面向网络安全治理的用户身份识别技术与挑战

张广胜[1]，康 昭[2]，田 玲[2*]

(1. 军委政法委员会某单位 北京 100120；2. 电子科技大学计算机科学与工程学院 成都 611731)

【摘要】网络用户身份识别对维护网络安全、推动网络身份管理制度建设具有重要价值。网络用户身份识别既是用户画像、行为预测、精准服务的研究基础，也是水军账号甄别、网络社会治理、涉网犯罪打击的技术支撑。分析了用户身份识别技术的进展，及其在机器人水军识别、目标社区检测和跨社交网络用户对齐方面的应用。首先，从用户身份识别的定义与发展历程出发，介绍了用户身份识别方法的分类；其次，对不同特征下的机器人水军识别方法进行了阐述，并分析了不同方法的主要适用场景；然后，针对水军相关的目标社区检测任务，梳理了目标社区检测技术的发展；其次，对现有跨社交网络用户对齐技术进行了分类。最后，对用户身份识研究当前面临的挑战进行了论述，并对其未来作出了展望。

关 键 词 机器人水军识别； 目标社区检测； 社交网络； 用户身份识别； 用户对齐

中图分类号 TP391 **文献标志码** A doi:10.12178/1001-0548.2022106

User Identity Identification Technologies and Challenges for Network Security Governance

ZHANG Guangsheng[1], KANG Zhao[2], and TIAN Ling[2*]

(1. Investigation Technology Center PLCMC Beijing 100120;

2. School of Computer Science and Engineering, University of Electronic Science and Technology of China Chengdu 611731)

Abstract Network user identity identification (UII) is significant to maintain network security and promotes the construction of network identity management system. UII is not only the fundamental for user network portrait, action prediction, and accurate delivery service, but also the technical pillar for social bot detection, network social governance, and crack down cybercrime. The progress of UII technology and its applications in bot detection, community detection, and user identity linkage across social networks are analyzed. At first, from the definition and development history of UII, the classification of UII methods is introduced. Second, a brief overview of bot detection methods with different characteristics is performed, and their main applicable scenarios are pointed out. Then, social bots related community detection techniques are analyzed. Furthermore, the existing methods for user identity linkage across social network platforms are surveyed and categorized. Finally, we discusses the current challenges of user identity research and its future prospects.

Key words bot detection; community detection; social network; user identity identification; user identity linkage

近年来，在线社交网络 (online social network，OSN) 在世界范围内迅速普及，截止 2021 年底，全球已有 50 亿用户加入了社交网络，比 2020 年增长了 13%。社交网络已深度融入人们的工作与生活，特别是伴随 5G、大数据、人工智能、元宇宙等新技术发展，现实世界与虚拟空间进一步相互交叉融合，形成了横跨物理域、信息域和认知域的新型社交网络空间，社交网络空间认知域的主体是用户，决定网络空间安全的最主要因素仍然是“人”。用户为充分满足自身需求，通常参与到多个社交网络平台中，这对社交网络平台的精准服务推荐、网络画像和用户行为分析及信息内容监管提出了更高要求。

与此同时，巨大的用户群高频度通过社交网络参与到各国网络政治生活和网络社会治理活动，网络谣言、虚假信息等违法有害内容被机器人水军制

收稿日期：2022－04－11；修回日期：2022－06－21

基金项目：国家社会科学基金 (2020SKJJB019)；四川省科技计划 (重点研发)(2021YFG0018，2022YFG0038)

作者简介：张广胜 (1975－)，男，博士，正高级工程师，主要从事大数据、网络政治安全及智慧侦查等方面的研究.

*通信作者：田玲，E-mail：lingtian@uestc.edu.cn

造传播，给国家意识形态安全带来严重影响。特别是随着计算宣传兴起，认知空间对抗日趋激烈，敌我双方在社交媒体上大量布设机器人水军，精准实施大规模舆论干预和认知操控，给国家安全带来了严峻挑战。准确识别社交网络用户身份、精准甄别水军账号对维护网络安全、推动国家网络身份管理制度建设具有重要价值，也是网络社会治理、打击涉网违法犯罪活动的重要支撑。因此，研究用户身份识别方法具有重要的现实意义。

本文对近年来社交网络用户身份识别相关研究进行了综合分析。首先从用户身份识别的概念出发，对该研究领域的发展历程进行回顾。其次，详细介绍了用户身份识别面向网络安全治理的 3 个主要应用领域，即机器人水军识别、目标社区检测和跨社交网络用户对齐。最后，对社交网络用户身份识别领域的现有问题和挑战进行了探讨，对该领域的未来研究方向和趋势作出了展望。

1　用户身份识别主要方法

本章将从用户身份识别的发展历程引入，介绍用户身份识别的主要方法，并按照所使用的数据对其进行分类。

1.1　用户身份识别的发展历程

对于社交网络中的社交活动而言，用户身份必不可少，有效识别用户身份对于实际应用和科学研究均具有重要意义。用户身份识别包含用户所属群体或角色推测、用户身份同一性判定和用户身份认证[1]。近年来，用户身份识别研究得到了迅猛发展，该领域的部分代表性方法如下所示。

2009 年，利用用户名属性实现映射的 CCCUE 模型[2] 被提出。从确立各社团对应的关键词集合开始，CCCUE 模型通过不断增删社团成员对应的前缀或后缀，实现对目标社团成员的有效识别。

2010 年，考虑到不同账号影响程度的差异问题，利用 FOAF(friend of a friend) 词汇表进行账号属性匹配的 UPMF 模型[3]，为账号不同属性进行人工或自动地分配权重，并结合字符串和语义相似度指标实现属性值比较，实现对用户身份的有效识别。

由于匿名账户难以确定其各属性的权重分配问题，从不同账号对应生成内容及其书写风格存在的相异性角度分析，文献 [4] 提出 ELUR 模型，利用朴素贝叶斯和 KL 散度分析匿名用户评论内容及书写风格，从而实现对匿名用户身份的有效识别。

考虑用户在不同社交网络中属性存在一定的相似性，利用这一特点结合机器学习算法对账号属性进行建模。2013 年，通过在 Twitter 等 5 个社交网络中评估账号匹配的一系列关联方法，MLSN 模型[5] 仅利用账号公开属性实现对单个账号的有效关联，实现用户身份识别。

2014 年，HYDRA 模型[6] 将生成内容和账号属性进行结合，进而识别用户身份。HYDRA 模型通过分析用户跨社交网络的高阶结构，实现对用户信息链接和结构一致性的多目标优化，进而实现对用户身份的有效识别。

虽然基于用户属性信息在一定程度能够有效识别用户身份，但大多数情况下，用户出于隐私保护等原因，会对其账号进行修改，因此仅基于用户公开属性的识别算法正确率会有所降低。2016 年，基于用户内容风格的 MUSIC 模型[7] 利用词嵌入技术结合用户信息构建用户内容风格模型，并将跨社交网络用户对齐问题归约为单社交网络中的分类问题，从而实现对用户身份的有效识别。

由于对用户属性人工赋权的方法存在较大的主观性，为完善属性赋权的客观性，提高身份识别的准确性，2017 年，IE-MSNUIA 算法[8] 利用信息熵赋予用户属性权重，进一步完成用户身份识别。通过分析用户各属性项的数据类型及其对应的物理含义，并利用其对应的信息熵值赋予权重，IE-MSNUIA 算法融合多个属性进行决策，能够有效识别用户身份。2018 年，针对生成内容复杂度、规范性、时效性等进行综合分析，IOIU 模型[9] 进一步提升了用户识别的有效性。IOIU 模型充分利用文本内容、多媒体以及内容的发布时间序列，融合 4 类方法实现对组织用户和个人用户的有效区分。

2019 年，UISN-UD 模型[10] 在不使用用户隐私信息的前提下，通过刻画用户名和显示名称中的信息冗余，并基于信息冗余实现用户账号匹配，UISN-UD 模型在兼顾用户隐私安全的同时增加了身份识别的准确性。2021 年，TIW-UI 算法[11] 根据两级信息熵权重分配实现对各属性权重的分配，该算法能够有效识别用户身份。TIW-UI 算法通过聚合用户的属性信息和行为信息，并结合双向匹配算法实现用户账号匹配。

1.2　用户身份识别方法的分类

本节将结合用户识别发展历程，根据使用数据的不同，将现有的用户身份识别方法分为五类，即基于账号属性、生物特征、网络拓扑结构、生成内

容和行为模式的身份识别，并对这几类方法分别进行详细介绍。

1.2.1 基于账号属性的身份识别

用户在各大社交网络上注册时都会被要求填写包含用户名等账号属性的档案信息。这些账号属性在很大程度上直观反映了用户身份，也为区分组织账号和个人账号提供了有力支撑，是早期相关研究的着重点。

文献 [2] 最早将账号属性运用于身份识别研究，通过对用户名等简单信息增加或删除后缀实现映射。文献 [12] 提出的 OUSA 模型则针对用户名属性提取了上千种属性，并计算向量之间的相似度。

然而仅仅依靠用户名等单一属性的用户身份识别方法存在鲁棒性差、准确性低等问题，不能完全满足用户身份识别的需求。文献 [3] 利用 FOAF 词汇表，将用户的多个属性信息进行匹配，以此来计算账号之间的相似度。在此基础上，文献 [13] 基于账号属性提出带权重的用户身份识别算法，该算法从语法和语义这两个方面进行相似度计算。

随着机器学习的发展，文献 [5] 通过分析决策树、支持向量机等有监督分类模型的效果，验证了朴素贝叶斯模型在用户身份识别任务中的鲁棒性。然而，基于朴素贝叶斯等有监督分类模型的用户身份识别方法依赖于大量标注样本数据，在实际应用中的泛化性能较差。文献 [8] 利用账号属性的信息熵值为各属性项分配权重。在此基础上，文献 [11] 提出两级信息熵的权重分配方法，进一步提升了用户身份识别的准确率。

随着各大社交网络平台对用户隐私信息的保护不断加强，部分用户账号属性信息难以获取。对此，文献 [10] 提出了 UISN-UD 模型，该模型基本不涉及用户的个人隐私信息，仅利用用户名和显示名称中丰富的信息冗余来进行用户身份识别，简单易实现。

基于账号属性的身份识别方法能够有效识别用户身份，然而这些方法均依赖于用户数据的真实性和完整性。在实际应用中，出于隐私保护等考虑，用户通常不会提供自己真实完整的信息，这类方法的用户身份识别效果会受到较大限制。

1.2.2 基于生物特征的身份识别

随着人脸识别等计算机视觉模型在各领域中逐步得到应用，生物特征在用户身份识别研究中也越来越受到重视。

用户在社交过程中经常会发布个人照片等信息，人脸识别方法在用户身份识别中可以很好地发挥作用。文献 [14] 通过用户头像进行分析，并结合人脸识别技术对用户进行身份关联。在人脸识别等深度学习模型出现之前，文献 [15] 尝试利用虹膜进行用户身份识别，提出 IPUI 模型，之后又尝试运用步态信息识别用户身份，并提出 GBHI 模型[16]。由于通常很难获得用户生物特征数据，这类方法的应用受到了一定的限制。

1.2.3 基于网络拓扑结构的身份识别

基于网络拓扑结构的身份识别本质上是将用户之间的好友关系、社交关系建模成网络拓扑结构，并对网络中节点之间的相似度进行计算。

文献 [17] 将社交关系视为个人的身份标签，即将“你认识的人”作为用户身份认证因素，提出 FFA 模型。文献 [18] 最早将网络拓扑结构应用于用户身份识别，即以少量已知的种子节点为出发点，通过不断地迭代更新匹配到新的节点，进而实现账号的身份识别。然而，这种方法的准确率和召回率较低。随后，通过将账号属性和图相似性进行结合，文献 [19] 在 Facebook 社交网络和电子邮件网络之间进行一一映射，进而识别用户身份，但这样的映射存在一对一冲突的问题。

基于网络拓扑结构的用户身份识别方法大多数是有监督学习的。文献 [20] 针对无监督场景提出了 FRUI-P 模型，该模型运用随机游走的思想，采用基于负采样技术的连续词袋模型 (CBOW) 来对网络向量进行学习，为每个用户的网络结构提取特征向量并将其应用于用户身份识别。FRUI-P 模型能够在无需知道种子节点的情况下精确识别用户身份，可以生成有监督和半监督的用户身份识别方法所需的先验知识。

随着神经网络在各个领域中的广泛应用，图神经网络具有良好的网络拓扑结构嵌入性能，在用户身份识别中得到了广泛关注。

考虑到社交网络的异质性和用户关系的稀疏性，文献 [21] 研究基于异构图的用户身份识别方法，该方法在组织账号的识别上有较好的表现。

相较于账号属性，用户的网络拓扑结构包含的虚假信息更少，更适合用于识别用户身份。

1.2.4 基于生成内容的身份识别

生成内容是指用户在社交网络中产生的发布内容、评论等各类社交行为信息，能够反映用户的兴趣、爱好等。出于不同的经营目的，组织账号和个人账号在生成内容的措辞、文本长度等特征上具有

较为明显的区别。基于生成内容的身份识别能够有效区分组织账号和个人账号。

文献 [4] 基于对用户生成内容的书写风格分析和总结进行用户身份识别。结合账号属性、生成内容和其他用户数据，文献 [6] 提出 HYDRA 模型来识别用户身份。针对用户生成内容风格，文献 [7] 利用 Doc2Vec 将生成内容表示为向量形式，进而识别用户身份。综合用户的地理位置、发表内容等信息，文献 [22] 提出 MNA 模型计算用户在社交网络中的相似性以用于识别用户身份。文献 [9] 针对生成内容的复杂性、规范性、多媒体特性和时序性等多个维度，为每个维度提出对应的计算方法，但是该方法不能同时考虑多个维度。

此类方法取决于用户生成内容的数量和质量，不适合部分不活跃的用户。

1.2.5　基于行为模式的身份识别

有学者将用户发布内容、点赞、评论等行为视作用户行为特征，并将用户的轨迹信息视为用户的行为模式。用户轨迹信息在一定程度上映射出了用户在现实生活中的移动轨迹，也可以被视作用户产生的一类社交信息。

通过总结用户轨迹信息中地理位置的共现频率，文献 [23] 设计了基于多源位置数据处理的用户身份识别算法，但该算法参数过多，增大了识别用户身份所需的计算开销。文献 [24] 则将地理位置坐标转化为对应位置的语义，利用由语义位置组成的文本表示用户轨迹，并通过计算用户轨迹之间的相似度实现用户身份识别。

用户访问每个地点的次数也被用于识别用户身份，文献 [25] 假定用户在特定时间内对某个地理位置的访问次数服从泊松分布，并利用概率函数计算用户账号的同一性概率。

部分工作则以轨迹信息的时间和空间两个维度为出发点，将原始多源时空数据转换为三部图，并通过最优划分求解得到用户账号匹配结果[26]。用户身份识别主要方法如表 1 所示。

表 1　用户身份识别主要方法

方法类别	特征或属性	模型或算法
基于账号属性	用户名、性别、年龄、身份等	CCCUE[2]、OUSA[12]、UPMF[3]、MLSN[5]、IE-MSNUIA[8]、TIW-UI[11]、UISN-UD[10]
基于生物特征	人脸、指纹、虹膜等	FRR[14]、IPUI[15]、GBHI[16]
基于网络拓扑结构	好友关系、点赞、转发等	DASN[18]、ECOSN[19]、FRUI-P[20]、HeteroUI[21]
基于生成内容	发表内容、书写风格等	ELUR[4]、HYDRA[6]、MNA[22]、MUSIC[7]、IOIU[9]
基于行为模式	轨迹信息、时间序列信息等	AUI[23]、UBM[24]、POIS[25]

2　机器人水军识别

随着社交媒体的普及，越来越多的证据表明网络水军的数量在不断增多，而机器人水军对用户身份识别研究具有重要影响。本章将从机器人水军的定义及识别的重要意义出发，介绍机器人水军的识别方法以及面临的挑战。

2.1　机器人水军

机器人水军，也称社交机器人 (social bot, social spammer)，是社交平台中最常见的一种恶意程序。随着智能技术的高速发展，机器人水军开始具备人类用户的特征，它们对信息传播和扩散过程具有重要影响。机器人水军通过关注一些有影响力的人，有目的、有计划地在各平台上讨论某个事件，制造虚假信息、传播谣言，甚至操纵公众舆论，使事件发酵，从而达到“炒作”效果。

在一些特定的话题中，当机器人水军数量达到一定比重时，就可以通过改变公众意见使其传播观点最终成为主流观点。当大量的机器人水军账号被创造出来并在社交平台上广泛传播时，它们会给公众和网民的安全带来严重的负面影响。据估计，2017 年活跃在 Twitter 的 15% 帐户和 2019 年活跃在 Facebook 中的 11% 帐户为机器人水军账户。

在政治或经济利益受到极度威胁时，机器人水军数量会急剧增加。在 2016 年美国总统大选前的几个月里，Twitter 上与大选有关的所有推文中，有近五分之一的机器人水军账号通过影射有关问题和事件，对总统选举产生巨大影响。因此，美国国防部高级研究计划局 (DARPA) 举办了一场竞赛，试图寻找对抗机器人水军的有效策略。在 2017 年法国总统大选前也出现类似事件，机器人水军大量散播马克龙竞选文件，并扩散虚假消息，对总统大选造成了极大影响。2018 年 12 月，欧盟委员会发

布了反虚假信息行动计划，该计划将机器人水军视为一种“在社交媒体上传播和放大分裂性内容和争辩”的技术。2019 年的一项研究报告表明，关于美国股票走势的 Twitter 作者中 71% 很可能是机器人。在线加密数字货币讨论中机器人的存在也占类似比例。

目前，对机器人水军的影响仍然缺乏广泛的共识，一些研究人员认为它们在增加虚假信息的传播、两极分化和仇恨言论方面发挥着关键作用。在中国，针对微博网络机器人水军的研究还处于以僵尸账户为主的阶段。实际上，水军账户除了僵尸账户还包含劫持账户、雇佣账户和核心账户等多种账户，每种账户的特征表现各不相同，这也是水军特征选择困难的原因之一。

因此，机器人水军识别作为用户身份识别的典型应用，其目的是对机器人和人类加以区分，在维护社会稳定、避免网络陷阱、确保隐私安全等方面具有重要意义。

2.2 机器人水军识别方法

现有的机器人水军识别方法主要分为 3 类：传统算法、机器学习算法以及混合算法，本文提及的机器人水军识别主要方法如表 2 所示。

表 2 机器人水军识别主要方法

算法	特征或属性	模型或算法
传统算法	无	honeypot[27]
机器学习算法	DTW距离、用户账户内容、行为信息、关系网络、内容和历史、时间、转发量、 IP地址、报文数目	DeBot[27]、BeDM[28]、RF[29]、SVM[30]、Graph-Based[31]
混合算法	用户数据、推文内容、IP地址、发布时间频率	Stweeler[32]、Markov BOTection[33]、Clustering[34]、Deep Forest[35]、MDM[36]、DeG-Spam[37]

2.2.1 传统的机器人水军识别

早期机器人水军识别主要针对垃圾邮件发送者 (spammer)，因为这种垃圾邮件发送者数量规模较小、行为没有高度隐蔽性，并且产生的垃圾信息具有明显的特征，可通过大量识别，建立黑名单、白名单来记录可疑用户和正常用户，以此提高水军识别效率。

蜜罐技术 (honeypot) 作为传统机器人水军识别算法，其本质为一种对攻击方进行欺骗的技术，通过布置一些信息作为诱饵，诱使攻击方实施攻击，从而达到识别攻击方的效果。文献 [38] 通过捕获和分析部署社交蜜罐，从社交网络社区搜集对应用户的属性值并进行统计，最后通过构建分类器实现机器人水军识别。

2.2.2 基于机器学习算法的机器人水军识别

机器人水军识别的机器学习算法包括朴素贝叶斯、随机森林、贝叶斯网络、K 近邻聚类算法和决策树算法等。这些算法往往通过抽取用户的相关特征进行用户分类，将机器人水军识别归到分类问题中。

传统的相关系数 (如 Pearson) 是非弹性的，不适合机器人控制器、网络延迟和社交应用内部延迟而形成的活动时间序列。2016 年，文献 [27] 通过动态时间规整 (DTW) 算法来允许时间扭曲，改进了时间相关的身份识别算法，提出名为 DeBot 的机器人水军识别算法。该算法采用滞后敏感的散列技术，将发表信息的用户散列到可疑相关用户桶后，再利用层次聚类算法和人物关系图谱，验证可疑用户与特定账户侦听器之间的相关性，最后输出被判定为机器人的用户，从而实现机器人水军识别。

2017 年，文献 [28] 将深度神经网络用于融合用户内容和用户行为信息，并首次将其应用于机器人水军识别。通过在一个真实的 Twitter 数据集上进行了大量实验，验证了该方法的有效性。同年，文献 [29] 利用机器学习算法对新浪微博的机器人水军进行识别。分别采用决策树 C4.5 和随机森林算法进行数据分析，并对博文发布设备、声誉率、重复率、传播率 4 个特征重要性做验证，最终机器人水军识别 F 值达到 94%。

2018 年，文献 [30] 提出了一种机器学习算法，该算法利用一系列特征，包括用户名长度、转发率、时间模式、情感表达、关注者与朋友的比例和消息的多样性来识别机器人水军。结果表明在 Twitter 数据集中的误识别率低于 2.25%。

使用机器学习的机器人水军识别具有网络流级特征，现有的基于流的方法通常会产生很高的极端计算开销并且不能完全捕捉可能暴露恶意主机的网络通信模式。2019 年，文献 [31] 利用有监督和无

监督机器学习方法，提出了两阶段、基于图的机器人水军识别系统。该系统对摄入的网络流进行图转化之后提取相应特征，在第一阶段利用无监督的机器学习只对可能的良性主机进行修剪，第二阶段则利用有监督的机器学习实现较高精度的机器人检测。

2.2.3　混合的机器人水军识别

混合算法将多种算法、多种用户特征进行结合，其目标是通过整合所有这些特性来获得更高的效率和准确性。

文献 [32] 提出 Stweeler 框架，该框架通过对用户数据、推文内容 (包括地理位置)、IP 地址、发布时间等进行特征提取，结合内容聚类算法、贝叶斯算法和时空轨迹分析算法，对机器人水军进行识别。机器人账户与普通用户之间往往有多重联系，如果仅基于图这单一联系进行机器人水军检测，无法全面有效地区分机器人账户和普通用户。因此，文献 [39] 提出一种融合基于用户、基于内容和基于图特征的混合技术来识别机器人水军。其中，基于用户的特征是根据用户账户的关系和属性而建立的，与之相关的属性包括关注者和追随者的数量、年龄等。通过从推文内容和情感、推文账户及使用情况中进行信息提取。利用高级流特征捕获机器人的网络行为来构造马尔可夫链，可以产生与内容无关且加密弹性的行为特征。因此，文献 [33] 基于机器人水军的网络流行为构建马尔可夫链，进而提出了保护隐私的机器人水军识别系统 BOTection。

以上所提及的大部分方法都需要手动标记大量数据集，人工开销大。为了解决这个问题，基于社交网络对等用户之间的接受度，文献 [34] 提出了完全无监督的机器人水军检测方法。其中，对等用户之间的接受度表示两个用户之间在多个主题上的共同兴趣。

在复杂关系网络中，即使机器人水军试图隐藏它们的恶意意图，也不能改变用户之间的关系连接。因此，目前越来越多的机器人水军检测研究更倾向于利用关系连接而非文本内容构建检测框架。采用深度森林算法，文献 [35] 基于用户之间的交互量重新定义了一组特征，在个别数据集上能够达到 97.55% 的识别准确率。基于循环神经网络技术，文献 [36] 提出 MDM 模型，利用隐藏在关系序列中的用户长期依赖以及短期依赖来检测机器人水军。类似地，基于深度图神经网络，文献 [37] 结合偶发关系和固有关系提出 DeG-Spam 模型。该模型从异构信息网络的角度进行潜在特征分量的提取，提升特征空间构建的全面性，进而提升 5%～10% 的机器人水军识别准确率。

3　目标社区检测

社交网络中的机器人水军具有集群现象，当机器人聚集的数量足够多时，会出现僵尸网络 (botnet)，这类网络为非法活动提供平台，正在成为网络安全最严重的威胁。因此，目标社区检测能对识别甚至遏制僵尸网络的形成具有重要意义。本章将从目标社区的定义及其检测的意义出发，并对现有目标社区检测方法进行分类。

3.1　目标社区

社交网络由一组节点和连接这些节点的边组成。节点代表个体或实体，边对应节点之间的交互关系。具有相似品味、选择和偏好的人在社交网络中产生关联的趋势导致了虚拟集群或社区的形成。“水军社区”作为社交网络中大量传播虚假信息的机器人集群，对用户人隐私和网络安全造成了极大的威胁。将“水军社区”作为检测的目标社区，可以在一定程度上遏止谣言的进一步传播。

俄乌冲突作为 2022 年的重大地缘政治事件，在政治、军事、经济、文化等多个方面引发了激烈的交锋，更是促进了信息化舆论战这一新兴的战场形式的快速发展。相关势力借助“水军社区”的力量，在各网络平台有针对性地散发虚假信息，制造战争迷雾，利用信息的传播过程制造有利于自身诉求的“信息茧房”。同时，通过频繁炒作、蓄意煽动、博取同情等夸张的渲染手段给对手贴上恶性的脸谱化标签，在抓住网民眼球的同时进行舆论洗脑，巩固公众对于敌人的仇恨情绪，从而争取意识形态斗争的绝对优势。“水军社区”的有效检测有助于追踪网络舆情，有利于维护网络正常秩序。

3.2　目标社区检测方法

基于综合特征和重叠网络的目标社区总体检测方案包含 3 个主要步骤：1) 利用与垃圾信息相关的内容对社交网络数据集进行处理并设计构建转发关系网络，挖掘转发关系网络中的重叠社区结构，进而获取水军团体的结构特征；2) 分析垃圾信息的内容特征与行为特征以及重叠社区结构所包含的网络特征，从而构建综合特征；3) 结合综合特征对嫌疑水军团体进行识别验证，并汇总结果。

社交网络中的水军存在于复杂的水军结构中，通常水军只是社交网络中一个具有较强传播信息能力的普通节点，但当有“任务”时，它们会“全

体”出动，传播垃圾信息并迅速使其成为热点，发送内容与垃圾信息具有高度的语义相似性，反映出网络水军群体在散播信息时在特定时间内的特性。通过分析目标社区节点在特定时间内传播的内容信息，研判其是否发送过垃圾信息，以达到进一步排除重叠社区结构中的无关节点，最终得到水军团体。

3.2.1 基于内容特征的目标社区检测

在互联网络发展初期，由于水军在社交平台推送的商业广告、垃圾邮件等信息特征明显、易识别，因此基于内容的目标社区检测方法成为早期“水军社区”检测的主要方法。

基于内容的目标社区检测方法引入自然语言处理的思想及方式，将水军团体生成内容中如 URL 的模式特征和特殊的关键词等显著特征从网络中识别出[40]，具有情感倾向对意见文本进行分析[41]，来帮助挖掘网络“水军社区”。基于内容特征的目标社区检测方法目前连邮件网络系统中的水军都很难识别，更难满足现今社交网络中水军识别的需求任务要求。因此，当前基于内容特征的目标社区检测方法，主要通过与其他特征结合，进行“水军社区”的综合检测。

3.2.2 基于行为特征的目标社区检测

用户相关信息可以由用户行为特征反映。如网络水军的突发性行为明显不同于正常用户行为表现。基于行为特征的目标社区检测通过分析网络水军行为，定义水军特征，根据分类算法，判别社交网络用户的网络水军，进而实现“水军社区”检测。

水军通常利用大众的非工作时间进行邮件发送，文献 [42] 根据水军活动时间以及邮件中是否存在 URL 提取水军两个行为特征，提出 BeaKS 过滤器，文献 [43] 将水军机器人生产的邮件内容、邮件发送周期等特征作为辨别机器人的重要依据，进而实现“水军社区”检测。文献 [44] 提出 SBCD 和 DA-SBCD 模型，前者用于区分社交僵尸网络社区中的合法参与者，而后者重建社区，并在现场更准确地检测社交僵尸网络。文献 [45] 通过分析 YouTube 视频网站中的网络水军行为数据，利用人工标记的方法标明数据集中的网络水军，基于启发式机器学习方法检测“水军社区”。

面对当今网络水军行为的复杂性、多样性，传统的基于用户行为特征的目标社区检测利用用户行为特征的单一属性，已无法满足复杂社交网络环境中 “水军社区”检测的需求。

3.2.3 基于网络特征的目标社区检测

基于网络特征的目标社区检测方法，主要分为基于网络结构特征和基于网络环境层级特征的方法。

传统的基于网络特征的目标社区检测依据邮件往来记录构建用户关系网络来进行“水军社区”检测。由于社交网络自身结构的稳定性，其拓扑特征难以受用户行为所影响[46]，基于网络结构特征的“水军社区”检测研究通过利用网络水军无法隐藏其在网络结构上的行为特征这一特点，得到了广泛重视。

尽管网络水军显现的用户特征愈加趋于正常用户，但是其在社交网络环境中表现的异常行为仍然较易识别。文献 [47] 利用谱聚类的方法检测模糊社区和识别不稳定节点。文献 [48] 提出 PUID 算法，根据初始社交网络中的方向和兴趣向量计算权重，从而得到边缘之间的相似性，再做分层聚类算法检测社区。文献 [49] 根据网络水军表现活跃时，引起的网络负载突增和流量集中于某些链路等网络环境变化现象进行水军识别。

基于网络结构特征的“水军社区”检测能够解决其他方法无法适用于网络水军用户特征趋向正常用户的检测问题，能够更加有效地阻止水军进一步发展。目前该方法已经成为“水军社区”检测研究的主要方式之一，但利用不同的网络结构特征时，其检测效率差别较大。

3.2.4 基于影响力的目标社区检测

基于影响力分析的目标社区检测，通常先寻找社交网络中在相应环境下能够对其他用户产生影响的意见领袖，再判断其是否为网络水军。

对社交网络中的用户进行影响力评级，其评级越高表明该用户在传播虚假信息过程中贡献越大。文献 [50] 统计了基于网络拓扑、用户行为等影响力度量方法。社交网络中存在传播能力很强的非机器人用户节点 (如具有影响力的明星)，使用基于影响力的方法能够检测出有影响力的节点，但就其节点本身的特质无法表示该节点属于网络水军。这种情况下可以结合该节点 (即高评级用户) 传播信息的频率进行水军检测，如果社交网络中节点长时间内不传播任何信息，表明其不具备较强的信息传播能力，很有可能不是一个网络水军。因此，缩小用户传播虚假信息的覆盖面可以通过把控高评级用户来实现。文献 [51] 提出的 LT 模型将社会网络划分为不相交的若干社区，通过在每个社区求得最大化传播的影响力总和，组合优化社区划分。

除此之外，也可以通过寻找间接检测“水军社区”的支撑结构。支撑结构是指对特定成员影响力构成起到重要作用的网络群体。但在实际应用中，节点影响力度量计算复杂，很难高效地找到支撑结构。而且，若寻找到的某些节点的支撑结构与其他社区节点孤立存在，该结构也无法进一步传播信息。

3.2.5　基于综合特征的目标社区检测

基于综合特征的目标社区检测方法比单一特征的检测方法可以更全面、更准确地分析网络水军的特征。由于这些网络水军普遍会关注目标用户或花费大量时间以等待目标用户关注自己，文献 [52] 首先将图论相关理论知识运用到对 Twitter 中的网络水军的初步搜索中，根据用户的影响力特征提高识别网络水军的准确率。文献 [53] 基于 PageRank，提取了新浪微博中帐户的相关属性以及账户之间的关系，可以得到社区领导者，从而对社区进行检测。文献 [54] 综合分析 Twitter 用户行为特征和发表的 Tweet 来识别该用户是否为网络水军。

文献 [55] 从行为特征角度分析网络水军形成的垃圾信息的内容特征，来识别隐藏在国内社交媒体平台的网络水军。

基于综合特征的目标社区检测方法能够充分识别并利用网络水军的特征，从而更准确地检测“水军社区”。但识别社交网络中 “水军社区”特征的更有效选取，是亟需解决的关键问题。

3.2.6　基于重叠社区结构的目标社区检测

传统的基于非重叠社区结构的目标社区检测方法，是通过将社交网络分成几个互不相通的社区，所在社区的节点各不相同。该检测算法包括模块度优化算法、层次聚类算法、谱聚类算法等。因为各个社区之间通常都是存在联系的、相互重叠且彼此交叉的，导致传统的社区划分方法不适用于大多数现实的网络结构。现实中，有些节点并不属于某单一社区，而是同时隶属多个社区。具有不同偏好的用户在社交网络中被划分到不同的社区，如在作家协作网络中，某一作家能够和一个或多个作家进行合作。由此可以得出基于重叠社区结构的目标社区检测方法更符合实际和更具研究意义。

目前，重叠社区结构由于其潜在的研究价值，已成为目标社区检测的重点研究对象。从社交网络中的节点和边两个角度划分按照其标准和对象的不同将算法分为两种类别，一类是通过对社区进行划分、聚类和共有节点发现等方法寻找网络中的重叠节点[56]；另一类则是通过社交网络中的边特征进行社区划分。网络中某个节点的连接边数不唯一，因此能进一步根据边与社区的隶属关系规则对节点进行划分，间接发现重叠节点，进而发现重叠社区结构[57]。“水军社区”中的机器人水军往往隶属于多个社区，利用重叠社区结构的目标社区检测技术能够较为准确地区分真人账户和机器人账户。

上述内容对现阶段目标社区检测方法从基于内容、行为、网络、影响力和重叠社区 6 个特征，分别阐述其所应用的场景及对应算法在该场景下解决的问题和存在的局限，并进一步在表 3 中对比分析当前目标社区检测方法的优缺点以及典型代表模型。

表 3　目标社区检测主要方法优缺点对比

目标社区检测技术	主要优点	主要缺点	代表模型
基于内容特征	信息缺失性低	识别场景简单	文本分类算法[40]、倾向性分析算法[41]
基于行为特征	异常特征易于区分	属性单一	BeaKS[42]、SBCD[44]、DA-SBCD[44]
基于网络特征	数据完整且易获取	存在网络异构性	谱聚类[47]、PUID[48]、SpaDeS[49]
基于影响力	影响力大的节点易于检测	节点影响力度计算复杂	LT model[51]
基于综合特征	检测更加全面，且特征分析准确率高	“水军社区”特征识别困难	PageRank[53]、HITS[54]、SVM[55]
基于重叠社区结构	克服了边聚类产生的无效重叠节点	节点社区划分时易混淆	Cat[56]、基于链接划分的算法[57]

4　跨社交网络用户对齐

随着在线社交网络平台的日益普及和多样化发展，越来越多的用户参与到多个社交网络平台中，网络安全治理问题也日渐困难。仅对分析单一社交网络进行分析难以有效识别用户身份，急需高效的跨社交网络用户身份识别方法。本章将从跨社交网络用户对齐的定义出发，介绍跨社交网络用户对齐的现有方法及面临的挑战。

4.1　用户对齐

用户对齐 (user alignment, UA) 也称为用户识别

(user identification, UI) 或用户身份链接 (user identity linkage, UIL) 等，旨在链接跨社交网络中的同一自然人[58]。有效的用户对齐有助于全面刻画用户特征，有利于用户迁徙分析、用户好友推荐和信息传播分析[59-60]。

一般而言，电子邮件地址、手机号码及身份证号等具有唯一性的用户属性，可以被直接用于确定用户身份。然而，出于隐私保护等原因，这些用户属性通常很难被获取。因此，用户名、发布内容、好友关系等社交网络平台公开信息往往被用于跨社交网络用户对齐。

4.2 跨社交网络用户对齐方法

本节主要介绍现有的跨社交网络用户对齐方法，将首先介绍跨社交网络用户对齐技术框架，之后介绍 3 类跨社交网络用户对齐技术，它们分别基于规则、机器学习和深度学习。

4.2.1 跨社交网络用户对齐技术框架

现有的跨社交网络用户对齐技术框架，包含数据预处理、候选集生成、标记数据获取、特征提取、用户对齐算法 5 个部分。其中，数据预处理是为了保留与当前任务相关的属性子集，并将数据处理为后续可用的形式。候选集生成则旨在限定匹配的用户范围，从而降低匹配计算的复杂度。在跨社交网络用户对齐研究中，标记数据代表预先匹配的用户对。

4.2.2 基于规则的跨社交网络用户对齐

跨社交网络用户对齐研究中基于规则的跨社交网络用户对齐是早期研究的重点方法。

最具代表性的基于规则的跨社交网络用户对齐方法主要包含：1) 经数据预处理操作，从社交网络中提取属性子集；2) 为每个属性设计相应的评分规则，并计算候选集中候选用户对的各属性评分；3) 求解候选用户对的匹配度，即属性评分的加权求和；4) 利用特定的匹配算法进行跨社交网络用户对齐。基于规则的跨社交网络用户对齐方法依据规则可以被分为基于匹配度最大化和基于传播这两类方法。

根据候选集与目标用户具有相同的最大匹配度时称其为对齐用户。

早期的基于匹配度最大化规则的跨社交网络用户对齐研究大多利用用户自身公开的属性进行用户对齐。文献 [2] 提出直接利用用户名实现用户对齐的 CCCUE 模型。结合用户名和标签，文献 [61] 提出 MUS 模型实现跨社交网络用户对齐。将用户昵称、生日等用户属性表示为向量，文献 [62] 提出 VBCA 算法进行跨社交网络用户对齐。结合用户名的独特性，文献 [63] 提出能够实现跨社交网络用户对齐的 EUU 模型。

虽然文本属性较易获取，但文本属性在不同社交网络之间存在较大差异，因此仅利用文本属性难以很好地实现跨社交网络用户对齐。与此同时，用户在社交网络中的结构特征能够表示用户之间的关系，这也为基于规则的跨社交网络用户识别提供了新的思路。文献 [64] 提出基于最大公共子图的迭代式算法 MCS_INA 实现跨社交网络用户对齐。由于社交网络中用户之间的关系十分复杂，且通常难以获取大规模社交网络的完整结构信息，仅仅利用社交网络结构难以很好实现跨社交网络用户对齐。因此，研究者们开始尝试综合利用网络结构与文本属性，进行基于规则的跨社交网络用户对齐。通过比较朋友列表，文献 [65] 提出 FLDPL 模型实现跨社交网络用户对齐。通过定义用户的动态核心兴趣，文献 [66] 提出 DCIM 算法进行跨社交网络用户对齐。

在基于传播规则的跨社交网络用户对齐中，传播表现为迭代，即结合网络结构和已匹配的用户信息迭代地发现新匹配用户。

文献 [18] 提出 DASN 模型，该模型通过迭代搜索具有相同度数和邻居数的 k 团 (k-clique) 实现跨社交网络用户对齐。基于共同邻居计数规则，文献 [67] 提出 User-Matching 算法实现迭代的跨社交网络用户对齐。利用用户的朋友关系，文献 [68] 提出 FRUI 算法迭代地实现跨社交网络用户对齐。

考虑到社交网络结构的复杂性，部分研究结合文本属性和网络拓扑结构实现基于传播的跨社交网络用户对齐。文献 [69] 提出 MED 模型，该模型综合考虑账号属性相似性和网络结构相似性。结合网络结构和公开账号属性，文献 [70] 提出 MPSN 模型实现跨社交网络用户对齐。综合利用账号属性相似度和网络结构相似度，文献 [71] 提出 UALI 模型进行跨社交网络用户对齐。结合网络结构的链接信息和账号属性，文献 [72] 提出 CLA 算法，该算法能够实现有效的跨社交网络用户对齐。

4.2.3 基于传统机器学习的跨社交网络用户对齐

随着机器学习的快速发展，大量机器学习方法被应用于跨社交网络用户对齐中，并取得了很好的效果。

按照标记数据的数量，基于传统机器学习的跨

社交网络用户对齐可分为 3 类：基于监督学习的跨社交网络用户对齐、基于无监督学习的跨社交网络用户对齐及基于半监督学习的跨社交网络用户对齐。

基于监督学习的跨社交网络用户对齐方法需要提供将预先已匹配用户对作为监督学习的标记数据，这类方法通常将跨社交网络用户对齐转换为分类问题。

文献 [73] 提出 ISY 模型，该模型综合考虑用户名、教育背景等属性，并利用提升 (boosting) 技术整合弱分类器。通过分析用户名体现的用户行为特性，文献 [74] 提出结合监督学习的 MOBIUS 模型。利用用户名、地点等属性，文献 [75] 提出 OPL 模型，该模型以监督学习的方式实现跨社交网络用户对齐。综合考虑用户的 k-跳朋友和显示名字，文献 [76] 提出结合有监督机器学习的 UI-FR 和 UI-FRName 模型。将用户属性和网络结构进行结合，文献 [77] 提出 JLA 模型进行有监督的跨社交网络用户对齐。充分考虑用户名及其他账号属性、社交网络结构，并结合有监督的机器学习，文献 [78] 提出 EMOSN 模型实现跨社交网络用户对齐。

基于无监督学习的跨社交网络用户对齐缺乏标记数据，该类方法可通过手动设置规则进而转换为基于监督学习的跨社交网络用户对齐，或者结合无监督的表示学习和对齐算法实现跨社交网络用户对齐。

结合用户名的稀有性，文献 [79] 提出一个能够自动标记训练样本的无监督学习模型，并将其记为 Model 2。利用用户名独特性等一系列自定义规则自动生成标记数据，文献 [80] 提出无监督学习框架 CoLink 进行跨社交网络用户对齐。为了识别多个社交网络之间的共享账号，文献 [81] 提出无监督框架 UMA。文献 [82] 提出 UUIL 模型，该模型从分布层面进行跨社交网络用户对齐。

相比于基于监督学习的跨社交网络用户对齐方法，基于无监督学习的跨社交网络用户对齐方法由于缺乏标记数据，导致其性能较低。基于半监督学习的跨社交网络用户对齐能够充分利用少量标记数据和大量无标记数据，获取数据潜在分布，进而提升跨社交网络用户对齐性能。

综合匹配用户属性与网络结构，融合全局一致性匹配，文献 [83] 提出半监督模型 COSNET。

深入挖掘文本和图像等属性，文献 [6] 提出半监督的多目标优化框架 HYDRA 实现跨社交网络用户对齐。利用超图学习用户之间的高阶关系，文献 [59] 提出半监督模型 MAH 进行跨社交网络用户对齐。综合特征提取和网络对齐，文献 [84] 提出半监督框架 SSF 实现跨社交网络用户对齐。

4.2.4　基于深度学习的跨社交网络用户对齐

近年来，基于深度学习的跨社交网络用户对齐方法得到广泛关注。深度学习能够很好地表示社交网络结构，基于深度学习的方法进一步提升了跨社交网络用户对齐性能。

通过学习用户关注或粉丝关系对应的网络嵌入，文献 [85] 提出 IONE 模型实现了跨社交网络用户对齐。将深度强化学习和半监督学习进行结合，文献 [86] 提出 DeepLink 模型进行跨社交网络用户对齐。将跨平台同构性作为用户身份对齐的补充，文献 [87] 提出半监督的跨社交网络用户对齐模型，并将其命名为 MSUIL。

由于不同社交网络平台中用户信息、网络结构等存在较大差异，基于社交网络同构假设的跨社交网络用户对齐方法难以捕捉该差异性。近年来，基于异构图和异构数据的跨社交网络用户对齐受到广泛关注。在异构图的背景下，文献 [88] 提出半监督的 dNAME 模型实现跨社交网络用户对齐。将异构社交网络中的用户及其交互行为嵌入到统一的低维空间，文献 [89] 提出 TransLink 模型进行跨社交网络用户对齐。考虑到用户行为数据具有异构性，文献 [90] 结合深度神经网络提出 DPLink 模型实现跨社交网络用户对齐。

5　面临的挑战及未来研究方向

本章将详细阐述当前用户身份识别技术面临的挑战，并对未来的可行研究方向作出展望。

5.1　用户身份识别面临的挑战

目前，传统的用户身份识别算法取得了一定进展，尤其是机器人水军识别、目标社区检测和跨社交网络用户对齐都引起了研究人员的极大兴趣。然而，仍然存在许多挑战，主要体现在数据关联挖掘、特征模型训练和复杂场景建模这 3 个方面。

5.1.1　海量用户数据的关联挖掘

在挖掘网络用户产生的海量数据时，不同用户实体间的相互关联复杂且隐蔽。而且社交网络出于对用户隐私的保护，电话号码、Email 地址等较为敏感的用户信息往往不对外公开，同时、不同实体之间通过相互关联形成复杂的关系图，产生大量结构化与非结构化数据，加大了关联关系的挖掘难度，因此对身份识别技术提出了新的挑战。

5.1.2 特征模型的训练

在机器人水军识别方面，采用在线分析方法时，分析速率除了受算法本身效率影响外，还与数据传输速率和接受窗口大小有关，这使得分析和扩展性较差。目标社区检测方面，传统的社区检测方法不能有效解决高维度和多样性特征的网络结构问题，可能会陷入局部最优解情况，从而无法检测社交网络中的“水军社区”，同时当前的目标社区检测算法侧重于提高模型的有效性，忽略了其在时间复杂度和空间复杂度方面的效率。跨社交网络用户对齐目前使用的迁移学习算法适用于完全重叠或完全不重叠情况，在面对部分重叠场景时受到样本数目的巨大影响，难以确保在当前社交网络环境下身份识别的精准性。

5.1.3 复杂社交网络场景的建模

传统的用户身份识别的提出通常针对小规模数据集和一些简化的场景，无法有效适用于大型的社交网络，如面对数据量大、数据类型及结构类型多样的复杂场景，难以捕捉用户之间潜在语义关系来获取用户表征。现实世界的多个社交网络很可能发生部分重叠，且随时间快速演化，严重影响了模型的有效性和可扩展性。因此，需要针对这些新场景进行有效建模，尤其是要考虑其演化特征。

5.2 研究展望

鉴于传统模型难以满足日益增长的应用需求，亟需探索适用性广、拓展性强、准确高效的用户身份识别新方法。本节从五个方面对未来用户身份识别研究进行展望。

5.2.1 基于多视角融合的用户身份识别

随着社交网络复杂度越来越高，用户数据量越来越庞大，用户所拥有的特征属性也不断增多。用户身份识别过程中所需的数据集往往很庞大，很难提取到用户身份识别任务所需的全部特征，虽然当前部分研究工作综合考虑了多方面的用户特征，但构建用户身份识别模型时使用的特征量仍然较小。因此，未来可采用多视角融合的技术进行用户身份识别。该技术可以从不同特征切入，如该用户的词汇特征、句法特征、账户特征、网络特征、行为特征等，以此来构建较完整的用户身份识别特征体系以确保用户身份识别的有效性。

5.2.2 基于集成学习的用户身份识别

集成学习框架通过组合多个弱监督模型以得到一个更好更全面的强监督模型，该框架在容错性和数据集规模方面具有较强优势。在集成学习框架中，即使某个弱分类器得到了错误的预测，其他弱分类器也能纠正错误。同时，它在各个规模的数据集上都有较好的策略。因此，未来用户身份识别研究可采用集成学习的方法，通过筛选出多个有效的个体学习器，采用合理的组合方式，最终实现用户身份识别的高效准确。

5.2.3 基于模型优化的用户身份识别

现有用户身份识别算法通常旨在提升识别的准确率，而忽略了算法的时间复杂度和空间复杂度，因此算法往往效率不高。而且社交网络环境是动态的，其对应的数据分析具有时间敏感性。如果算法不能及时识别用户身份，可能错过有效管控信息传播的最佳时间。因此，未来的用户身份识别算法需要降低模型复杂度，并进一步提高效率。为此，可以探索将模型参数优化、模型结构自动定义、降维等模型优化的方法应用于用户身份识别模型构建中，以此节省用户身份识别所需的计算成本。

5.2.4 基于心理认知的用户身份识别

用户在社交网络空间的思维活动体现了用户的心理，而人的心理通常由人格因素和人的身份属性两因素决定，前者决定了人的不同行为，后者是人心理活动最核心的内容。反之，从社交网络用户的心理可以洞察用户的身份属性。因此，未来可以充分利用心理学方面的研究成果，从心理认知的角度对用户身份属性进行预测，进一步提升身份识别精度。

5.2.5 面向新应用场景的用户身份识别

网络治理作为维护国家安全稳定的重要组成部分，不仅可以有效打击线上犯罪团伙，还可以配合公安巡检部门基于网络关联信息对在逃嫌犯开展追逃工作。同时，加强迅速锁定网络舆情战威胁来源的能力，有利于监管部门及时做出相应的反制措施。另一方面，在民用领域实现用户身份的精准识别，可以提高社交网络平台对于事件真实热度、蓄意煽动等不良行为的把控能力，提升部分高危网络用户进行恶意炒作法律法规或道德底线人员的永久线上封禁，最大程度维护网络环境的健康性，提升网络用户的社交体验。总之，随着信息技术的发展，新的应用场景会不断涌现，需要发展新的身份识别技术。

6 结 束 语

用户身份识别为社交网络平台提供精准服务、

实施高效监管奠定了坚实基础，也为维护国家安全、网络空间安全、推进意识形态建设提供了重要保障。本文对用户身份识别的研究工作和应用现状进行了阐述、分析和总结，从用户身份识别的基本概念出发，系统地介绍了现有的三大主要应用领域，即机器人水军识别、目标社区检测和跨社交网络用户对齐。此外，结合当前研究进展，本文对用户身份识别的未来研究方向作出了展望。希望本文能够为用户身份识别领域研究提供理论指导和创新思路。

参　考　文　献

[1] 张树森, 梁循, 弭宝瞳, 等. 基于内容的社交网络用户身份识别方法[J]. 计算机学报, 2019, 42(8): 1739-1754.
ZHANG S S, LIANG X, MI B T, et al. Content-Based social network user identification methods[J]. Chinese Journal of Computers, 2019, 42(8): 1739-1754.

[2] ZAFARANI R, LIU H. Connecting corresponding identities across communities[C]//Proceedings of the 3rd International Conference on Weblogs and Social Media. California: The AAAI, 2009, 3(1): 354-357.

[3] RAAD E, CHBEIR R, DIPANDA A. User profile matching in social networks[C]//Proceedings-13th International Conference on Network-Based Information Systems, Washington: IEEE, 2010: 297-304.

[4] ALMISHARI M, TSUDIK G. Exploring linkability of user reviews[M]//Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2012: 307-324.

[5] GOGA O, PERITO D, LEI H, et al. Large-Scale correlation of accounts across social networks[R]. Berkeley: University of California at Berkeley, 2013.

[6] LIU S, WANG S, ZHU F, et al. HYDRA: Large-scale social identity linkage via heterogeneous behavior modeling [C]//Proceedings of the ACM SIGMOD International Conference on Management of Data. [S. l.]: ACM, 2014: 51-62.

[7] SHA Y, LIANG Q, ZHENG K. Matching user accounts across social networks based on users message[J]. Procedia Computer Science, 2016, 80: 2423-2427.

[8] 吴铮, 于洪涛, 刘树新, 等. 基于信息熵的跨社交网络用户身份识别方法[J]. 计算机应用, 2017, 37(8): 2374-2380.
WU Z, YU H T, LIU S X, et al. User identification across multiple social networks based on information entropy[J]. Journal of Computer Applications, 2017, 37(8): 2374-2380.

[9] ZHANG S S, LIANG X, ZHANG X, et al. On identification of organizational and individual users based on social content measurements[J]. IEEE Transactions on Computational Social Systems, 2018, 5(4): 961-972.

[10] LI Y, PENG Y, ZHANG Z, et al. Matching user accounts across social networks based on username and display name[J]. World Wide Web, 2019, 22(3): 1075-1097.

[11] XING L, DENG K K, WU H H, et al. Exploiting two-level information entropy across social networks for user identification[J]. Wireless Communications and Mobile Computing, 2021: 1082391.

[12] WANG Y, LIU T, TAN Q, et al. Identifying users across different sites using usernames[J]. Procedia Computer Science, 2016, 80: 376-385.

[13] CORTIS K, SCERRI S, RIVERA I, et al. An ontology-based technique for online profile resolution[C]// International Conference on Social Informatics. Cham: Springer, 2013: 284-298.

[14] ACQUISTI A, GROSS R, STUTZMAN F. Face recognition and privacy in the age of augmented reality[J]. Journal of Privacy and Confidentiality, 2014, 6(2): 1-20.

[15] 王蕴红, 朱勇, 谭铁牛. 基于虹膜识别的身份鉴别[J]. 自动化学报, 2002, 28(1): 1-10.
WANG Y H, ZHU Y, TAN T N. Biometrics personal identification based on iris pattern[J]. Acta Automatica Sinica, 2002, 28(1): 1-10.

[16] 王亮, 胡卫明, 谭铁牛. 基于步态的身份识别[J]. 计算机学报, 2003(3): 353-360.
WANG L, HU W M, TAN T N. Gait-Based human identification[J]. Chinese Journal of Computers, 2003(3): 353-360.

[17] BRAINARD J, JUELS A, RIVEST R L, et al. Fourth-Factor authentication: Somebody you know[C]// Proceedings of the ACM Conference on Computer and Communications Security. New York: ACM, 2006: 168-178.

[18] NARAYANAN A, SHMATIKOV V. De-anonymizing social networks[C]//2009 30th IEEE Symposium on Security and Privacy. [S.l.]: IEEE, 2009: 173-187.

[19] CUI Y, PEI J, TANG G, et al. Finding email correspondents in online social networks[J]. World Wide Web, 2013, 16(2): 195-218.

[20] ZHOU X, LIANG X, DU X, et al. Structure based user identification across social networks[J]. IEEE Transactions on Knowledge and Data Engineering, 2018, 30(6): 1178-1191.

[21] LI M, CAI L, YU A, et al. HeteroUI: A framework based on heterogeneous information network embedding for user identification in enterprise networks[C]//International Conference on Information and Communications Security. Cham: Springer, 2019: 165-180.

[22] KONG X, ZHANG J, YU P S. Inferring anchor links across multiple heterogeneous social networks[C]// Proceedings of the 22nd ACM international conference on Information & Knowledge Management. [S.l.]: ACM, 2013: 179-188.

[23] CAO W, WU Z, WANG D, et al. Automatic user identification method across heterogeneous mobility data sources[C]//2016 IEEE 32nd International Conference on Data Engineering (ICDE). [S.l.]: IEEE, 2016: 978-989.

[24] HAN X, WANG L, XU S, et al. Linking social network accounts by modeling user spatiotemporal habits[C]//2017 IEEE International Conference on Intelligence and Security Informatics (ISI). [S.l.]: IEEE, 2017: 19-24.

[25] RIEDERER C, KIM Y, CHAINTREAU A, et al. Linking

users across domains with location data: Theory and validation[C]//Proceedings of the 25th International Conference on World Wide Web. Canada: [s.n.] 2016: 707-719.

[26] HAN X, WANG L, XU L, et al. Social media account linkage using user-generated geo-location data[C]//2016 IEEE Conference on Intelligence and Security Informatics (ISI). [S.l.]: IEEE, 2016: 157-162.

[27] CHAVOSHI N, HAMOONI H, MUEEN A. DeBot: Twitter bot detection via warped correlation[C]//2016 IEEE 16th International Conference on Data Mining (ICDM). [S.l.]: IEEE, 2016: 817-822.

[28] CAI C, LI L, ZENGI D. Behavior enhanced deep bot detection in social media[C]//2017 IEEE International Conference on Intelligence and Security Informatics: Security and Big Data. [S.l.]: IEEE, 2017: 128-130.

[29] JIN D, TENG J Q. Study of bot detection on Sina-Weibo based on machine learning[C]//2017 International Conference on Service Systems and Service Management. [S.l.]: IEEE, 2017: 1-5.

[30] EFTHIMION P G, PAYNE S, PROFERES N. Supervised machine learning bot detection techniques to identify social twitter bots[J]. SMU Data Science Review, 2018, 1(2): 5.

[31] ABOU DAYA A, SALAHUDDIN M A, LIMAM N, et al. A graph-based machine learning approach for bot detection[C]//2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM). [S. l.]: IEEE, 2019: 144-152.

[32] GILANI Z, WANG L, CROWCROFT J, et al. Stweeler: A framework for twitter bot analysis[C]//Proceedings of the 25th International Conference Companion on World Wide Web. Canada: [s.n.], 2016: 37-38.

[33] ALAHMADI B A, MARICONTI E, SPOLAOR R, et al. BOTection: Bot detection by building Markov Chain models of bots network behavior[C]//Proceedings of the 15th ACM Asia Conference on Computer and Communications Security. [S.l.]: ACM, 2020: 652-664.

[34] KOGGALAHEWA D, XU Y, FOO E. An unsupervised method for social network spammer detection based on user information interests[J]. Journal of Big Data, 2022, 9(1): 1-35.

[35] DAOUADI K E, REBAÏ R Z, AMOUS I. Bot detection on online social networks using deep forest[C]//Computer science on-line conference. Cham: Springer, 2019: 307-315.

[36] YIN J, LI Q, LIU S, et al. Leveraging multi-level dependency of relational sequences for social spammer detection[J]. Neurocomputing, 2021, 428: 130-141.

[37] GUO Z, TANG L, GUO T, et al. Deep graph neural network-based spammer detection under the perspective of heterogeneous cyberspace[J]. Future Generation Computer Systems, 2021, 117: 205-218.

[38] LEE K, CAVERLEE J, WEBB S. Uncovering social spammers: social honeypots+ machine learning[C]// Proceedings of the 33rd International ACM SIGIR Conference on Research and Development in Information Retrieval. [S.l.]: ACM, 2010: 435-442.

[39] MATEEN M, IQBAL M A, ALEEM M, et al. A hybrid approach for spam detection for Twitter[C]//2017 14th International Bhurban Conference on Applied Sciences and Technology (IBCAST). [S. l.]: IEEE, 2017: 466-471.

[40] SRIRAM B, FUHRY D, DEMIR E, et al. Short text classification in twitter to improve information filtering[C]//Proceedings of the 33rd International ACM SIGIR Conference on Research and Development in Information Retrieval. [S.l.]: ACM, 2010: 841-842.

[41] LIU B. Sentiment analysis and subjectivity[J]. Handbook of Natural Language Processing, 2010(2): 627-666.

[42] BHAT V H, MALKANI V R, SHENOY P D, et al. Classification of email using BeaKS: Behavior and keyword stemming[C]//IEEE Region 10 Annual International Conference, Proceedings/TENCON. [S.l.]: IEEE, 2011: 1139-1143.

[43] HUSNA H, PHITHAKKITNUKOON S, PALLA S, et al. Behavior analysis of spam botnets[C]//2008 3rd International Conference on Communication Systems Software and Middleware and Workshops. [S.l.]: IEEE, 2008: 246-253.

[44] LINGAM G, ROUT R R, SOMAYAJULU D V L N, et al. Social botnet community detection: A novel approach based on behavioral similarity in twitter network using deep learning[C]//Proceedings of the 15th ACM Asia Conference on Computer and Communications Security. [S.l.]: ACM, 2020: 708-718.

[45] BENEVENUTO F, RODRIGUES T, ALMEIDA V, et al. Identifying video spammers in online social networks[C]//Proceedings of the 4th International Workshop on Adversarial Information Retrieval on the Web. [S.l.]: ACM, 2008: 45-52.

[46] SONG J, LEE S, KIM J. Spam filtering in twitter using sender-receiver relationship[C]//International Workshop on Recent Advances in Intrusion Detection. Berlin, Heidelberg: Springer, 2011: 301-317.

[47] JIANG J Q, DRESS A W M, YANG G. A spectral clustering-based framework for detecting community structures in complex networks[J]. Applied Mathematics Letters, 2009, 22(9): 1479-1482.

[48] LI C, BAI J, WENJUN Z, et al. Community detection using hierarchical clustering based on edge-weighted similarity in cloud environment[J]. Information Processing & Management, 2019, 56(1): 91-109.

[49] LAS-CASAS P H B, GUEDES D, ALMEIDA J M, et al. SpaDeS: Detecting spammers at the source network[J]. Computer Networks, 2013, 57(2): 526-539.

[50] 吴信东, 李毅, 李磊. 在线社交网络影响力分析[J]. 计算机学报, 2014, 37(4): 735-752.
WU X D, LI Y, LI L. Influence analysis of online social networks[J]. Chinese Journal of Computers, 2014, 37(4): 735-752.

[51] NI Q, GUO J, WU W et al. Continuous influence-based community partition for social networks[J]. IEEE Transactions on Network Science and Engineering, 2021(8): 1-9.

[52] GAYO AVELLO D, BRENES MARTÍNEZ, D J. Overcoming spammers in Twitter: A tale of five algorithms[C]//CERI. Madrid: [s. n.], 2010: 41-52.
[53] WANG R, ZHANG W, DENG H, et al. Discover community leader in social network with PageRank[C]//International Conference in Swarm Intelligence. Berlin, Heidelberg: Springer, 2013: 154-162.
[54] BENEVENUTO F, MAGNO G, RODRIGUES T, et al. Detecting spammers on Twitter[C]//Collaboration, Electronic Messaging, Anti-Abuse and Spam Conference (CEAS). Washington: ACM, 2010: 12.
[55] CHEN C, WU K, SRINIVASAN V, et al. Battling the internet water army: Detection of hidden paid posters[C]//2013 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2013). [S.l.]: IEEE, 2013: 116-120.
[56] FANI H, BAGHERI E. Community detection in social networks[J].Encyclopedia with Semantic Computing and Robotic Intelligence, 2017, 1: 1630001.
[57] AHN Y Y, BAGROW J P, LEHMANN S. Link communities reveal multiscale complexity in networks[J]. Nature, 2010, 466(7307): 761-764.
[58] GUO X, LIU Y, LIU L, et al. User identity linkage across social networks via community preserving network embedding[C]//Australasian Conference on Information Security and Privacy. Cham: Springer, 2020: 621-630.
[59] TAN S, GUAN Z, CAI D, et al. Mapping users across networks by manifold alignment on hypergraph[C]// Proceedings of the AAAI Conference on Artificial Intelligence. [S.l.]: AAAI, 2014: 159-165.
[60] SHU K, WANG S, TANG J, et al. User identity linkage across online social networks: A review[C]//ACM SIGKDD Explorations Newsletter. [S.l.]: ACM, 2017, 18(2): 5-17.
[61] IOFCIU T, FANKHAUSER P, ABEL F, et al. Identifying users across social tagging systems[C]//Proceedings of the International AAAI Conference on Web and Social Media. [S.l.]: AAAI, 2011, 5(1): 522-525.
[62] VOSECKY J, HONG D, SHEN V Y. User identification across multiple social networks[C]//2009 the 1st International Conference on Networked Digital Technologies. [S.l.]: IEEE, 2009: 360-365.
[63] PERITO D, CASTELLUCCIA C, KAAFAR M A, et al. How unique and traceable are usernames?[C]//International Symposium on Privacy Enhancing Technologies Symposium. Berlin, Heidelberg: Springer, 2011: 1-17.
[64] 冯朔, 申德荣, 聂铁铮, 等. 一种基于最大公共子图的社交网络对齐方法[J]. 软件学报, 2019, 30(7): 2175-2187.
FENG S, SHEN D R, NIE T Z, et al. Maximum common subgraph based social network alignment method[J]. Journal of Software, 2019, 30(7): 2175-2187.
[65] LABITZKE S, TARANU I, HARTENSTEIN H. What your friends tell others about you: Low cost linkability of social network profiles[C]//Proc 5th International ACM Workshop on Social Network Mining and Analysis. San Diego: ACM, 2011: 1065-1070.
[66] NIE Y, JIA Y, LI S, et al. Neurocomputing identifying users across social networks based on dynamic core interests[J]. Neurocomputing, 2016, 210: 107-115.
[67] KORULA N, LATTANZI S. An efficient reconciliation algorithm for social networks[J]. Proceedings of the VLDB Endowment, 2014, 7(5): 377-388.
[68] ZHOU X, LIANG X, ZHANG H et al. Cross-Platform identification of anonymous identical users in multiple social media networks[J]. IEEE Transactions on Knowledge and Data Engineering, 2016, 28(2): 411-424.
[69] BUCCAFURRI F, LAX G, NOCERA A, et al. Discovering links among social networks[C]//Joint European Conference on Machine Learning and Knowledge Discovery in Databases. Berlin, Heidelberg: Springer, 2012: 467-482.
[70] BENNACER N, NANA JIPMO C, PENTA A, et al. Matching user profiles across social networks[C]// International Conference on Advanced Information Systems Engineering. Cham, Springer, 2014: 424-438.
[71] SHEN Y, JIN H. Controllable information sharing for user accounts linkage across multiple online social networks[C]//Proceedings of the 23rd ACM International Conference on Conference on Information and Knowledge Management. [S.l.]: ACM, 2014: 381-390.
[72] 王李冬, 胡克用, 周微微, 等. 基于 CLA 算法的跨社交平台用户身份匹配[J]. 计算机应用与软件, 2019, 36(4): 217-222.
WANG L D, HU K Y, ZHOU W W, et al. Cross-Social platform user identification based on cla algorithm[J]. Computer Applications and Software, 2019, 36(4): 217-222.
[73] MOTOYAMA M, VARGHESE G. I seek you: Searching and matching individuals in social networks[C]// Proceedings of the 11th International Workshop on Web Information and Data Management. [S. l.]: ACM, 2009: 67-75.
[74] ZAFARANI R, LIU H. Connecting users across social media sites: A behavioral-modeling approach[C]// Proceedings of the 19th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. [S.l.]: ACM, 2013: 41-49.
[75] ZHANG H, KAN M Y, LIU Y, et al. Online social network profile linkage[C]//Asia Information Retrieval Symposium. Cham: Springer, 2014: 197-208.
[76] LI Y, SU Z, YANG J, et al. Exploiting similarities of user friendship networks across social networks for user identification[J]. Information Sciences, 2020, 506: 78-98.
[77] BARTUNOV S, KORSHUNOV A, PARK S T, et al. Joint link-attribute user identity resolution in online social networks[C]//Proceedings of the 6th International Conference on Knowledge Discovery and Data Mining, Workshop on Social Network Mining and Analysis. [S.l.]: ACM. 2012: 1-9.
[78] PELED O, FIRE M, ROKACH L, et al. Entity matching in online social networks[C]//2013 International Conference on Social Computing. [S.l.]: IEEE, 2013: 339-344.
[79] LIU J, ZHANG F, SONG X, et al. What's in a name? An unsupervised approach to link users across

communities[C]//Proceedings of the 6th ACM International Conference on Web Search and Data Mining. [S. l.]: ACM, 2013: 495-504.

[80] ZHONG Z, CAO Y, GUO M, et al. Colink: An unsupervised framework for user identity linkage [C]//Proceedings of the AAAI Conference on Artificial Intelligence. [S. l.]: ACM, 2018: 5714-5721.

[81] ZHANG J, PHILIP S Y. Multiple anonymized social networks alignment[C]//2015 IEEE International Conference on Data Mining. [S. l.]: IEEE, 2015: 599-608.

[82] LI C, WANG S, YU P S, et al. Distribution distance minimization for unsupervised user identity linkage[C]//Proceedings of the 27th ACM International Conference on Information and Knowledge Management. [S. l.]: ACM, 2018: 447-456.

[83] ZHANG Y, TANG J, YANG Z, et al. Cosnet: Connecting heterogeneous social networks with local and global consistency[C]//Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. [S. l.]: ACM, 2015: 1485-1494.

[84] HU Z, WANG J, CHEN S, et al. A semi-supervised framework with efficient feature extraction and network alignment for user identity linkage[C]//International Conference on Database Systems for Advanced Applications. Cham, Springer, 2021: 675-691.

[85] LIU L, CHEUNsG W K, LI X, et al. Aligning users across social networks using network embedding [C]//International Joint Conference on Artificial Intelligence. New York: IJCAI, 2016: 1774-1780.

[86] ZHOU F, LIU L, ZHANG K, et al. Deeplink: A deep learning approach for user identity linkage[C]//IEEE INFOCOM 2018-IEEE Conference on Computer Communications. [S. l.]: IEEE, 2018: 1313-1321.

[87] LI C, WANG S, WANG H, et al. Partially shared adversarial learning for semi-supervised multi-platform user identity linkage[C]//Proceedings of the 28th ACM International Conference on Information and Knowledge Management. [S. l.]: ACM, 2019: 249-258.

[88] ZHOU F, WEN Z, TRAJCEVSKI G, et al. Disentangled network alignment with matching explainability[C]//IEEE INFOCOM 2019-IEEE Conference on Computer Communications. [S. l.]: IEEE, 2019: 1360-1368.

[89] ZHOU J, FAN J. Translink: User identity linkage across heterogeneous social networks via translating embeddings[C]//IEEE INFOCOM 2019-IEEE Conference on Computer Communications. [S. l.]: IEEE, 2019: 2116-2124.

[90] FENG J, ZHANG M, WANG H, et al. Dplink: User identity linkage via deep neural network from heterogeneous mobility data[C]//The World Wide Web Conference. [S. l.]: ACM, 2019: 459-469.

编 辑 蒋 晓