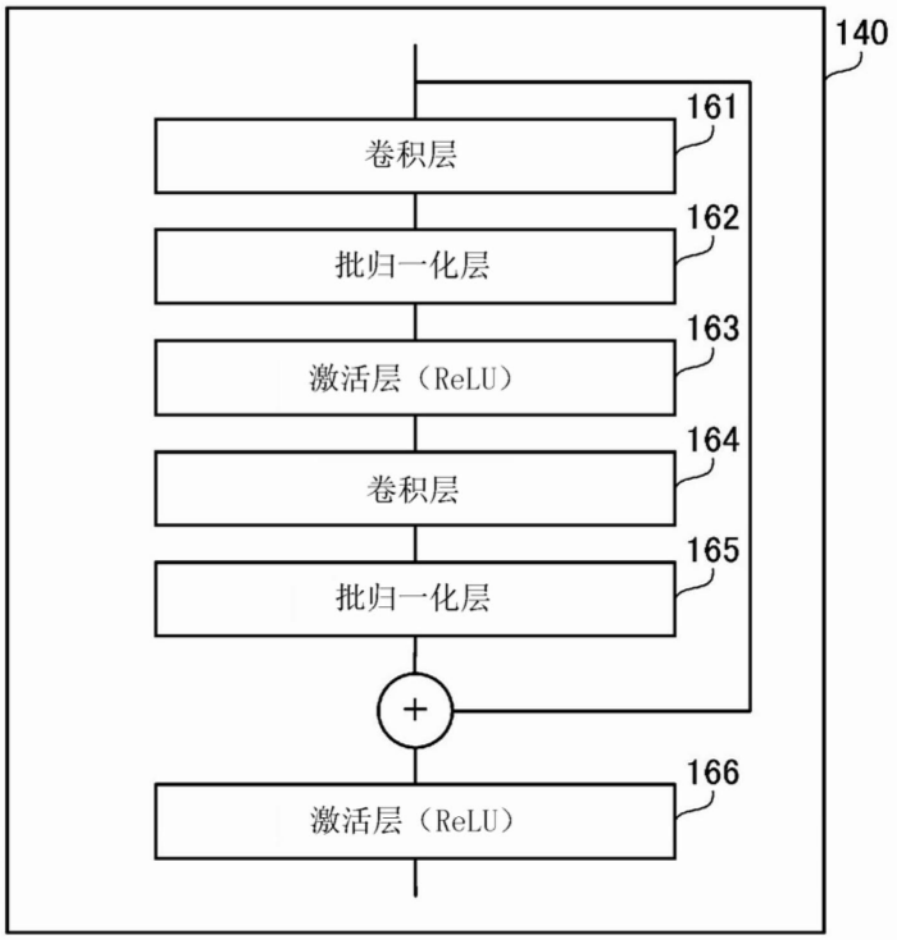

140
161
卷积层
162
批归一化层
163
激活层（ReLU）
164
卷积层
165
批归一化层
+
166
激活层（ReLU）

图6

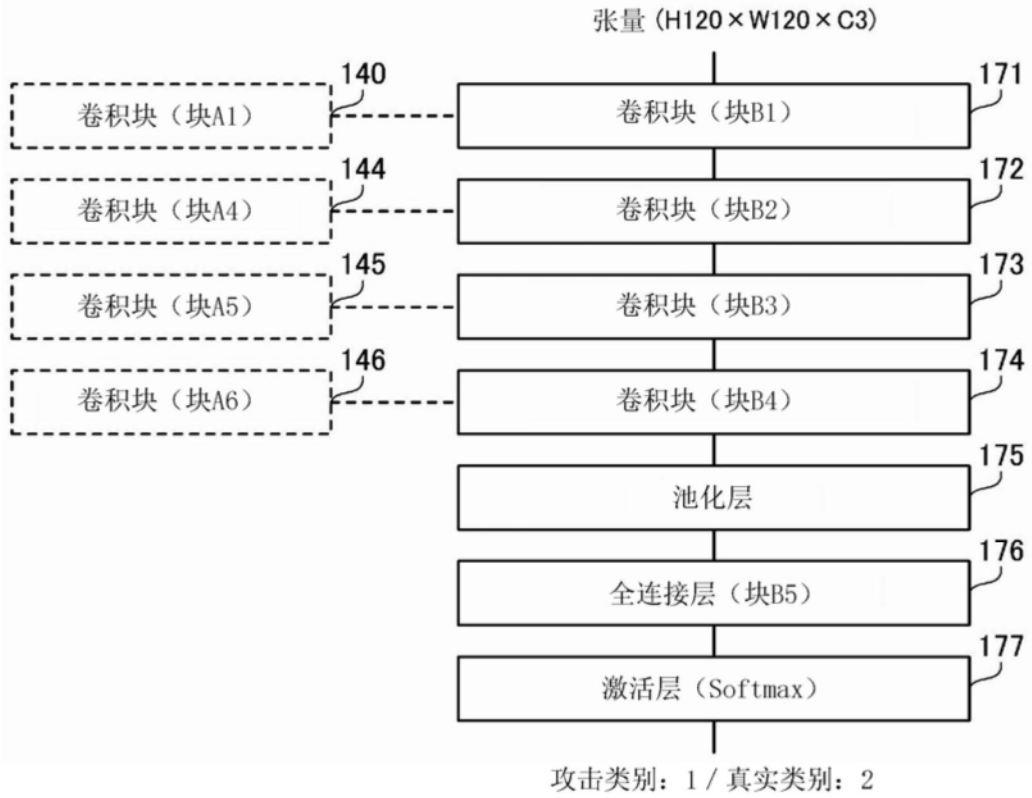

张量（H120×W120×C3）
卷积块（块A1）
140
卷积块（块A4）
144
卷积块（块A5）
145
卷积块（块A6）
146
卷积块（块B1）
171
卷积块（块B2）
172
卷积块（块B3）
173
卷积块（块B4）
174
池化层
175
全连接层（块B5）
176
激活层（Softmax）
177
攻击类别：1 / 真实类别：2

图7

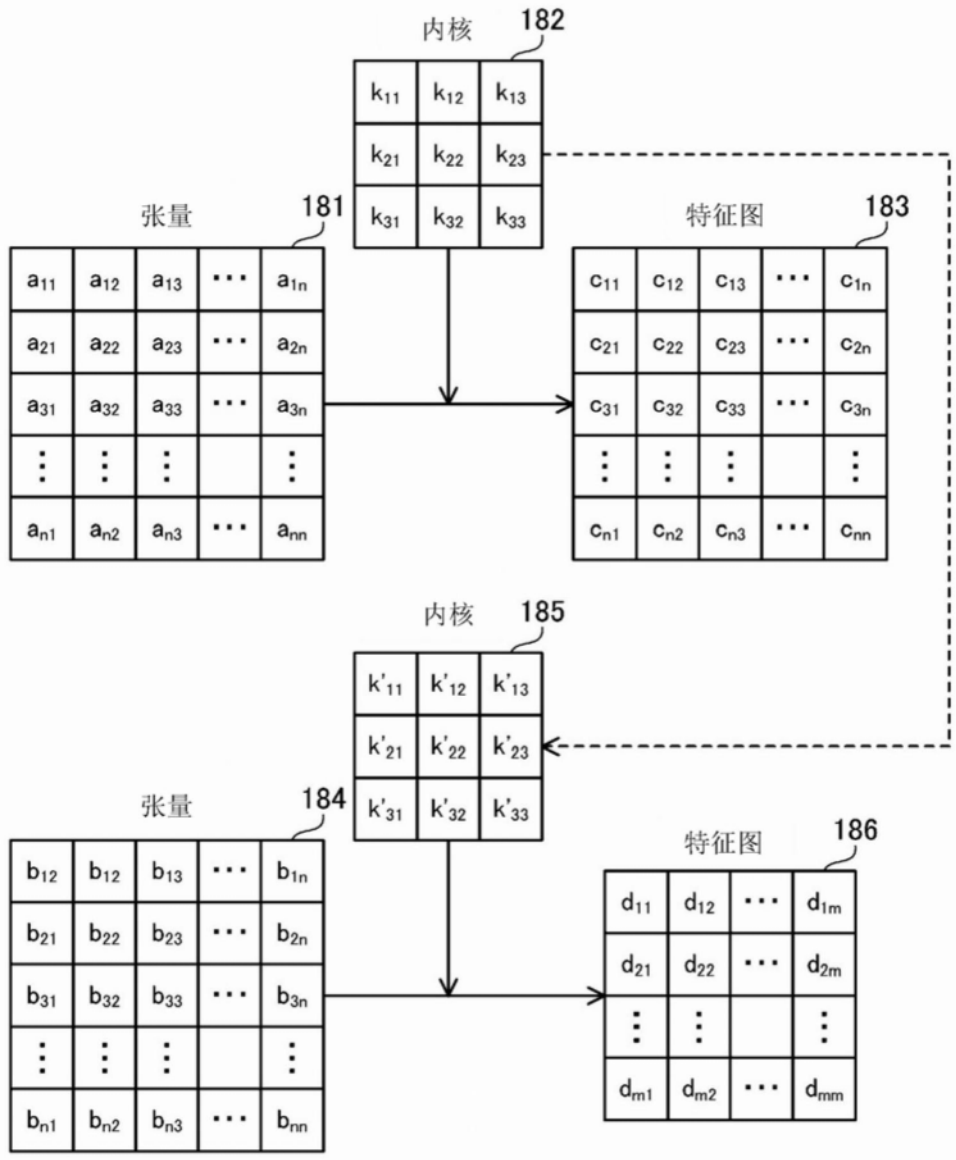

内核
182
k11 k12 k13
k21 k22 k23
k31 k32 k33
张量
181
特征图
183
内核
185
张量
184
特征图
186

图8


机器学习
S10
按每三帧分割面部的动态图像
S11
将各帧归一化
S12
与教师标签组合生成训练数据
S13
生成包含块A1～A10的3D_CNN（模型A）
S14
优化模型A的参数
S15
生成包含块B1～B5的3D_CNN（模型B）
S16
复制块A1、A4、A5、A6的参数
S17
使用训练数据优化模型B的参数（迁移学习）
S18
保存模型B
结束

图9

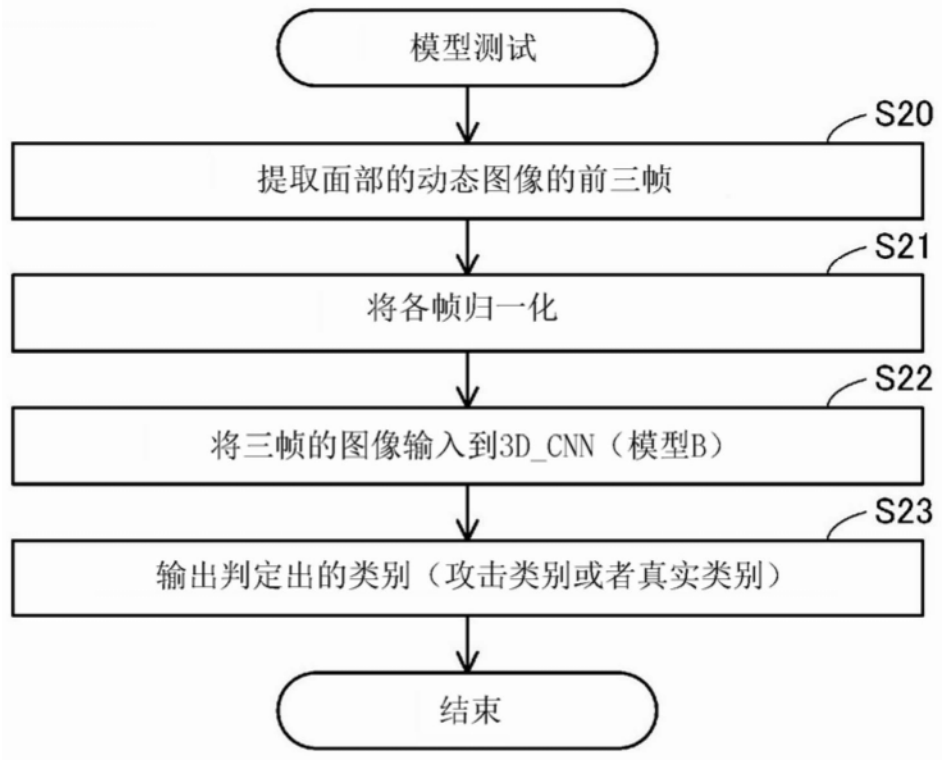

模型测试
S20
提取面部的动态图像的前三帧
S21
将各帧归一化
S22
将三帧的图像输入到3D_CNN（模型B）
S23
输出判定出的类别（攻击类别或者真实类别）
结束

图10