

**本科毕业论文（设计）**

**外文翻译及原稿**

|  |  |
| --- | --- |
| 译文1题目： | Online Student Authentication and Proctoring System Based on Multimodal Biometrics Technology |
| 原稿1出处： | IEEE Access |

|  |  |
| --- | --- |
| 学 院： | 计算机科学与技术，软件学院 |
| 专 业： | 软件工程 |
| 班 级： | 移动应用开发2001 |
| 学 号： | 202003150317 |
| 学生姓名： | 沈周 |
| 指导老师： | 陈波 |
| 提交日期： |  |

**基于多模态生物识别的学生在线认证和监考系统**

**摘要**

在线学生的身份验证和监考是当今在线学习面临的关键挑战之一。特别是对于在线认证和认可，培训机构需要验证完成学习过程并获得学分的在线学生是否为注册了课程。此外，他们还需要确保这些学生在完成在线培训的所有活动时没有作弊或不当行为。COVID-19大流行加速了在线教育战略的迁移和实施，因此需要安全的机制来验证和监督在线学生。如今，有几种不同程度自动化的技术可供选择。在本文中，我们深入描述了一种基于不同生物识别技术的验证和自动监考系统（系统工作流程以及人工智能算法）的解决方案，其具有以下特点并解决了市面上的一些主要问题：高度可扩展、自动化、可承受的负载、用户硬件和软件要求少、可靠且学生在该系统中处于被动地位。最后，本文讨论了大规模系统的技术性能测试、用户的可用性-隐私感知调查及其结果。

**关键词**

生物识别认证、云计算、计算机视觉、数据科学在教育方面的应用，远程教育和在线学习，机器学习，安全，计算机视觉。

1. **介绍**

毫无疑问，在线学习在过去几年中一直备受欢迎。这种现象并不令人意外，因为在线学习使教育机构能够以更低的成本覆盖更多的学生。教育机构正在提供在线课程，以利用在线学习的好处。特别是自从大规模开放在线课程（MOOC）出现以来。另一方面，COVID-19对提供面对面教学的传统机构构成了挑战，这些机构不得不在短时间内迁移到完全在线教育模式，这是受到疫情的迫使。然而，在线学习的实施也面临着挑战。

电子学习存在严重的不足，即缺乏有效的机制来确保用户在系统登录以及整个会话过程中的身份验证。特别是对于在线认证和认可，培训机构需要验证完成学习过程并获得学分的在线学习者是否确实是注册课程的学生。身份验证方法不足会影响在线获得的证书和认证的可靠性。

在没有在线学习者身份真实性的确证的情况下，对完全在线教育的愿景受到阻碍，而对在线学习者所获得的知识和技能的评估也变得不可靠。为了防止损害在线认证的可信度，验证必须以恒定或持续的方式进行。同时，验证应该是非侵入性和非干扰性的，不会干扰学习过程。

在线监考通常指监考人员（人类）通过网络摄像头监视考试。它还包括在远程进行的用于验证考生是否是应该参加考试的人的过程。在线监考最早由Kryterion[1],[2]于2006年提出，于2008年将其作为技术解决方案推广。从那时起，其他几个组织也跟随Kryterion的领导，开发了更有能力的技术替代方案并受到了关注，例如在线监考。

现今市场上有商业解决方案以及研究出版物尝试解决这个问题。其中一些只进行身份验证，其他一些进行监视，有些是实时监控，另一些记录会话。有些只涵盖考试或特定活动。有些是完全基于人的解决方案（不可扩展），或者是完全自动的解决方案（不可靠）。也有一些科学方法正在发展将部分上述功能结合起来的想法。然而，目前还没有一种综合且可靠的解决方案，将多模态连续认证与连续的视觉和音频监控、设备活动监控以及锁定选项和人工监督（仅在必要时）结合起来，以确保100%可靠的结果。

在这项工作中，我们提出了一个新系统，满足了商业解决方案所需的一切。它基于网络应用程序，通过持续的生物特征（面部、声音、打字）识别系统（生物特征无法丢失、被盗或重新创建），为在线学生提供连续认证身份服务，以及通过自动图像和音频处理（设备监控和锁定以及不当行为检测）实现自动持续监考，从而使在线课程能够为机构和学生提供双方受益的价值。该解决方案基于高精度的生物特征识别和数字信号处理算法，并辅以人工监督，用于在自动算法无法确定可靠结果的情况下。它可用于持续认证学习者，无论是在整个学习过程中还是仅在电子学习的某些敏感阶段。它是非接触式的，只需要较低程度的用户合作。此外，整个系统基于云计算技术，消除了在线学习提供者的地理和技术障碍。

本文的组织如下。第二部分概述了一些相关工作，并突出了我们方法的主要区别。第三部分描述了整个系统概述和工作流程。第四部分包含核心模块的科学技术描述。第五部分介绍了系统测试，以衡量算法的性能，并进行了用户体验评估的调查。第六部分呈现了测试结果。最后，第七部分得出了结论并提出了未来的工作。

1. **相关工作**

随着互联网世界的增长（包括电子学习、电子银行、电子赌博、电子政府等），对在线用户进行身份验证和监控的能力变得越来越重要。自从第一个基于人的在线监考系统问世以来，近几年出现了各种基于生物特征的全自动或半自动身份验证和监考技术。生物特征已被证明是基于生理或行为特征识别人的最佳方法之一。这些技术可以分为两类：基于物理特征和基于行为特征。前者包括面部识别、指纹扫描仪、虹膜扫描仪、静脉匹配等。后者包括语音识别、手写识别、击键动态等。已经证明没有任何技术能够独立提供正确答案，但是结合不同的解决方案将根据客户需求提供适当的功能。此外，大多数远程身份验证监考技术都涉及一定程度的人为干预，以确保完全可靠的服务，从而限制了其规模。

这些生物特征技术已被广泛用于各种目的，并在我们日常生活中变得越来越普遍。然而，很少有这些技术成功应用于在线学习验证。

1. ***商业解决方案***

一些初始方法已经作为商业解决方案被带到市场上。本文接下来回对这些服务进行一个概览。

1. **完全实时在线监考**

学生通过视频远程监考。远程监考是为参加在线考试的学生提供的一种实时在线服务。学生预约后，将被带到在线监考室，在那里他们将通过网络摄像头与两个在线监考中心之一的实时监考员连接。学生将他们的屏幕连接到监考员那里，这使得监考员能够看到他们的电脑屏幕。监考员要求他们出示身份证件，并回答一些关于自己的问题，以验证他们是否确实是正确的学生。在考试期间，监考员通过网络摄像头直接观察学生。这是一种安全完整的考试监考解决方案，但由于它是一种非自动化解决方案，在整个学习过程中无法进行连续身份验证。此外，它需要高速互联网通道来传输视频数据，可能对世界各地的某些地区来说是无法承受的，并且对学生来说不是被动的。市场上一些商业解决方案包括ProctorU [4]，Examity [5] 和Software Secure - PSI [6]。

1. **被记录和回顾的监考**

会话被记录下来，计算机监视着学生。随后，人员可以随时回顾录像。在这些系统中，学生使用自己的计算机和网络摄像头记录评估会话，整个考试过程中记录了学生和周围环境。教师可以快速查看评估细节，甚至观看录制的视频。录制监考与现场监考具有相同的局限性。此外，这是一种被动系统。然而，没有人分析视频，因此教师必须观看所有视频，以便检测到不良行为并保持现场监考的优势。市场上一些商业解决方案包括Kryterion [1]，ProctorExam [7]，Respondus [8]，Remote Proctor [9]，ProctorCam [10]，B virtual [11]和Learner verified [12]。

1. **全自动解决方案**

计算机监控学生，对其进行身份验证，并确定他们是否作弊。这些是自动和被动的解决方案。它们只涵盖考试开始和工作提交过程的开始部分。然而，在这种系统中，用户必须完全积极参与（他们必须输入预定义的段落并自己拍摄身份照片）。此外，这种系统不会持续覆盖所有学习过程。市场上一些商业解决方案包括Proctorio [13]，ProctorTrack [14]，Comprobo [15]，Sumadi [16]，ProctorFree [17]，HonorLock [18]和ExamSoft [19]。

1. **认证技术**

识别技术被用来根据先前对某些生物特征的检查来认证学生。它们通常建立在先前/期间/之后的分析基础上，以验证最初注册课程的同一学生是否确实是参加考试的同一学生。常见的识别技术包括面部识别、指纹识别或语音识别。在过去一年中，诸如击键动态（它根据节奏、压力和风格识别打字模式）等新的生物特征程序越来越受欢迎。识别技术很可能在与其他可用技术的某种组合一起使用时效果最佳。

1. **监控技术**
2. 网络摄像头和麦克风是最早用来替代现场监考员的技术之一，在市场上大多数远程考试监考解决方案中都有应用。当摄像头是计算机的一部分时，它们可以记录个别学生，当摄像头放置在教室时，它们可以记录群体。它们可以监视学生的行为，无论他们是否作弊，是否从其他学生那里得到帮助，是否使用移动设备、书籍等。网络摄像头/麦克风技术通常需要大量的存储能力，以便在必要时可以审查视频记录。
3. 计算机锁定能够监视学生在计算机上进行的活动，防止他们在考试时“浏览互联网”。这种监控只在学生进行可以评估的活动时才会进行。

所引用的商业解决方案均未提供多模态生物特征认证解决方案或全程学习课程（不仅限于考试）的连续认证/监考服务（基于自动分析）。此外，这项工作提出了一种全新的商业方法，以克服诸如低速互联网连接（使用数据样本，而非连续的大量视频信号）或昂贵的额外硬件/软件要求（使用不需安装且完全集成在LMS网络应用程序中）等障碍。

1. ***科学与学术方法***
2. **技术工作**

尽管现今仍然存在一些非生物特征的身份验证方法[20]，但最新的在线学生身份验证自动化尝试往往采用生物特征技术；如面部[21]–[26]、指纹[27]或打字[28]，[29]。另一方面，一些方法尝试它们的一些组合，例如面部和语音[30]或面部、语音和打字[31]，[32]。所有这些方法主要侧重于学生身份验证，而不提供监考服务。

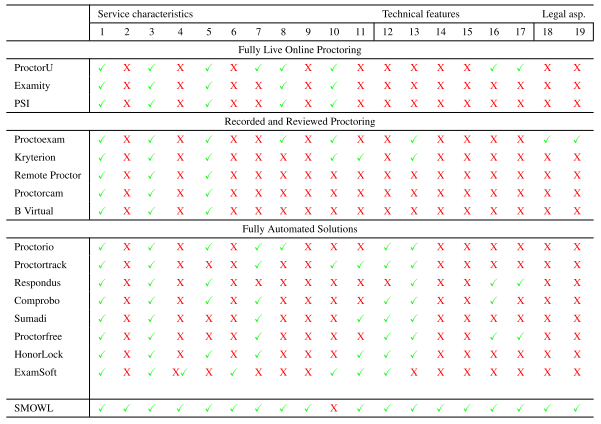
通过面部认证结合其他生物特征，如语音或打字识别，电子学习平台可以在学生进行活动时验证欺诈的缺陷。

我们在本文中提出的工作的主要创新贡献包括三种主要生物特征的全新组合工作流程，提供持续且非侵入式的认证服务。它还向系统添加了基于图像和音频信号处理的新的自动连续监考功能。此外，它整合了计算机活动监控和锁定功能，最后，它甚至通过自动警报补充了服务，触发最低限度的人工监督，从而保证了结果的可靠性。

最近对安全和隐私的关注也为与在线监考相关的这一主题提供了最新的研究[33]。

1. **用户体验相关工作**

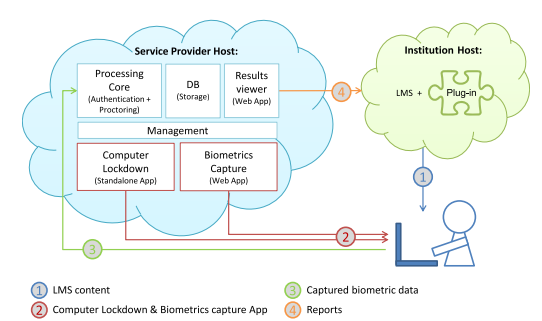
另一方面，很少有研究完成了对教师和学生使用此类身份验证和监考方法的用户体验的研究。其中一项完成了关于将面部验证应用于教育领域的研究，成功取得了积极的结果[34]。其目标是确保学生的身份验证正确，并准确了解他们在电脑前阅读或进行虚拟活动的时间量。

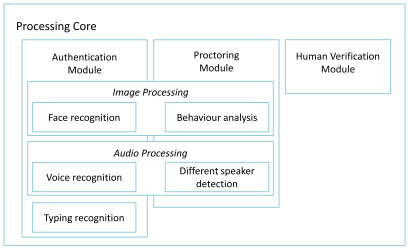
表格一：商业解决方案与SMOWL（本文描述的解决方案）的对比。服务特性：1-整个考试或会话期间的身份验证；2-多模态生物特征认证（至少2种不同的）；3-考试监控；4-连续（整个课程）监控；5-不诚实行为检测；6-完全被动和非侵入式系统；7-自动分析结果；8-100%保证和可靠的结果；9-个性化警报；10-人工实时监考员；11-设备监控。技术特性：12-可扩展的系统；13-学生灵活访问 - 无需预约；14-身份验证和监考无需额外的软件/硬件安装；15-可在低速连接下工作；16-完全集成在机构LMS中；17-多浏览器和设备。法律方面：18-欧盟托管解决方案；19-GDPR合规。√- 是 | ×- 否.

同样，还提出了一种面部认证机制。这确保了学生不会被冒名顶替以提高他们在虚拟测试中的分数。

1. **系统概览**

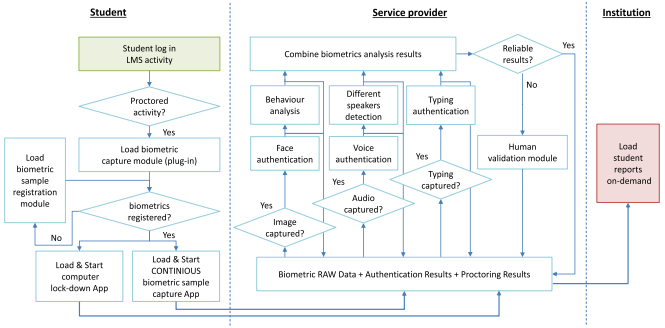
我们在这项工作中提出的系统旨在为以下两个方面提供实用的网络安全解决方案：a）持续的在线用户识别（使用生物特征技术）和b）使用自动信号处理和计算机监控系统进行监控。身份验证过程基于自动识别面部图像（由网络摄像头捕获）、音频剪辑（由麦克风捕获）和击键动态（由键盘捕获），在整个在线交互过程中验证确实是应该是的人。监控过程也由网络摄像头和麦克风支持，持续检查学生是否有任何不当行为（使用禁止的设备和应用程序，接受帮助等）。它还在考试或培训课程期间锁定计算机（需事先在学员计算机上安装并获得同意），防止用户在完成课程时访问网页或其他文档。

该系统可用于任何在线用户身份验证，但专门针对提供在线课程、培训和学位认证的机构，包括经过验证的MOOC和为员工提供的企业培训。该系统可以帮助电子学习提供者实现他们的目标，通过追踪学生真实性和行为的证据可追溯性，向教育质量机构申请其课程的学分。它可用于跟踪学生在整个电子学习过程中或在敏感阶段的持续身份验证。图一显示了系统的一般设置，图二详细描述了处理核心

**图一.认证与监考系统设置**

**图二.处理核心描述**

完整的系统工作流程嵌入在云计算应用程序中，可以在任何地方使用，消除了地理和技术上的障碍。其一般操作方案如下，并在图三中给出了更详细的描述。

1. 该系统已集成到培训中心的虚拟校园中（可用于不同的LMS平台）。
2. 培训中心发送一个代码（唯一的学生标识符）和学生的图像注册到系统中。根据系统的数据隐私政策，系统使用图像、音频剪辑等，而不是身份信息，因此缺少与学生个人数据（如姓名、年龄或地址）的连接。
3. 当学生第一次进入虚拟校园时，系统会获取生物特征样本（图片、简短语音、预定义段落打字），这些样本将帮助我们创建跟踪生物模型。
4. 此后，每当学生连接工作时，将随机和连续地获取生物特征样本。这些数据被发送到云端的服务器上。在线管理模块存储并分析数据，然后将其与之前为身份验证目的创建的生物模型进行比较，并进行分析以检测不当行为。所有存储、分析和结果报告以及警报创建任务都在在线服务器上执行，使机构的集成、支持和维护任务变得更加简单和透明。在此期间，计算机锁定模块可以为监控目的而激活。
5. 结果导致一个不断更新的个人用户报告，培训中心可以访问该报告。

**图三.系统工作流程**

表格二：最先进的解决方案与SMOWL（本文描述的解决方案）之间的比较。身份验证方法：1-面部识别；2-语音识别；3-打字识别；4-整个会话期间的持续身份验证（不仅仅是在开始时）。监考-监控方法：5-图像处理；6-音频处理；7-屏幕截图捕获；8-设备信息捕获（活动窗口、打开的进程、外围设备、复制/粘贴命令等）。监考-设备锁定：9-设备锁定。保证：10-提供人工监督以澄清疑问，提供100%保证和可靠的结果。

系统的关键特征是:

1. **持续性的、非计划性系统。**

监考和认证过程在整个会话期间进行，不仅在用户登录时进行。此外，在电子学习情况下，它可以跟踪课程的每个会话，不仅仅是评估。它非常灵活。服务全天候提供，任何地点都可使用。不需要事先安排。

1. **被动和非侵入式系统。**

该系统为学生提供了一种被动系统，用于拍照、音频剪辑或击键模式。它不需要学生的合作，也是无接触的。因此，在图像方面，当学生的姿势/外貌/装饰/表情或房间的光照条件无法控制时（野外环境），系统能够正常工作，获取到低对比度的图像，并由于错误的位置或学生外貌/装饰/表情的变化而出现局部遮挡。关于音频剪辑，麦克风只在检测到一些噪音时才记录声音，如果学生保持沉默，则不会录制任何声音。剪辑随后进行分析，如果在录音中检测到声音，则与学生注册时收集的数据进行比较，以验证其身份，或者在录音中存在不同的声音时检测作弊行为。

1. **自动化和可扩展的。**

所有的采集、验证、数据管理和监控报告模块都是通过云计算技术在云中作为服务进行的。照片和模式是自动和随机地获取的，并与注册过程中创建的生物特征模型进行比较。这种可扩展的自动设置使得将此解决方案应用于拥挤的场景（如MOOCs）成为可能。

1. **对终端用户要求少**

基于云的（SaaS）自动化解决方案。所需硬件 - 软件（HW/SW）：基本网络摄像头、麦克风、键盘和任何更新的浏览器。最终用户无需安装任何东西。该系统可以在任何设备、平台、操作系统和浏览器上运行，无需安装。

1. **自动分析结果**

100%保证结果，并配备定制警报。如果无法确认自动验证（如果照片或音频剪辑的质量不符合系统自动验证学生所需的标准），将设置由工作人员进行手动检查，以确保结果达到100%的准确性。

1. **完全集成在客户LMS中**

它可以通过通用API集成到任何学习管理系统（LMS）中，但它还针对Moodle、Moodlerooms、Blackboard、OpenedX、Canvas等（最常用的LMS）提供了特定的插件。

1. **安全**

数据通过安全的互联网协议传输，并存储在安全的云服务器中。

1. **私密**

用户的身份得到保护，因为我们只处理与用户代码相关的数据，而不是与身份相关的数据，这些用户代码由在线实体提供。

1. ***数据捕捉与存储模块***

该模块从学生的网络摄像头、麦克风和键盘捕获数据。该应用程序的核心是使用最新的HTML5标准在Web浏览器中实现的。该应用程序被下载到学生的终端并在无需任何安装的情况下执行。每当用户连接到LMS中的课程、测验或特定练习时，将随机连续地获取预定义周期的图片、音频剪辑和击键动态样本。这些数据通过SSL加密通道与用户识别码一起发送到云服务器。系统的在线管理模块存储并分析这些图像。

1. ***认证模块***

一旦所有数据存储在云服务器中，就会与与学生识别码相关联的生物特征模型进行比较，该模型在注册时创建，并已使用最新的正面数据进行更新。结果存储在系统数据库中。系统的识别和训练算法使用最新的人工智能算法（在第四部分中有解释），这些算法不断提高其识别精度和对光线、位置和学生外观（如身体变化和配饰，如帽子、眼镜等）变化问题、音频剪辑中的噪音以及打字样本的变异性的鲁棒性。认证结果是每个生物特征认证模块结果（面部、语音和打字）的组合。

1. ***监考与计算机锁定系统***

在监控会话期间，用于身份验证目的的捕获图像和音频剪辑将使用不同的技术进行处理，以便检测学生在电子学习活动期间的不当行为。因此，系统能够检测学生是否在接受帮助（通过电话、面对面朋友的帮助等），或者是否在查阅禁止使用的文档（书籍、其他连接到互联网的设备等）。所有这些行为在某些面对面学习活动中可能被严格禁止，根据机构的荣誉守则。

此外，如果有学生试图欺骗系统，例如在摄像头前安装照片或用他人的身份证图像替换，系统将检测到并报告作弊行为。还会检测到尝试将另一张图像或视频信号插入摄像头的行为。

另一方面，系统包含一个计算机锁定模块。在整个在线会话期间，计算机锁定模块将监控学生的计算机，检测连接的外围设备、活动窗口、计算机信息（硬件/软件）、执行的程序或进程、浏览历史/网页和复制-粘贴命令。每个会话中捕获的所有信息都存储在数据库中。

1. ***人类验证系统***

作为质量保证的一部分，必须设置一个随机数据和结果审计。这项任务将测试质量保证机制的定义和实施，同时连接大量学生。它将基于随机数据的交叉验证（由不同人员验证的相同图像、语音和击键模式）对在会话期间捕获的图像、语音和击键样本进行验证。此外，当照片或音频的质量未达到所需的阈值时，将由受过培训的人员进行人工验证，以提供学生100%可靠的验证。

1. ***结果呈现模块***

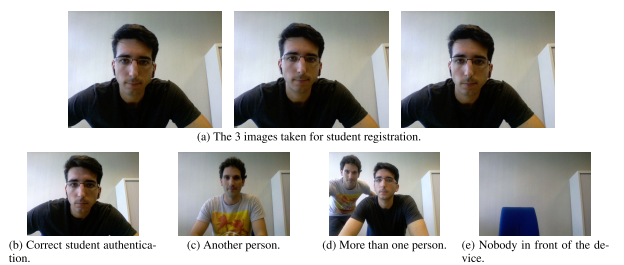
最终结果由数据表示模块呈现。它根据需求创建图形图表和表格，24小时/365天作为动态网页。最终报告可以以不同格式下载或打印。此外，数据表示模块还在发生预定义的禁止行为时生成自动警报。

1. **认证与监考模块植入**

如前文所述，本文介绍的系统包含基于人工智能的用户身份验证模块，以及用于设备监控的计算机锁定技术。在本节中，将详细解释身份验证模块背后的科学算法以及计算机监控技术的功能和技术。

1. ***面部检测与识别***

该系统包括一个面部检测和识别模块，通过使用注册时的面部照片创建生物特征模型。该模块的输出结果被分成五组确定：a) 是否有人在网络摄像头前，b) 在网络摄像头前有多少人（如果有的话），c) 这些人中是否有一个是应该在屏幕前的人，d) 当图像中只有一个人时，这个人是否是应该在那里的人，e) 应该在那里的人是否没有参与任何不当行为（阅读书籍或使用电子设备）。图4中展示了一些例子。

**图四.身份验证和监考系统捕获并分析的图像示例。**

文献中有不同的面部检测方法。然而，当处理捕获图像的姿势和光照变化时，很少有方法足够稳健（请记住，照片是在学生不注意的情况下随机拍摄的）。本文提出的面部检测程序基于FaceBoxes方法。该方法以其在面部检测数据集和基准（FDDB）基准（Jain和Learned-Miller，2010）中获得比其他测试过的方法更好的结果而闻名。图像处理和身份验证过程以文献[39]中提出的方法作为基准参考，用于提取和规范化面部纹理。该算法包含以下子任务：（1）面部检测，（2）在面部区域检测面部特征点，（3）根据检测到的点进行可变参数3D面部模型调整。然而，系统被动性的要求使得必须不断改进检测和认证算法以应对输入图像的高变异性。从这个参考工作开始，已经添加了一系列改进：

1. **姿势与表情校正**

一种名为M3L（多层次、多模态、多任务学习）的新方法 [40] 被用来改善面部特征点和其他面部属性（面部和眼睛的姿势）的检测效率。M3L 通过使用现有数据之间的相关性来解决通过神经网络层次结构提取所有这些面部和眼睛数据的问题。此外，一种新的多层次可变形 3D 面部模型调整将变形误差均匀分布，区分三个阶段，在估计中具有不同级别的优先级（从大到小）：（1）姿势，（2）人际变形（特定用户的面部形状）和（3）个人内部变形（由于面部表情引起的变形）。

1. **外观规范化 ，特征选择与分类**

通过深度神经网络 [41] 提取生物特征已经得到改进，通过对拥有 100 万张图像、10 万个个体的数据库进行训练，该数据库具有极大的外观和面部形状、光照、面部表情、配饰和姿势的变异性（Guo 等人，2016）。

1. **光照归一化**

照明归一化的过程采用了分层方法，对整个面部区域以及特定的、归一化的面部区域进行分析。这种归一化是使用对比有限自适应直方图均衡化（CLAHE）算法 [42] 进行的，该算法在每个 RGB 色彩通道上局部均衡化图像，突出对比度。

1. **对部分遮挡情况的鲁棒性**

遮挡检测基于 MobileNet-SSD 神经网络 [2], [43]。通过结合人体检测器和面部检测器，系统在至少部分遮挡时的检测中增强了鲁棒性。在这些情况下，人体检测器（身体）比面部检测器更加稳健。因此，如果检测到一个人，但没有检测到面部，那么这个面部很可能至少部分被遮挡。在这种情况下，将考虑面部检测警报。此外，已经实现并适应了 [44] 中提出的方法，以处理规范化面部图像的遮挡。面部检测返回的部分遮挡面部剪切比理想情况多。通常这些遮挡是由用户的手放在面前或者摄像头只指向面部的上半部分引起的。这种遮挡会对后续的面部关键点检测和生物特征向量提取产生负面影响。该系统包括了来自生成对抗网络的面部图像合成 [45]，该网络从训练模型中获取接近的面部特征来填补被遮挡的部分。通过这种方式，遮挡的负面影响可以减少。

1. ***声音检测与识别***

该模块实现了一个连续语音检测和认证算法。该算法基于 Kaldi 工具 [46] 和 [47] 中方法的实现。两者都包括开发生物特征模型、每个说话者特征的向量表示的工具。该算法涉及四个任务：

1. **通过VOIP对音频进行分析、解释和归一化**

由于VoIP（该系统基于的技术）中使用了G.711编解码器和64 kbps的比特率，这意味着为了压缩音频信号而丢失了重要信息，因此来自可用声学数据库的所有训练数据都被转换为此编码和格式。通过这种方式，可以在不同的频率范围内获取训练和评估音频匹配。信号预处理被集成以丢弃不包含语音（沉默、音乐或噪音）的声学段。VAD语音活动检测模块的最终版本采用了GMM高斯混合模型和Kaldi代码工具中提出的处理函数进行开发。共进行了3个模型训练水平。它们之间的区别在于为了更强的鲁棒性而对训练数据进行的转换，以应对应用场景中的高声学变异性。

1. **背景和发言者建模**

说话者建模基于d-向量或使用深度神经网络的说话者嵌入。这种解决方案在鲁棒性和准确性方面表现更好。实施遵循了Google在2018年提出的解决方案。在这种方法中，生成了一个基于LSTM单元的循环神经网络。它接收特定音频的声学特征（Mel滤波器组）作为输入，并返回其d-向量。一旦训练完成，神经网络就可以使用说话者的声学特征生成d-向量。然后，生成一个质心，被视为说话者的生物特征。

1. **模式比较**

对于验证或识别过程，给定声学特征向量及其关联的d-向量，它们与每个说话者的质心在一个新的相似度矩阵中进行比较。

1. **流媒体音频的发言者分割**

该语音分割系统采用了 d-向量或说话者嵌入和基于循环神经网络的聚类模型。这种方法旨在解决传统的聚类方法的问题，传统方法会独立处理句子，很难从大量标记数据提供的信息中获益。该系统基于[48]的工作。使用独立的文本音频识别网络从240毫秒的窗口中提取d-向量或说话者嵌入，重叠率为50%。基于高斯模型的声活检测器用于消除无声部分，并将信号分割成小于400毫秒的段。这些段被转换为d-向量，并包含在基于循环神经网络的语音分割系统中。

1. ***输入识别***

击键动态是一种有效的行为生物特征，它捕捉了个体在键盘上输入时表现出的习惯模式或节奏。根据神经生理学分析，这些打字风格是独特的，就像手写或签名一样，这是由于它们具有相似的神经机制。因此，它们可以用于验证个体身份。

本文提出的系统在动态文本中应用了击键动态，即对用户输入的任何文本进行连续分析。静态文本中的击键动态需要较少的实现工作，并且在文献中也达到了较低的错误率。然而，动态文本分析是必要的，以确保最终学生在认证过程中的被动性，而不会通过要求他们打字预定义段落来打扰他们（通常与进行中的电子学习活动无关）。这种方法考虑到一个人的击键动态可能会在不同的心理和情绪状态下发生变化。例如，研究表明，疲劳的人通常打字速度较慢，犯的错误也更多，因此，每个打字样本都被存储以使识别模型更加稳健。

击键动态分析模块涉及两个独特的过程：

1. **特征提取**

提取的特征（详细的时间信息）是以下瞬间之间的时间差：

1. DT: 按键被按下并释放的瞬间
2. PR: 按键被按下并且下一个键被释放的瞬间。
3. FT: 按键被释放并且下一个键被按下的瞬间。
4. PP: 按键被按下并且下一个键也被按下的瞬间。
5. RR: 按键被释放并且下一个键也被释放的瞬间。

根据开发和测试周期中进行的不同分析，DT（停留时间）和FT（飞行时间）特征被认为是最相关的，并且它们相应地被加权。此外，还单独计算了一定数量的打字错误（例如“删除”和“退格”键的按下次数），作为辅助参数。

1. **提取特征的分类**

该模块采用CNN+RNN模型[54]来学习更完整的个人按键输入模式以进行连续身份验证。 30个按键数据的序列长度（性能最佳）被向量化，然后被分成固定长度的按键特征序列，以便将按键序列输入到RNN网络中。 输入数据经过CNN预处理（提取较高级别的按键特征），提高了网络模型的性能。

1. ***计算机监控***

在线监考的需求已经发生了变化。最近，市场不仅寻求识别学生，还要验证他们是否在使用设备进行活动时进行任何作弊或不允许的行为。换句话说，最大的变化之一毫无疑问是希望监控学生在进行可评估活动时设备内的活动。

该开发的目标是获得一个能够监控学生在其计算机上进行的活动的应用程序。这种监控仅在学生进行可以由监考系统评估和监督的活动时进行。由于客户可以从不同的操作系统访问考试，因此目标是开发一个多平台应用程序。用户界面尽可能小，以便在进行可评估活动时不会打扰学生。但是，它足够大和可见，以便学生知道他们正在受到监视。

通过应用程序获取的数据将存储在数据库或系统服务器上，因此，必须确保应用程序符合所有与保密性和数据保护相关的标准和法规。该软件使用Electron JS开发，这是一个可以简单实现多平台应用程序开发的框架。此外，它基于Web应用程序技术（以及数据捕获模块），这意味着不需要在设备上本地安装即可执行。就要求而言，系统监控工具满足以下要求：

1. **活动窗口检测**

该功能是该应用程序中的关键方面之一。系统不仅获取活动窗口的名称，还获取其截图。

1. **打开/运行进程的检测**

此监控功能使我们能够了解学生打开了哪些程序以及何时打开了它们，如果有的话，还能知道何时关闭它们。

1. **外围设备**

计算机有不同类型的外围设备可以连接。系统知道学生连接了多少个键盘、麦克风、屏幕和摄像头。对于摄像头，系统还知道它们的名称，以便检测虚拟摄像头。

1. **设备信息**

每台计算机都有特定的组件，使其成为独一无二的，如主板或处理器。为了确定两个用户是否使用同一台计算机，收集了有关计算机及其连接的信息：处理器、主板、IP、制造商名称、操作系统等。

1. **浏览历史记录**

该工具特别用于评估考试，学生需要回答提出的问题。学生可以使用任何类型的浏览器来搜索这些问题的答案。因此，用户可能会在没有必要的知识的情况下正确回答。为了打击这种行为，或者至少对其进行监控，系统会在活动期间收集用户的浏览历史记录。系统记录的不仅是URL，还有网站的标题和进入时间。

1. **复制/粘贴指令**

与前面的点密切相关的是复制和粘贴事件。为了防止学生作弊、复制答案或将考题发送给其他人，有必要监控这些事件。特别是，在评估活动期间，记录用户进行的每一次复制和粘贴文本的事件。此外，还收集学生所截屏的屏幕截图，例如，如果学生截屏了测验页面以便将考题发送给其他人。

1. **屏幕截图**

为了监控我们尚未考虑到的行为，系统会定期进行屏幕截图。这些屏幕截图让系统能够识别新的作弊方法。

**表格三.：每种特征类型的捕获样本数量**

考虑到在线学生通常使用相同的设备/浏览器/连接执行他们的在线活动，系统会分析与计算机硬件/软件相关的信息，以及 IP 地址，并利用同一用户的这些信息在时间上的变化来触发更严格的自动和手动身份验证和监考分析。

1. **测试**

该系统通过在3个不同国家（拉丁美洲、欧洲和亚洲）的5个不同的电子学习机构（3所大学，2个培训中心）中进行了超过57项活动的测试。

共有350名学生使用认证和监控系统进行了评估活动，涵盖了三种不同的一般类别：考试（22项）、简短测验（10项）和论坛讨论（25项）活动。选择这些活动是因为它们使教师能够设计需要学生在平台上花费更多时间并获得更完整的生物特征认证和监考系统体验的活动。

包含测试活动的课程有3种类型的页面：（1）内容页面，其中包括关于主题的文本、图表和图片，（2）简短测验或更广泛考试的页面，学生必须回答之前阅读或可视化的内容，（3）论坛活动，教师通过动态问题促进与课程内容相关的讨论。

此外，这些活动在3种不同的LMS平台上进行了测试：Moodle、Blackboard和OpenEdx，以检查系统与全球最常用的LMS平台的兼容性和集成性。

学生完成这些活动的平均时间为1小时42分钟。

1. ***技术测试***

系统在活动期间每隔5-8秒随机捕获图像，每当学生发言或键入文本时，就会捕获音频和键入样本。收集的数据如表3所示。图像/音频/键入算法已经在捕获的每个样本中进行了深入测试。

所有图像至少包含80%的面部区域（当捕获到人物照片时），并且在应用亮度和对比度滤镜（如有必要）后足以区分面部特征的照明充足。另一方面，音频样本的信噪比（SNR）足够接受，可以由人类识别说话者。

1. ***用户体验测试***

另外，还进行了不同的调查。这项调查的目的是分析学生和教师对这类系统的包含以便未来接受的看法。

在2018-19学年期间，对350名学生和50名教师进行了有关这项技术适用性的调查。一旦他们完成了，学生们就会回答有关他们经验的问卷。在这项工作中，我们呈现了最显著的问题：

1. *您认为将生物特征认证和监考应用于学习活动是否合适？*
2. *您认为这种生物特征认证和监考应该在电子学习中实施吗？*
3. *您认为这种生物特征认证和监考应该在所有在线大学中实施吗？*
4. *如果可以选择，您是否希望在进行活动时加入此软件，以证明您已完成活动，并且您不会因为其他人要求完成活动而受到伤害？*
5. *您认为监控远程教育以避免作弊是公平的吗？*
6. *在进行课程活动时，如果认证和监控系统正常工作，您会感到舒适吗？*

**对教师来说，最显著的问题是以下问题：**

1. *您是否希望在您的活动中引入生物特征认证和监考工具？*
2. *您认为使用这种系统会避免电子学习活动中的欺诈吗？*
3. *在您看来，使用该系统会提高您课程的价值和声誉吗？*
4. *您认为在电子学习环境中需要透明且不会打扰学生的认证和监考系统吗？*

当前研究的问题以七点Likert量表回答：完全不同意（1）、不同意（2）、稍微不同意（3）、不同意也不同意（4）、稍微同意（5）、同意（6）和强烈同意（7）。

1. **结果**
2. 技术结果

在这一部分，展示了人工智能模块的处理结果。由于无法手动标记学生的击键动态样本（我们无法看到或听到），表格4只显示了图像和音频处理结果。精确度和召回率数据是基于一个完全标记的数据库计算得出的。

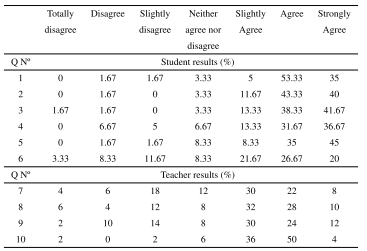
**表格四：认证和自动监考模块与人工智能技术的性能比较：a) 对学生身份进行认证，b) 确定学生是否独自一人，c) 在线练习/考试期间检测不当行为，如使用电子设备或书籍。**

另一方面，对自动系统的误报和漏报进行了分析。关于面部认证，78%的失败是由于不适当的姿势导致的过度遮挡，12%是由于光线不足，主要是由于学生站在逆光的错误位置。对于声音认证，53%的失败是由于信号的输入幅度过低，33%是由于背景噪音。在确定学生是否独自一人时，基于图像处理的监控在87%的情况下由于遮挡而失败（关于个体之间的接近或因为某些人的一部分突出在图像中），5%是因为非学生人员在图像中距离太远。最后，声音监测在85%的情况下由于将第二个声音（通常具有较低的信号幅度）与背景噪音混淆，4%的情况是因为两个或多个声音在完全相同的时刻重叠。其余的错误（包括大部分不当行为检测中的错误）是在条件允许的情况下进行的认证和监控错误。

正如结果表所示，高精度和召回率几乎使得人工干预在最终结果报告的准确性方面几乎是不必要的。然而，仍然需要人工验证。在测试过程中，所有的假阳性和假阴性（以及低真阳性和真阴性的比率）都被引导到人工交叉验证。这一举措确保了给定最终结果的100%准确性。

1. ***用户体验结果***

除其他问题外，学生被问及该系统是否适合用于验证学生身份和在线学习过程中的监督，他们在七点Likert量表中的平均得分为6.01。然而，对于教师对这种类型的系统在在线学习环境中的有效性和适用性的看法并不像学生那么积极。在表5中，分析了最显着问题的结果。

**表格五：技术适用性调查结果。**

如果我们根据最显着问题的结果来分析学生的看法，大多数调查回答都非常积极和欢迎。首先，学生表示使用任何类型的生物识别软件来监控学生是否作弊是公平的。学生在七点Likert量表中给出了6.03分的平均值，换句话说，这意味着他们认为这个问题的评价是“我同意”。其次，学生被问及是否应该在具有虚拟学习平台的面对面大学中实施软件，他们对这个问题有一个很好的看法，平均接近6（具体为5.79），对应于七点Likert量表中的“我同意”。

被问及教育中实施生物识别认证和监督软件为何如此受到87%被调查学生的欢迎，主要原因是他们意识到那些作弊的学生对其他学生是不公平的。

在这一经验中，可以看出存在相当积极的平均值。因此，学生认为生物识别认证和监控在Moodle课程中是适当的（平均在同意和非常同意之间）。此外，他们认为在本文中介绍的系统是积极的经验。

最后，教师被问及（以自由回答类型的问题）什么是调查教师结果的主要原因。值得注意的是，所有原因都与隐私问题有关；他们认为学生会感到a）被观察到（83％），b）不舒服（58％），c）担心计算机应用程序正在记录/管理他们的个人数据（72％）（根据他们的调查结果，学生并不真正担心）。任何给定的原因论证都缺乏对这种系统使用的适用性，有效性或便利性的认识。此外，其中78%明确承认这种类型的应用程序在不久的将来对在线学生进行身份验证和监督在他们的在线学习活动中的必要性。

1. **结论与未来工作**

系统有必要了解在网络学习课程中注册的学生是否与完成学习过程并获得学分的学生是同一人。在这项工作中，我们提出了一种通过持续的生物特征识别系统（面部、语音、打字）和持续在线监考系统提供连续认证身份服务的应用程序。这使得在线课程能够利用既有利于机构又有利于学生的东西。

技术结果显示，完全自动化、持续（而非预定）、被动（对学生而言）、可扩展、完全集成于LMS（硬件要求较少）、安全和私密的生物特征认证和监考解决方案是可负担且可靠的。此外，它们已存在于当前的网络学习供应商市场上。作为未来的工作，需要更强大的生物特征模型，以避免由于面部姿势和光线以及噪音条件的变化而导致的不良偏差，并仅通过人工交叉验证来保证质量保证的需要（而不是为了补充自动系统的限制）。

基于对系统使用情况的调查，研究表明，本文提出的解决方案被认为是一种能够验证学生身份的系统，目的是防止作弊，并且应该将该系统作为LMS中的必要和适当的解决方案进行集成。因此，这种生物特征系统被定位为一种有前途的工具，可用于远程教育，为改善当前的LMS提供了各种可能性。提供的结果提供了定性和定量数据，支持在远程教育中使用这种软件以防止学生在完成他们的虚拟职责时作弊。

机构、教师和学生都可以在其网络学习经验中受益于这一系统。尽管有必要进行课堂考试，以便在现实生活的专业市场中与竞争对手竞争，但学生对网络学习课程的更好和更可靠的学分感兴趣。教师可以在学科期间管理和做出决策，而无需等待课堂考试。最后，机构的尊重基于其学习系统和成绩的质量，而这些成绩是其学生。确保在网络学习环境中获得学分的人是完成了机构学习计划的人至关重要。

**致谢**

本文提出的系统是一种商业解决方案，名为Smiley Owl（SMOWL），该解决方案已根据优先权号和标题申请了专利：EP18382363-‘‘使用多模态生物识别验证在线服务用户身份的方法和系统’’。作者要感谢Smowltech公司，该公司开发了描述的系统并在全球市场上推广。他们还要感谢Vicomtech研究中心，该中心支持了本文中介绍的图像和音频处理核心算法。

**引用文献**

[1] Kryterion. (2021). Kryterion Global Testing Solutions. [Online]. Available :https://www.kryteriononline.com/

[2] A. G. Howard, M. Zhu, B. Chen, D. Kalenichenko, W. Wang, T. Weyand,M. Andreetto, and H. Adam, ‘‘MobileNets: Efficient convolutional neural networks for mobile vision applications,’’ 2017, arXiv:1704.04861.[Online]. Available: http://arxiv.org/abs/1704.04861

[3] A. A. Jain, A. K. Flynn, and P. J. Ross, Handbook of Biometrics .Springer, 2008. [Online]. Available: https://www.springer.com/gp/book/9780387710402#aboutBook

[4] ProctorU. (2021). The Leading Proctoring Solution for Online Exams.[Online]. Available: https://www.proctoru.com/

[5] Examity. (2021). Better Test Integrity. [Online]. Available: https://examity.com/

[6] PSIOnline. (2021). Certification Testing Services and Programs. [Online].Available: https://www.psionline.com/en-gb/certification/

[7] ProctorExam. (2021). Infrastructure for Online Proctoring & Invigilation.[Online]. Available: https://proctorexam.com/

[8] (2021). Assessment Tools for Learning Services. [Online]. Available: https://web.respondus.com/

[9] RemoteProctor. (2021). Remote Proctor. [Online]. Available: https://remoteproctor.com/

[10] OnVUE. (2021). OnVUE. [Online]. Available: https://home.pearsonvue.com/Test-Owner/Deliver/Online-proctored.aspx

[11] BVirtual. (2021). Online Proctoring Redefined. [Online]. Available :https://bvirtualinc.com/

[12] L. Verified. (2021). Make Your Online Learning Defensible. [Online].Available: https://learnerverified.com/

[13] Proctorio. (2021). A Comprehensive Learning Integrity Platform. [Online].Available: https://proctorio.com/

[14] Proctortrack. (2021). Trusted Exam Integrity | Remote Online Proctoring.[Online]. Available: https://www.proctortrack.com/

[15] Comprobo. (2021). Online Validation. [Online]. Available: https://comprobo.co.uk/

[16] Sumadi. (2021). Al-Powered Proctoring. [Online]. Available: https://sumadi.net/

[17] ProctorFree. (2021). Secure Online Proctoring. [Online]. Available: http://proctorfree.com/

[18] HonorLock. (2021). Honorlock On-Demand Online Proctoring Service.[Online]. Available: https://honorlock.com/

[19] ExamSoft. (2021). Learning Assessments Tools & Software. [Online].Available :https://https://examsoft.com/

[20] Y. Khlifi and H. El-Sabagh, ‘‘A novel authentication scheme for eassessments based on student behavior over e-learning platform,’’ Int. J.Emerg. Technol. Learn., vol. 12, no. 4, pp. 62–89, 2017. [Online]. Available: https://online-journals.org/index.php/i-jet/article/view/6478

[21] Z. Zhang, M. Zhang, Y. Chang, S. Esche, and C. Chassapis, ‘‘A virtual laboratory system with biometric authentication and remote proctoring based on facial recognition,’’ Comput. Educ. J., vol. 7, no. 4, pp. 74–84,2016.

[22] Z. Zhang, E.-S. Aziz, S. Esche, and C. Chassapis, ‘‘A virtual proctor with biometric authentication for facilitating distance education,’’ in Online Engineering & Internet of Things, M. E. Auer and D. G. Zutin, Eds. Cham,Switzerland: Springer, 2018, pp. 110–124.

[23] H. S. G. Asep and Y. Bandung, ‘‘A design of continuous user verification for online exam proctoring on M-learning,’’ in Proc. Int. Conf. Electr. Eng.Informat. (ICEEI), Jul. 2019, pp. 284–289.

[24] L. K. Musambo and J. Phiri, ‘‘Student facial authentication model based on OpenCV’s object detection method and QR code for Zambian higher institutions of learning,’’ Int. J. Adv. Comput. Sci. Appl., vol. 9, no. 5,Jan. 2018.

[25] F. Guillen-Gamez, I. García-Magariño, and G. Palacios, Comparative Analysis Between Different Facial Authentication Tools for Assessing Their Integration in m-Health Mobile Applications. Cham, Switzerland:Springer, Mar. 2018, pp. 1153–1161. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-319-77712-2\_110

[26] S. Sawhney, K. Kacker, S. Jain, S. N. Singh, and R. Garg, ‘‘Real-timesmart attendance system using face recognition techniques,’’ in Proc.9th Int. Conf. Cloud Comput., Data Sci. Eng. (Confluence), Jan. 2019,pp. 522–525.

[27] A. Alshbtat, N. Zanoon, and M. Alfraheed, ‘‘A novel secure fingerprintbased authentication system for student’s examination system,’’ Int. J. Adv.Comput. Sci. Appl., vol. 10, no. 9, pp. 515–519, 2019. [Online]. Available:https://thesai.org/Publications/ViewPaper?Volume=10&Issue=9&Code=IJACSA&SerialNo=68

[28] J. V. Monaco, J. C. Stewart, S.-H. Cha, and C. C. Tappert, ‘‘Behavioral biometric verification of student identity in online course assessment and authentication of authors in literary works,’’ in Proc. IEEE 6th Int. Conf.Biometrics, Appl. Syst. (BTAS), Sep. 2013, pp. 1–8.

[29] E. Flior and K. Kowalski, ‘‘Continuous biometric user authentication in online examinations,’’ in Proc. Int. Conf. Inf. Technol., Jan. 2010,pp. 488–492.

[30] Y. Atoum, L. Chen, A. X. Liu, S. D. H. Hsu, and X. Liu, ‘‘Automated online exam proctoring,’’ IEEE Trans. Multimedia, vol. 19, no. 7, pp. 1609–1624,Jul. 2017.

[31] A. Okada, I. Noguera, L. Alexieva, A. Rozeva, S. Kocdar, F. Brouns,T. Ladonlahti, D. Whitelock, and A. Guerrero-Roldán, ‘‘Pedagogical approaches for e-assessment with authentication and authorship verification in higher education,’’ Brit. J. Educ. Technol., vol. 50, no. 6,pp. 3264–3282, Nov. 2019.

[32] G. Fenu, M. Marras, and L. Boratto, ‘‘A multi-biometric system for continuous student authentication in e-learning platforms,’’ Pattern Recognit.Lett., vol. 113, pp. 83–92, Oct. 2018.

[33] L. Slusky, ‘‘Cybersecurity of online proctoring systems,’’ J. Int. Technol. Inf. Manage., vol. 29, no. 3, pp. 56–83, 2020.

[34] F. Guillen-Gamez, J. Bravo, and I. García-Magariño, ‘‘Students’ perception of the importance of facial authentication software in mood le tools,’’Int. J. Eng. Educ., vol. 33, pp. 84–90, Jan. 2017.

[35] A. Ullah, H. Xiao, and T. Barker, ‘‘A dynamic profile questions approach to mitigate impersonation in online examinations,’’ J. Grid Comput., vol. 17,no. 2, pp. 209–223, Jun. 2019, doi: 10.1007/s10723-018-9442-6.

[36] S. A. Razak, N. H. M. Nazari, and A. Al-Dhaqm, ‘‘Data anonymization using pseudonym system to preserve data privacy,’’ IEEE Access, vol. 8,pp. 43256–43264, 2020.

[37] L. Li, X. Mu, S. Li, and H. Peng, ‘‘A review of face recognition technology,’’ IEEE Access, vol. 8, pp. 139110–139120, 2020.

[38] S. Zhang, X. Zhu, Z. Lei, H. Shi, X. Wang, and S. Z. Li, ‘‘FaceBoxes:A CPU real-time face detector with high accuracy,’’ in Proc. IEEE Int. JointConf. Biometrics (IJCB), Oct. 2017, pp. 297–309. [Online]. Available:

https://www.sciencedirect.com/science/article/abs/pii/S0925231219310719

[39] L. Unzueta, W. Pimenta, J. Goenetxea, L. P. Santos, and F. Dornaika,‘‘Efficient generic face model fitting to images and videos,’’ Image Vis. Comput., vol. 32, no. 5, pp. 321–334, May 2014.

[40] X. Liu, X. Ma, J. Wang, and H. Wang, ‘‘M3L: Multi-modality mining for metric learning in person reidentification,’’ Pattern Recognit., vol. 76,pp. 650–661, Apr. 2018.

[41] F. Schroff, D. Kalenichenko, and J. Philbin, ‘‘FaceNet: A unified embedding for face recognition and clustering,’’ in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), Jun. 2015, pp. 815–823. [Online]. Available: https://ieeexplore.ieee.org/document/7298682

[42] K. Zuiderveld, ‘‘Contrast limited adaptive histogram equalization,’’ in Graphics Gems IV. 1994. [Online]. Available: https://dl.acm.org/doi/10.5555/180895.180940

[43] W. Liu, D. Anguelov, D. Erhan, C. Szegedy, S. Reed, C. Y. Fu, and A. C. Berg, SSD: Single Shot Multibox Detector (Lecture Notes in Computer Science: Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). Springer, 2016. [Online]. Available: https://www.

springer.com/gp/book/9783319464770

[44] R. A. Yeh, C. Chen, T. Y. Lim, A. G. Schwing, M. Hasegawa-Johnson, and M. N. Do, ‘‘Semantic image inpainting with deep generative models,’’ in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), Jul. 2017, pp. 6882–6890. [Online]. Available: https://ieeexplore.ieee.org/document/8100211

[45] I. J. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, ‘‘Generative adversarial nets,’’ in Proc. 27th Int. Conf. Neural Inf. Process. Syst. (NIPS), vol. 2. Cambridge, MA, USA: MIT Press, 2014, pp. 2672–2680. [Online]. Available :http://dl.acm.org/citation.cfm?id=2969033.2969125[46] D. Povey, A. Ghoshal, G. Boulianne, L. Burget, O. Glembek, N. Goel,M. Hannemann, P. Motlicek, Y. Qian, P. Schwarz, J. Silovsky, G. Stemmer, and K. Vesely, ‘‘The kaldi speech recognition toolkit,’’ in Proc. IEEE Workshop Autom. Speech Recognit. Understand. (ASRU), Waikoloa, HI, USA. Piscataway, NJ, USA: IEEE Signal Processing Society, Dec. 2011, p. 30. [Online]. Available: https://dblp.org/db/conf/asru/asru2011.html

[47] L. Wan, Q. Wang, A. Papir, and I. L. Moreno, ‘‘Generalized end-to-end loss for speaker verification,’’ in Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP), Apr. 2018, pp. 4879–4883. [Online]. Available: https://ieeexplore.ieee.org/document/8462665

[48] Q. Wang, C. Downey, L. Wan, P. A. Mansfield, and I. L. Moreno, ‘‘Speaker diarization with LSTM,’’ in Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP), Apr. 2018, pp. 5239–5243. [Online]. Available: https://ieeexplore.ieee.org/document/8462628

[49] Y. Zhong, Y. Deng, and A. K. Jain, ‘‘Keystroke dynamics for user authentication,’’ in Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. Workshops, Jun. 2012, pp. 117–123. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6239225

[50] H. Crawford, ‘‘Keystroke dynamics: Characteristics and opportunities,’’ in Proc. 8th Int. Conf. Privacy, Secur. Trust, Aug. 2010, p. 20108.

[51] A. T. Kiyani, A. Lasebae, K. Ali, M. U. Rehman, and B. Haq, ‘‘Continuous user authentication featuring keystroke dynamics based on robust recurrent confidence model and ensemble learning approach,’’ IEEE Access, vol. 8, pp. 156177–156189, 2020.

[52] A. F. M. N. H. Nahin, J. M. Alam, H. Mahmud, and K. Hasan, ‘‘Identifying emotion by keystroke dynamics and text pattern analysis,’’ Behav. Inf. Technol., vol. 33, no. 9, pp. 987–996, Sep. 2014.

[53] R. Moskovitch, C. Feher, A. Messerman, N. Kirschnick, T. Mustafić, A. Camtepe, B. Löhlein, U. Heister, S. Möller, L. Rokach, and Y. Elovici, ‘‘Identity theft, computers and behavioral biometrics,’’ in Proc. IEEE Int. Conf. Intell. Secur. Informat., Jun. 2009, pp. 155–160. [Online]. Available: https://ieeexplore.ieee.org/document/5137288

[54] L. Xiaofeng, Z. Shengfei, and Y. Shengwei, ‘‘Continuous authentication by free-text keystroke based on CNN plus RNN,’’ Procedia Comput. Sci., vol. 147, pp. 314–318, Jan. 2019.