

## 预测异常样本的方法和装置

### 相关申请的交叉引用

[01] 本专利申请要求于 2018 年 3 月 15 日提交的、申请号为 201810215700 .0、发明名称为“预测异常样本的方法和装置”的中国专利申请的优先权，该申请的全文以引用的方式并入本文中。

### 技术领域

[02] 本说明书一个或多个实施例涉及利用计算机进行样本分类领域，尤其涉及预测异常样本的方法和装置。

### 背景技术

[03] 随着计算机和互联网技术的发展，产生了大量的数据和样本。在许多场景下，需要对这些数据和样本进行分类，例如区分它是正常样本还是异常样本。例如，在支付和交易业务中，经常需要区分正常交易样本和异常交易样本（例如，套现，金融欺诈类交易等），从而更好地预防支付风险。在安全访问领域，经常需要区分正常访问数据和异常访问数据，其中异常访问数据往往来源于一些用户试图通过非法访问的方式，达到入侵或获取非法数据目的。这样的异常访问数据常常具有比较大的危害，对这类数据进行识别和预测，从而阻止异常访问，对于数据安全至关重要。

[04] 随着人工智能和机器学习的兴起，越来越多的业务场景开始引入机器学习来进行数据分析，包括样本的分类和预测。一般来说，机器学习需要运用大量数据来训练模型，特别是有监督的学习，需要利用已知类别的样本，或称为已标定的样本，来训练和调整分类器，然后才能用来对未知样本进行分类。

[05] 然而，在许多情况下，异常样本往往难以采集和标定。一方面，异常样本本身通常数量更少，另一方面，异常样本往往非常隐蔽，难以被发现，例如异常访问的数据通常难以被察觉。因此，能够获取并识别出的异常样本的数量很少，这使得监督学习难以进行。

[06] 因此，希望能有改进的方案，能够更加有效地对异常样本进行预测。

## 发明内容

- [07] 本说明书一个或多个实施例描述了一种方法和装置，能够在仅获取正常历史样本集，且样本维度较高的情况下，有效地对未知样本进行预测。
- [08] 根据第一方面，提供了一种预测异常样本的方法，包括：
- 5 [09] 获取待测样本，所述待测样本包括维度为第一数目的特征数据；
- [10] 采用多个降维方法，分别对所述待测样本进行降维处理，以获得多个处理样本，其中所述多个降维方法中的第  $i$  降维方法  $P_i$ ，将所述待测样本处理为维度为  $D_i$  的处理样本  $S_i$ ，维度  $D_i$  小于所述第一数目；
- [11] 将所述多个处理样本分别对应输入多个处理模型，以获得各个处理样本的打分，
- 10 其中所述多个处理模型中的第  $i$  处理模型  $M_i$ ，基于预先采用支持向量域描述 SVDD 方式在对应维度  $D_i$  的空间中所确定的超球面  $Q_i$ ，为对应的处理样本  $S_i$  打分；
- [12] 根据所述各个处理样本的打分确定所述待测样本的综合分；
- [13] 根据所述综合分，确定所述待测样本是否为异常样本。
- [14] 在一种可能的方案中，上述多个降维方法包括运算降维方法和特征采样降维方法
- 15 中的至少一种。
- [15] 在一个实施例中，上述运算降维方法包括以下中的一种或多种：主成分分析 PCA 方法，最小绝对收缩和选择算子 LASSO 方法，线性判别式分析 LDA 方法，小波分析方法。
- [16] 在一个实施例中，上述特征采样降维方法包括以下中的一种或多种：随机采样方法，
- 20 哈希采样方法，过滤式特征选择方法，包裹式特征选择方法。
- [17] 根据一个实施例，上述第  $i$  处理模型  $M_i$  通过以下步骤训练：获取已知为正常的历史样本集，所述历史样本集的样本维度为所述第一数目；采用所述第  $i$  降维方法  $P_i$ ，将所述历史样本集处理为样本维度为  $D_i$  的低维历史样本集  $L_i$ ；采用支持向量域描述 SVDD 方式，在维度为  $D_i$  的空间中确定所述超球面  $Q_i$ ，使得该超球面  $Q_i$  所包围的低维历史样本集  $L_i$  中的样本数目与该超球面的半径之间的关系满足预定条件。
- 25 [18] 根据一种实施方式，为对应的处理样本  $S_i$  打分包括：确定所述处理样本  $S_i$  在对应维度空间中与所述超球面  $Q_i$  的相对位置；根据所述相对位置，确定处理样本  $S_i$  的打分。

- [19] 根据可能的实施方式，上述相对位置包括以下之一：所述处理样本  $S_i$  位于所述超球面  $Q_i$  之外、之内或之上；所述处理样本  $S_i$  在对应维度空间中距离所述超球面  $Q_i$  的中心的距离；所述处理样本  $S_i$  在对应维度空间中距离所述超球面  $Q_i$  的最近表面的距离。
- [20] 在一个实施例中，确定所述待测样本的综合分包括：对所述各个处理样本的打  
5 分进行加权求和，获得所述综合分，
- [21] 根据第二方面，提供一种预测异常样本的装置，包括：
- [22] 获取单元，配置为获取待测样本，所述待测样本包括维度为第一数目的特征数据；
- [23] 多个降维单元，所述多个降维单元分别采用多个降维方法，对所述待测样本进行降维处理，以获得多个处理样本，其中所述多个降维方法中的第  $i$  降维方法  $P_i$ ，将所述  
10 待测样本处理为维度为  $D_i$  的处理样本  $S_i$ ，维度  $D_i$  小于所述第一数目；
- [24] 多个打分单元，配置为通过多个处理模型对所述多个处理样本进行打分，其中所述多个处理模型中的第  $i$  处理模型  $M_i$ ，基于预先采用支持向量域描述 SVDD 方式在对应维度  $D_i$  的空间中所确定的超球面  $Q_i$ ，为对应的处理样本  $S_i$  打分；
- [25] 综合单元，配置为根据所述各个处理样本的打分确定所述待测样本的综合分；
- 15 [26] 确定单元，配置为根据所述综合分，确定所述待测样本是否为异常样本。
- [27] 根据第三方面，提供了一种计算机可读存储介质，其上存储有计算机程序，当所述计算机程序在计算机中执行时，令计算机执行第一方面的方法。
- [28] 根据第四方面，提供了一种计算设备，包括存储器和处理器，其特征在于，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现第一方面的方法。
- 20 [29] 通过本说明书实施例提供的方法和装置，针对待测样本，采用多种降维方法分别对其进行降维，然后对于降维后的多个处理样本，分别基于 SVDD 模型确立的超球面，对处理样本进行打分，最后根据多个打分的综合结果判定待测样本是否异常。由于采用多种不同的降维方法，每种降维方法所得到的特征可以互相补充，最大限度地避免了降维带来的信息损失。同时，由于经过降维处理，使得 SVDD 模型的应用变得实际可行，
- 25 避免了维度“爆炸”带来的计算障碍。在此基础上，综合考虑各个 SVDD 模型的结果，可以对待测样本进行全面的评估，准确的预测。

## 附图说明

[30] 为了更清楚地说明本发明实施例的技术方案，下面将对实施例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发明的一些实施例，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它的附图。

- [31] 图 1 为本说明书披露的一个实施例的实施场景示意图；
- [32] 图 2A 示出 SVM 模型的示意图；
- [33] 图 2B 示出 SVDD 模型的示意图；
- [34] 图 3 示出根据一个实施例的建立预测模型的示意图；
- 10 [35] 图 4 示出根据一个实施例的预测异常样本的方法流程图；
- [36] 图 5 示出根据一个实施例的预测异常样本的过程示意图；
- [37] 图 6 示出根据一个实施例的预测异常样本的装置的示意性框图。

## 具体实施方式

- [38] 下面结合附图，对本说明书提供的方案进行描述。
- 15 [39] 图 1 为本说明书披露的一个实施例的实施场景示意图。如图 1 所示，计算平台 100，例如支付宝服务器，基于正常的历史样本集（例如正常的历史交易样本集），采用支持向量域描述 SVDD 方式训练一个预测模型。训练过程中，为避免样本维度太高带来的计算困难，对于各个历史样本，计算平台 100 采用多种降维方法对其分别进行降维，得到多个降维样本集，然后采用 SVDD 方式分别对降维样本集进行学习，得到多个处理模型，
- 20 这些处理模型可以认为是预测模型的子模型，由这些子模型的组合构成上述预测模型。如此，在获取到未知的待测样本时，将待测样本采用相同的降维方式进行降维，对应输入该预测模型中的各个子模型，通过各个子模型对待测样本进行打分，最后根据打分的综合结果来预测该待测样本是否为异常样本。下面分别描述以上两个阶段的具体实施过程。
- 25 [40] 首先，描述上述预测模型的建立和训练。如前所述，对样本进行有监督的学习，从而训练预测模型的一项主要困难在于，异常样本难以获得，数量太少，不足以对其进行监督学习。为此，本说明书的实施例采用支持向量域描述(Support Vector Domain

Description)SVDD 方式, 仅仅基于正常历史样本来构建模型。下面描述 SVDD 方式的  
处理方式。

[41] 支持向量域描述 SVDD 是基于支持向量机 SVM (Support Vector Machine) 思想发  
展而来的一种模型。支持向量机 SVM 模型仍然是一种监督学习模型, 需要预先将样本  
5 标定为不同类。训练过程中, 首先将样本向量映射到一个高维空间中, 在这个空间中建  
立一个最大间隔超平面, 以分开不同类的样本。图 2A 示出 SVM 模型的示意图。在图  
2A 中, 以二维情况下对样本进行二分类为例进行示意。如图 2A 所示, 在分开样本数据  
(两类样本分别示出为圆圈和 ×) 的超平面的两边建有两个互相平行的超平面 (虚线示  
出), 分隔超平面使这两个平行超平面的距离最大化。这两个平行超平面上的样本点称  
10 为支持向量。

[42] 基于支持向量机 SVM 模型发展的支持向量域描述 SVDD 则可以基于给定某一类别  
的样本进行训练。图 2B 示出 SVDD 模型的示意图。如图 2B 所示, SVDD 模型的主要  
思想是, 给定一定数量的同类样本, 例如, 正常历史样本, 将这些样本映射到高维空间  
中, 然后在这个高维空间中试图建立一个椭球, 使得该椭球尽量小, 同时囊括尽量多的  
15 样本。可以理解的是, 上述“椭球”的概念只是为了便于描述, 在高维空间中, 上述椭  
球实际上对应高维空间的超球面。换言之, SVDD 模型的目标就是, 对于各个已知的  
正常样本  $x_i$ , 在  $x_i$  对应的空间中求一个中心为  $a$ , 半径为  $R$  的最小超球面, 使得落入这  
个球形内部 (到球心的距离小于  $R$ ) 的样本点的数目尽可能多, 也就是构造目标函数  $F$ :

$$F(R, \vec{a}, \xi) = R^2 + C \sum_{i=1}^N \xi_i \quad (1)$$

20 [43] 使得:

$$\|(\vec{x}_i - \vec{a})\|^2 \leq R^2 + \xi_i \quad \forall i, \xi_i \geq 0 \quad (2)$$

[44] 可以理解的是, 希望超球面半径  $R$  尽可能小 (第一条件), 与希望该超平面囊括  
尽可能的样本点 (第二条件), 两者是数学上矛盾的两个条件。因此, 在上述公式中设  
定了参数  $C$ , 用以衡量对第一条件和第二条件的考虑比例。例如,  $C$  值更大的情况下,  
25 就会更偏向于找一个可以囊括更多样本点的超球面;  $C$  值更小的情况下, 就会更偏向于  
找一个更小的超球面。确定的超球面可以用于对未知样本进行预测: 如果未知样本落入  
该超球面, 那么较大概率该未知样本为正常样本; 如果未知样本位于该超球面之外, 则  
为潜在的异常样本。

[45] 尽管 SVDD 模型可以基于单一类型的样本数据进行建模, 例如基于正常样本进行建模, 但是在样本数据的维度较大的情况下, 容易出现“维度爆炸”, 计算效率难以满足要求。如果对样本数据进行降维处理, 又会损失一些有用的信息, 使得训练结果不够准确。因此, 在说明书的实施例中, 创新性地采用多种方式并行降维, 互为补充, 然后

5 对降维的样本数据分别采用 SVDD 方式, 来获得多个子模型, 由该多个子模型综合构成预测模型。

[46] 图 3 示出根据一个实施例的建立预测模型的示意图。如图 3 所示, 首先获取已知为正常的历史样本集  $H$ , 其中包括已知正常的多个历史样本。一般地, 这些历史样本具有较高的维度。例如, 交易样本涉及的特征数据可以包括, 买方信息、卖方信息、交易

10 对象信息、交易时间、交易地点、与该交易有关的交易记录等等, 其中每一项又可以进一步细化, 因此在一些情况下, 交易样本常常包括上千维, 甚至几千维的特征数据。又例如, 访问样本涉及的特征数据可以包括, 访问发起方的网络地址、个人信息、发起时间、发起地点、访问目标的网络地址、相关访问记录等等, 因此, 正常访问样本的维度通常也在几百到上千维之间。

15 [47] 对于这些高维历史样本构成的样本集  $H$ , 采用多种 ( $N$  种) 降维方法 ( $P_1, P_2, \dots, P_i, \dots, P_N$ ), 分别对样本集  $H$  进行降维, 以得到多个 ( $N$  个) 低维历史样本集 ( $L_1, L_2, \dots, L_i, \dots, L_N$ )。具体地,  $N$  种降维方法中的任一降维方法  $P_i$ , 通过对高维历史样本集  $H$  进行降维处理, 可以得到维度为  $D_i$  的低维历史样本集  $L_i$ 。通过  $N$  种降维方法得到的  $N$  个低维历史样本集的维度可以不相同, 但是均小于原始样本的维度。

20 [48] 图 3 示意性示出了  $N=4$  的情况。更具体地, 在图 3 中, 多种降维方法具体为: 第一、第二、第三、第四降维方法, 这几种降维方法分别对原始的高维历史样本集进行降维处理, 分别得到第一、第二、第三、第四低维样本集, 其维度分别为  $D_1, D_2, D_3$  和  $D_4$ 。

[49] 上述的降维方法可以采用各种已知的、以及以后可能采用的降维算法。

25 [50] 在一个实施例中, 上述多种降维方法包括运算降维方法。运算降维方法是对原始高维样本中的特征数据进行线性或非线性的运算, 得到维度降低的处理样本。一般地, 处理样本中的特征值并不直接对应于原始样本中的某个特征, 而是原始样本中多个特征共同运算的结果。

[51] 例如, 运算降维方法包括主成分分析 PCA (Principal Component Analysis) 方法。

主成分分析 PCA 方法通过线性正交变换将原始数据  $n$  维数据变换为一组各维度线性无关的表示, 变换后的结果中, 第一个主成分具有最大的方差值, 每个后续的成分在与前述主成分正交条件限制下具有最大方差。

5 [52] 更具体地, 假设有  $m$  条  $n$  维数据, 根据 PCA 方法, 首先将原始数据按列组成  $n$  行  $m$  列矩阵  $X$ , 对该矩阵  $X$  的每一行进行零均值化 (即减去这一行的均值), 然后求出其协方差矩阵  $C$ , 以及矩阵  $C$  的特征值及对应的特征向量。接着, 将上述特征向量按对应特征值大小从上到下按行排列成矩阵, 取前  $k$  行组成矩阵  $P$ , 并取  $Y=PX$  作为最后得到的降维到  $k$  维后的数据。

10 [53] 在一个具体例子中, 运算降维方法包括最小绝对收缩和选择算子 LASSO (Least absolute shrinkage and selection operator) 方法。该方法是一种压缩估计, 其基本思想是在回归系数的绝对值之和小于一个常数的约束条件下, 使残差平方和最小化。

[54] 在一个具体例子中, 数学上的小波分析过程中的一些变换操作可以排除一些干扰数据, 也可以起到降维作用, 因此也可以将其作为一种运算降维方法。

15 [55] 其他的运算降维的例子还包括, 例如, 线性判别 LDA (Linear Discriminant Analysis) 方法, 拉普拉斯特征映射, 矩阵奇异值分解 SVD, LLE 局部线性嵌入 (Locally linear embedding) 等等。

[56] 在一个实施例, 上述多种降维方法还可以包括特征采样方法, 或称为特征选择。特征采样方法是从原始高维样本的特征数据中选择其中的一部分进行采样, 即形成一个特征子集, 由该特征子集构成维度降低的处理样本。此时, 处理样本中的特征值可以直接对应于原始样本中的某个特征。可以理解的是, 可以采用多种采样方法来进行特征采样。  
20

[57] 在一个具体例子中, 采用随机采样方法对原始数据进行特征采样, 也就是, 从原始高维样本中随机选择一部分特征构成处理样本。在另一例子中, 采用哈希采样方法进行特征采样。根据该方法, 对原始高维样本进行哈希运算, 根据哈希运算的结果, 确定选择哪些特征数据。  
25

[58] 在特征选择领域, 为了评价选择出的特征子集对原始高维样本的代表性和预测性, 会引入特征评估函数。根据特征评估函数的不同, 特征采样还可以分为过滤式 (Filter) 特征选择方法和包裹式 (Wrapper) 特征选择方法。过滤式特征选择方法一般不依赖具体的学习算法来评价特征子集, 而是根据数据集的内在特性来评价每个特征的预测能力,

从而找出排序较优的若干个特征组成特征子集。通常，此类方法认为最优特征子集是由若干个预测能力较强的特征组成的。包裹式特征选择方法，又称为封装式特征选择方法，用后续的学习算法嵌入到特征选择过程中，通过测试特征子集在此算法上的预测性能来决定它的优劣，而极少关注特征子集中单个特征的预测性能。

- 5 [59] 以上列举了多种运算式降维方法的例子和多种特征采样式降维方法的例子。本领域技术人员可以根据要处理的数据特点，例如根据图 3 获取的历史样本集中历史样本的维度、数据分布、数据结构等特点，选择适当的降维方法。

- [60] 例如，在图 3 的例子中，假定获取的正常历史样本集中，各个历史样本维度为 1000 维，那么在一个例子中，第一降维方法可以采用 PCA 方法，降维得到 100 维的第一低维样本集，第二降维方法可以采用随机采样方法，降维得到 300 维的第二低维样本集，第三降维方法可以采样哈希采样方法，降维得到 200 维的第三低维样本集，等等。
- 10

[61] 可以理解的是，以上仅仅是一个举例。在不同实施例，采用的降维方法的数目 (N) 可以更多或更少，采取的具体降维方法可以与以上例子不同，对于任意的具体降维方法，降维比例的设定也可以不同。

- 15 [62] 在对原始历史样本集 H 分别进行降维的基础上，就可以基于降维得到的 N 个低维历史样本集，采用 SVDD 方式进行学习。具体地，对于通过降维方法  $P_i$  得到的第 i 个低维历史样本集  $L_i$  (对应维度为  $D_i$ )，采用支持向量域描述 SVDD 方式，在维度为  $D_i$  的空间中确定超球面  $Q_i$ ，使得该超球面  $Q_i$  所包围的低维历史样本的数目与该超球面的半径之间的关系满足预定条件。如前所述，根据支持向量域描述 SVDD 方法的主旨思想，通过之前的公式 (1) 和公式 (2) 确定超球面  $Q_i$ ，希望上述超球面  $Q_i$  能够包围尽量多的低维历史样本，且具有尽量小的半径。所包围的低维历史样本的数目与该超球面的半径之间的关系通过其中的参数 C 进行设定。
- 20

- [63] 如此，针对各个低维历史样本集  $L_i$  确立了对应的超球面  $Q_i$ 。如前所述，如此确定的超球面  $Q_i$  囊括了对应维度空间中大多数的低维历史样本，而并非绝对囊括所有的样本，因此仍然会有正常样本落在超球面之外。相应地，在一个实施例中，在训练阶段，还对正常的历史样本集中所有样本，在其低维空间中相对于超球面  $Q_i$  的距离分布进行统计。例如统计所有正常样本在各个低维空间中距离超球面  $Q_i$  中心的平均距离，最大距离等。这些统计的距离可用于确定预测阶段所需的判定阈值。
- 25

[64] 通过以上过程，针对正常的历史样本集，采用 SVDD 模型对其进行了学习。更具

体地, 采用多种降维方法分别对历史样本集进行降维, 然后对于各个降维后的样本集, 分别采用 SVDD 模型确立对应的超球面。由于采用多种不同的降维方法, 每种降维方法所得到的特征可以互相补充, 最大限度地避免了降维带来的信息损失。同时, 由于经过降维处理, 使得 SVDD 的应用变得实际可行, 避免了维度“爆炸”带来的计算障碍。

5 [65] 在此基础上, 可以采用通过以上方式建立的模型来预测未知样本。

[66] 图 4 示出根据一个实施例的预测异常样本的方法流程图, 该方法的执行主体可以是图 1 所示的计算平台。如图 4 所示, 该实施例中预测异常样本的方法包括以下步骤: 步骤 41, 获取待测样本, 其包括维度为第一数目的特征数据; 步骤 42, 采用多个降维方法, 分别对所述待测样本进行降维处理, 以获得多个处理样本, 其中所述多个降维方法中的第  $i$  降维方法  $P_i$ , 将所述待测样本处理为维度为  $D_i$  的处理样本  $S_i$ , 维度  $D_i$  小于所述第一数目; 步骤 43, 将多个处理样本分别对应输入多个处理模型, 以获得各个处理样本的打分, 其中第  $i$  处理模型  $M_i$ , 基于预先采用支持向量域描述 SVDD 方式在对应维度空间中确定的超球面  $Q_i$ , 为对应的处理样本  $S_i$  打分; 步骤 44, 根据各个处理样本的打分确定所述待测样本的综合分; 步骤 45, 根据所述综合分, 确定所述待测样本是否  
10 为异常样本。下面描述以上各个步骤的具体执行方式。

[67] 首先在步骤 41, 获取待测样本  $T$ 。可以理解, 待测样本是分类未知的样本, 并且与用于模型训练的历史样本一样都是高维样本, 更具体地, 待测样本与前述历史样本集中的历史样本具有相同的维度。该维度数目在此称为第一数目。

[68] 接着在步骤 42, 采用多个降维方法, 分别对待测样本  $T$  进行降维处理, 以获得多个处理样本。可以理解, 此处的多个降维方法与训练阶段的多个降维方法分别对应一致。具体地, 上述多个降维方法中的第  $i$  降维方法  $P_i$ , 将所述待测样本  $T$  处理为维度为  $D_i$  的处理样本  $S_i$ , 维度  $D_i$  小于所述第一数目。通过多个降维方法分别得到的多个处理样本的维度之间可以不同, 但是均小于待测样本的原始维度 (第一数目)。  
20

[69] 如前所述, 降维方法可以采用各种已知的、以及以后可能采用的降维算法, 例如  
25 包括运算降维方法, 特征采样方法。运算降维方法进一步包括以下中的一项或多项: 主成分分析 PCA 方法、最小绝对收缩和选择算子 LASSO 方法、小波分析方法、线性判别 LDA 方法、拉普拉斯特征映射、矩阵奇异值分解 SVD、LLE 局部线性嵌入, 等等。特征采样方法进一步包括以下中的一项或多项: 随机采样方法、哈希采样方法、过滤式特征选择方法、包裹式特征选择方法, 等等。以上各种具体降维方法的具体描述可以参见  
30 之前的说明, 在此不再赘述。但需要理解的是, 不管具体采用了哪几种降维方法, 步骤

42 中采用的多种降维方法需与历史样本学习阶段的降维方法相一致。

[70] 在通过多种降维方法将待测样本降维为多个处理样本之后，在步骤 43，将该多个处理样本分别对应输入多个处理模型，以获得各个处理样本的打分，其中第  $i$  处理模型  $M_i$ ，基于预先采用支持向量域描述 SVDD 方式在对应维度空间中确定的超球面  $Q_i$ ，为  
5 对应的处理样本  $S_i$  打分。

[71] 可以理解，在历史样本学习阶段，已经采用支持向量域描述 SVDD 方式，在各个降维之后的空间中确定了相应的超球面  $Q_i$ ，该超球面  $Q_i$  具有尽量小的半径且能够囊括尽量多的降维后的历史样本。因此，该超球面  $Q_i$  可以用于判断或预测具有相同维度的、当前输入的处理样本是异常样本的可能性。具体地，在一个实施例中，通过打分的方式  
10 来衡量这样的可能性。

[72] 在一个实施例中，处理模型  $M_i$  为对应的处理样本  $S_i$  打分的过程可以包括：确定处理样本  $S_i$  在对应维度空间中与超球面  $Q_i$  的位置关系；根据所述位置关系，确定处理样本  $S_i$  的打分。

[73] 更具体地，上述位置关系可以是，处理样本  $S_i$  位于所述超球面  $Q_i$  之外、之内或之上。例如，在一个示例中，处理模型  $M_i$  可以设定为，如果处理样本  $S_i$  在对应维度空间（ $D_i$  维空间）中位于超球面  $Q_i$  之内，则其打分为 1；如果处理样本  $S_i$  正好位于超球面  $Q_i$  的表面上（类似于支持向量），则其打分为 0.5；如果处理样本  $S_i$  位于超球面  $Q_i$  之外，则其打分为 0 分。如此，较高的分数意味着，该处理样本  $S_i$  有较大的可能对应于正常样本。  
15

[74] 在一个实施例中，上述位置关系可以是与超球面  $Q_i$  的距离。更具体地，在一个例子中，处理模型  $M_i$  根据处理样本  $S_i$  在对应维度空间中距离超球面  $Q_i$  的中心的距离  $d$ ，为该处理样本  $S_i$  打分。其中，处理样本  $S_i$  和超球面的中心分别对应于维度为  $D_i$  的空间中的点，因此距离  $d$  的计算可以采用多维空间中两点距离的计算方式来确定。在计算得到距离  $d$  的基础上，例如可以根据以下公式计算处理样本  $S_i$  的打分  $G_i$ ：  
20

25 [75]  $G_i = \exp(-d)$  (3)

[76] 根据该公式 (3)， $G_i$  取值在 0 到 1 之间，且处理样本  $S_i$  距离超球面  $Q_i$  中心的距离越小，即越接近超球面中心， $d$  越小， $G_i$  值越大；处理样本  $S_i$  距离超球面  $Q_i$  中心的距离越大，即越远离超球面中心， $d$  越大， $G_i$  值越小。如此，较大的  $G_i$  分值意味着，该处理样本  $S_i$  有较大概率对应于正常样本。

[77] 在另一实施例中，通过不同的方式计算处理样本  $S_i$  与超球面的距离。例如，在一些 SVDD 模型下，获取到的超球面  $Q_i$  并不对应于一个各向同性的正球体，而是在不同方向具有不同“半径”，类似于三维空间的椭球。在这样的情况下，在一个实施例中，首先判断处理样本  $S_i$  是否位于超球面  $Q_i$  之内，如果位于超球面  $Q_i$  之内，则令  $G_i=1$ ；  
5 如果处理样本  $S_i$  位于超球面  $Q_i$  之外，那么计算处理样本  $S_i$  在对应维度空间中与超球面  $Q_i$  的最近表面的距离  $d$ ，并根据该距离  $d$ ，利用公式 (3) 计算得分  $G_i$ 。

[78] 以上仅仅是给出了基于预先确定的超球面对处理样本进行打分的具体例子。在阅读这些例子的情况下，本领域技术人员可以对其进行修改、替换、结合或扩展，从而采用更多种打分方式，这些都应该涵盖在本说明书的构思之中。并且，步骤 43 中，多个  
10 处理模型分别对相应维度的处理样本进行打分，其中多个处理模型各自采用的打分算法可以相同，也可以不同。

[79] 在步骤 43 中各个处理模型  $M_i$  分别为各个处理样本  $S_i$  进行打分的基础上，接着在步骤 44，根据各个处理样本的打分确定待测样本的综合分。

[80] 根据一个实施例，在该步骤中，对各个处理样本的打分直接求和，将求和结果作为综合分。在另一实施例中，预先为各个处理模型的打分分配一定的权重，根据分配的  
15 权重，对各个处理样本的打分进行加权求和，由此获得所述综合分。

[81] 于是，在步骤 45，根据所述综合分，确定待测样本是否为异常样本。根据一个实施例，在该步骤中，将步骤 44 确定的综合分与预先确定的阈值进行比较，根据比较结果，确定待测样本是否为异常样本。可以理解，该阈值的确定与步骤 43 中的打分算法  
20 有关。例如，在根据公式 (3) 进行打分的情况下，更高的综合分意味着，待测样本有更大概率对应于正常样本。另一方面，在一个实施例，上述阈值可以根据样本学习阶段的统计来确定。如前所述，在样本学习阶段，还可以对正常的历史样本集中所有样本，在其低维空间中相对于超球面  $Q_i$  的距离分布进行统计。在一个实施例中，根据这些距离统计，采用与步骤 43 一致的打分算法，对正常的历史样本计算综合分的统计，根据  
25 综合分统计来确定判定阈值。基于如此确定的阈值，在步骤 45 中，就可以简单地通过阈值比较来确定，待测样本是否为异常样本。

[82] 图 5 示出根据一个实施例的预测异常样本的过程示意图，并且，图 5 的预测过程是基于图 3 所建立的预测模型而实现的。如图 5 所示，首先获取高维的待测样本  $T$ 。待测样本  $T$  的维度与图 3 所示的历史样本集  $H$  中的样本维度相同。接着，采用多种降维  
30 方法，分别待测样本  $T$  进行降维，得到多个处理样本。具体地，与图 3 对应地，上述多

种降维方法具体为：第一、第二、第三、第四降维方法，这几种降维方法分别对原始的待测样本 T 进行降维处理，分别得到第一、第二、第三、第四处理样本，其维度分别为 D1, D2, D3 和 D4。

[83] 然后，将第一、第二、第三、第四处理样本分别对应输入第一、第二、第三、第四处理模型，以获得各个处理样本的打分。具体地，第一处理模型基于图 3 中获得的超球面 Q1，为第一处理样本打分 G1，第二处理模型基于图 3 中获得的超球面 Q2，为第二处理样本打分 G2，第三处理模型基于图 3 中获得的超球面 Q3，为第三处理样本打分 G3，第四处理模型基于图 3 中获得的超球面 Q4，为第四处理样本打分 G4。然后，根据各个处理样本的打分 G1-G4 确定待测样本的综合分 G，根据该综合分 G，确定所述待测样本是否为异常样本。

[84] 通过以上过程，针对待测样本，采用多种降维方法分别对其进行降维，然后对于降维后的多个处理样本，分别基于 SVDD 模型确立的超球面，对处理样本进行打分，最后根据多个打分的综合结果判定待测样本是否异常。由于采用多种不同的降维方法，每种降维方法所得到的特征可以互相补充，最大限度地避免了降维带来的信息损失。同时，由于经过降维处理，使得 SVDD 模型的应用变得实际可行，避免了维度“爆炸”带来的计算障碍。在此基础上，综合考虑各个 SVDD 模型的结果，可以对待测样本进行全面的评估，准确的预测。

[85] 根据另一方面的实施例，还提供一种预测异常样本的装置。图 6 示出根据一个实施例的预测异常样本的装置的示意性框图。如图 6 所示，该装置 600 包括：获取单元 61，配置为获取待测样本，所述待测样本包括维度为第一数目的特征数据；多个降维单元 62，所述多个降维单元分别采用多个降维方法，对所述待测样本进行降维处理，以获得多个处理样本，其中所述多个降维方法中的第 i 降维方法  $P_i$ ，将所述待测样本处理为维度为  $D_i$  的处理样本  $S_i$ ，维度  $D_i$  小于所述第一数目；多个打分单元 63，配置为通过多个处理模型对所述多个处理样本进行打分，其中所述多个处理模型中的第 i 处理模型  $M_i$ ，基于预先采用支持向量域描述 SVDD 方式在对应维度  $D_i$  的空间中所确定的超球面  $Q_i$ ，为对应的处理样本  $S_i$  打分；综合单元 64，配置为根据所述各个处理样本的打分确定所述待测样本的综合分；确定单元 65，配置为根据所述综合分，确定所述待测样本是否为异常样本。在图 6 中，多个降维单元 62 和多个打分单元均示意性示出为 3 个，但是可以理解，降维单元和打分单元的数目可以根据需要进行设定，并不局限于图 6 的图示。

[86] 在一个实施例中，上述多个降维单元 62 所采用的多个降维方法包括运算降维方法

和特征采样降维方法中的至少一种。

[87] 根据一个实施例，上述运算降维方法包括以下中的一种或多种：主成分分析 PCA 方法，最小绝对收缩和选择算子 LASSO 方法，线性判别式分析 LDA 方法，小波分析方法。

- 5 [88] 根据一个实施例，上述特征采样降维方法包括以下中的一种或多种：随机采样方法，哈希采样方法，过滤式特征选择方法，包裹式特征选择方法。

[89] 在一个实施例中，上述第  $i$  处理模型  $M_i$  通过第  $i$  训练装置（未示出）训练，所述第  $i$  训练装置包括：样本集获取模块，配置为获取已知为正常的历史样本集，所述历史样本集的样本维度为所述第一数目；第  $i$  降维模块，配置为采用所述第  $i$  降维方法  $P_i$ ，

- 10 将所述历史样本集处理为样本维度为  $D_i$  的低维历史样本集  $L_i$ ；超球面确定模块，配置为采用支持向量域描述 SVDD 方式，在维度为  $D_i$  的空间中确定所述超球面  $Q_i$ ，使得该超球面  $Q_i$  所包围的低维历史样本集  $L_i$  中的样本数目与该超球面的半径之间的关系满足预定条件。

[90] 根据一个实施例，上述多个打分单元 63 配置为：确定所述处理样本  $S_i$  在对应维度

- 15  $D_i$  的空间中与所述超球面  $Q_i$  的相对位置；根据所述相对位置，确定处理样本  $S_i$  的打分。

[91] 在一个实施例中，所述相对位置包括以下之一：

[92] 所述处理样本  $S_i$  位于所述超球面  $Q_i$  之外、之内或之上；

[93] 所述处理样本  $S_i$  在对应维度空间中距离所述超球面  $Q_i$  的中心的距离；

[94] 所述处理样本  $S_i$  在对应维度空间中距离所述超球面  $Q_i$  的最近表面的距离。

- 20 [95] 根据一个实施例，综合单元 64 配置为：对所述各个处理样本的打分进行加权求和，获得所述综合分。

[96] 通过以上装置，针对待测样本，采用多种降维方法分别对其进行降维，各个降维方法互相补充，以此避免降维带来的信息损失。对于降维后的多个处理样本，分别基于 SVDD 模型确立的超球面，对处理样本进行打分，最后根据多个打分的综合结果判定待  
25 测样本是否异常。由此，综合考虑各个 SVDD 模型的结果，对待测样本进行全面评估，准确预测。

[97] 根据另一方面的实施例，还提供一种计算机可读存储介质，其上存储有计算机程序，当所述计算机程序在计算机中执行时，令计算机执行结合图 3 到图 5 所描述的方法。

[98] 根据再一方面的实施例，还提供一种计算设备，包括存储器和处理器，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现结合图 3 到图 5 所述的方法。

5 [99] 本领域技术人员应该可以意识到，在上述一个或多个示例中，本发明所描述的功能可以用硬件、软件、固件或它们的任意组合来实现。当使用软件实现时，可以将这些功能存储在计算机可读介质中或者作为计算机可读介质上的一个或多个指令或代码进行传输。

10 [100] 以上所述的具体实施方式，对本发明的目的、技术方案和有益效果进行了进一步详细说明，所应理解的是，以上所述仅为本发明的具体实施方式而已，并不用于限定本发明的保护范围，凡在本发明的技术方案的基础之上，所做的任何修改、等同替换、改进等，均应包括在本发明的保护范围之内。

### 权利要求书

1、一种预测异常样本的方法，包括：

获取待测样本，所述待测样本包括维度为第一数目的特征数据；

5 采用多个降维方法，分别对所述待测样本进行降维处理，以获得多个处理样本，其中所述多个降维方法中的第  $i$  降维方法  $P_i$ ，将所述待测样本处理为维度为  $D_i$  的处理样本  $S_i$ ，维度  $D_i$  小于所述第一数目；

将所述多个处理样本分别对应输入多个处理模型，以获得各个处理样本的打分，其中所述多个处理模型中的第  $i$  处理模型  $M_i$ ，基于预先采用支持向量域描述 SVDD 方式在对应维度  $D_i$  的空间中所确定的超球面  $Q_i$ ，为对应的处理样本  $S_i$  打分；

10 根据所述各个处理样本的打分确定所述待测样本的综合分；

根据所述综合分，确定所述待测样本是否为异常样本。

2、根据权利要求 1 所述的方法，其中所述多个降维方法包括运算降维方法和特征采样降维方法中的至少一种。

3、根据权利要求 2 所述的方法，其中所述运算降维方法包括以下中的一种或多种：  
15 主成分分析 PCA 方法，最小绝对收缩和选择算子 LASSO 方法，线性判别式分析 LDA 方法，小波分析方法。

4、根据权利要求 2 所述的方法，其中所述特征采样降维方法包括以下中的一种或多种：随机采样方法，哈希采样方法，过滤式特征选择方法，包裹式特征选择方法。

5、根据权利要求 1 所述的方法，其中所述第  $i$  处理模型  $M_i$  通过以下步骤训练：  
20 获取已知为正常的历史样本集，所述历史样本集的样本维度为所述第一数目；

采用所述第  $i$  降维方法  $P_i$ ，将所述历史样本集处理为样本维度为  $D_i$  的低维历史样本集  $L_i$ ；

采用支持向量域描述 SVDD 方式，在维度为  $D_i$  的空间中确定所述超球面  $Q_i$ ，使得该超球面  $Q_i$  所包围的低维历史样本集  $L_i$  中的样本数目与该超球面的半径之间的关系满足  
25 预定条件。

6、根据权利要求 1 中所述的方法，其中为对应的处理样本  $S_i$  打分包括：

确定所述处理样本  $S_i$  在对应维度空间中与所述超球面  $Q_i$  的相对位置；

根据所述相对位置, 确定处理样本  $S_i$  的打分。

7、根据权利要求 6 所述的方法, 其中所述相对位置包括以下之一:

所述处理样本  $S_i$  位于所述超球面  $Q_i$  之外、之内或之上;

所述处理样本  $S_i$  在对应维度空间中距离所述超球面  $Q_i$  的中心的距离;

5 所述处理样本  $S_i$  在对应维度空间中距离所述超球面  $Q_i$  的最近表面的距离。

8、根据权利要求 1 所述的方法, 其中根据所述各个处理样本的打分确定所述待测样本的综合分包括: 对所述各个处理样本的打分进行加权求和, 获得所述综合分。

9、一种预测异常样本的装置, 包括:

获取单元, 配置为获取待测样本, 所述待测样本包括维度为第一数目的特征数据;

10 多个降维单元, 所述多个降维单元分别采用多个降维方法, 对所述待测样本进行降维处理, 以获得多个处理样本, 其中所述多个降维方法中的第  $i$  降维方法  $P_i$ , 将所述待测样本处理为维度为  $D_i$  的处理样本  $S_i$ , 维度  $D_i$  小于所述第一数目;

多个打分单元, 配置为通过多个处理模型对所述多个处理样本进行打分, 其中所述多个处理模型中的第  $i$  处理模型  $M_i$ , 基于预先采用支持向量域描述 SVDD 方式在对应维度  $D_i$  的空间中所确定的超球面  $Q_i$ , 为对应的处理样本  $S_i$  打分;

15 综合单元, 配置为根据所述各个处理样本的打分确定所述待测样本的综合分;

确定单元, 配置为根据所述综合分, 确定所述待测样本是否为异常样本。

10、根据权利要求 9 所述的装置, 其中所述多个降维方法包括运算降维方法和特征采样降维方法中的至少一种。

20 11、根据权利要求 10 所述的装置, 其中所述运算降维方法包括以下中的一种或多种: 主成分分析 PCA 方法, 最小绝对收缩和选择算子 LASSO 方法, 线性判别式分析 LDA 方法, 小波分析方法。

12、根据权利要求 10 所述的装置, 其中所述特征采样降维方法包括以下中的一种或多种: 随机采样方法, 哈希采样方法, 过滤式特征选择方法, 包裹式特征选择方法。

25 13、根据权利要求 9 所述的装置, 其中所述第  $i$  处理模型  $M_i$  通过第  $i$  训练装置训练, 所述第  $i$  训练装置包括:

样本集获取模块, 配置为获取已知为正常的历史样本集, 所述历史样本集的样本维

度为所述第一数目；

第  $i$  降维模块，配置为采用所述第  $i$  降维方法  $P_i$ ，将所述历史样本集处理为样本维度为  $D_i$  的低维历史样本集  $L_i$ ；

- 5 超球面确定模块，配置为采用支持向量域描述 SVDD 方式，在维度为  $D_i$  的空间中确定所述超球面  $Q_i$ ，使得该超球面  $Q_i$  所包围的低维历史样本集  $L_i$  中的样本数目与该超球面的半径之间的关系满足预定条件。

14、根据权利要求 9 所述的装置，其中所述多个打分单元配置为：

确定所述处理样本  $S_i$  在对应维度  $D_i$  的空间中与所述超球面  $Q_i$  的相对位置；

根据所述相对位置，确定处理样本  $S_i$  的打分。

- 10 15、根据权利要求 14 所述的装置，其中所述相对位置包括以下之一：

所述处理样本  $S_i$  位于所述超球面  $Q_i$  之外、之内或之上；

所述处理样本  $S_i$  在对应维度空间中距离所述超球面  $Q_i$  的中心的距离；

所述处理样本  $S_i$  在对应维度空间中距离所述超球面  $Q_i$  的最近表面的距离。

- 15 16、根据权利要求 9 所述的装置，其中所述综合单元配置为：对所述各个处理样本的打分进行加权求和，获得所述综合分。

17、一种计算机可读存储介质，其上存储有计算机程序，当所述计算机程序在计算机中执行时，令计算机执行权利要求 1-8 中任一项的所述的方法。

18、一种计算设备，包括存储器和处理器，其特征在于，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现权利要求 1-8 中任一项所述的方法。