基于模态一致性的协同训练多模态学习：一种隐私保护方法

苗 园　詹德川

（南京大学计算机软件新技术国家重点实验室　南京 210023）

摘　要　复杂的数据对象通常是由来自不同信息源或提取方式的多模态特征描述的。因此，多模态学习引起了研究者的广泛关注。通过利用多个模态信息之间的关系，多模态学习能够很好地提升学习效果。 在一些真实应用场景中，不同模态的数据特征可能来自于不同的私有数据源，要求在学习模型训练和测试时数据源之间的信息不能共享，也即在利用多模态之间的关系的同时保护数据隐私。现有的多模态学习方法中，子空间方法和先融合方法不适用于这种场景，因为这两类方法需要使用所有的原始数据特征；后融合方法基于模态个体分类器的预测结果的，但无法利用模态之间的关系来提升个体分类器的性能；协同训练方法难以处理包含多个模态的数据，因此也不能适用于该场景。本文定义了一种新的模态一致性指标，在协同训练框架下通过利用所有其它模态个体分类器对未标记数据的预测结果的后融合来增大某个模态的训练集，提出了一种新颖的保护数据特征隐私的多模态学习方法。多个真实数据集上的实验结果显示了该算法的有效性。

关键词　机器学习，半监督，多模态，协同训练，隐私保护

中图法分类号　TP391.4　　**文献标识码**　A

View Consistency based Co-training style Multi-View Learning: A Privacy-Preserving Approach

MIAO Yuan　ZHAN De-chuan

(National Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210023, China)

Abstract　Complex media objects are often described by multi-view feature groups collected from diverse domains or information channels. Multi-view learning, which attempts to exploit the relationship among multiple views to improve learning performance, has drawn extensive attention. It is noteworthy that in some real-world applications, features of different views may come from different private data repositories, and thus, it is desired to exploit view relationship with data privacy preserved simultaneously, i.e. not to share data features with other data repositories when training and testing the model. Existing multi-view learning approaches such as subspace methods and pre-fusion methods are not applicable in this scenario because they need to access the whole features, whereas late-fusion approaches could not exploit information from other views to improve the individual view-specific learners. Co-training methods can hardly deal with multiple views. Under the framework of co-training, by using view consistency defined on all the other view-specific classifiers' predictions on new unlabeled examples to enlarge training set of one view, this paper proposed a novel privacy-preserving multi-view learning approach. Empirical investigations on real datasets verify the validity of the proposed method on various tasks.

Keywords　Machine learning，Semi-supervised，Multi-modal，Co-training, Privacy-preserving

1　引言

随着互联网的快速发展，大量复杂数据对象可以从多种信息渠道被获取，例如一条新闻可以同时被文字、音频、视频和超链接描述[1]。在本文中，我们主要关注数据来源于多个私有信息渠道的问题，即在处理过程中不能共享数据特征。这类问题经常出现在许多场景中，例如，不同用户只享有对数据库部分视图的访问权限，或多模态数据分析中的各部分模态信息来自若干具有竞争合作关系的公司。

为了分析来自多种信息渠道的复杂数据对象，多模态学习引起了广泛关注。现有的多模态学习方法可以大致分为四种：多模态子空间学习算法先获得多个模态的共享子空间，然后在共享子空间中对模型进行优化[2][3]；以多核学习[4]为代表的前融合算法通过对每个模态上产生的核进行加权联结来融合数据特征；后融合算法对建立在每个模态数据上的个体分类器的预测结果进行结合，得到一个提升了的综合分类器，但没有对个体分类器进行增强[5]；基于分歧的算法主要考虑如何基于两个不同模态之间的一致性并利用未标记数据来提升个体分类器的性能[6][7]。

前面提到的多模态学习算法已经在多种任务中取得了很好的分类效果，但是不少已有多模态学习风范需要对多个模态的数据进行信息互访，不适合对隐私数据访问进行限制的竞争合作场景。例如，子空间方法需利用所有的模态特征进行子空间学习，必然牵涉对所有模态特征的访问[2][3]；前融合策略需要在训练之前获得所有模态的特征取值[4][11]，因此无法保护不同信息来源的数据隐私。与之相反，后融合策略只利用各个模态的子分类器的预测结果进行融合，因此无需访问全部模态的隐私数据，具有隐私保护能力。然而，后融合策略不能利用其它渠道的信息来提升个体分类器的性能[5]。基于分歧的协同训练方法也不需要模态特征信息互访，然而此类方法依赖于诸如两个模态要满足冗余、独立的性质的强假设；虽然最近的一些理论研究[8][9]对这一假设进行了放松，目前仍然没有比较有效的算法，更为重要的是此类方法难以拓展到模态数量较大的场景中。

为了能够在增进融合前的各子分类器的性能同时避免不同模态之间的信息互访，本文提出了一种新颖的协同训练风范的多模态学习方法 Multi-Training，从而适用于竞争合作场景下的多模态数据隐私保护。在协同训练方法中，最为重要的是每一轮未标记样本待被加入某个模态的训练集时，需要对其进行的置信度打分。在本文提出的方法中，我们使用了基于后融合的置信度打分法，用以选择最为确定的样本

苗 园(1992－)，女，硕士生，主要研究方向为多模态学习，E-mail：miaoy@lamda.nju.edu.cn；詹德川(1982－)，男，副教授，硕士生导师，主要研究方向为距离度量学习、多模态学习。

进行协同训练迭代。从而使新提出的方法同时具有后融合和协同训练的优点。在多个真实数据集上的实验结果表明，Multi-Training 能够在大部分数据集上取得最好的表现，并在其它数据集上具有可比较的效果。

2 相关工作

如何利用多个模态之间的关系是多模态学习的基本考虑。正如上文所提，有四种多模态学习方法，它们的区别主要在利用模态之间关系的策略不同。子空间方法寻找模态之间的关联，并在学习得到的共享子空间中进行后续的任务。例如，CCA 算法[2]对两个模态中的每个模态都定义一个线性投影，然后通过最大化两个模态的关联来得到一个共享子空间。其它一些子空间方法，例如 MvLDA[10]和 MvLPP[3]，也是采用相似的策略。先融合方法在训练模型之前先对数据特征或特征的衍生形式（如核[4]或距离[11]）进行融合。典型的做法是将多模态数据特征表示为多个核矩阵，然后在核空间中进行结合。多核学习，如 MKL 算法，是一种被广泛使用的先融合算法，它基于多个核学习一个线性的[12]或非线性的[13]的结合。然而，子空间方法和先融合方法都需要直接访问所有模态的特征。

后融合方法，如 RLF 算法[5]，对每个模态的个体分类器的预测结果进行融合，并不访问模态的特征。RLF 算法将每个模态的个体分类器给出的置信得分向量转换为表示测试样本两两之间关系的矩阵，然后求得一个秩为 2 的共享矩阵，使得每个个体分类器的关系矩阵能够被分解为共享矩阵加上一个稀疏的偏差矩阵。利用共享矩阵恢复出融合的置信得分向量，能够得到一个更准确的预测结果。但个体分类器的训练阶段没有涉及到融合过程，这使得后融合方法不能帮助提升个体分类器的性能。

基于分歧的方法是一种半监督学习方法，基本考虑是基于模态之间的一致性来设计训练过程、基于模态各自的差异性来提升对方的学习效果。协同训练[6]是其中一种简单、有效的算法。协同训练先利用有标记样本在每个模态上各自训练一个分类器，然后用一个模态的个体分类器对未标记样本的预测结果来增大另一模态的训练集。这类算法利用很少的有标记训练样本，最后可以得到提升了的模态个体分类器和整体分类器（需要采用额外的策略得到，如计算联合概率），但一般只适用于具有两个模态的数据。

在充分考虑了已有的多模态学习方法在竞争合作场景中的优势和不足之后，我们提出的 Multi-Training 算法将 Co-Training 和 RLF 算法进行改进和结合。利用模态个体分类器对未标记样本的预测值的一致性结果实现模态之间的互相提升，同时使用 one-vs.-rest 策略保持每个模态数据的差异性。基于这样的模型，Multi-Training 算法既能实现对模态个体分类器的性能和综合分类效果的同时提升，也能够保护模态的数据特征不被其它模态的分类器访问，因此能够有效适用于竞争合作场景。

3 Multi-Training 学习框架

本节将详细介绍我们提出的 Multi-Training 算法。在多模态学习中，一个样本通常由多组特征描述，而这多组特征对应着同一个标记。不失一般性地，假设有K个模态，每个模态有n个样本，包括n个有标记样本和$n-l$个无标记样本。所有模态的有标记样本组成集合L，所有的未标记样本组成集合U。第i个样本$\mathbf{x}_i$由一组模态指定的向量$\mathbf{x}_{i,k} \in \mathbb{R}^{d_k}$表示，其中$d_k$是第$k$个模态的维度。对于有标记样本，如果是二分类问题，$\mathbf{x}_i$具有标记$y_i \in \{0,1\}$；如果是多分类问题，假设共有$C$个类别，$\mathbf{x}_i$的标记$y_i$为一个含有$C$个元素的向量，其中$y_{i,j}=1$表示第$i$个样本属于第$j$个类别，否则$y_{i,j}=0$。第$k$个模态上的所有数据的矩阵表示为$X_k=\left[\mathbf{x}_{1,k}^T;\mathbf{x}_{2,k}^T;\dots;\mathbf{x}_{n,k}^T\right]\in\mathbb{R}^{n\times d_k}$，对应的标记矩阵为$Y\in\{0,1\}^{l\times C}$。每个模态上的个体分类器表示为$h_k:\mathbf{x}_{i,k}\to\hat{y}$，其中$\mathbf{x}_{i,k}\in\mathbb{R}^{d_k}$，$\hat{y}\in\mathbb{R}^C$。

3.1 未标记样本的选择策略

协同训练算法是一种半监督学习算法，能够基于少量的昂贵的有标记数据集、利用大量的廉价的未标记数据集来不断提升分类器的性能。在分类器估计出未标记样本的标记之后，选择哪些样本加入之前的训练集，是半监督学习方法的主要关注点。协同训练是选出预测置信度最高的若干个未标记样本。针对多模态数据的半监督学习一般利用模态的一致性来选择，例如决策相同[14]。然而 Li Ming 等人和 Wang Wei 等人证明了，在模态数量较多的情况，使用相同决策或者多数决策投票会使得协同训练模型过早收敛并且不能取得良好的分类效果。为了更好地处理多模态数据，本文提出的 Multi-Training 引入了后融合策略对未标记样本的置信度估计进行了改进：具体地，对于第k个模态，我们先对除了第k个模态之外的所有模态的个体分类器的对未标记数据子集u的预测结果进行鲁棒后融合（RLF[5]），然后将融合结果中置信度最高的若干样本加入之前的训练集。

在 RLF 中，给定一个模态的个体分类器的置信度得分向量$\mathrm{s}=[s_1,s_2,\dots,s_u]$，$u$是未标记数据子集的大小。考虑到各个个体分类器给出的绝对置信度之间可能存在较大差异，不能直接对原始得分进行融合。RLF 建立一个表示测试样本两两之间比较关系的矩阵$T\in\mathbb{R}^{m\times m}$，其中

$$T_{ij}=\mathrm{sign}(s_j-s_k), \tag{1}$$

虽然每个模态的关系矩阵会存在稀疏的偏差，但所有模态的关系矩阵之间应该具有一致性。因此可以将得分融合问题形式化为计算一个秩为 2 的共享关系矩阵$\hat{T}$，使得每个模态上关系矩阵 T_k可以被分解为共享矩阵$\hat{T}$加上一个稀疏的偏差矩阵E_k，

$$\begin{aligned}&\min_{\hat{T},E_k}\left\|\hat{T}\right\|_*+\lambda\textstyle\sum_{k=1}^{K}\|E_k\|_1,\\ &\text{s.t } T_k=\hat{T}+E_k,k=1,\dots,K,\\ &\hat{T}=-\hat{T}^T.\end{aligned} \tag{2}$$

$\|\cdot\|_*$表示矩阵的核范数，即矩阵的奇异值之和。由于矩阵的秩的离散性质，直接限制$\mathrm{rank}(\hat{T})=2$不好优化，因此用核范数代替矩阵的秩得到一个凸优化问题。引入拉格朗日乘子Y_i，公式(2)等价为：

$$\begin{aligned}&\min_{\hat{T},E_k}\left\|\hat{T}\right\|_*+\lambda\textstyle\sum_{k=1}^{K}\|E_k\|_1+\sum_{k=1}^{K}\langle Y_k,T_k-\hat{T}-E_k\rangle\\ &+\frac{\mu}{2}\textstyle\sum_{k=1}^{K}\left\|T_k-\hat{T}-E_k\right\|_F^2,\end{aligned} \tag{3}$$

$\mu>0$是惩罚参数，$\langle\cdot\rangle$表示内积算子。RLF 使用 ALM 即增广拉格朗日算法来解决这个优化问题。ALM 采用 SVT 作为求解程序，保证得到的$\hat{T}$具有反对称性，因此可以去掉公式(2)中的反对称约束。在迭代优化过程中，不断对奇异值进行截断，直到$\hat{T}$的秩等于 2。

解出最优的一致性关系矩阵$\hat{T}$之后，我们可以恢复出K个模态个体分类器的一致性置信度得分向量$\hat{\mathrm{s}}$：

$$\left(\frac{1}{m}\right)\hat{T}\mathrm{e}=arg\min_{\hat{\mathrm{s}}}\left\|\hat{T}^T-(\hat{\mathrm{s}}\mathrm{e}^T-\mathrm{e}\hat{\mathrm{s}}^T)\right\|_F^2. \tag{4}$$

3.2 Multi-Training算法

算法 1 描述了我们提出的 Multi-Training 算法。给定多模态数据集$X=\{X_1,\dots,X_K\}$和标记矩阵Y，X包括有标记训练集L和未标记集合U，并建立一个包含u个样本的未标记子集U'。先考虑二分类问题。对于每个模态k，首先，Multi-Training 利用L建立$k-1$个不同的分类器，记为$S_{\sim k}=\{h_1,h_2,\dots,h_{k-1},h_{k+1},\dots,h_K\}$，$h_i$是基于除了$k$之外的模态$i$的。然后，让每个$h_i$都对未标记样本子集$U'$进行预测，计算得到

算法 1 Multi-Training 算法

1：**输入：**多标记训练数据$X=\{X_1,\dots,X_K\}$，标记矩阵Y

2：将X分为有标记训练样本集合L和未标记样本集合U

3：**对于每个类别c：**

4：$\{h_1^c,\dots,h_K^c,\}=\mathrm{BiMT}(L,U,Y_{01})$，其中 $Y_{01}=\begin{cases}1, & \text{如果标记为}c\\ 0, & \text{否则}\end{cases}$

5：$\hat{h}_k=\max_h\{h_k^1,\dots,h_k^c\}$

6：**输出：**模态多分类器$\hat{h}_k$

算法 2 针对二分类问题的$\mathrm{BiMT}(L,U,Y_{01})$

1：**输入：**有标记训练样本集合L，未标记样本集合U，标记矩阵Y_{01}

2：从U中随机选取u个样本，建立未标记样本子集U'

3：**进行t次迭代：**

4：　**对于每个模态k：**

5：　　利用L在除了k的每个模态上训练一个分类器，记为$S_{\sim k}=\{h_1,h_2,\dots,h_{k-1},h_{k+1},\dots,h_K\}$

6：　　根据公式(4)，得到$S_{\sim k}$在U'上的一致性置信度得分向量$\hat{s}_{\sim k}$

7：　　从U'中选出一致性置信度最高的p个正样本和n个负样本，加入到L中

8：　　从U中随机选取$p+n$个样本补充到U'中

9：**输出：**模态二分类器h_k

这$k-1$个分类器的一致性结果$\hat{s}_{\sim k}$。根据$\hat{s}_{\sim k}$，从U'中选取最有可能是正样本的p个样本和最有可能是负样本的n个样本，连同它们的预测标记一起加到L中。最后，从U中随机选取$p+n$个样本补充到U'中。和协同训练方法[6]一致，我们使用的$u=75$，$p=1$，$n=3$。算法 2 给出了针对二分类问题的 Multi-Training 算法 BiMT。第 4 行对多个模态采用“一对多”策略，对第k个模态训练集的更新是基于所有其它模态的预测结果的，维护了每个模态的差异性，使模态的互相提升成为可能。第 6 行利用多个分类器的一致性结果来选取未标记样本，使得加入训练集的未标记样本的预测标记更加准确，同时分类器在每个模态上单独训练和更新的设置，保护了多模态数据隐私。

对于多分类问题，只要在“一对多”策略下将问题先转化为多个二分类问题，再使用BiMT算法即可。算法 1 详细描述了这一过程。

4 实验分析

我们在 12 个真实的多模态数据集上进行了实验。本节先给出通用的实验设置。然后通过和目前表现最好的一些多模态学习方法进行对比，表现 Multi-Training 算法的有效性。

4.1 通用的实验设置

实验中用到的数据是具有两个模态或者多个模态（超过两个）的数据集。表 1 给出了数据集的简要描述。Citeseer 数据集[16]本身有 4 个模态，即内容、入境、出境、城市，我们的实验里选择了内容模态和城市模态（同[17]）。WebKB 数据集[16]包含四个大学的网页信息：Cornell，Texas，Washington 和 Wisconsin，由学生、项目、课程、材料和教员 5 个类别以及内容和引用 2 个模态描述。我们的实验中把四个大学的信息分别作为四个数据集来处理。Newsgroup 数据集[17]是由从 20-Newsgroup 数据集抽取出的 6 组信息构成的，即 M2、M5、M10、NG1、NG2、NG3。每组包含 10 个样本集合，我们选择每组的第一个样本集合进行实验。数据集包含 3 个模态，对应三种不同的文本处理方法得到的特征[17]。Reuters 数据集[17]构造于 Reuters RCV1/RCV2 多语言测试集组，英语、法语、德语、意大利语和西班牙语 5 种不同的语言构成了多模态信息[17]。

表 1 数据集简要描述

数据集	类别数	样本数	模态数	模态维度
Citeseer	6	3264	2	3703, 3264
Cornell	5	195	2	1703, 195
Texas	5	185	2	1703, 185
Washington	5	217	2	1703, 217
Wisconsin	5	262	3	1703, 262
News-M2	2	500	3	2000, 2000, 2000
News-M5	5	500	3	2000, 2000, 2000
News-M10	10	500	3	2000, 2000, 2000
News-NG1	2	500	3	2000, 2000, 2000
News-NG2	5	400	3	2000, 2000, 2000
News-NG3	5	1000	3	2000, 2000, 2000
Reuters	6	1600	5	2000, 2000, 2000, 2000, 2000

由于 Multi-Training 利用了上文提到的四种类别的多模态学习的优点，因此我们和四种类别的方法都进行了对比。对于我们的方法和所有对比方法，我们都进行了 10 次重复实验并记录平均结果。每次随机抽取 70%数据作为训练集，剩下的作为测试集。在训练集中，随机抽取 30%作为标记数据，剩下的 70%为未标记数据。参数被设置为$t=10$，$u=75$，$p=1$，$n=3$。对比实验中的协同训练[6]方法也采用了这一参数设置。

4.2 与融合方法进行对比

我们和先融合方法中的 3 种多核学习（MKL）算法和目前表现最好的后融合算法 RLF（Robust Late Fusion）[5]进行比较。3 种 MKL 算法分别是：CABMKL（Centered Alignment-Based MKL）[18]、SimpleMKL[19]和 LMKL（Localized MKL）[13]。在 RLF 中，我们使用在最小平方损失函数下的最优分类器作为初始分类器。 由于融合方法对于多模态数据只能

表 2 与融合方法和子空间方法对比的分类准确率（准确率±标准差）

数据集	Multi-Training	前融合方法		后融合方法		子空间方法		
		CABMKL	SimpleMKL	LMKL	RLF	MvCCA	MvLPP	MvMFA
Citeseer	.687±013	**.692±013**	.687±019	.682±012	.672±013	.541±090	.497±089	.640±027
Cornell	**.664±040**	.636±064	.626±057	.630±058	.626±046	.564±044	.490±057	.561±070
Texas	**.709±049**	.602±050	.618±049	.612±039	.675±052	.681±034	.643±050	.704±072
Washington	**.732±027**	.696±024	.682±028	.705±040	.691±055	.650±049	.674±052	.676±046
Wisconsin	.730±056	.740±032	.747±032	**.754±029**	.681±052	.648±053	.599±098	.653±056
News-M2	**.979±011**	.881±053	.820±054	.805±042	.945±009	.844±046	.849±045	.932±019
News-M5	**.919±015**	.866±034	.903±033	.884±031	.885±021	.419±064	.629±085	.527±098
News-M10	**.800±017**	.708±042	.720±039	.672±026	.754±032	.274±053	.292±045	.241±047
Mews-NG1	**.955±016**	.925±022	.890±068	.859±062	.921±035	.791±025	.771±066	.905±035
News-NG2	**.928±008**	.907±026	.900±026	.842±024	.892±028	.282±026	.414±060	.438±080
News-NG3	**.919±018**	.910±013	.898±022	.851±019	.880±012	.217±021	.276±024	.360±030
Reuters	**.708±021**	.693±029	.687±019	.670±018	.704±018	.626±027	.554±021	.650±024

表 3 与基于分歧的方法对比的分类准确率（准确率±标准差）

模态	数据集	Multi-Training	CoTrain	CoLap	KCCA
1	CIT	**.638±012**	.209±000	.210±002	.240±006
	COR	**.664±056**	.442±018	.420±000	.386±120
	TEX	**.684±063**	.559±020	.531±000	.543±014
	WAS	**.731±046**	.464±017	.464±000	.464±022
	WIS	**.767±065**	.482±024	.450±005	.460±012
2	CIT	**.468±026**	.209±000	.307±020	.216±027
	COR	**.426±053**	.422±006	.420±000	.204±065
	TEX	**.592±069**	.549±018	.531±000	.467±060
	WAS	**.588±027**	.471±009	.470±012	.373±065
	WIS	**.472±065**	.452±007	.462±022	.346±072
综合	CIT	**.671±013**	.209±000	.286±019	.221±026
	COR	**.664±059**	.422±006	.420±000	.260±072
	TEX	**.709±059**	.578±029	.531±000	.504±077
	WAS	**.732±027**	.464±000	.464±000	.479±082
	WIS	**.730±056**	.450±005	.450±005	.428±043

输出一个分类结果，因此我们用 Multi-Training 算法的综合结果（平均准确率和标准差）和这些算法进行比较，并用各个模态分类器的一致性结果作为最终的融合结果。

表 2 给出了 12 个数据集上的分类结果，加粗表示在每个数据集上的最好表现。可以清楚地发现，Multi-Training 算法在大部分数据集上都取得了更好的结果，并且更加稳定。在多于两个模态的数据集上，Multi-Training 算法能够超过所有对比方法，并且提升幅度比较大。这可能是因为多个模态能够提供更多的预测一致性信息，使得对未标记样本的选择更加可靠。

4.3 与子空间方法进行对比

虽然子空间方法能够输出每个模态上的分类结果，由于版面限制，这里只给出综合结果的比较。子空间方法的综合结果是通过概率投票得到的。我们和 3 种子空间学习算法进行了对比实验：MvCCA（multi-view Canonical Correlation Analysis）、MvLPP（multi-view Locality Preserving Projections）和 MvMFA（multi-view Marginal Fisher Analysis）[3]。

从表 2 的结果可以看出，Multi-Training 算法在所有数据集上都超过了子空间方法，同时具有更高的稳定性。尤其在一些文本数据集上，例如 News-NG2 或 Reuters，我们的算法显著好于其它对比方法。

4.4 和基于分歧的方法进行对比

值得注意的是，融合风格和子空间学习风格的多模态学习方法都需要在训练阶段不断访问所有模态的特征，因此这些方法实际上不适用于多模态信息来自于多个私有渠道的场景。而基于分歧的方法和 Multi-Training 算法一样，能够只基于模态预测结果来提升分类器性能，而不需要直接接触原始特征。因此我们和基于分歧的多模态方法进行了对比。

由于大部分的基于分歧的多模态方法都是针对具有 2 个模态的数据的，这一节的对比实验都是在两模态数据集上进行的。我们和经典的协同训练算法[6]、CoLap（Co-Regularized Laplacian SVM）[20]和 KCCA（Kernel CCA）[21]了对比，其中 KCCA 使用的是默认参数的 RBF 核。这些算法都能既提供每个模态的分类结果，也能提供两个模态的总体结果。我们展示了 Multi-Training 算法和所有对比方法在每个模态上的结果和总体结果。

详细的结果列在表 3 中，CIT、COR、TEX、WAS 和 WIS 分别表示数据集 Citeseer、Cornell、Texas、Washington 和 Wisconsin，经典的协同训练算法简记为 CoTrain。从表 4 的结果中可以发现，无论是模态的个体分类器表现、还是综合结果，我们的 Multi-Training 算法都取得了最好的结果，并且相较对比方法有大幅度的提升。进一步验证了 Multi-Training 算法在多模态学习竞争合作场景下的有效性。

结束语 本文提出了一种新颖的多模态隐私保护学习框架 Multi-Training，通过寻找来自多个私有渠道的特征之间的关系来提升每个模态的个体分类器的性能。在这种场景下，一个模态的特征信息不能被其它模态共享。本文利用后融合策略对模态个体分类器对未标记样本预测值的评估来选择未标记样本，用来加入已有训练集中，实现模态之间的互相提升，同时使用 one-vs.-rest 策略保持每个模态数据的差异性。利用一致性结果作为未标记样本的选择标准，能够保证对未标记样本的预测更加准确，所选择的样本更具有代表性。在我们的模型中，模态的个体分类器的性能能够在不接触其它模态的特征的前提下得到提升，因此很好地保护了多模态数据的隐私。我们在多个真实数据集上和一些目前标准最好的多模态学习方法进行了对比，实验结果表明了 Multi-Training 算法在处理多模态数据时的优越性。

参考文献

[1] Jin Xin, Zhuang Fu-zhen, Xiong Hui, et al. Multi-task multi-view learning for heterogeneous tasks. In Proceedings of the 23rd ACM International Conference on Information and Knowledge Management, pages 441–450, Shanghai, China, 2014.

[2] David R H, Sandor S, and John S T. Canonical correlation analysis: An overview with application to learning methods. Neural Computation, 16(12):2639–2664, 2004.

[3] Abhishek S, Abhishek K, Hal D, et al. Generalized multiview analysis: A discriminative latent space. In Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, pages 2160–2167, Providence, RI., 2012.

[4] Mehmet G, Ethem A. Multiple kernel learning algorithms. Journal of Machine Learning Research, 12:2211–2268, 2011.

[5] Ye Guang-nan, Liu Dong, I-Hong J, et al. Robust late fusion with rank minimization. In Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, pages 3021–3028, Providence, RI.,

2012.
[6] Avrim B, Tom M. Combining labeled and unlabeled data with co-training. In Proceedings of the 11th Annual Conference on Computational Learning Theory, pages 92–100, Madison, WI., 1998.
[7] Wang Wei, Zhou Zhi-hua. Multi-view active learning in the non-realizable case. In Advances in Neural Information Processing Systems 23, pages 2388–2396. Cambridge, MA.: MIT Press, 2010.
[8] Wang Wei, Zhou Zhi-hua. A new analysis of co-training. In Proceedings of the 27th International Conference on Machine Learning, pages 1135–1142, Haifa, Israel, 2010.
[9] Wang Wei, Zhou Zhi-hua. Co-training with insufficient views. In Proceedings of the 5th Asian Conference on Machine Learning, pages 467–482, Canberra, Australia, 2013.
[10] Kan Mei-na, Shan Shi-guang, Zhang Hai-hong, et al. Multi-view discriminant analysis. In Proceedings of the 12th European Conference on Computer Vision, pages 808–821, Florence, Italy, 2012.
[11] Zhai Deming, Chang Hong, Shan Shi-guang, et al. Multiview metric learning with global consistency and local smoothness. ACM Transactions on Intelligent Systems and Technology, 3(3): Article 53, 2012.
[12] Corinna C, Mehryar M, Afshin R. Two-stage learning kernel algorithms. In Proceedings of the 27th International Conference on Machine Learning, pages 239–246, Haifa, Israel, 2010.
[13] Mehmet G, Ethem A. Localized multiple kernel learning. In Proceedings of the 25th International Conference on Machine Learning, pages 352–359, Helsinki, Finland, 2008.
[14] Zhou Zhi-hua, Li Ming. Tri-training: Exploiting unlabeled data using three classifiers[J]. Knowledge and Data Engineering, IEEE Transactions on, 2005, 17(11): 1529-1541.
[15] Ye Han-jia, Zhan De-chuan, Miao Yuan, et al. Rank Consistency based Multi-View Learning: A Privacy-Preserving Approach. In Proceedings of the 24th ACM International on Conference on Information and Knowledge Management. ACM, 2015: 991-1000.
[16] Prithviraj S, Galileo N, Mustafa B, et al. Collective classification in network data. AI Magazine, 29(3):93–106, 2008.
[17] Gilles B, Clement G. Co-clustering of multi-view datasets: A parallelizable approach. In Proceedings of the IEEE 12th International Conference on Data Mining, pages 828–833, Brussels, Belgium, 2012.
[18] Corinna C, Mehryar M, Afshin R. Two-stage learning kernel algorithms. In Proceedings of the 27th International Conference on Machine Learning, pages 239–246, Haifa, Israel, 2010.
[19] Alain R, Francis B, Stephane C, et al. SimpleMKL. Journal of Machine Learning Research, 9:2491–2521, 2008.
[20] Vikas S, Partha N, Mikhail B. A co-regularization approach to semi-supervised learning with multiple views. In Proceedings of ICML workshop on Learning with Multiple Views, pages 74–79, Bonn, Germany, 2005.
[21] David H, Sandor S, John S. Canonical correlation analysis: An overview with application to learning methods. Neural Computation, 16(12):2639–2664, 2004.

苗园，江苏省南京市栖霞区仙林大道 163 号南京大学仙林校区计算机科学技术楼 327 室，210023，15996265636，miaoy@lamda.nju.edu.cn

詹德川，江苏省南京市栖霞区仙林大道 163 号南京大学仙林校区计算机科学技术楼 1017 室，210023，18951679162，zhandc@lamda.nju.edu.cn