

模型训练方法、特征提取方法、装置、设备及介质

相关申请的交叉引用

本申请要求在 2023 年 11 月 14 日提交中华人民共和国国家知识产权局、申请号为 202311518180.8、申请名称为“模型训练方法、特征提取方法、装置、设备及介质”的中国
5 专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及数据处理技术领域，尤其涉及一种特征提取模型训练方法、卷积神经网络
10 训练方法、模型训练方法、特征提取方法、装置、设备及介质。

背景技术

隐私计算中的多方安全计算（Secure Multi-Party Computation, MPC）是在无可信第三
方情况下，多个参与方协同完成计算目标，并保证每个参与方除计算结果外均不能得到其
他参与方的任何输入信息，可以很好的保护用户的隐私信息。

15 其中，如果输入信息是包含用户的隐私信息的图像时，为了保护用户的隐私信息，可
以对该图像进行特征提取，基于提取到的特征向量进行多方安全计算。然而，如何快捷准
确地提取到高精度的图像特征向量，是目前亟需解决的一个技术问题。

发明内容

20 本申请提供了一种特征提取模型训练方法、卷积神经网络训练方法、模型训练方法、
特征提取方法、装置、设备及介质，用以快捷准确地提取到高精度的图像特征向量。

第一方面，本申请提供了一种特征提取模型训练方法，所述方法包括：

针对获取到的任一第一样本图像，基于训练完成的卷积神经网络，获得所述第一样本
图像的第一特征向量；并基于预设的图像处理方式，将所述第一样本图像处理为一维序列，
25 将所述一维序列输入到待训练的特征提取模型中，基于所述特征提取模型，获得所述第
一样本图像的第二特征向量；基于所述第二特征向量，对所述第一特征向量进行校准，获得
校准后的第一基准特征向量，其中，所述特征提取模型是基于 MPCFormer 模型的框架结
构与语义视觉 Transformer 模型 SETR 的训练逻辑训练所得的模型；

30 基于所述第一基准特征向量、所述第一样本图像携带的标签特征向量以及配置的第一
损失函数，对所述特征提取模型进行训练。

在一种可能的实施方式中，所述获得所述第一样本图像的第二特征向量之后，所述基
于所述第二特征向量，对所述第一特征向量进行校准之前，所述方法还包括：

对所述第二特征向量进行全局平均池化，获得所述第二特征向量中每一维特征对应的
全局特征向量信息，并基于概率分布函数，获得所述全局特征向量信息中每一维特征对应
35 的重要性权重系数；基于所述每一维特征对应的重要性权重系数，对所述第二特征向量进
行校准，获得校准后的第二特征向量；基于校准后的第二特征向量，进行后续基于所述第
二特征向量，对所述第一特征向量进行校准的步骤。

在一种可能的实施方式中，所述第一损失函数中包含所述每一维特征对应的重要性权
重系数。

在一种可能的实施方式中，所述基于所述第二特征向量，对所述第一特征向量进行校准，获得校准后的第一基准特征向量，包括：

对所述第二特征向量中包含的每一维特征与所述第一特征向量中包含的每一维特征进行同或运算，获得校准后的第一基准特征向量。

- 5 在一种可能的实施方式中，所述将所述第二特征向量中包含的每一维特征与所述第一特征向量中包含的每一维特征进行同或运算之后，所述获得校准后的第一基准特征向量之前，所述方法还包括：

对所述同或运算后得到的向量进行归一化处理，基于归一化处理后的向量，确定校准后的第一基准特征向量。

- 10 在一种可能的实施方式中，所述特征提取模型使用的激励函数包含：2quad 激励函数。

在一种可能的实施方式中，所述特征提取模型为基于知识蒸馏得到的模型。

第二方面，本申请提供了一种卷积神经网络训练方法，所述方法包括：

- 针对获取到的任一第二样本图像，将所述第二样本图像输入到待训练的卷积神经网络中，基于所述卷积神经网络，获得所述第二样本图像的第三特征向量；并基于预设的图像
15 处理方式，将所述第二样本图像处理为一维序列，将所述一维序列输入到训练完成的特征提取模型中，基于所述特征提取模型，获得所述第二样本图像的第四特征向量；基于所述第四特征向量，对所述第三特征向量进行校准，获得校准后的第二基准特征向量，其中，所述特征提取模型是基于 MPCFormer 模型的框架结构与语义视觉 Transformer 模型 SETR 的训练逻辑训练所得的模型；

- 20 基于所述第二基准特征向量、所述第二样本图像携带的标签特征向量以及配置的第二损失函数，对所述卷积神经网络进行训练。

在一种可能的实施方式中，所述基于所述第四特征向量，对所述第三特征向量进行校准，获得校准后的第二基准特征向量，包括：

- 25 对所述第四特征向量中包含的每一维特征与所述第三特征向量中包含的每一维特征进行同或运算，获得校准后的第二基准特征向量。

在一种可能的实施方式中，所述将所述第四特征向量中包含的每一维特征与所述第一特征向量中包含的每一维特征进行同或运算之后，所述获得校准后的第二基准特征向量之前，所述方法还包括：

- 30 对所述同或运算后得到的向量进行归一化处理，基于归一化处理后的向量，确定校准后的第二基准特征向量。

第三方面，本申请提供了一种模型训练方法，所述方法包括：

- 针对获取到的任一第三样本图像，基于待训练的卷积神经网络，获得所述第三样本图像的第五特征向量；并基于预设的图像处理方式，将所述第三样本图像处理为一维序列，将所述一维序列输入到待训练的特征提取模型中，基于所述特征提取模型，获得所述第三
35 样本图像的第六特征向量；基于所述第六特征向量，对所述第五特征向量进行校准，获得校准后的第三基准特征向量，其中，所述特征提取模型是基于 MPCFormer 模型的框架结构与语义视觉 Transformer 模型 SETR 的训练逻辑训练所得的模型；

- 40 基于所述第三基准特征向量、所述第三样本图像携带的标签特征向量以及配置的第一损失函数，对所述特征提取模型进行训练；并基于所述第三基准特征向量、所述第三样本图像携带的标签特征向量以及配置的第二损失函数，对所述卷积神经网络进行训练。

第四方面，本申请提供了一种特征提取方法，所述方法包括：

接收待处理图像；

基于第一方面和第三方面任一项所述方法训练得到的特征提取模型、或者基于第二方面和第三方面任一项所述的方法训练得到的卷积神经网络，获得所述待处理图像的特征向量。

在一种可能的实施方式中，所述方法还包括：

基于所述特征向量，进行多方安全计算。

第五方面，本申请提供了一种特征提取模型训练装置，所述装置包括：

第一校准模块，用于针对获取到的任一第一样本图像，基于训练完成的卷积神经网络，获得所述第一样本图像的第一特征向量；并基于预设的图像处理方式，将所述第一样本图像处理为一维序列，将所述一维序列输入到待训练的特征提取模型中，基于所述特征提取模型，获得所述第一样本图像的第二特征向量；基于所述第二特征向量，对所述第一特征向量进行校准，获得校准后的第一基准特征向量，其中，所述特征提取模型是基于 MPCFormer 模型的框架结构与语义视觉 Transformer 模型 SETR 的训练逻辑训练所得的模型；

第一训练模块，用于基于所述第一基准特征向量、所述第一样本图像携带的标签特征向量以及配置的第一损失函数，对所述特征提取模型进行训练。

在一种可能的实施方式中，所述第一校准模块，还用于：

对所述第二特征向量进行全局平均池化，获得所述第二特征向量中每一维特征对应的全局特征向量信息，并基于概率分布函数，获得所述全局特征向量信息中每一维特征对应的重要性权重系数；基于所述每一维特征对应的重要性权重系数，对所述第二特征向量进行校准，获得校准后的第二特征向量；基于校准后的第二特征向量，进行后续基于所述第二特征向量，对所述第一特征向量进行校准的步骤。

在一种可能的实施方式中，所述第一损失函数中包含所述每一维特征对应的重要性权重系数。

在一种可能的实施方式中，所述第一校准模块，具体用于：

对所述第二特征向量中包含的每一维特征与所述第一特征向量中包含的每一维特征进行同或运算，获得校准后的第一基准特征向量。

在一种可能的实施方式中，所述第一校准模块，还用于：

对所述同或运算后得到的向量进行归一化处理，基于归一化处理后的向量，确定校准后的第一基准特征向量。

在一种可能的实施方式中，所述特征提取模型使用的激励函数包含：2quad 激励函数。

在一种可能的实施方式中，所述特征提取模型为基于知识蒸馏得到的模型。

第六方面，本申请提供了一种卷积神经网络训练装置，所述装置包括：

第二校准模块，用于针对获取到的任一第二样本图像，将所述第二样本图像输入到待训练的卷积神经网络中，基于所述卷积神经网络，获得所述第二样本图像的第三特征向量；并基于预设的图像处理方式，将所述第二样本图像处理为一维序列，将所述一维序列输入到训练完成的特征提取模型中，基于所述特征提取模型，获得所述第二样本图像的第四特征向量；基于所述第四特征向量，对所述第三特征向量进行校准，获得校准后的第二基准特征向量，其中，所述特征提取模型是基于 MPCFormer 模型的框架结构与语义视觉

Transformer 模型 SETR 的训练逻辑训练所得的模型;

第二训练模块, 用于基于所述第二基准特征向量、所述第二样本图像携带的标签特征向量以及配置的第二损失函数, 对所述卷积神经网络进行训练。

在一种可能的实施方式中, 所述第二校准模块, 具体用于:

- 5 对所述第四特征向量中包含的每一维特征与所述第三特征向量中包含的每一维特征进行同或运算, 获得校准后的第二基准特征向量。

在一种可能的实施方式中, 所述第二校准模块, 还用于:

对所述同或运算后得到的向量进行归一化处理, 基于归一化处理后的向量, 确定校准后的第二基准特征向量。

- 10 第七方面, 本申请提供了一种模型训练装置, 所述装置包括:

第三校准模块, 用于针对获取到的任一第三样本图像, 基于待训练的卷积神经网络, 获得所述第三样本图像的第五特征向量; 并基于预设的图像处理方式, 将所述第三样本图像处理为一维序列, 将所述一维序列输入到待训练的特征提取模型中, 基于所述特征提取模型, 获得所述第三样本图像的第六特征向量; 基于所述第六特征向量, 对所述第五特征
15 向量进行校准, 获得校准后的第三基准特征向量, 其中, 所述特征提取模型是基于 MPCFormer 模型的框架结构与语义视觉 Transformer 模型 SETR 的训练逻辑训练所得的模型;

- 第三训练模块, 用于基于所述第三基准特征向量、所述第三样本图像携带的标签特征向量以及配置的第一损失函数, 对所述特征提取模型进行训练; 并基于所述第三基准特征
20 向量、所述第三样本图像携带的标签特征向量以及配置的第二损失函数, 对所述卷积神经网络进行训练。

第八方面, 本申请提供了一种特征提取装置, 所述装置包括:

接收模块, 用于接收待处理图像;

- 提取模块, 用于基于第一方面和第三方面任一项所述方法训练得到的特征提取模型、
25 或者基于第二方面和第三方面任一项所述的方法训练得到的卷积神经网络, 获得所述待处理图像的特征向量。

在一种可能的实施方式中, 所述装置还包括:

多方安全计算模块, 用于基于所述特征向量, 进行多方安全计算。

- 第九方面, 本申请还提供了一种电子设备, 所述电子设备至少包括处理器和存储器,
30 所述处理器用于执行存储器中存储的计算机程序时实现如上述任一所述方法的步骤。

第十方面, 本申请提供了一种计算机可读存储介质, 其存储有计算机程序, 所述计算机程序被处理器执行时实现如上述任一所述方法的步骤。

- 由于本申请实施例中, 可以将第一样本图像处理为一维序列, 将该一维序列输入到特征提取模型, 使得特征提取模型可以对该第一样本图像进行特征提取, 而且本申请实施例中特征提取模型是基于 MPCFormer 模型的框架结构与 SETR 模型的训练逻辑训练所得的模型, 从而可以使得特征提取模型可以基于自注意力机制捕捉到更准确的人脸等特征向量 (第二特征向量), 可以基于该第二特征向量对由卷积神经网络获取的第一特征向量进行校准, 获得能够更准确的表达图像特征的第一基准特征向量, 基于该第一基准特征向量以及配置的第一损失函数, 对特征提取模型进行训练, 可以提高训练完成的特征提取模型确定 (提取) 图像特征向量的准确性, 实现快捷准确地提取到高精度的图像特征向量的目的。
40

另外，本申请实施例中特征提取模型是基于 MPCFormer 模型的框架结构与 SETR 模型的训练逻辑训练所得的模型，从而可以使得特征提取模型可以获得像素级别精准的特征向量，进而提高训练完成的特征提取模型确定（提取）图像特征向量的准确性。另外，本申请实施例中可以基于自注意力机制对将第一特征向量等中不重要的特征进行削弱或者
5 去除（忽略），从而可以得到更少而精的特征向量，从而可以在提高获得的特征向量的准确性的同时，还可以减少计算耗时，提高效率，并且不带来额外的计算开销，还可以削弱 MPC 的通信瓶颈。

附图说明

10 为了更清楚地说明本申请实施例或相关技术中的实施方式，下面将对实施例或相关技术描述中所需要使用的附图作一简单地介绍，显而易见地，下面描述中的附图是本申请的一些实施例，对于本领域普通技术人员来讲，还可以根据这些附图获得其他的附图。

图 1 示出了一些实施例提供的第一种特征提取模型训练过程示意图；

图 2A 示出了一些实施例提供的一种基于相关技术中的卷积神经网络获得的第一特征
15 向量对应的图像示意图；

图 2B 示出了一些实施例提供的一种基于特征提取模型获得的第二特征向量对应的图像示意图；

图 3 示出了一些实施例提供的第二种特征提取模型训练过程示意图；

图 4 示出了一些实施例提供的第三种特征提取模型训练过程示意图；

20 图 5 示出了一些实施例提供的不同激励函数的通信时长示意图；

图 6 示出了一些实施例提供的一种 Transformer 模型示意图；

图 7 示出了一些实施例提供的一种 SETR 模型示意图；

图 8 示出了一些实施例提供的一种卷积神经网络训练过程示意图；

图 9 示出了一些实施例提供的一种多方安全计算过程示意图；

25 图 10 示出了一些实施例提供的一种模型训练过程示意图；

图 11 示出了一些实施例提供的一种特征提取过程示意图；

图 12 示出了一些实施例提供的一种特征提取模型训练装置示意图；

图 13 示出了一些实施例提供的一种卷积神经网络训练装置示意图；

图 14 示出了一些实施例提供的一种模型训练装置示意图；

30 图 15 示出了一些实施例提供的一种特征提取装置示意图；

图 16 示出了一些实施例提供的一种电子设备结构示意图。

具体实施方式

为了快捷准确地提取到（获得）高精度的图像特征向量，本申请提供了一种特征提取
35 模型训练方法、卷积神经网络训练方法、模型训练方法、特征提取方法、装置、设备及介质。

为使本申请的目的和实施方式更加清楚，下面将结合本申请示例性实施例中的附图，对本申请示例性实施方式进行清楚、完整地描述，显然，描述的示例性实施例仅是本申请一部分实施例，而不是全部的实施例。

需要说明的是，本申请中对于术语的简要说明，仅是为了方便理解接下来描述的实施方式，而不是意图限定本申请的实施方式。除非另有说明，这些术语应当按照其普通和通常的含义理解。

本申请中说明书和权利要求书及上述附图中的术语“第一”、“第二”、“第三”等是用于区别类似或同类的对象或实体，而不必然意味着限定特定的顺序或先后次序，除非另外注明。应该理解这样使用的用语在适当情况下可以互换。

术语“包括”和“具有”以及他们的任何变形，意图在于覆盖但不排他的包含，例如，包含了一系列组件的产品或设备不必限于清楚地列出的所有组件，而是可包括没有清楚地列出的或对于这些产品或设备固有的其它组件。

术语“模块”是指任何已知或后来开发的硬件、软件、固件、人工智能、模糊逻辑或硬件或/和软件代码的组合，能够执行与该元件相关的功能。

最后应说明的是：以上各实施例仅用以说明本申请的技术方案，而非对其限制；尽管参照前述各实施例对本申请进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分或者全部技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本申请各实施例技术方案的范围。

本申请实施例所有实施方式对数据的获取、存储、使用、处理等均符合国家法律法规的相关规定。

实施例 1:

图 1 示出了一些实施例提供的第一种特征提取模型训练过程示意图，如图 1 所示，该过程包括以下步骤：

S101: 针对获取到的任一第一样本图像，基于训练完成的卷积神经网络，获得所述第一样本图像的第一特征向量；并基于预设的图像处理方式，将所述第一样本图像处理为一维序列，将所述一维序列输入到待训练的特征提取模型中，基于所述特征提取模型，获得所述第一样本图像的第二特征向量；基于所述第二特征向量，对所述第一特征向量进行校准，获得校准后的第一基准特征向量，其中，所述特征提取模型是基于 MPCFormer 模型的框架结构与语义视觉 Transformer 模型 SETR 的训练逻辑训练所得的模型。

在一种可能的实施方式中，特征提取模型可以为基于 MPCFormer 模型的框架结构与语义视觉 Transformer (SETR) 模型的训练逻辑训练所得的模型，其中，针对如何基于 MPCFormer 模型的框架结构与 SETR 模型的训练逻辑获得本申请实施例中的特征提取模型，在后续再进行介绍，在此先不赘述。

在一种可能的实施方式中，在对特征提取模型进行训练时，为了提高特征提取模型获得的特征向量的准确性，可以从第一样本图像集中获取任一第一样本图像，将获取到的该第一样本图像输入到训练完成的卷积神经网络 (Convolutional Neural Network, CNN)，如深度残差网络 (ResNet) 等中，卷积神经网络对第一样本图像进行特征提取，获得该第一样本图像的第一特征向量。其中，第一样本图像可以为包含用户隐私信息，如人脸等生物特征的图像，本申请对第一样本图像不作具体限定。

在一种可能的实施方式中，还可以基于预设的图像处理方式，将第一样本图像处理为一维序列，将一维序列输入到待训练的特征提取模型中，基于特征提取模型对第一样本图像进行特征提取，获得第一样本图像的第二特征向量；基于第二特征向量，对第一特征向

量进行校准,从而可以获得更准确的特征向量(第一基准特征向量)。

具体的,考虑到特征提取模型的框架结构为基于 MPCFormer 模型的框架结构,相关技术中的 MPCFormer 模型通常是用于处理自然语言,为了使得特征提取模型可以处理图像,在本申请实施例中,可以将第一样本图像处理为一维序列,将一维序列输入到特征提取模型中,并且采用对语义视觉 Transformer (SEgmentation TRansformer, SETR) 模型的训练逻辑来训练特征提取模型,使得特征提取模型的运算逻辑与 SETR 模型的运算逻辑相同,从而可以使特征提取模型不仅可以处理图像,还可以基于 SETR 模型的运算逻辑,获取到像素级别更精确的图像特征,并基于多头自注意力机制等,得到更准确(少而精)的图像特征(特征向量),进而可以提高多方安全计算(MPC)的快捷性和准确性。其中,针对如何将第一样本图像处理为一维序列,以及如何基于 MPCFormer 模型的框架结构与 SETR 模型的训练逻辑获得本申请实施例中的特征提取模型,在后续再进行介绍,下面先对基于第二特征向量,对第一特征向量进行校准的过程进行解释说明。

为方便理解,本申请实施例中将第一特征向量用 F 表示,将第二特征向量用 A 表示,基于第二特征向量 A ,对第一特征向量进行校准时,可以采用第二特征向量 A 池化第一特征向量 F ,即对第二特征向量(Attention Maps)中包含的每一维特征与第一特征向量中包含的每一维特征进行同或运算($\odot$),例如,对第二特征向量(Attention Maps)中的第 k 个向量(Attention Map)进行同或运算后得到的向量 $v_k = \sum_{i,j} F_{i,j,k} \odot A_{i,j,k}$,其中“ i,j,k ”表示第 k 个向量(Attention Map)的第 i 行、第 j 列像素。

在一种可能的实施方式中,对第二特征向量中包含的每一维特征与第一特征向量中包含的每一维特征进行同或运算时,可以是在第二特征向量与第一特征向量中相对应的特征的像素均较高时,认为该特征的像素较优质,将同或运算后得到的相应特征的像素配置为较高像素等。而如果任何一方对应的特征的像素较差时,则认为该特征的像素较差,将同或运算后得到的相应特征的像素配置为较低像素等,从而可以通过校准获得更准确(少而精)的图像特征(特征向量)。

可选的,以第二特征向量为例,若某特征的像素高于第二特征向量中特征的平均像素时,可以认为该特征的像素较高,反之,若某特征的像素不高于第二特征向量中特征的平均像素时,可以认为该特征的像素较差。同样的,如果第一特征向量中某特征的像素高于第一特征向量中特征的平均像素时,可以认为该特征的像素较高,反之,若该特征的像素不高于第一特征向量中特征的平均像素,可以认为该特征的像素较差。其中,上述对第二特征向量中包含的每一维特征与第一特征向量中包含的每一维特征进行同或运算的具体计算过程只是示例性说明,本申请对同或运算的具体计算过程不作具体限定。

在一种可能的实施方式中,将第二特征向量中包含的每一维特征与第一特征向量中包含的每一维特征进行同或运算之后,可以基于全连接层(Fully Connected Layer)对同或运算后得到的向量进行归一化处理,归一化到同样大小的特征空间,然后将归一化处理后的向量再求平均,获得校准后的第一基准特征向量,即最终校准后的第一基准特征向量 $f = \frac{1}{K} \sum_k v_k$ 。

参阅图 2A 和图 2B,其中,图 2A 示出了一些实施例提供的一种基于相关技术中的卷积神经网络获得的第一特征向量对应的图像示意图。图 2B 示出了一些实施例提供的一种基于特征提取模型获得的第二特征向量对应的图像示意图。其中,图 2B 中黑色区域为不相关特征区域,可以看出,特征提取模型可以利用自注意力 Attention 机制捕捉到图像中更具体的人脸特征,而忽略图像中其余不相关特征区域,Attention 机制使得真正有利用价值

的图像主题部分特征被提取出来。具体到人脸特征，效果可以表现为 Attention 可以筛选出人脸特征，而屏蔽如环境中的光照、背景等其余图像信息，将这些其余图像信息用黑色区域表示，从而可以得到更少而精、更准确的人脸特征。

在一种可能的实施方式中，以第一样本图像为包含人脸的图像为例，图像中的人脸可能会存在被遮挡或者角度倾斜的部分，为了削弱这部分特征，从而得到重点更突出更准确的人脸特征，在获得第一样本图像的第二特征向量 A 之后，基于第二特征向量 A ，对第一特征向量 F 进行校准之前，还可以对第二特征向量 A 进行校准，基于校准后的第二特征向量 $A^{\sim}$ 对第一特征向量进行校准，从而可以进一步提高获得的第一基准特征向量的准确性。其中，对第二特征向量 A 进行校准，获得校准后的第二特征向量 $A^{\sim}$ 的过程可以如下：

- 10 可选的，可以先对第二特征向量 A 进行全局平均池化 (Global Average Pooling, GAP)，获得第二特征向量中每一维特征对应的全局特征向量信息，并可以把获得的全局特征向量信息映射到 softmax 概率分布函数 ($f_{\text{ex}}(\cdot) = \text{softmax}(\cdot)$)，基于该 softmax 概率分布函数 (也可称为归一化指数函数)，使得第二特征向量 A 中比较重要的特征信息进一步被放大，并获得全局特征向量信息中每一维特征对应的重要性权重系数 s ，示例性的，重要性权重系数 s 可以为： $f_{\text{ex}}(\frac{1}{20^2} \sum_{i,j} A_{i,j,k})$ 。其中，可以是第二特征向量中比较重要的特征（如未被遮挡、角度也不偏斜的人脸特征）对应的重要性权重系数 s 较大，而第二特征向量中不太重要的特征（如被遮挡或者角度偏斜的人脸特征等）对应的重要性权重系数 s 较小，从而可以实现削弱人脸等特征中属于被遮挡或角度偏斜的部分，将 Attention Maps 中属于被遮挡或者角度偏斜的部分设置更低程度的激活（权重系数），从而进一步提高确定的第一基准特征向量的准确性的目的。

在一种可能的实施方式中，可以使用 sigmoid 函数对第二特征向量 A 进行变换，再将变换后的第二特征向量（如 $\text{sigmoid}(A_k)$ ）与相应的重要性权重系数 s_k 相乘，从而得到校准好的第二特征向量 $A^{\sim}$ 。示例性的，校准好的第二特征向量中 $A_k^{\sim} = s_k \cdot \text{sigmoid}(A_k)$ 。

- 25 获得校准好的第二特征向量 $A^{\sim}$ 后，可以基于校准好的第二特征向量 $A^{\sim}$ ，对第一特征向量 F 进行校准，从而得到第一基准特征向量 f 。其中，基于校准好的第二特征向量 $A^{\sim}$ ，对第一特征向量 F 进行校准的过程与基于第二特征向量 A 对第一特征向量 F 进行校准的过程类似，例如，可以对第二特征向量 (Attention Maps) $A^{\sim}$ 中包含的每一维特征与第一特征向量中包含的每一维特征进行同或运算 ($\odot$)，同或运算后得到的第 k 个向量 (Attention Map)： $v_k = \sum_{i,j} F_{i,j,k} \odot A_{i,j,k}^{\sim}$ ，在此不再赘述。

- 30 S102：基于所述第一基准特征向量、所述第一样本图像携带的标签特征向量以及配置的第一损失函数，对所述特征提取模型进行训练。

- 在一种可能的实施方式中，第一样本图像可以携带有预先配置的标签特征向量，其中，本申请对标签特征向量的配置过程不作具体限定。可以基于第一基准特征向量 f 、第一样本图像携带的标签特征向量以及配置的第一损失函数 L ，对特征提取模型进行训练，从而得到一个可以在线上部署的用于提取图像特征向量（如人脸图像的特征向量）的特征提取模型。

- 40 可选的，第一损失函数 L 中可以包含交叉熵损失函数、加权差异化正则损失函数以及 $L2$ 正则化损失函数。为了提取到高精度的图像特征向量，第一损失函数中可以包含每一维特征对应的重要性权重系数。示例性的，配置第一损失函数 L 中的交叉熵损失函数时，可以基于上述重要性权重系数 s_k 以及交叉熵损失项参数 $L_{\text{CE},k}$ ，来确定交叉熵损失函数。例如，可以根据每一维特征对应的重要性权重系数 s_k 与相应维度的交叉熵损失项参数 $L_{\text{CE},k}$ 的乘积

的加和值, 确定交叉熵损失函数。为方便理解, 用公式形式可以将交叉熵损失函数 L_{wce} 表示为: $L_{wce} = \sum_k s_k \cdot L_{ce,k}$ 。采用本申请实施例中的交叉熵损失函数 L_{wce} 可以使得 Attention Maps 中属于被遮挡或者角度偏斜的不重要的部分对模型收敛所带来的损失用其自身的重要性权重系数 s 约束掉, 使该部分损失不参与模型收敛的计算, 从而可以提高训练好的模型 (特征提取模型) 确定的特征向量的准确性。其中, 可以基于现有技术确定交叉熵损失项参数 $L_{ce,k}$, 在此不再赘述。

- 5 可选的, 配置第一损失函数 L 中的加权差异化正则损失函数时, 可以基于上述重要性权重系数 s_k 以及加权差异化损失项参数 $P_{i,j,k}$, 来确定加权差异化正则损失函数 L_{wdiv} 。为方便理解, 用公式形式可以将加权差异化正则损失函数 L_{wdiv} 表示为: $L_{wdiv} = 1 - \sum_{i,j} \max_k (s_k \cdot P_{i,j,k})$, 其中, 加权差异化损失项参数 $P_{i,j,k} = \frac{\exp(A_{i,j,k})}{\sum_{i,j} \exp(A_{i,j,k})}$, 加权差异化损失项参数 $P_{i,j,k}$ 可以认为是对于交叉重叠特征的惩罚项, 可以基于加权差异化正则损失函数 L_{wdiv} 将特征向量中具有交叉重叠的特征进行削弱或者去除, 使由该部分特征带来的损失等不参与模型收敛的计算, 从而可以提高训练好的模型 (特征提取模型) 确定的特征向量的准确性。其中, 可以基于现有技术确定加权差异化损失项参数 $P_{i,j,k}$, 在此不再赘述。另外, 也可以采用现有技术确定 L2 正则化损失函数 L_{reg} , 也不再赘述。

- 15 可选的, 可以为第一损失函数中的交叉熵损失函数 L_{wce} 、加权差异化正则损失函数 L_{wdiv} 以及 L2 正则化损失函数 L_{reg} 这三个子损失函数, 分别配置一个对应的权重, 基于各子损失函数分别与对应的权重的乘积的加和值, 确定损失函数 L 。示例性的, 交叉熵损失函数 L_{wce} 对应的权重用 λ_{wce} 表示, 加权差异化正则损失函数 L_{wdiv} 对应的权重用 λ_{wdiv} 表示, L2 正则化损失函数 L_{reg} 对应的权重用 λ_{reg} 表示, 则第一损失函数 $L = \lambda_{wce} L_{wce} + \lambda_{wdiv} L_{wdiv} + \lambda_{reg} L_{reg}$ 。其中, 基于第一损失函数对特征提取模型进行训练的具体训练过程可以采用现有技术, 在此不再赘述。本申请对各子损失函数对应的权重不作具体限定, 可以根据需求灵活设置。

- 25 可选的, 对特征提取模型进行训练时, 可以是根据第一基准特征向量与第一样本图像携带的标签特征向量是否一致, 确定该特征提取模型的识别结果是否准确。具体实施中, 若不一致, 说明该特征提取模型的识别结果不准确, 则需要对该特征提取模型的参数进行调整, 以期将基于特征提取模型获得的第一基准特征向量可以逐渐向标签特征向量趋近, 对特征提取模型进行训练。

- 30 具体实施中, 对特征提取模型中的参数进行调整时, 可以采用梯度下降算法, 对特征提取模型的参数的梯度进行反向传播, 从而对特征提取模型进行训练。

- 35 在一种可能的实施方式中, 可以对第一样本集中的每个第一样本图像都进行上述操作, 当满足预设的收敛条件时, 确定该特征提取模型训练完成。其中, 满足预设的收敛条件可以为第一样本集中的第一样本图像通过该原始特征提取模型, 被正确识别的样本图像的个数大于设定数量, 或对特征提取模型进行训练的迭代次数达到设置的最大迭代次数等。具体实施中可以灵活进行设置, 在此不做具体限定。

在一种可能的实施方式中, 在进行原始特征提取模型训练时, 可以把样本集中的样本图像分为训练样本图像和测试样本图像, 先基于训练样本图像对原始特征提取模型进行训练, 再基于测试样本图像对上述已训练的特征提取模型的可靠程度进行验证。

- 40 由于本申请实施例, 可以将第一样本图像处理为一维序列, 将该一维序列输入到特征提取模型, 使得特征提取模型可以对该第一样本图像进行特征提取, 而且本申请实施例中特征提取模型是基于 MPCFormer 模型的框架结构与 SETR 模型的训练逻辑训练所得的

模型,从而可以使得特征提取模型可以基于自注意力机制捕捉到更准确的人脸等特征向量(第二特征向量),可以基于该第二特征向量对由卷积神经网络获取的第一特征向量进行校准,获得能够更准确的表达图像特征的第一基准特征向量,基于该第一基准特征向量以及配置的第一损失函数,对特征提取模型进行训练,可以提高训练完成的特征提取模型确定(提取)图像特征向量的准确性,实现快捷准确地提取到高精度的图像特征向量的目的。

另外,本申请实施例中特征提取模型是基于 MPCFormer 模型的框架结构与 SETR 模型的训练逻辑训练所得的模型,从而可以使得特征提取模型可以获得像素级别精准的特征向量,进而提高训练完成的特征提取模型确定(提取)图像特征向量的准确性。另外,本申请实施例中可以基于自注意力机制对将第一特征向量等中不重要的特征进行削弱或者去除(忽略),从而可以得到更少而精的特征向量,从而可以在提高获得的特征向量的准确性的同时,还可以减少计算耗时,提高效率,并且不带来额外的计算开销,还可以削弱 MPC 的通信瓶颈。

为方便理解,下面通过一个具体实施例对本申请提供的特征提取模型训练过程进行解释说明。参阅图 3,图 3 示出了一些实施例提供的第二种特征提取模型训练过程示意图,该过程包括以下步骤:

S301:针对获取到的任一第一样本图像,基于训练完成的卷积神经网络,获得该第一样本图像的第一特征向量;并基于预设的图像处理方式,将第一样本图像处理为一维序列,将一维序列输入到待训练的特征提取模型中,基于特征提取模型,获得该第一样本图像的第二特征向量。其中,特征提取模型是基于 MPCFormer 模型的框架结构与 SETR 模型的训练逻辑训练所得的模型。

S302:对第二特征向量进行全局平均池化,获得第二特征向量中每一维特征对应的全局特征向量信息,并基于概率分布函数,获得全局特征向量信息中每一维特征对应的重要性权重系数;基于每一维特征对应的重要性权重系数,对第二特征向量进行校准,获得校准后的第二特征向量;基于校准后的第二特征向量,对第一特征向量进行校准,获得校准后的第一基准特征向量。

S303:基于第一基准特征向量、第一样本图像携带的标签特征向量以及配置的第一损失函数,对特征提取模型进行训练。

为方便理解,下面再通过一个具体实施例对本申请提供的特征提取模型训练过程进行解释说明。参阅图 4,图 4 示出了一些实施例提供的第三种特征提取模型训练过程示意图,该过程包括以下步骤:

获取到任一第一样本图像后,可以将该第一样本图像输入到训练完成的卷积神经网络(如 ResNet 等 CNN 神经网络)中,基于卷积神经网络对第一样本图像进行特征提取,获得该第一样本图像的特征图,即第一特征向量(Feature Maps)F。同时,可以将第一样本图像处理为一维序列,其中,将第一样本图像处理为一维序列的过程可以如下:

可以将长 $\times$ 宽 $\times$ 色彩通道数(C)为 $H \times W \times 3$ (单位:像素)的一张 2 维(2D)的第一样本图像(如人脸图像)切割(Split)为 $\frac{H}{16} \times \frac{W}{16} = \frac{HW}{256}$ 的多个小块,并将这些小块拉长为 一个长度为 $L=HW/256$ 的一维(1D)序列,将该一维序列作为输入嵌入(Imput Embedding),输入到待训练的特征提取模型(Transformer)中。可选的,还可以使用某种位置嵌入算法对原始图像位置信息进行编码,为一维序列中每个向量 e_i 添加对应的位置编码 p_i ,得到最终输入到特征提取模型的一维序列(输入序列)E,其中,E 可以表示为: $\{e_1+p_1, e_2+p_2, \dots, e_L+p_L\}$ 。

在一种可能的实施方式中，可以将一维序列输入到待训练的特征提取模型中，该特征提取模型的框架结构可以采用 MPCFormer 模型的框架结构，运算逻辑（也可称为训练逻辑）采用 SETR 模型的运算逻辑，可以基于该特征提取模型中的编码器（Encoder）等，获取到基于自注意力机制提取的第二特征向量（Attention Maps）。可选的，特征提取模型中的每个编码器可以分别由多头自注意力层（multi-head self-attention, MSA）和前馈神经网络（也可称为多层感知器，Multi-Layer Perceptron, MLP）组成，假设共有 L_e 个 Encoder。其中，第 1 层自注意力的输入是由 Z^{l-1} 计算得到的三维元组（query, key, value）：其中， $query = Z^{l-1} W_Q$, $key = Z^{l-1} W_K$, $value = Z^{l-1} W_V$ 。其中， W_Q , W_K , W_V 是可学习权重矩阵， d 为三维元组（query, key, value）的维度，则自注意力可以表示为：

$$SA(Z^{l-1}) = Z^{l-1} + \text{softmax}\left(\frac{Z^{l-1} W_Q (Z^{l-1} W_K)^T}{\sqrt{d}}\right) Z^{l-1} W_V.$$

多头（多层）自注意力即是由 m 个 SA 拼接起来得到， $MSA(Z^{l-1}) = [SA_1(Z^{l-1}); SA_2(Z^{l-1}); \dots; SA_m(Z^{l-1})] W_o$ ，其中 $W_o \in R^{md \times C}$ 。每个 Encoder 的输出： $Z^l = MSA(Z^{l-1}) + MLP(MSA(Z^{l-1})) \in R^{L \times C}$ ，所有 Encoder 的总输出为 $\{Z^1, Z^2, \dots, Z^{L_e}\}$ 。其中，将二维图像转换为一维序列，可以认为是将图像 $x \in R^{C \times H \times W}$ 转化为序列 $Z \in R^{L \times C}$ 。可选的，基于特征提取模型进行特征提取推理时，可以通过通用 MPC 计算引擎实现特征提取模型对第二特征向量 A（Attention Maps）的提取过程。

可选的，基于特征提取模型获取到第二特征向量 A 后，可以对第二特征向量 A 进行调整（图中称为基于 Attention Maps 的重新校准）。其中，对第二特征向量 A 进行校准时，可以先对第二特征向量进行全局平均池化（全局池化），获得第二特征向量中每一维特征对应的全局特征向量信息，并基于 softmax 概率分布函数（图中称为 SoftMax 归一化指数函数（ $\text{fex}()$ ）），获得所述全局特征向量信息中每一维特征对应的重要性权重系数 s （也可以用大写 S 表示）。另外，可以使用 sigmoid 函数对第二特征向量 A 进行变换，再将变换后的第二特征向量（ $\text{sigmoid}(A_k)$ ）与相应的重要性权重系数 s 相乘（校准乘积），从而得到校准好的第二特征向量 $A^{\sim}$ 。示例性的，校准好的第二特征向量中 $A_k^{\sim} = s_k \cdot \text{sigmoid}(A_k)$ 。

获得校准好的第二特征向量 $A^{\sim}$ 后，可以基于校准好的第二特征向量 $A^{\sim}$ ，对第一特征向量 F 进行校准，从而得到校准后的第一基准特征向量 f 。例如，可以对第二特征向量（Attention Maps） $A^{\sim}$ 中包含的每一维特征与第一特征向量中包含的每一维特征进行同或运算（ $\odot$ ），同或运算后得到的第 k 个向量（Attention Map）： $v_k = \sum_{i,j} F_{i,j,k} \odot A_{i,j,k}^{\sim}$ ，在此不再赘述。其中，通过上述同或运算对第一特征向量进行校准的过程也可称为基于注意力的池化处理过程。

可选的，获得第一基准特征向量后，可以基于第一基准特征向量以及配置的第一损失函数等，对特征提取模型进行训练。可以将训练得到的特征提取模型部署到线上用于提取人脸图像等图像的特征向量。

示例性的，在利用训练得到的特征提取模型进行特征提取时，可以在接收到待进行特征提取的待处理图像时，将待处理图像输入到训练得到的特征提取模型中，基于特征提取模型的输出结果，获得待处理图像的特征向量。

在一种可能的实施方式中，获得待处理图像的特征向量后，可以基于该特征向量，进行多方安全计算的过程。示例性的，可以将特征提取模型加密部署在服务端（Server 端），由一个或多个客户端（Client 端）加密上传图像等数据，多方协作推理或提取图像的特征向量等，进行多方安全计算的过程，其中，基于特征向量进行多方安全计算的过程可以采

用现有技术，在此不再赘述。

实施例 2:

为了保障多方安全计算的执行效率，降低参与多方安全计算的不同参与方的通信时延，在上述实施例的基础上，在本申请实施例中，所述特征提取模型使用的激励函数包含: 2quad
5 激励函数。另外，所述特征提取模型还可以为基于知识蒸馏得到的模型。

在一种可能的实施方式中，选用不同的激励函数可以对 MPC 计算引擎的计算效率产生不同的影响。参阅图 5，图 5 示出了一些实施例提供的不同激励函数的通信时长示意图。可以看出，当激励函数为一种基于高斯误差函数的激活函数（GaussianError Linear Units，可简称为 GELU 或 gelu）时，总运行时长（图中称为 total time）为 11s，其中参与方之间的通信时长（图中称为 comm, time）为 9.6s。当激励函数为 quad 时，总运行时长为 0.5s，其中参与方之间的通信时长为 9.6s。当激励函数为 softmax 时，总运行时长为 40s，其中参与方之间的通信时长为 34.1s。当激励函数为 2relu 时，总运行时长为 14.7s，其中参与方之间的通信时长为 12.8s。而当激励函数为 2quad ($\text{Softmax}(x) \approx \frac{(x+c)^2}{\sum (x+c)^2}$) 时，总运行时长为 3.2s，其中参与方之间的通信时长为 1.7s。可以看出，当特征提取模型的激励函数包含 2quad
15 激励函数时，可以大大减少参与方之间的通信时间以及总运行时间。可选的，特征提取模型的激励函数除了包含 2quad 激励函数之外，还可以包含 quad 激励函数（ $\text{GeLU}(x) \approx 0.125x^2 + 0.25x + 0.5$ ）。

在一种可能的实施方式中，为了提高特征提取模型的推理速度以及准确度，上述特征提取模型可以为基于知识蒸馏得到的小模型。例如可以将较大的特征提取模型
20 （MPCFormer 模型）通过知识蒸馏得到一个较小的模型，用基于知识蒸馏得到的小模型进行特征提取。

下面对基于 MPCFormer 模型的框架结构与 SETR 模型的训练逻辑得到特征提取模型的过程进行介绍。

Transformer 模型是 ChatGPT 大模型的基座，是一种基于自注意力机制的深度学习神经网络模型，可以高效并行处理序列数据。Transformer 模型是一种神经网络模型，它通过跟踪序列数据中的关系（如这句话中的单词）来学习上下文并因此学习含义，在语言理解尤其是大模型中取得了巨大的成功。在 Transformer 出现前，用户必须使用大型的标记数据集来训练神经网络，数据集的生产成本高昂而且耗时较长。Transformer 模型作为基础模型，在许多情况下，能够取代卷积神经网络（Convolutional Neural Networks, CNN）和循环神经网络（Recurrent Neural Network, RNN）。Transformer 模型可以是处理数据的大型编码器和解码器模块，基于编码器-解码器（Encoder-Decoder）框架实现，参阅图 6，图 6 示出了一些实施例提供的一种 Transformer 模型示意图。Transformer 模型大致分为编码器（Encoder）和解码器（Decoder）个两个部分，分别对应图 6 中的左右两部分（图中所示左右，其中左边部分对应编码器，右边部分对应解码器）。

具体的，Transformer 模型的输入部分（Inputs）包括（词嵌入转化）Input Embedding 和基于位置的词嵌入（也可称为位置编码，Positional Encoding）两部分。无论是文本还是图像，可以将 Input Embedding 的数字表示转变为向量表示，在高维空间获取文本间的关系或图像间的关系。在 Input Embedding 后加入了位置编码，可以将不同输入位置产生的不同含义的信息加入到向量中，增加位置信息的补充。其中，编码器和解码器两个部分都包含
40 输入，且两部分的输入的结构是相同的，只是推理时的用法不同，编码器只推理一次，而

解码器是类似 RNN 那样循环推理，不断生成预测结果。

Transformer 模型的编码器部分由 N 个编码器层堆叠而成，每个编码器层由两个子层连接结构构成。第一个子层包括一个多头自注意力层（multi-head self-attention, MSA）、规范化层和一个残差连接，第二个子层包括一个前馈全连接层（feedforward）、规范化层和一个残差连接，以此类推。两个子层都添加了一个相加并归一化层（Add & Norm）。每个编码器层完成一次对输入的特征提取过程，即编码过程。

Transformer 模型的解码器同样是堆叠了 N 个相同的层，不过和编码器中每层的结构稍有不同。对于解码器的每一层，除了编码器中的两个子层，解码器还包含一个子层：基于掩码的多头注意力层（Masked Multi-Head Attention），如图中所示，每个子层同样也用了相加并归一化层（Add & Norm）。

Transformer 模型的解码器根据编码器的结果以及上一次预测的结果，对目标进行特征提取操作，即解码过程。在输出时，通过线性层（全连接输出层，Linear）进行线性变化得到指定维度的输出，进行维度的转换。并且通过柔性最大值传输函数（Softmax）层将一维向量中的数字缩放到 0-1 的概率值域内，且加起来等于 1，得到模型的预测结果（Output Probabilities）。

可选的，Transformer 模型可以先在大型数据集上进行预训练，以获得一般的理解，然后在小型下游数据集上进行微调，以学习特定任务的特征。

Transformer 模型的推理过程可以表述为一个 2 方计算（2PC）。在 2PC 中，例如，用户一方输入数据，模型提供者一方输入 Transformer 模型。它们共同计算一个推理结果。在整个推理过程中，2PC 保证双方只知道关于自己的输入和结果的信息。可以基于安全多方计算和知识蒸馏技术，实现 MPC 多方参与的 Transformer 推理。MPCFormer 模型是采用经过训练（或微调）的 Transformer 模型，MPCFormer 模型是具有低推理延迟和高 ML 性能的 Transformer 模型，并可以采用给定的 MPC 进行部分近似计算，在计算使用时可以通过知识蒸馏技术构建高性能的近似 Transformer 模型。在推理期间，MPCFormer 模型利用 MPC 引擎实现私有模型推理。

其中，基于 MPCFormer 模型的推理过程可描述为：卷积计算阶段和推理阶段。卷积计算阶段可描述为： $S = \text{MPCFormer}(T, D, A)$ ，其中 T 为经过训练的 Transformer 模型，D 为输入的数据集，A 为基于 MPC 的计算过程。推理阶段可描述为： $y = \text{MPCs}(X)$ 。在基于 MPC 的 Transformer 模型推理中，GeLU 函数和 Softmax 函数是通信瓶颈（通信复杂度高的主要来源）。GeLU 函数计算慢（耗时长）是因为误差函数的计算需要通过高阶泰勒展开计算（涉及大量乘法运算），Softmax 函数计算慢是因为指数函数需要通过多次平方迭代来求值，同样涉及大量的乘法运算。

下面对 SETR 模型进行介绍。SETR 主要由三部分组成：输入→转换→输出。参阅图 7，图 7 示出了一些实施例提供的一种 SETR 模型示意图，其中，图 7 中的（a）部分主要为 SETR 模型的输入预处理及特征提取过程，（b）部分主要为渐进式上采样过程，（c）部分主要是多层级特征聚合过程。

首先，需要将原始的输入图片处理成 Transformer（SETR）能够支持的格式。即对输入图像进行切片处理，将每一个 2D 的图像切片（patch）为一个一维（1D）序列，将一维序列作为整体输入到模型中。为了对每个切片的空间信息进行编码，可以为每个局部位置都学习一个特定的嵌入，并将其添加到一个线性的投影函数中来形成最终的输入序列。如

如此一来, 尽管 Transofomer (SETR) 是无序的, 也仍然可以保留相对应的空间位置信息 (p)。

将一维序列输入到 SETR 模型, SETR 模型中的全连接层 (linear projection layers) 对一维序列进行处理, 获取到切片的向量 (Patch Embedding) 以及切片对应的位置信息向量 (Position Embedding)。SETR 模型中包含了若干个 transformer 层 (transformer layer)。可选的, 任一 transformer layer 主要包含了两个部分: 多头自注意力层 (Multi-head Self-Attention, MSA) 和多层感知器 (Multilayer Perceptron, MLP), 这两部分都连接了层归一化处理过程 (Layer Normalization, Layer Norm)。其中, Layer Norm 是一种用于深度神经网络中的归一化技术, 它可以对网络中的每个神经元的输出进行归一化, 使得网络中每一层的输出都具有相似的分布。

通过将一维序列输入到 Transformer 架构 (SETR 模型) 可以进行特征的提取, 编码器 (Encoder) 用于压缩原始输入图像的空间分辨率并逐步地提取更加高级的抽象语义特征, 解码器 (Decoder) 则用于将编码器所提取到的高级特征上采样到原始输入分辨率以进行像素级的预测, 实现图像的分割。

参阅图 7 中的 (b) 部分, Decoder 的目标是在原始的二维图像 ($H \times W$) 上生成分割结果, 需要将 Encoder 的输出 Z 从二维 $HW/256 \times C$ 重塑 (reshape) 为三维特征图 $H/16 \times W/16 \times C$ 。

解码器可以采用渐进上采样 (PUP)。具体的, 考虑到直接一步上采样会引入很大的噪声, 可以使用交替执行卷积和上采样的方法, 将上采样倍数设置为 2 倍, 以减轻噪声。从 $H/16 \times W/16$ 的 Z^{L_c} 得到原始图片大小, 共需执行 4 次上采样操作。

参阅图 7 中的 (c) 部分关于多层特征融合 (MLA) 的过程。与特征金字塔相似的多级特征融合, 但不同的是特征 Z^L 来自各层 Transformer 并具有相同的分辨率。每隔 L_c/M 层提取一层特征 $\{Z^m\}$ ($m \in \{L_c/M, 2L_c/M, \dots, ML_c/M\}$), 总共提取了 M 条路径的特征。其中, 每一层都是先将 Z^{L_c} 从 $HW/256 \times C$ 重塑到 $H/16 \times W/16 \times C$, 然后使用一个三层神经网络进行处理 (卷积核大小 $1 \times 1, 3 \times 3, 3 \times 3$), 在第一层和第三层分别将通道数减半, 然后在第三层之后进行 4 倍双线性插值上采样。并且从第 2 条路径开始, 依次融合前面路径的特征, 增强每条路径间的信息交互, 再次经过一个 3×3 的卷积层后, 将每条路径得到的特征图进行通道维度的拼接, 并采用 4 倍双线性插值进行上采样, 恢复出原图尺寸。

其中, 基于 MPCFormer 模型的框架结构与 SETR 的训练逻辑获得特征提取模型的过程, 可以理解为将图 7 的 (a) 部分中的 SETR 模型框架结构更换为 MPCFormer 模型框架结构, 仍然采用图 7 中 (b) 部分和图 7 中 (c) 部分中的训练逻辑 (运算逻辑) 来对 MPCFormer 模型进行训练, 从而可以获得特征提取模型。

实施例 3:

基于相同的技术构思, 本申请还提供了一种卷积神经网络训练方法, 参阅图 8, 图 8 示出了一些实施例提供的一种卷积神经网络训练过程示意图, 该过程包括以下步骤:

S801: 针对获取到的任一第二样本图像, 将所述第二样本图像输入到待训练的卷积神经网络中, 基于所述卷积神经网络, 获得所述第二样本图像的第三特征向量; 并基于预设的图像处理方式, 将所述第二样本图像处理为一维序列, 将所述一维序列输入到训练完成的特征提取模型中, 基于所述特征提取模型, 获得所述第二样本图像的第四特征向量; 基于所述第四特征向量, 对所述第三特征向量进行校准, 获得校准后的第二基准特征向量, 其中, 所述特征提取模型是基于 MPCFormer 模型的框架结构与语义视觉 Transformer 模型 SETR 的训练逻辑训练所得的模型。

在一种可能的实施方式中，在对卷积神经网络 (Convolutional Neural Network, CNN)，如深度残差网络 (ResNet) 等进行训练时，为了提高卷积神经网络获得的特征向量的准确性，可以从第二样本图像集中获取任一第二样本图像，将获取到的该第二样本图像输入到待训练的卷积神经网络中。其中，第二样本图像与第一样本图像可以相同，也可以不同，
5 本申请对此不作具体限定。示例性的，第二样本图像和第一样本图像可以为包含被遮挡人脸或者角度倾斜人脸的图像等。

可选的，卷积神经网络对第二样本图像进行特征提取，获得该第二样本图像的第三特征向量 F ，其中，为方便描述，将由卷积神经网络获得的第三特征向量与第一特征向量均用 F 表示。

10 在一种可能的实施方式中，还可以基于预设的图像处理方式，将第二样本图像处理为一维序列，将一维序列输入到训练完成的特征提取模型中，基于特征提取模型对第二样本图像进行特征提取，获得第二样本图像的第四特征向量。其中，本申请实施例中的特征提取模型与上述各实施例中的特征提取模型相同，均是基于 MPCFormer 模型的框架结构与 SETR 模型的训练逻辑所得的模型，在此不再赘述。其中，为方便描述，将由特征提取模型
15 获得的第四特征向量与第二特征向量均用 A 表示。

可选的，为了提高卷积神经网络获得的特征向量的准确性，可以基于第四特征向量 A 对第三特征向量 F 进行校准，获得校准后的第二基准特征向量 f 。其中，基于第四特征向量 A 对第三特征向量 F 进行校准的过程与上述实施例基于第二特征向量 A 对第一特征向量 F 进行校准的过程类似，例如，可以对第四特征向量中包含的每一维特征与第三特征向量中包含的每一维特征进行同或运算，获得校准后的第二基准特征向量。也可以对第四特征向量中包含的每一维特征与第三特征向量中包含的每一维特征进行同或运算，对同或运算后得到的向量进行归一化处理，基于归一化处理后的向量，确定校准后的第二基准特征向量。另外，还可以对第四特征向量进行全局平均池化，获得第四特征向量中每一维特征对应的全局特征向量信息，并基于概率分布函数，获得该全局特征向量信息中每一维特征对应的重要性权重系数，基于每一维特征对应的重要性权重系数，对第四特征向量进行校准，获得校准后的第四特征向量 ($A\sim$)；基于校准后的第四特征向量，对第三特征向量进行校准，在此不再赘述。

S802: 基于所述第二基准特征向量、所述第二样本图像携带的标签特征向量以及配置的第二损失函数，对所述卷积神经网络进行训练。

30 在一种可能的实施方式中，第二样本图像可以携带有预先配置的标签特征向量，其中，本申请对标签特征向量的配置过程不作具体限定。可以基于第二基准特征向量 f 、第二样本图像携带的标签特征向量以及配置的第二损失函数，对卷积神经网络进行训练，从而得到一个可以在线上部署的用于提取图像特征向量 (如人脸图像的特征向量) 的卷积神经网络。

35 可选的，第二损失函数中可以包含交叉熵损失函数、加权差异化正则损失函数以及 L2 正则化损失函数。其中，可以采用现有技术配置第二损失函数，在此不再赘述。

可选的，对卷积神经网络进行训练时，可以是根据第二基准特征向量与第二样本图像携带的标签特征向量是否一致，确定该卷积神经网络的识别结果是否准确。具体实施中，若不一致，说明该卷积神经网络的识别结果不准确，则需要对该卷积神经网络的参数进行调整，以期将基于卷积神经网络获得的第二基准特征向量可以逐渐向标签特征向量趋近，
40

对卷积神经网络进行训练。

具体实施中，对卷积神经网络中的参数进行调整时，可以采用梯度下降算法，对卷积神经网络的参数的梯度进行反向传播，从而对卷积神经网络进行训练。

在一种可能的实施方式中，可以对第二样本集中的每个第二样本图像都进行上述操作，
5 当满足预设的收敛条件时，确定该卷积神经网络训练完成。其中，满足预设的收敛条件可以为第二样本集中的第二样本图像通过该原始卷积神经网络，被正确识别的样本图像的个数大于设定数量，或对卷积神经网络进行训练的迭代次数达到设置的最大迭代次数等。具体实施中可以灵活进行设置，在此不做具体限定。

在一种可能的实施方式中，在进行原始卷积神经网络训练时，可以把样本集中的样本
10 图像分为训练样本图像和测试样本图像，先基于训练样本图像对原始卷积神经网络进行训练，再基于测试样本图像对上述已训练的卷积神经网络的可靠程度进行验证。

由于本申请实施例，可以将第二样本图像输入到特征提取模型，使得特征提取模型
15 可以对该第二样本图像进行特征提取，而且本申请实施例中特征提取模型是基于 MPCFormer 模型的框架结构与 SETR 模型的训练逻辑训练所得的模型，从而可以使得特征提取模型可以基于自注意力机制捕捉到更准确的人脸等特征向量（第四特征向量），可以基于该第四特征向量对由卷积神经网络获取的第三特征向量进行校准，获得能够更准确的表达图像特征的第二基准特征向量，基于该第二基准特征向量以及配置的第二损失函数，对卷积神经网络进行训练，可以提高训练完成的卷积神经网络确定（提取）图像特征向量的准确性，实现快捷准确地提取到高精度的图像特征向量的目的。

20 示例性的，在利用训练得到的卷积神经网络进行特征提取时，可以在接收到待进行特征提取的待处理图像时，将待处理图像输入到训练得到的卷积神经网络中，基于卷积神经网络的输出结果，获得待处理图像的特征向量。获得待处理图像的特征向量后，可以基于该特征向量，进行多方安全计算的过程。示例性的，参阅图 9，图 9 示出了一些实施例提供的一种多方安全计算过程示意图。可以将卷积神经网络部署在服务端（Server 端），通过
25 训练好的卷积神经网络获取到待处理图像的特征向量后，可以对特征向量秘密执行分片并发送至多个协作进行多方安全计算的客户端（Client 端），例如，将特征向量分为秘密共享分片 1 和秘密共享分片 2，可以将其中的秘密共享分片 1 分发给进行多方安全计算的参与方 1 的客户端，将秘密共享分片 2 分发给进行多方安全计算的参与方 2 的客户端等。各 Client 端以秘密分享的方式基于卷积神经网络（CNN）协作提取特征，进行多方安全计算。这种
30 多方安全计算的方式可以防止用户的人脸等生物特征隐私信息被泄露，提高用户数据的安全性。其中，基于特征向量进行多方安全计算的过程可以采用现有技术，在此不再赘述。

实施例 4:

基于相同的技术构思，本申请还提供了一种模型训练方法，参阅图 10，图 10 示出了一些实施例提供的一种模型训练过程示意图，该过程包括以下步骤：

35 S1001: 针对获取到的任一第三样本图像，基于待训练的卷积神经网络，获得所述第三样本图像的第五特征向量；并基于预设的图像处理方式，将所述第三样本图像处理为一维序列，将所述一维序列输入到待训练的特征提取模型中，基于所述特征提取模型，获得所述第三样本图像的第六特征向量；基于所述第六特征向量，对所述第五特征向量进行校准，获得校准后的第三基准特征向量，其中，所述特征提取模型是基于 MPCFormer 模型
40 的框架结构与语义视觉 Transformer 模型 SETR 的训练逻辑训练所得的模型。

在一种可能的实施方式中，可以同时分别对卷积神经网络和特征提取模型进行训练。例如，可以对卷积神经网络和特征提取模型进行训练时，为了提高训练完成的卷积神经网络和特征提取模型获得的特征向量的准确性，可以从第三样本图像集中获取任一第三样本图像，将获取到的该第三样本图像输入到待训练的卷积神经网络中。其中，第三样本图像与第一样本图像、第二样本图像可以相同，也可以不同，本申请对此不作具体限定。示例性的，第三样本图像可以为包含被遮挡人脸或者角度倾斜人脸的图像等。

可选的，卷积神经网络对第二样本图像进行特征提取，获得该第三样本图像的第五特征向量 F ，其中，为方便描述，将由卷积神经网络获得的第五特征向量、第三特征向量与第一特征向量均用 F 表示。

在一种可能的实施方式中，还可以基于预设的图像处理方式，将第三样本图像处理为一维序列，将一维序列输入到待训练的特征提取模型中，基于特征提取模型对第三样本图像进行特征提取，获得第三样本图像的第六特征向量。其中，本申请实施例中的特征提取模型与上述各实施例中的特征提取模型相同，均是基于 MPCFormer 模型的框架结构与 SETR 模型的训练逻辑所得的模型，在此不再赘述。其中，为方便描述，将由特征提取模型获得的第六特征向量、第四特征向量与第二特征向量均用 A 表示。

可选的，为了提高卷积神经网络、特征提取模型获得的特征向量的准确性，可以基于第六特征向量 A 对第五特征向量 F 进行校准，获得校准后的第三基准特征向量 f 。其中，基于第六特征向量 A 对第五特征向量 F 进行校准的过程与上述实施例中基于第二特征向量 A 对第一特征向量 F 进行校准的过程、以及基于第四特征向量 A 对第三特征向量 F 进行校准的过程类似，例如，可以对第六特征向量中包含的每一维特征与第五特征向量中包含的每一维特征进行同或运算，获得校准后的第三基准特征向量。也可以对第六特征向量中包含的每一维特征与第五特征向量中包含的每一维特征进行同或运算，对同或运算后得到的向量进行归一化处理，基于归一化处理后的向量，确定校准后的第三基准特征向量。另外，还可以对第六特征向量进行全局平均池化，获得第六特征向量中每一维特征对应的全局特征向量信息，并基于概率分布函数，获得该全局特征向量信息中每一维特征对应的重要性权重系数，基于每一维特征对应的重要性权重系数，对第六特征向量进行校准，获得校准后的第六特征向量 ($A\sim$)；基于校准后的第六特征向量，对第五特征向量进行校准等，在此不再赘述。

S1002：基于所述第三基准特征向量、所述第三样本图像携带的标签特征向量以及配置的第一损失函数，对所述特征提取模型进行训练；并基于所述第三基准特征向量、所述第三样本图像携带的标签特征向量以及配置的第二损失函数，对所述卷积神经网络进行训练。

其中，基于第三基准特征向量、第三样本图像携带的标签特征向量以及配置的第一损失函数，对特征提取模型进行训练的过程与上述实施例中基于第一基准特征向量、第一样本图像携带的标签特征向量以及配置的第一损失函数，对特征提取模型进行训练的过程类似，在此不再赘述。

基于第三基准特征向量、第三样本图像携带的标签特征向量以及配置的第二损失函数，对卷积神经网络进行训练的过程与上述实施例中基于第二基准特征向量、第二样本图像携带的标签特征向量以及配置的第二损失函数，对卷积神经网络进行训练的过程类似，在此不再赘述。

实施例 5:

基于相同的技术构思, 本申请还提供了一种特征提取方法, 参阅图 11, 图 11 示出了一些实施例提供的一种特征提取过程示意图, 该过程包括以下步骤:

S1101: 接收待处理图像。

- 5 S1102: 基于上述任一所述方法训练得到的特征提取模型或者卷积神经网络, 获得所述待处理图像的特征向量。

在一种可能的实施方式中, 所述方法还包括:

基于所述特征向量, 进行多方安全计算。

实施例 6:

- 10 基于相同的技术构思, 本申请提供了一种特征提取模型训练装置, 参阅图 12, 图 12 示出了一些实施例提供的一种特征提取模型训练装置示意图, 该装置包括:

第一校准模块 1201, 用于针对获取到的任一第一样本图像, 基于训练完成的卷积神经网络, 获得所述第一样本图像的第一特征向量; 并基于预设的图像处理方式, 将所述第一样本图像处理为一维序列, 将所述一维序列输入到待训练的特征提取模型中, 基于所述特征提取模型, 获得所述第一样本图像的第二特征向量; 基于所述第二特征向量, 对所述第一特征向量进行校准, 获得校准后的第一基准特征向量, 其中, 所述特征提取模型是基于 MPCFormer 模型的框架结构与语义视觉 Transformer 模型 SETR 的训练逻辑训练所得的模型;

- 20 第一训练模块 1202, 用于基于所述第一基准特征向量、所述第一样本图像携带的标签特征向量以及配置的第一损失函数, 对所述特征提取模型进行训练。

在一种可能的实施方式中, 所述第一校准模块 1201, 还用于:

- 对所述第二特征向量进行全局平均池化, 获得所述第二特征向量中每一维特征对应的全局特征向量信息, 并基于概率分布函数, 获得所述全局特征向量信息中每一维特征对应的重要性权重系数; 基于所述每一维特征对应的重要性权重系数, 对所述第二特征向量进行校准, 获得校准后的第二特征向量; 基于校准后的第二特征向量, 进行后续基于所述第二特征向量, 对所述第一特征向量进行校准的步骤。

在一种可能的实施方式中, 所述第一损失函数中包含所述每一维特征对应的重要性权重系数。

在一种可能的实施方式中, 所述第一校准模块 1201, 具体用于:

- 30 对所述第二特征向量中包含的每一维特征与所述第一特征向量中包含的每一维特征进行同或运算, 获得校准后的第一基准特征向量。

在一种可能的实施方式中, 所述第一校准模块 1201, 还用于:

对所述同或运算后得到的向量进行归一化处理, 基于归一化处理后的向量, 确定校准后的第一基准特征向量。

- 35 在一种可能的实施方式中, 所述特征提取模型使用的激励函数包含: 2quad 激励函数。

在一种可能的实施方式中, 所述特征提取模型为基于知识蒸馏得到的模型。

实施例 7:

基于相同的技术构思, 本申请提供了一种卷积神经网络训练装置, 参阅图 13, 图 13 示出了一些实施例提供的一种卷积神经网络训练装置示意图, 该装置包括:

- 40 第二校准模块 1301, 用于针对获取到的任一第二样本图像, 将所述第二样本图像输入

到待训练的卷积神经网络中，基于所述卷积神经网络，获得所述第二样本图像的第三特征向量；并基于预设的图像处理方式，将所述第二样本图像处理为一维序列，将所述一维序列输入到训练完成的特征提取模型中，基于所述特征提取模型，获得所述第二样本图像的第四特征向量；基于所述第四特征向量，对所述第三特征向量进行校准，获得校准后的第二基准特征向量，其中，所述特征提取模型是基于 MPCFormer 模型的框架结构与语义视觉 Transformer 模型 SETR 的训练逻辑训练所得的模型；

第二训练模块 1302，用于基于所述第二基准特征向量、所述第二样本图像携带的标签特征向量以及配置的第二损失函数，对所述卷积神经网络进行训练。

在一种可能的实施方式中，所述第二校准模块 1301，具体用于：

对所述第四特征向量中包含的每一维特征与所述第三特征向量中包含的每一维特征进行同或运算，获得校准后的第二基准特征向量。

在一种可能的实施方式中，所述第二校准模块 1301，还用于：

对所述同或运算后得到的向量进行归一化处理，基于归一化处理后的向量，确定校准后的第二基准特征向量。

实施例 8：

基于相同的技术构思，本申请提供了一种模型训练装置，参阅图 14，图 14 示出了一些实施例提供的一种模型训练装置示意图，该装置包括：

第三校准模块 1401，用于针对获取到的任一第三样本图像，基于待训练的卷积神经网络，获得所述第三样本图像的第五特征向量；并基于预设的图像处理方式，将所述第三样本图像处理为一维序列，将所述一维序列输入到待训练的特征提取模型中，基于所述特征提取模型，获得所述第三样本图像的第六特征向量；基于所述第六特征向量，对所述第五特征向量进行校准，获得校准后的第三基准特征向量，其中，所述特征提取模型是基于 MPCFormer 模型的框架结构与语义视觉 Transformer 模型 SETR 的训练逻辑训练所得的模型；

第三训练模块 1402，用于基于所述第三基准特征向量、所述第三样本图像携带的标签特征向量以及配置的第一损失函数，对所述特征提取模型进行训练；并基于所述第三基准特征向量、所述第三样本图像携带的标签特征向量以及配置的第二损失函数，对所述卷积神经网络进行训练。

实施例 9：

基于相同的技术构思，本申请提供了一种特征提取装置，参阅图 15，图 15 示出了一些实施例提供的一种特征提取装置示意图，该装置包括：

接收模块 1501，用于接收待处理图像；

提取模块 1502，用于基于第一方面和第三方面任一项所述方法训练得到的特征提取模型、或者基于第二方面和第三方面任一项所述的方法训练得到的卷积神经网络，获得所述待处理图像的特征向量。

在一种可能的实施方式中，所述装置还包括：

多方安全计算模块，用于基于所述特征向量，进行多方安全计算。

实施例 10：

基于相同的技术构思，本申请还提供了一种电子设备，图 16 示出了一些实施例提供的一种电子设备结构示意图，如图 16 所示，电子设备包括：处理器 1601、通信接口 1602、

存储器 1603 和通信总线 1604, 其中, 处理器 1601, 通信接口 1602, 存储器 1603 通过通信总线 1604 完成相互间的通信;

所述存储器 1603 中存储有计算机程序, 当所述程序被所述处理器 1601 执行时, 使得所述处理器 1601 执行上述任一方法实施例中的步骤, 在此不再赘述。

5 上述电子设备提到的通信总线可以是外设部件互连标准 (Peripheral Component Interconnect, PCI) 总线或扩展工业标准结构 (Extended Industry Standard Architecture, EISA) 总线等。该通信总线可以分为地址总线、数据总线、控制总线等。为便于表示, 图中仅用一条粗线表示, 但并不表示仅有一根总线或一种类型的总线。

通信接口 1602 用于上述电子设备与其他设备之间的通信。

10 存储器可以包括随机存取存储器 (Random Access Memory, RAM), 也可以包括非易失性存储器 (Non-Volatile Memory, NVM), 例如至少一个磁盘存储器。可选地, 存储器还可以是至少一个位于远离前述处理器的存储装置。

上述处理器可以是通用处理器, 包括中央处理器、网络处理器 (Network Processor, NP) 等; 还可以是数字指令处理器 (Digital Signal Processing, DSP)、专用集成电路、现场可编程门阵列或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。

实施例 11:

基于相同的技术构思, 本申请实施例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内存储有可由电子设备执行的计算机程序, 当所述程序在所述电子设备上运行时, 使得所述电子设备执行时实现上述任一方法实施例中的步骤, 在此不再赘述。

20 基于相同的技术构思, 本申请提供了一种计算机程序产品, 所述计算机程序产品包括: 计算机程序代码, 当所述计算机程序代码在计算机上运行时, 使得计算机执行时实现上述应用于电子设备的任一方法实施例所述的方法。

在上述实施例中, 可以全部或部分地通过软件、硬件、固件或者其任意组合来实现, 可以全部或部分地以计算机程序产品的形式实现。所述计算机程序产品包括一个或多个计算机指令, 在计算机上加载和执行所述计算机指令时, 全部或部分地产生按照本申请实施例所述的流程或功能。

本领域内的技术人员应明白, 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。

本申请是参照根据本申请的方法、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。

40 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。

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

5 方框或多个方框中指定的功能的步骤。

显然，本领域的技术人员可以对本申请进行各种改动和变型而不脱离本申请的精神和范围。这样，倘若本申请的这些修改和变型属于本申请权利要求及其等同技术的范围之内，则本申请也意图包含这些改动和变型在内。

10

权利要求

- 1、一种特征提取模型训练方法，所述方法包括：
- 针对获取到的任一第一样本图像，基于训练完成的卷积神经网络，获得所述第一样本图像的第一特征向量；并基于预设的图像处理方式，将所述第一样本图像处理为一维序列，
- 5 将所述一维序列输入到待训练的特征提取模型中，基于所述特征提取模型，获得所述第一样本图像的第二特征向量；基于所述第二特征向量，对所述第一特征向量进行校准，获得校准后的第一基准特征向量，其中，所述特征提取模型是基于 MPCFormer 模型的框架结构与语义视觉 Transformer 模型 SETR 的训练逻辑训练所得的模型；
- 10 基于所述第一基准特征向量、所述第一样本图像携带的标签特征向量以及配置的第一损失函数，对所述特征提取模型进行训练。
- 2、根据权利要求 1 所述的方法，其中，所述获得所述第一样本图像的第二特征向量之后，所述基于所述第二特征向量，对所述第一特征向量进行校准之前，所述方法还包括：
- 对所述第二特征向量进行全局平均池化，获得所述第二特征向量中每一维特征对应的全局特征向量信息，并基于概率分布函数，获得所述全局特征向量信息中每一维特征对应
- 15 的重要性权重系数；基于所述每一维特征对应的重要性权重系数，对所述第二特征向量进行校准，获得校准后的第二特征向量；基于校准后的第二特征向量，进行后续基于所述第二特征向量，对所述第一特征向量进行校准的步骤。
- 3、根据权利要求 2 所述的方法，其中，所述第一损失函数中包含所述每一维特征对应的重要性权重系数。
- 20 4、根据权利要求 1 所述的方法，其中，所述基于所述第二特征向量，对所述第一特征向量进行校准，获得校准后的第一基准特征向量，包括：
- 对所述第二特征向量中包含的每一维特征与所述第一特征向量中包含的每一维特征进行同或运算，获得校准后的第一基准特征向量。
- 5、根据权利要求 4 所述的方法，其中，所述将所述第二特征向量中包含的每一维特征与所述第一特征向量中包含的每一维特征进行同或运算之后，所述获得校准后的第一基准特征向量之前，所述方法还包括：
- 25 对所述同或运算后得到的向量进行归一化处理，基于归一化处理后的向量，确定校准后的第一基准特征向量。
- 6、根据权利要求 1 所述的方法，其中，所述特征提取模型使用的激励函数包含：2quad 激励函数。
- 30 7、根据权利要求 1 所述的方法，其中，所述特征提取模型为基于知识蒸馏得到的模型。
- 8、一种卷积神经网络训练方法，所述方法包括：
- 针对获取到的任一第二样本图像，将所述第二样本图像输入到待训练的卷积神经网络
- 35 中，基于所述卷积神经网络，获得所述第二样本图像的第三特征向量；并基于预设的图像处理方式，将所述第二样本图像处理为一维序列，将所述一维序列输入到训练完成的特征提取模型中，基于所述特征提取模型，获得所述第二样本图像的第四特征向量；基于所述第四特征向量，对所述第三特征向量进行校准，获得校准后的第二基准特征向量，其中，所述特征提取模型是基于 MPCFormer 模型的框架结构与语义视觉 Transformer 模型 SETR

的训练逻辑训练所得的模型；

基于所述第二基准特征向量、所述第二样本图像携带的标签特征向量以及配置的第二损失函数，对所述卷积神经网络进行训练。

- 9、根据权利要求 8 所述的方法，其中，所述基于所述第四特征向量，对所述第三特征向量进行校准，获得校准后的第二基准特征向量，包括：

对所述第四特征向量中包含的每一维特征与所述第三特征向量中包含的每一维特征进行同或运算，获得校准后的第二基准特征向量。

- 10、根据权利要求 9 所述的方法，其中，所述将所述第四特征向量中包含的每一维特征与所述第一特征向量中包含的每一维特征进行同或运算之后，所述获得校准后的第二基准特征向量之前，所述方法还包括：

对所述同或运算后得到的向量进行归一化处理，基于归一化处理后的向量，确定校准后的第二基准特征向量。

- 11、一种模型训练方法，所述方法包括：

- 针对获取到的任一第三样本图像，基于待训练的卷积神经网络，获得所述第三样本图像的第五特征向量；并基于预设的图像处理方式，将所述第三样本图像处理为一维序列，将所述一维序列输入到待训练的特征提取模型中，基于所述特征提取模型，获得所述第三样本图像的第六特征向量；基于所述第六特征向量，对所述第五特征向量进行校准，获得校准后的第三基准特征向量，其中，所述特征提取模型是基于 MPCFormer 模型的框架结构与语义视觉 Transformer 模型 SETR 的训练逻辑训练所得的模型；

- 12、根据权利要求 11 所述的方法，其中，所述基于所述第三基准特征向量、所述第三样本图像携带的标签特征向量以及配置的第一损失函数，对所述特征提取模型进行训练；并基于所述第三基准特征向量、所述第三样本图像携带的标签特征向量以及配置的第二损失函数，对所述卷积神经网络进行训练。

- 12、一种特征提取方法，所述方法包括：

接收待处理图像；

- 25 基于权利要求 1-7、11 任一项所述方法训练得到的特征提取模型、或者基于权利要求 8-11 任一项所述的方法训练得到的卷积神经网络，获得所述待处理图像的特征向量。

- 13、根据权利要求 12 所述的方法，所述方法还包括：

基于所述特征向量，进行多方安全计算。

- 14、一种特征提取模型训练装置，所述装置包括：

- 30 第一校准模块，用于针对获取到的任一第一样本图像，基于训练完成的卷积神经网络，获得所述第一样本图像的第一特征向量；并基于预设的图像处理方式，将所述第一样本图像处理为一维序列，将所述一维序列输入到待训练的特征提取模型中，基于所述特征提取模型，获得所述第一样本图像的第二特征向量；基于所述第二特征向量，对所述第一特征向量进行校准，获得校准后的第一基准特征向量，其中，所述特征提取模型是基于 MPCFormer 模型的框架结构与语义视觉 Transformer 模型 SETR 的训练逻辑训练所得的模型；

第一训练模块，用于基于所述第一基准特征向量、所述第一样本图像携带的标签特征向量以及配置的第一损失函数，对所述特征提取模型进行训练。

- 15、一种卷积神经网络训练装置，所述装置包括：

- 40 第二校准模块，用于针对获取到的任一第二样本图像，将所述第二样本图像输入到待

训练的卷积神经网络中，基于所述卷积神经网络，获得所述第二样本图像的第三特征向量；并基于预设的图像处理方式，将所述第二样本图像处理为一维序列，将所述一维序列输入到训练完成的特征提取模型中，基于所述特征提取模型，获得所述第二样本图像的第四特征向量；基于所述第四特征向量，对所述第三特征向量进行校准，获得校准后的第二基准特征向量，其中，所述特征提取模型是基于 MPCFormer 模型的框架结构与语义视觉 Transformer 模型 SETR 的训练逻辑训练所得的模型；

第二训练模块，用于基于所述第二基准特征向量、所述第二样本图像携带的标签特征向量以及配置的第二损失函数，对所述卷积神经网络进行训练。

16、一种模型训练装置，述装置包括：

10 第三校准模块，用于针对获取到的任一第三样本图像，基于待训练的卷积神经网络，获得所述第三样本图像的第五特征向量；并基于预设的图像处理方式，将所述第三样本图像处理为一维序列，将所述一维序列输入到待训练的特征提取模型中，基于所述特征提取模型，获得所述第三样本图像的第六特征向量；基于所述第六特征向量，对所述第五特征向量进行校准，获得校准后的第三基准特征向量，其中，所述特征提取模型是基于

15 MPCFormer 模型的框架结构与语义视觉 Transformer 模型 SETR 的训练逻辑训练所得的模型；

第三训练模块，用于基于所述第三基准特征向量、所述第三样本图像携带的标签特征向量以及配置的第一损失函数，对所述特征提取模型进行训练；并基于所述第三基准特征向量、所述第三样本图像携带的标签特征向量以及配置的第二损失函数，对所述卷积神经网络进行训练。

20 17、一种特征提取装置，所述装置包括：

接收模块，用于接收待处理图像；

获得模块，用于基于权利要求 1-7、11 任一项所述方法训练得到的特征提取模型、或者基于权利要求 8-11 任一项所述的方法训练得到的卷积神经网络，获得所述待处理图像的特征向量。

25 18、一种电子设备，所述电子设备至少包括处理器和存储器，所述处理器用于执行存储器中存储的计算机程序时实现如权利要求 1-13 任一所述方法的步骤。

19、一种计算机可读存储介质，其存储有计算机程序，所述计算机程序被处理器执行时实现如权利要求 1-13 任一所述方法的步骤。