

基于隐私保护的训练样本生成方法和装置

技术领域

本说明书涉及数据处理技术领域，尤其涉及一种基于隐私保护的训练样本生成方法和装置。

5 背景技术

随着互联网的发展和普及，各种基于网络进行的活动都在源源不断的产生数据，许多企业、政府甚至个人等都掌握着大量的用户数据。数据挖掘技术能够从大量的数据中发现有价值的知识、模式、规则等信息，为科学研究、商业决策、过程控制等提供辅助支持，成为数据利用的重要方式。

10 在一些应用场景中，用于挖掘的数据包含了很多敏感信息，例如金融行业的数据、政府部门的数据等。如何将这些敏感信息在数据挖掘的过程中作为隐私保护起来，成为一个越来越受人关注的问题。

发明内容

有鉴于此，本说明书提供一种基于隐私保护的训练样本生成方法，被挖掘的原始数据包括 m 个原始样本，每个原始样本包括 d 维的原始向量 x 和输出标记值 y ， m 、 d 为自然数，所述方法包括：

生成 n 个 d 维的转换向量 π ，每个转换向量 π 由随机选取的若干个原始样本的 yx 之和确定；

将所述 n 个转换向量 π 作为二分类模型的训练样本。

20 本说明书提供的一种基于隐私保护的二分类模型训练方法，包括：

获取 n 个 d 维的转换向量 π 作为训练样本；每个所述转换向量 π 由随机选取的若干个原始样本的 yx 之和确定，所述原始样本为原始数据的 m 个样本之一，每个原始样本包括 d 维的原始向量 x 和输出标记值 y ， m 、 d 为自然数，

基于所述训练样本，对二分类模型进行训练，得到结果模型。

本说明书还提供了一种基于隐私保护的训练样本生成装置，被挖掘的原始数据包括 m 个原始样本，每个原始样本包括 d 维的原始向量 x 和输出标记值 y ， m 、 d 为自然数，所述装置包括：

- 5 转换向量生成单元，用于生成 n 个 d 维的转换向量 π ，每个转换向量 π 由随机选取的若干个原始样本的 yx 之和确定；

训练样本生成单元，用于将所述 n 个转换向量 π 作为二分类模型的训练样本。

本说明书提供的一种基于隐私保护的二分类模型训练装置，包括：

- 10 训练样本获取单元，用于获取 n 个 d 维的转换向量 π 作为训练样本；每个所述转换向量 π 由随机选取的若干个原始样本的 yx 之和确定，所述原始样本为原始数据的 m 个样本之一，每个原始样本包括 d 维的原始向量 x 和输出标记值 y ， m 、 d 为自然数，

- 15 模型训练单元，用于基于所述训练样本，对二分类模型进行训练，得到结果模型。

本说明书提供的一种计算机设备，包括：存储器和处理器；所述存储器上存储有可由处理器运行的计算机程序；所述处理器运行所述计算机程序时，执行上述基于隐私保护的训练样本生成方法所述的步骤。

- 20 本说明书提供的一种计算机设备，包括：存储器和处理器；所述存储器上存储有可由处理器运行的计算机程序；所述处理器运行所述计算机程序时，执行上述基于隐私保护的二分类模型训练方法所述的步骤。

本说明书提供的一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器运行时，执行上述基于隐私保护的训练样本生成方法所述的步骤。

- 25 本说明书提供的一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器运行时，执行上述基于隐私保护的模型训练方法所述的步骤。

由以上技术方案可见，本说明书的实施例中，采用 m 个原始样本中的原始向量 X 和输出标记值 y ，将随机选取的若干个 yx 之和作为转换向量，使得采用 n 个转换向量进行二分类模型训练得到的结果模型、与采用原始数据进行训练相一致，不会受到随机量的影响，并且每个转换向量均由若干个原始样本和随机量生成，极难从转换向量还原出原始数据，因此本说明书的实施例既能

5 既能为隐私信息提供良好的保护，又能得到与采用原始数据相一致的挖掘结果。

附图说明

图 1 是本说明书实施例中一种应用基于隐私保护的训练样本生成方法的流程图；

10

图 2 是本说明书实施例中一种基于隐私保护的二分类模型训练方法的流程图；

图 3 是本说明书应用示例中一种数据挖掘过程的流程示意图；

图 4 是运行本说明书实施例的设备的一种硬件结构图；

15 图 5 是本说明书实施例中一种基于隐私保护的训练样本生成装置的逻辑结构图；

图 6 是本说明书实施例中一种基于隐私保护的模型训练装置的逻辑结构图。

具体实施方式

20 本说明书的实施例提出一种新的基于隐私保护的训练样本生成方法和一种新的基于隐私保护的二分类模型训练方法，从 m (m 为自然数) 个 d (d 为自然数) 维的原始向量 x 和输出标记值 y ，随机生成 n (n 为自然数) 个 d 维的转换向量 π ，转换向量的生成方式使得令基于转换向量的损失函数最小的二分类模型，即是令基于原始向量和输出标记值的损失函数最小的模型，

25 从而可以将采用转换向量训练所得的结果模型作为原始数据的数据挖掘结果。

本说明书的实施例可以运行在任何具有计算和存储能力的设备上，如手机、平板电脑、PC（Personal Computer，个人电脑）、笔记本、服务器等设备；还可以由运行在两个或两个以上设备的逻辑节点，相互协同来实现本说明书实施例中的各项功能。

- 5 本说明书的实施例中，原始数据为带有输出标记值的训练样本，样本容量为 m ，即包括 m 个样本（将原始数据的样本称为原始样本），每个原始样本包括 d 维的原始向量 x 、以及输出标记值 y 。设第 i （ i 为从 1 到 m 的自然数）个原始样本中，原始向量为 x_i ，输出标记值为 y_i 。

本说明书的实施例中，基于隐私保护的训练样本生成方法的流程如图 1
10 所示，基于隐私保护的模型训练方法的流程如图 2 所示。

步骤 110，生成 n 个 d 维的转换向量 π ，每个转换向量 π 由随机选取的 0 到 m 个原始样本的 yx 之和确定。

在 m 个原始样本中，随机选出 0 到 m 个原始样本，计算每个选出的原始样本的 yx ，将这些 yx 的和值作为一个转换向量 π 。每次选出的原始样本的
15 数目可以是固定的，也可以是随机的，不做限定。

由于每个 yx 是一个 d 维的向量，所生成的转换向量 π 也是一个 d 维的向量。

生成转换向量 π 的具体方式可以有多种，本说明书的实施例不做限定，以下举两个例子进行说明。

- 20 第一个例子：在一些应用场景中，采用正负符号来作为二分类的输出标记值，即 y 的取值为 $-v$ 或 v （ v 为实数）。这种情形下，可以这样生成转换向量：

生成一个 m 维向量 σ ，随机将 $-v$ 或 v 作为 σ 每一维的取值，将 $\frac{1}{2} \sum_{i=1}^m (y_i + \sigma_i) x_i$ 作为一个转换向量 π ；其中， σ_i 为向量 σ 的第 i 维；

- 25 重复上述过程 n 次得到 n 个转换向量 π 。

由于 $\frac{1}{2}(y_i + \sigma_i)$ 或者为 0，或者为 y_i ，转换向量 π 可以是任意的 0 到 m 个

原始样本的 yx 的和值。

在第一个例子中，设基于原始数据的线性模型为：

$$Y(x) = \theta^T x \quad \text{式 1}$$

式 1 中， θ^T 为 d 维的权重向量，则基于原始数据的二分类算法的损失函

5 数如式 2 所示：

$$F_{\log}(S, \theta) = \frac{1}{m} \sum_i \log [1 + \exp(-y_i \theta^T x_i)] \quad \text{式 2}$$

式 2 中， $S = \{(x_i, y_i) \mid i = 1, 2, \dots, m\}$ 。

设基于转换向量的线性模型为：

$$Y(\pi) = \theta^T \pi \quad \text{式 3}$$

10 则基于转换向量的二分类算法的损失函数如式 4 所示：

$$F_{\exp}^r(S, \theta, U) = \frac{1}{n} \sum_{\sigma \in U} \exp(-\theta^T \pi_{\sigma}), U \subseteq \Sigma_m \quad \text{式 4}$$

式 4 中， π_{σ} 为由 σ 生成的转换向量， $\Sigma_m = \{-v, +v\}^m$ 。

以下以 $v = 1$ 为例，来说明 $F_{\log}(S, \theta)$ 与 $F_{\exp}^r(S, \theta, U)$ 之间存在与 σ 无关的线性关系，推导过程如下：

15 定义： $\tilde{\pi}_{\sigma} = \sum_i \sigma_i x_i, \forall \sigma \in \Sigma_m$ ，转换向量 π_{σ} 可以表示为： $\pi_{\sigma} = 1/2 (\tilde{\pi}_{\sigma} + \tilde{\pi}_y)$ ，

则以下等式成立：

$$\begin{aligned} F_{\log}(S, \theta) &= \frac{1}{m} \sum_i \log (1 + \exp(-y_i \theta^T x_i)) \\ &= \frac{1}{m} \sum_i \log \left(\sum_{y \in \{-1, 1\}} \exp \left(\frac{1}{2} \cdot y \theta^T x_i \right) \right) - \frac{1}{m} \cdot \frac{1}{2} \cdot \theta^T \tilde{\pi}_y \\ &= \frac{1}{m} \log \sum_{\sigma \in \Sigma_m} \exp \left(\frac{1}{2} \cdot \theta^T \tilde{\pi}_{\sigma} \right) - \frac{1}{m} \cdot \frac{1}{2} \cdot \theta^T \tilde{\pi}_y \\ &= \frac{1}{m} \log \sum_{\sigma \in \Sigma_m} \exp \left(\frac{1}{2} \cdot \theta^T \tilde{\pi}_{\sigma} \right) + \frac{1}{m} \cdot \log \exp \left(-\frac{1}{2} \cdot \theta^T \tilde{\pi}_y \right) \\ &= \frac{1}{m} \log \sum_{\sigma \in \Sigma_m} \exp \left(\frac{1}{2} \cdot \theta^T (\tilde{\pi}_{\sigma} - \tilde{\pi}_y) \right) \end{aligned}$$

$$\begin{aligned}
&= \frac{1}{m} \log \sum_{\sigma \in \Sigma_m} \exp \left(-\frac{1}{2} \cdot \theta^\top (\tilde{\pi}_\sigma + \tilde{\pi}_y) \right) \\
&= \log(2) + \frac{1}{m} \log \frac{1}{2^m} \sum_{\sigma \in \Sigma_m} \exp \left(-\frac{1}{2} \cdot \theta^\top (\tilde{\pi}_\sigma + \tilde{\pi}_y) \right) \\
&= \log(2) + \frac{1}{m} \log \frac{1}{2^m} \sum_{\sigma \in \Sigma_m} \exp \left(-\theta^\top \pi_\sigma \right) \\
&= \log(2) + \frac{1}{m} \log F_{\exp}^r(S, \theta, \Sigma_m) .
\end{aligned}$$

可见, $F_{\log}(S, \theta)$ 与 $F_{\exp}^r(S, \theta, \Sigma_m)$ 之间为线性关系。当 $U \subseteq \Sigma_m$ 时, $F_{\log}(S, \theta)$ 与 $F_{\exp}^r(S, \theta, U)$ 之间的线性关系仍然成立, 并且与 σ 无关。这样, 使得 $F_{\log}(S, \theta)$ 最小的 θ 就是使得 $F_{\exp}^r(S, \theta, U)$ 最小的 θ , 即式 5 成立:

$$5 \quad \arg \min_{\theta} F_{\log}(S, \theta) = \arg \min_{\theta} F_{\exp}^r(S, \theta, U) \quad \text{式 5}$$

从上述论证过程可以得知, 采用若干个转换向量 π 对二分类模型进行训练, 与采用原始数据对二分类模型进行训练, 得出的结果模型是一致的。

第二个例子: 生成一个 m 维向量 w , 随机将 0 或者 1 作为 w 每一维的取值, 将 $\sum_{i=1}^m w_i y_i x_i$ 作为一个转换向量 π 。其中, w_i 为向量 w 的第 i 维。重复上述过程 n 次可以得到 n 个转换向量 π 。

由于 w_i 或者为 0, 或者为 1, 转换向量 π 可以是任意的 0 到 m 个原始样本的 yx 的和值。第二个例子中对 y 的取值没有限制。

基于类似于第一个例子中的论证过程可以得出同样的结论, 采用若干个转换向量 π 对二分类模型进行训练, 会得到与采用原始数据对二分类模型进行训练相一致的结果模型, 具体的论证过程不再赘述。

在数据提供方, 步骤 120, 将所述 n 个转换向量 π 作为二分类模型的训练样本。

在数据挖掘方, 步骤 210, 获取 n 个 d 维的转换向量 π 作为训练样本; 每个转换向量 π 由随机选取的若干个原始样本的 yx 之和确定, 原始样本为原始数据的 m 个样本之一, 每个原始样本包括 d 维的原始向量 x 和输出标记值 y 。

数据提供方将步骤 120 中生成的训练样本, 输出至数据挖掘方。数据挖掘方可以采用任意的方式从数据提供方获得训练样本, 本说明书的实施例不

做限定。

在数据挖掘方，步骤 220，基于该训练样本，对二分类模型进行训练，得到结果模型。

数据挖掘方在得到训练样本后，以该训练样本来对二分类模型进行训练。

- 5 由于原始数据中的输出标记值已经体现在转换向量 π 中，而由 n 个转换向量 π 构成的训练样本没有标记值，可以采用无监督学习算法进行训练，得出结果模型。

- 本说明书的实施例对二分类模型没有限制，例如可以采用 Boosting（增强）算法、SGD（Stochastic gradient descent，随机梯度下降）、SVRG（Stochastic variance reduced gradient，随机方差减小梯度）、Adagrad（Adaptive Gradient，自适应梯度）等等。

采用某种具体的二分类模型训练 n 个转换向量 π 构成的训练样本的方式与现有技术相同。以下给出采用 Boosting 算法进行训练的一个例子，其他算法可参照实现，不再详述。

- 15 Boosting 算法的初始化：设 n 个转换向量 π 构成的样本空间为： $\delta^r = \{\pi_1, \pi_2, \dots, \pi_n\}$ ；预设 Boosting 算法的迭代次数 T（T 为自然数）；将线性模型 θ 的初始值 θ_0 置为 d 维的 0 向量；将 n 维中间变量 ω 的初始值 ω_1 置为每个维度均等于 $1/n$ ；预先计算 π_{*k} ，k 为从 1 到 d 的每个自然数， π_{*k} 为 n 个转换向量 π 在第 k 个维度的最大值。

- 20 Boosting 算法的从第 1 轮到第 T 轮的迭代过程：

设当前的迭代轮次为 t，对于 π 的每一维 k，计算： $r_k = \frac{1}{\pi_{*k}} \sum_{j=1}^n \omega_j \pi_{jk}$ ，将使 $|r_k|$ （ r_k 的绝对值）最大的 k 记为 $l(t)$ ，根据式 6 和式 7 计算 r_t 和 α_t ：

$$r_t = \frac{1}{\pi_{*l(t)}} \sum_{j=1}^n \omega_{tj} \pi_{jl(t)} \quad \text{式 6}$$

$$\alpha_t = \frac{1}{2\pi_{*l(t)}} \log \frac{1+r_t}{1-r_t} \quad \text{式 7}$$

- 25 再按照式 8 计算用于下一迭代轮次的 n 维中间变量 $\omega_{(t+1)}$ 的每一维度的

值:

$$\omega_{(t+1)j} \leftarrow \omega_{tj} * \left(\frac{1 - \frac{r_t \pi_{ju(t)}}{\pi_{ju(t)}}}{1 - r_t^2} \right) \quad \text{式 8}$$

式 8 中, j 为从 1 到 n 的每个自然数。

在 T 轮迭代完毕后, 可根据式 9 得到训练所得的结果模型 θ_T :

$$\theta_{Tk} = \sum_{t: u(t)=k} \alpha_t, \quad \forall k \in [d] \quad \text{式 9}$$

式 9 中, θ_{Tk} 为 d 维向量 θ_T 的第 k 维。

可见, 本说明书的实施例中, 从 m 个 d 维的原始向量 x 和输出标记值 y , 随机生成 n 个 d 维的转换向量 π , 每个转换向量 π 由随机选取的若干个 yx 之和确定, 并以 n 个转换向量 π 为训练样本进行二分类模型训练, 得到与采用原始数据进行训练相一致的结果模型, 从而不仅因在生成转换向量的过程中, 10 因采用了多个原始样本且引入了随机量, 使得还原原始数据极其困难, 并且能得到与采用原始数据相一致的挖掘结果, 避免了信息失真。

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。

在本说明书的一个应用示例中, 数据提供方委托数据挖掘方进行分类规则的数据挖掘, 数据挖掘方以二分类线性模型为基础来构建数据分类规则。数据提供方的原始数据 $S = \{(x_i, y_i) \mid i = 1, 2, \dots, m\}$, 其中 $x_i \in R^d$ (即 x_i 为 d 20 维向量), $y_i \in \{1, -1\}$ (即输出标记值 y_i 的取值为 -1 或 1)。由于数据提供方的原始数据中包含用户的敏感信息, 需要进行隐私保护。

能够提供隐私保护的分类数据挖掘流程如图 3 所示。

步骤 310, 获取原始数据的 m 个样本。

25 步骤 320, 采用原始数据计算 n 个 Rado (Rademacher Observations, 拉

德马赫观察资料)。每个 Rado 为一个 d 维向量, 记为 π_σ , 是本应用示例中的转换向量。

每个 Rado 的计算方法如下: 生成 m 为向量 σ , σ 每一维的取值为 -1 或者 1, 随机确定; 根据式 10 确定对应于该 σ 的 Rado:

$$\pi_\sigma = \frac{1}{2} \sum_{i=1}^m (\sigma_i + y_i) x_i, \quad \sigma \in \Sigma_m, \quad \Sigma_m = \{-1, +1\}^m \quad \text{式 10}$$

以下举例说明: 假设原始数据共 5 个样本, 原始向量 x 的维度 $m=4$, 原始数据如表 1 所示:

样本序号	y	x			
		第 1 维	第 2 维	第 3 维	第 4 维
1	1	1	2	3	4
2	-1	3	4	5	6
3	-1	5	6	7	8
4	1	7	8	9	10
5	1	6	9	3	5

表 1

设在生成一个 Rado 时, 向量 σ 的随机值为 $\sigma = \{-1, 1, -1, 1, 1\}$, 根据式 10 计算 π_σ 的各个维度值:

$$\begin{aligned} \text{第 1 维} : & \frac{1}{2}(1 + (-1)) * 1 + \frac{1}{2}(-1 + 1) * 3 + \frac{1}{2}((-1) + (-1)) * 5 + \\ & \frac{1}{2}(1 + 1) * 7 + \frac{1}{2}(1 + 1) * 6 = 8 \end{aligned}$$

$$\begin{aligned} \text{第 2 维} : & \frac{1}{2}(1 + (-1)) * 2 + \frac{1}{2}(-1 + 1) * 4 + \frac{1}{2}((-1) + (-1)) * 6 + \\ & \frac{1}{2}(1 + 1) * 8 + \frac{1}{2}(1 + 1) * 9 = 11 \end{aligned}$$

$$\begin{aligned} \text{第 3 维} : & \frac{1}{2}(1 + (-1)) * 3 + \frac{1}{2}(-1 + 1) * 5 + \frac{1}{2}((-1) + (-1)) * 7 + \\ & \frac{1}{2}(1 + 1) * 9 + \frac{1}{2}(1 + 1) * 3 = 5 \end{aligned}$$

$$\begin{aligned} \text{第 4 维} : & \frac{1}{2}(1 + (-1)) * 4 + \frac{1}{2}(-1 + 1) * 6 + \frac{1}{2}((-1) + (-1)) * 8 + \\ & \frac{1}{2}(1 + 1) * 10 + \frac{1}{2}(1 + 1) * 5 = 7 \end{aligned}$$

可以得到一个 Rado 为{8,11,5,7}。

随机生成 n 个向量 σ ，即可得到 n 个 Rado。

步骤 310 和 320 运行在数据提供方控制的设备或逻辑节点上。数据提供方将生成 n 个 Rado 作为待挖掘的数据，提供给数据提供方。

5 步骤 330，采用 Boosting 算法，以 n 个 Rado 为训练样本，对二分类线性模型进行训练，得到结果模型。

步骤 330 运行在数据提供方控制的设备或逻辑节点上。数据提供方根据训练所得的二分类线性结果模型，生成多分类规则，交付给数据提供方。将数个二分类线性结果模型转换为多分类规则的方式可参照现有技术实现，不
10 再赘述。

与上述流程实现对应，本说明书的实施例还提供了一种基于隐私保护的训练样本生成装置、和一种基于隐私保护的二分类模型训练装置。上述装置均可以通过软件实现，也可以通过硬件或者软硬件结合的方式实现。以软件实现为例，作为逻辑意义上的装置，是所在设备的 CPU(Central Process Unit，
15 中央处理器)将对应的计算机程序指令读取到内存中运行形成的。从硬件层面而言，除了图 4 所示的 CPU、内存以及存储器之外，上述装置所在的设备通常还包括用于进行无线信号收发的芯片等其他硬件，和/或用于实现网络通信功能的板卡等其他硬件。

图 5 所示为本说明书实施例提供的一种基于隐私保护的训练样本生成装置，被挖掘的原始数据包括 m 个原始样本，每个原始样本包括 d 维的原始向量 x 和输出标记值 y ， m 、 d 为自然数，所述装置包括转换向量生成单元和训练样本生成单元，其中：转换向量生成单元用于生成 n 个 d 维的转换向量 π ，
20 每个转换向量 π 由随机选取的若干个原始样本的 yx 之和确定；训练样本生成单元用于将所述 n 个转换向量 π 作为二分类模型的训练样本。

25 可选的，所述 y 的取值为 $-v$ 或 v ， v 为实数；所述转换向量生成单元具体用于：生成一个 m 维向量 σ ，随机将 $-v$ 或 v 作为 σ 每一维的取值，将

$\frac{1}{2}\sum_{i=1}^m(y_i + \sigma_i)x_i$ 作为一个转换向量 π , y_i 为第 i 个原始样本的输出标记值, x_i 为第 i 个原始样本的原始向量, σ_i 为向量 σ 的第 i 维; 重复上述过程 n 次得到 n 个转换向量 π 。

可选的, 所述转换向量生成单元具体用于: 生成一个 m 维向量 w , 随机
5 将 0 或者 1 作为 w 每一维的取值, 将 $\sum_{i=1}^m w_i y_i x_i$ 作为一个转换向量 π , w_i 为向量 w 的第 i 维, y_i 为第 i 个原始样本的输出标记值, x_i 为第 i 个原始样本的原始向量; 重复上述过程 n 次得到 n 个转换向量 π 。

图 6 所示为本说明书实施例提供的一种基于隐私保护的二分类模型训练装置, 包括训练样本获取单元和模型训练单元, 其中: 训练样本获取单元用于获取 n 个 d 维的转换向量 π 作为训练样本; 每个所述转换向量 π 由随机选取
10 的若干个原始样本的 yx 之和确定, 所述原始样本为原始数据的 m 个样本之一, 每个原始样本包括 d 维的原始向量 x 和输出标记值 y , m 、 d 为自然数, 模型训练单元用于基于所述训练样本, 二分类模型进行训练, 得到结果模型。

可选的, 所述二分类模型包括: 增强 Boosting 算法、随机梯度下降 SGD
15 算法、随机方差减小梯度 SVRG 算法、或自适应梯度 Adagrad 算法。

本说明书的实施例提供了一种计算机设备, 该计算机设备包括存储器和处理器。其中, 存储器上存储有能够由处理器运行的计算机程序; 处理器在运行存储的计算机程序时, 执行本说明书实施例中基于隐私保护的训练样本生成方法的各个步骤。对基于隐私保护的训练样本生成方法的各个步骤的详
20 细描述请参见之前的内容, 不再重复。

本说明书的实施例提供了一种计算机设备, 该计算机设备包括存储器和处理器。其中, 存储器上存储有能够由处理器运行的计算机程序; 处理器在运行存储的计算机程序时, 执行本说明书实施例中基于隐私保护的二分类模型训练方法的各个步骤。对基于隐私保护的二分类模型训练方法的各个步骤
25 的详细描述请参见之前的内容, 不再重复。

本说明书的实施例提供了一种计算机可读存储介质, 该存储介质上存储

有计算机程序，这些计算机程序在被处理器运行时，执行本说明书实施例中基于隐私保护的训练样本生成方法的各个步骤。对基于隐私保护的训练样本生成方法的各个步骤的详细描述请参见之前的内容，不再重复。

本说明书的实施例提供了一种计算机可读存储介质，该存储介质上存储
5 有计算机程序，这些计算机程序在被处理器运行时，执行本说明书实施例中基于隐私保护的二分类模型训练方法的各个步骤。对基于隐私保护的二分类模型训练方法的各个步骤的详细描述请参见之前的内容，不再重复。

以上所述仅为本说明书的较佳实施例而已，并不用以限制本申请，凡在本申请的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含
10 在本申请保护的范围之内。

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。

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）。
15 内存是计算机可读介质的示例。

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
20 media），如调制的数据信号和载波。

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。

- 5 本领域技术人员应明白，本说明书的实施例可提供为方法、系统或计算机程序产品。因此，本说明书的实施例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，本说明书的实施例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。

权利要求书

1. 一种基于隐私保护的训练样本生成方法，被挖掘的原始数据包括 m 个原始样本，每个原始样本包括 d 维的原始向量 x 和输出标记值 y ， m 、 d 为自然数，所述方法包括：

- 5 生成 n 个 d 维的转换向量 π ，每个转换向量 π 由随机选取的若干个原始样本的 yx 之和确定；

 将所述 n 个转换向量 π 作为二分类模型的训练样本。

2. 根据权利要求 1 所述的方法，所述 y 的取值为 $-v$ 或 v ， v 为实数；

 所述生成 n 个 d 维的转换向量 π ，每个转换向量 π 由随机选取的若干个原始
10 样本的 yx 之和确定，包括：生成一个 m 维向量 σ ，随机将 $-v$ 或 v 作为 σ 每一维的取值，将 $\frac{1}{2} \sum_{i=1}^m (y_i + \sigma_i) x_i$ 作为一个转换向量 π ， y_i 为第 i 个原始样本的输出标记值， x_i 为第 i 个原始样本的原始向量， σ_i 为向量 σ 的第 i 维；重复上述过程 n 次得到 n 个转换向量 π 。

3. 根据权利要求 1 所述的方法，所述生成 n 个 d 维的转换向量 π ，每个
15 转换向量 π 由随机选取的若干个原始样本的 yx 之和确定，包括：生成一个 m 维向量 w ，随机将 0 或者 1 作为 w 每一维的取值，将 $\sum_{i=1}^m w_i y_i x_i$ 作为一个转换向量 π ， w_i 为向量 w 的第 i 维， y_i 为第 i 个原始样本的输出标记值， x_i 为第 i 个原始样本的原始向量；重复上述过程 n 次得到 n 个转换向量 π 。

4. 一种基于隐私保护的二分类模型训练方法，包括：

20 获取 n 个 d 维的转换向量 π 作为训练样本；每个所述转换向量 π 由随机选取的若干个原始样本的 yx 之和确定，所述原始样本为原始数据的 m 个样本之一，每个原始样本包括 d 维的原始向量 x 和输出标记值 y ， m 、 d 为自然数，

 基于所述训练样本，对二分类模型进行训练，得到结果模型。

5. 根据权利要求 4 所述的方法，所述二分类模型包括：增强 Boosting
25 算法、随机梯度下降 SGD 算法、随机方差减小梯度 SVRG 算法、或自适应梯度 Adagrad 算法。

6. 一种基于隐私保护的训练样本生成装置, 被挖掘的原始数据包括 m 个原始样本, 每个原始样本包括 d 维的原始向量 x 和输出标记值 y , m 、 d 为自然数, 所述装置包括:

转换向量生成单元, 用于生成 n 个 d 维的转换向量 π , 每个转换向量 π 由
5 随机选取的若干个原始样本的 yx 之和确定;

训练样本生成单元, 用于将所述 n 个转换向量 π 作为二分类模型的训练样本。

7. 根据权利要求 6 所述的装置, 所述 y 的取值为 $-v$ 或 v , v 为实数;

所述转换向量生成单元具体用于: 生成一个 m 维向量 σ , 随机将 $-v$ 或 v
10 作为 σ 每一维的取值, 将 $\frac{1}{2} \sum_{i=1}^m (y_i + \sigma_i) x_i$ 作为一个转换向量 π , y_i 为第 i 个原始样本的输出标记值, x_i 为第 i 个原始样本的原始向量, σ_i 为向量 σ 的第 i 维; 重复上述过程 n 次得到 n 个转换向量 π 。

8. 根据权利要求 6 所述的装置, 所述转换向量生成单元具体用于: 生成一个 m 维向量 w , 随机将 0 或者 1 作为 w 每一维的取值, 将 $\sum_{i=1}^m w_i y_i x_i$ 作为一
15 个转换向量 π , w_i 为向量 w 的第 i 维, y_i 为第 i 个原始样本的输出标记值, x_i 为第 i 个原始样本的原始向量; 重复上述过程 n 次得到 n 个转换向量 π 。

9. 一种基于隐私保护的二分类模型训练装置, 包括:

训练样本获取单元, 用于获取 n 个 d 维的转换向量 π 作为训练样本; 每个所述转换向量 π 由随机选取的若干个原始样本的 yx 之和确定, 所述原始样
20 本为原始数据的 m 个样本之一, 每个原始样本包括 d 维的原始向量 x 和输出标记值 y , m 、 d 为自然数,

模型训练单元, 用于基于所述训练样本, 对二分类模型进行训练, 得到结果模型。

10. 根据权利要求 8 所述的装置, 所述二分类模型包括: 增强 Boosting
25 算法、随机梯度下降 SGD 算法、随机方差减小梯度 SVRG 算法、或自适应梯度 Adagrad 算法。

11. 一种计算机设备，包括：存储器和处理器；所述存储器上存储有可由处理器运行的计算机程序；所述处理器运行所述计算机程序时，执行如权利要求 1 到 3 任意一项所述的步骤。

12. 一种计算机设备，包括：存储器和处理器；所述存储器上存储有可由处理器运行的计算机程序；所述处理器运行所述计算机程序时，执行如权利要求 4 到 5 任意一项所述的步骤。

13. 一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器运行时，执行如权利要求 1 到 3 任意一项所述的步骤。

14. 一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器运行时，执行如权利要求 4 到 5 任意一项所述的步骤。