步态识别数据安全标准化研究

李 强[1] 刘麒赟[1] 宋立峰[2] 程少龙[3] 林 清[4] 张 娅[5]

（1.银河水滴科技（北京）有限公司；2. 山东省公安厅科技安全中心；3. 山东省公安厅信息通信处四支队；4.中山市公安局刑警支队；5.宜宾职业技术学院电子信息与人工智能学院）

摘　要：步态识别是基于步态所包含的自然人生物学特性和行为特性对自然人进行辨识的技术，其物理基础是人类个体不同的生理结构和行走习惯。目前，步态识别技术已在学术和商业化应用方面取得了巨大发展。步态识别数据作为一种重要的生物特征数据，目前存在着数据滥采滥用、未采用有效的安全防范措施等突出问题。本文通过分析解读国内第一部步态识别数据国家标准，旨在让步态识别数据相关方了解步态识别数据处理活动、安全风险和安全要求，进一步提高步态识别产品和服务的整体安全水平。

关键词：步态识别，数据安全，数据处理活动，应用场景

DOI编码：10.3969/j.issn.1674-5698.2023.04.010

Research on Standardization of Security of Gait Recognition Data

LI Qiang[1] LIU Qi-yun[1] SONG Li-feng[2] CHENG Shao-long[3] LIN Qing[4] ZHANG Ya[5]

(1. Watrix Technology Co., Ltd.; 2. Center for Science and Technology Security of Public Security Department of Shandong Province; 3. The Fourth Detachment of Department of Information and Communication, Public Security Department of Shandong Province; 4. Criminal Investigation Detachment of Zhongshan Public Security Bureau; 5. School of Electronic Information and Artificial Intelligence, Yibin Vocational and Technical College)

Abstract: Gait recognition refers to the analysis of human identity by identifying people's body shape and walking posture, and its physical basis is the different physiological structure and walking habits of each person. At present, gait recognition technology has made great progress in academic and commercial applications. Gait recognition data, as an important biometric data, currently has prominent problems such as data indiscriminate collection and abuse, and failure to adopt effective security precautions. This paper analyzes the first Chinese national standard for gait recognition data, aiming to make gait recognition data stakeholders understand gait recognition data processing activities, security risks and security requirements, and further improve the overall security level of gait recognition related products and services.

Keywords: gait recognition, data security, data processing activities, application scenarios

作者简介：李强，标准化主管，高级工程师，博士，研究方向为多媒体信息处理、信息技术标准化。

刘麒赟，副总裁，工程师，硕士，研究方向为软件工程与大数据。

宋立峰，山东省公安厅科技安全中心主任，正高级工程师，研究方向为警务信息技术。

程少龙，山东省公安厅信息通信处四支队四级高级警长，工程师，硕士，研究方向为计算机工程与技术。

林清，四级主管，高级工程师，硕士，研究方向为影像检验、视频结构化研究。

张娅，宜宾职业技术学院电子信息与人工智能学院院长，副教授，软件工程硕士，研究方向为计算机软件、人工智能。

1 引言

步态识别是生物识别技术中无直接接触的情况下长距离识别人的重要指标。当一个人行走时，可以观察到约24个单独的参数和运动[1]，这些参数和运动形成了步态的独特性。随着计算机视觉（CV）技术的发展，可以通过视频中自然人的生物特征（人体骨骼，轮廓，行走时的变化）和抽象特征来识别，步态识别系统利用CV算法，识别人的形状及其移动方式，检测视频中的人形轮廓并分析其运动。这些数据共同创建了步态行为模型。

步态识别相关研究始于2000年，美国国防部高级研究计划局和中国科学院自动化研究所同时开始步态识别的研究，发展至今，我国的步态识别技术水平在世界范围内已居首位。近年来，在国家和行业政策推动下，步态识别逐渐走向实际应用，例如：在公共安全领域，基于视频监控，可以迅速发现特定人员，预防危险事件发生；在康养领域，可以用于疗养院，以便在患者跌倒时提醒工作人员；在医疗领域，可以帮助诊断神经系统疾病并计划康复治疗；此外，在科教文体、智能家居等领域中,步态识别也有适合的应用场景。

国内对于生物特征数据安全已有相关法律规定。我国立法与司法在保护个人生物识别信息权利的基础上，确立了以风险预防及利益平衡理念和原则为引导，对个人生物信息安全法实行多层次、等级化和体系化的法律保护，构建个人生物信息安全的法律法规体系[2]。《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》中规定了生物特征、敏感信息、个人数据的强制性要求，明确了个人信息保护原则是个人生物识别信息利用的最基本规则。在上位法律法规的指引下，国家陆续出台了GB/T 35273–2020《信息安全技术 个人信息安全规范》、GB/T 37973–2019《信息安全技术 大数据安全管理指南》等标准，较宽泛地约束了数据安全管理要求。

在细分领域标准化方面，现有大部分生物特征识别标准涉及指纹识别、虹膜识别、人脸识别，内容包含生物特征数据交换格式、图像数据质量、设备等。相较指纹识别、虹膜识别、人脸识别等生物特征识别技术，步态识别技术起步相对较晚，标准化程度也相对滞后，根据“全国标准信息公共服务平台”，截至2020年，在信息化领域，没有“步态识别”相关标准。

当前，步态识别数据存在滥采滥用、未采用有效的安全防范措施等突出问题，个人的合法权益和社会公共利益不时受到侵害。为了解决这一问题，2020年12月–2022年11月，银河水滴科技（北京）有限公司联合国内20余家单位联合负责编制了国内第一部步态识别领域数据安全国家标准GB/T 41773–2022《信息安全技术 步态识别数据安全要求》，围绕个人信息处理的最小必要原则，从规范个人信息控制者在收集、保存、使用、共享、转让、公开披露等信息处理环节中的相关行为出发，规定了步态识别数据收集、存储、传输、使用、加工、提供、公开、删除等数据全生命周期处理活动的安全要求，同时给出了身份识别、非身份识别、科学研究3种场景下的步态识别活动及其风险，为不同的步态识别数据处理者规范数据处理活动，监管部门、第三方评估机构对步态识别数据处理活动进行监督、管理、评估提供了标准依据。

本文以《信息安全技术 步态识别数据安全要求》为基础，介绍步态识别的基本概念、步态数据处理活动和主要风险以及不同场景下的步态识别数据活动和安全要求。

2 概述

与其他生物特征识别算法一样，步态识别的基础为步态数据，通常是使用多个源或采集设备（摄像机、运动传感器等）来获取数据。采集的数据经过多个识别步骤，一般的步态识别过程如图1所示。利用步态识别算法处理接收到的数据，通过轮廓检测、人形分割获得单个人的特征，然后特征提取算法提取步态信息，并有效区分不同的步态。步态识别算法在处理视频数据和传感器数据时会有所不同。

借助大数据和机器学习技术，可以根据获得的数据和模型改进识别系统。通过大量的步态数据学习和建模，能够提升步态识别模型的识别精度和泛化能力，因此，当处理相似的步态时，经过训练的模

型和算法可以分离细微的细节并将其输入数据库，可以获得更好的识别结果。

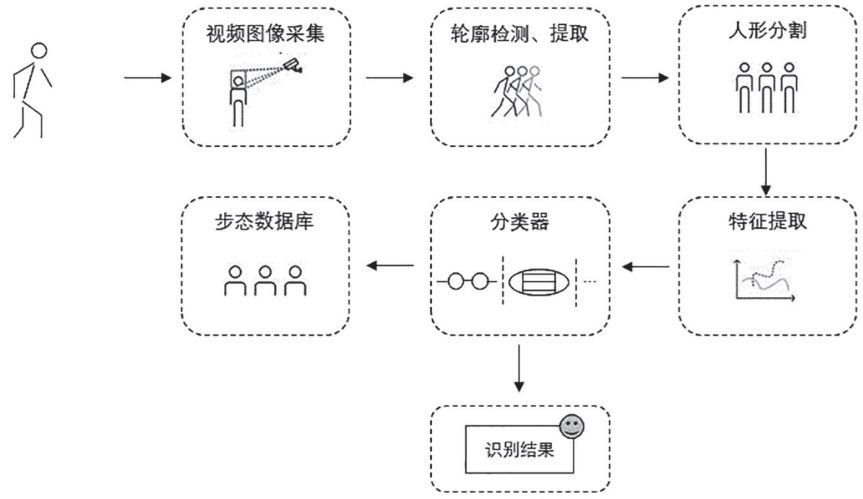

图1 步态识别示意图

由于步态识别技术的易用性，仅利用常规的监控摄像头即可进行数据获取和身份识别，越来越多的组织可以低成本大量收集和使用步态数据信息，并利步态识别算法和技术对不特定人员进行身份识别和轨迹跟踪。步态识别技术给生活、工作及社会公共安全带来技术便利和保障的同时，也面临着非法收集、滥用、泄露个体生物特征信息等问题，因此步态识别中的数据安全保护成为了步态识别领域中的重要问题。

3 步态数据处理活动和主要风险

步态识别数据活动涉及的数据处理角色包括数据主体（步态识别数据所标识或者关联的自然人）、数据处理者、公共安全管理机构、第三方服务平台等，数据处理过程包括：数据收集–>数据的存储和传输–>数据的使用–>数据的加工、提供、公开–>数据的删除，涉及数据的全生命周期。

步态识别数据的收集：

（1）需求提出：组织或个人对数据主体提出步态识别数据及关联信息使用需求的活动；

（2）知情同意书签订：数据主体了解步态识别数据的使用目的、方式、范围及步态识别数据处理者名称和联系方式等信息后，双方共同完成的签订知情同意书活动；

（3）步态样本收集：收集自然人行走视频，并从中提取步态样本的活动。步态样本包括步态视频、图像序列等信息。此活动中会产生相应的关联信息，如：收集时间、收集地点、收集对象、收集者、收集方式、样本类型、规格、单位、样本保存期限等。

步态识别数据的存储和传输：在数据主体知情同意情况下，对步态识别数据及关联信息进行存储和传输的活动。

步态识别数据的使用：识别、检测、统计所获取的步态识别数据及关联信息。此活动中会产生数据主体的关联数据，如：步态特征、舞蹈姿态特征、体育竞技特征、行为康复特征等，此活动会产生统计分析数据，如：比对日志、舞蹈评分合格统计、体育竞技违规统计等。

步态识别数据的加工、提供、公开：在数据主体同意的前提下，将步态识别数据及关联信息进行加工、提供和公开的活动。

步态识别数据的删除：在账户注销、授权撤回、授权到期、申请删除等情况下不可逆地删除步态识别数据及关联信息的活动。

步态识别数据活动中常见安全风险主要包括：未经数据主体单独同意收集步态识别数据、紧耦合存储步态识别数据和关联信息、超授权范围使用步态识别数据、篡改步态识别数据、混淆识别对象或改变识别结果、数据传输或提供环节产生泄漏、未删除授权过期的步态识别数据等风险。常见安全风险见表1。

4 不同场景步态识别数据活动和安全要求

步态识别数据活动典型应用场景包括身份识别应用场景、非身份识别应用场景和科学实验场景。

身份识别应用场景是指步态识别数据用于识

表1 步态识别数据活动及安全风险

活动	安全风险
数据的收集	数据主体未被告知数据处理目的或未表示单独同意即被收集步态数据
数据的存储和传输	数据处理者未采用有效的安全措施和管理方法，如：过度存储、未采取加密措施等，产生敏感信息数据泄露、非法使用等风险； 数据处理者未采用有效安全措施导致数据被泄露或被窃取
数据的使用	在非身份识别数据被应用于身份识别场景，科研数据被应用于商业场景等
数据的加工、提供、公开	加工的目的、结果超出授权范围，或基于加工结果被滥用的风险； 在特征提取过程中，数据处理者未采用相应的技术手段，导致提取过程或结果数据被逆向还原，产生数据主体敏感信息泄露的风险； 在数据提供活动中，数据处理者超出授权范围提供数据，导致数据泄露、滥用风险； 在数据处理者委托第三方接入处理步态识别数据的活动中，未采用有效监控，导致受委托方产生数据泄漏、滥用等风险； 在数据公开披露活动中，数据处理者非法公开披露的风险； 个人身份信息和步态识别数据在应用界面、网站页面等上展示时，数据处理者未采用脱敏、去标识化等安全措施，或超出授权范围展示数据，造成数据泄露的风险
数据的删除	数据处理者未及时删除授权过期数据，或达到业务目的后继续存储数据，造成数据被恢复、泄露的风险，导致数据主体权益受损

别数据主体身份的场景。典型应用场景包括远程身份监控、步态门禁等。数据活动如图2所示。

非身份识别应用场景是指步态识别数据用于统计、检测或行为特征分析等活动的场景，不进行数据主体身份识别或验证。典型应用场景包括教育培训领域的舞蹈姿态分析，医疗领域的早期病症诊断、步态康复分析，社会治理领域的涉毒人员行为分析等。数据活动如图3所示。

科学实验场景是指步态识别数据用于开展与步态有关的科学实验活动的场景。典型应用场景包括高校或科研机构进行步态识别或步态分析算法研究、开展算法竞赛或评比等。数据活动如图4所示。

不同场景下步态识别安全要求见表2。

表2 不同场景下步态识别安全要求

活动＼场景	身份识别	非身份识别	科学实验
数据收集	明确告知、风险提示		
	/	不关联身份信息	书面同意
数据存储和传输	数据加密、访问控制		
	分类存储	/	/
数据使用	明确告知、特殊用途单独同意		
	/	/	不应用于商业目的
数据加工、提供、公开	不可逆处理、安全分级、数据监督		
数据删除	及时且不可恢复		

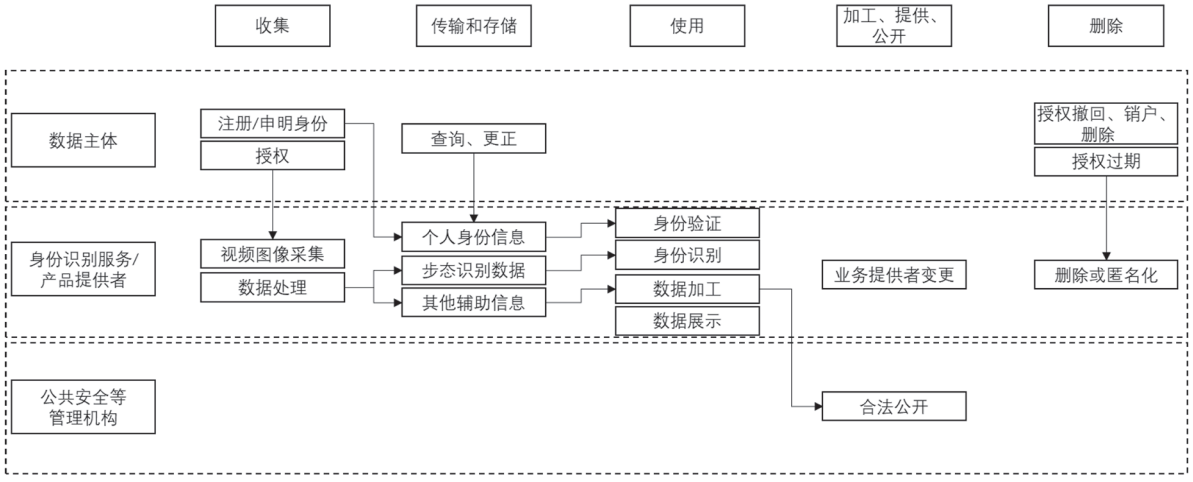

图2 身份识别应用场景下的数据活动图

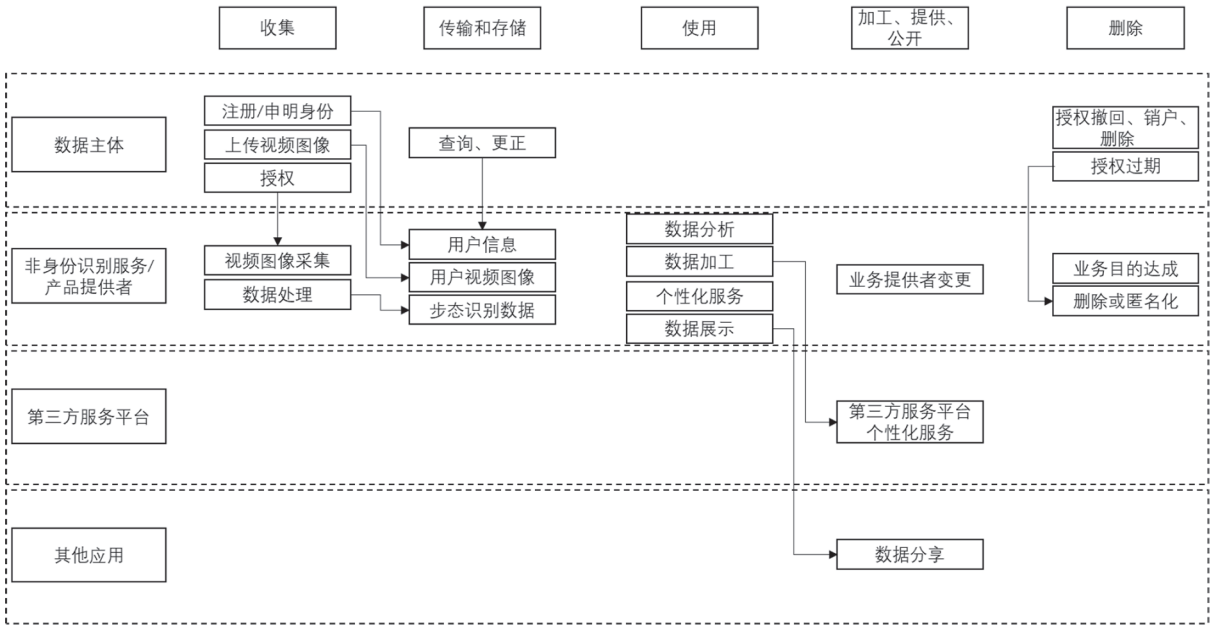

图3 非身份识别类场景下的数据活动图

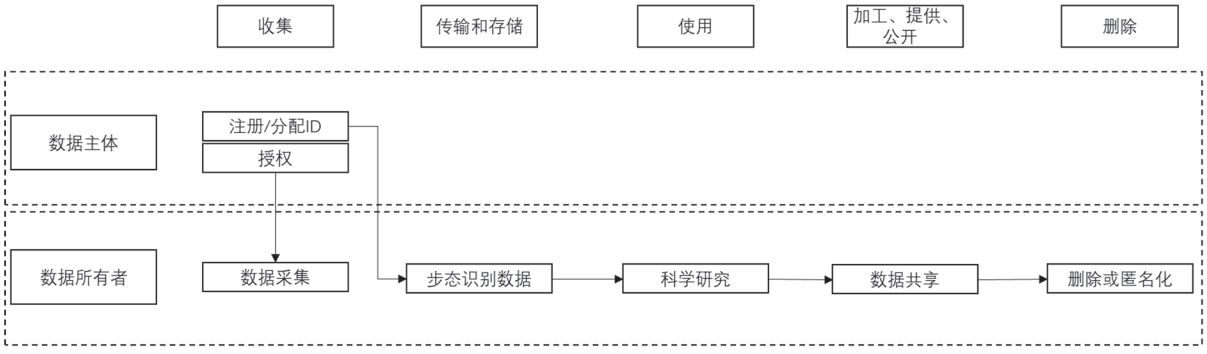

图4 科学实验场景下的数据活动图

5 总 结

步态识别以其特有的技术和应用领域，已经成为国内外科研院所和企业看好的朝阳产业方向，未来将得到更大规模的研究和产业化发展，同时也亟需标准化规范引领行业发展。《信息安全技术 步态识别数据安全要求》以步态识别数据的安全保护为目标，规定了步态识别数据活动范围和主要风险，明确了步态识别数据的最小安全基线要求，为开展步态识别数据大规模安全应用提供了标准支撑，填补了行业空白。以步态识别数据安全标准为起点，未来将进一步推动步态识别领域基础、技术、软硬件、测评、应用体系标准化建设，提高步态识别技术产品和应用服务水平。

参考文献

[1] WAN Changsheng, WANG Li, Phoha Vir V. A Survey on Gait Recognition[J]. ACM Computing Surveys, 2018,51(5): 1–35.

[2] 张勇.个人生物信息安全的法律保护——以人脸识别为例[J]. 江西社会科学, 2021,(5):157–168.