Computer Science and Application 计算机科学与应用, 2025, 15(1), 126-135
Published Online January 2025 in Hans. https://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2025.151013

Hans汉斯

一种基于Lifelog的隐私保护模型

王玉祥，刘国奇，倪佳琦*

沈阳建筑大学计算机科学与工程学院，辽宁 沈阳

收稿日期：2024年12月22日；录用日期：2025年1月19日；发布日期：2025年1月28日

摘　要

隐私问题一直是Lifelog研究领域的热点问题之一。然而，由于目前数据集中存在隐私风险，这不但限制了研究者公开Lifelog数据集，也妨碍了研究者之间分享他们的数据集及研究成果。随着可穿戴设备和智能手机的广泛应用，Lifelog研究进入了一个新的阶段，其数据类型也变得愈发丰富，通常涵盖GPS、视频、图片、文本、语音等多种形式。针对目前多种数据格式的Lifelog数据集，我们提出了一个LPPM (Lifelog Privacy Protection Model)隐私保护模型。针对不同的数据类型，该模型可以选择不同的隐私策略。同时该模型还提出了一种基于场景的图片隐私策略SPP (Scene-Based Privacy Protection)，该策略将首先预测Lifelog图片的场景，然后根据场景选取不同的隐私保护方法。我们在LiuLifelog数据集上对提出的模型进行了验证，通过LPPM模型对数据集的处理，我们认为我们的Lifelog数据集达到了可公开的程度，图片中大多数隐私被很好地掩盖了，这进一步说明我们提出的模型方法是有效的。

关键词

Lifelog，隐私保护，隐私策略，数据公开

A Privacy Protection Model Based on Lifelog

Yuxiang Wang, Guoqi Liu, Jiaqi Ni*

School of Computer Science and Engineering, Shenyang Jianzhu University, Shenyang Liaoning

Received: Dec. 22nd, 2024; accepted: Jan. 19th, 2025; published: Jan. 28th, 2025

Abstract

Privacy issues have always been a hot topic in the field of Lifelog research. However, due to the current privacy risks present in datasets, researchers are not only limited in publicly sharing Lifelog datasets but also hindered in sharing their datasets and research findings among themselves. With the widespread adoption of wearable devices and smartphones, Lifelog research has entered a new

*通讯作者。

文章引用: 王玉祥, 刘国奇, 倪佳琦. 一种基于 Lifelog 的隐私保护模型[J]. 计算机科学与应用, 2025, 15(1): 126-135.
DOI: 10.12677/csa.2025.151013

stage, and the data types have become increasingly rich, typically encompassing various forms such as GPS, video, images, text, and audio. In response to the current multi-format Lifelog datasets, we propose an LPPM (Lifelog Privacy Protection Model) privacy protection model. For different data types, this model can choose different privacy strategies. Moreover, the model proposes a scene-based image privacy strategy called SPP (Scene-based Privacy Protection), which will first predict the scenes of Lifelog images and then select different privacy protection methods based on the scenes. We validated the proposed model on the LiuLifelog dataset. Through the processing of the dataset using the LPPM model, we believe our Lifelog dataset has reached a publishable level, with most privacy in the images well obscured. This further demonstrates the effectiveness of our proposed model and method.

Keywords

Lifelog, Privacy Protection, Privacy Strategy, Data Public

1. 引言

早在 20 世纪 40 年代，Vannevar Bush 就提出了一个 Memex 的概念，通过 Memex，人们可以对 Memex 中的内容进行文本形式的用户创建，这使得 Memex 非常接近于 Lifelog 的早期形式[1]。上世纪 80 年代，Steve Mann 开始通过可穿戴设备拍摄照片的方式来记录自己的生活经历[2]。随着数字化时代的到来和各种应用程序的发展，人们开始使用智能设备、传感技术和社交媒体记录生活，个人生活记录开始不再局限于传统的文字和图片，而是成为了一种涵盖文字[3]、图片[4]、视频[5]、音频[6]、位置[7] [8]等多种形式的多元化信息数据。这些信息数据中包含了个人日常生活中的方方面面，形成了个人大数据，也就是所谓的 Personal Big Data (PBD) [9]。这些数据被应用在各种场景、实现各种目的[10]-[12]。然而人们在记录 Lifelog 的过程中难免会涉及到个人以及周围家人朋友的隐私信息，包括但不限于家庭住址、社交关系[13]、兴趣爱好[14]、行为习惯[15]、个人健康数据[16] [17] (例如步数、睡眠质量、心率)等。在这对个人生活无所不包的数据洪流中，Lifelog 隐私的保护日益成为一个关键性的问题[18]-[20]。因此，如何在保持 Lifelog 技术便利性的同时有效保护用户隐私成为一个亟待解决的问题[21] [22]。

An-Zi Yen 在文献[23]中将 Lifelog 中的隐私保护问题列为 Lifelog 领域十大问题之一[23]。Md Sadek Ferdous 在文献[24]中首次提出了第一个关于 Lifelog 的隐私威胁模型，确定了视觉 Lifelog 的几种威胁，展示了现有的隐私指导方针和其他领域保护隐私的方法[24]。Cathal Gurrin 在文献[25]中提出了一个关于 Lifelog 隐私的定义，他将 Lifelog 分为五个阶段，他认为在这五个阶段中，只有在访问和发布阶段，必须进行限制，以保护第三方的隐私[25]。他还同 Rashmi Gupta 一起调查了其团队的 25 名 Lifelog 项目参与者，了解他们对 Lifelog 数据隐私的担忧，探讨并收集共享 Lifelog 数据参与者的隐私问题[26]。

目前在 Lifelog 隐私保护的研究领域中，主要侧重于揭示 Lifelog 存在的隐私问题和指出当前 Lifelog 中隐私保护的重要性，呼吁研究人员重视 Lifelog 隐私问题[27] [28]。但其对具体如何去保护 Lifelog 中的隐私研究工作存在明显不足，同时忽视了对其他形式的 Lifelog 的隐私问题和 Lifelog 数据如何公开的问题，最后在目前的 Lifelog 隐私研究领域也没有考虑不同的用户对于隐私的保护程度要求不同[29]-[31]。我们通过研究分析目前视觉 Lifelog 和其他形式的 Lifelog 中存在的隐私问题并根据我们的 Liulifelog 数据

集提出了 LPPM 模型，该模型对不同的 Lifelog 数据类型采用不同的隐私处理方法，可以根据用户在隐私偏好管理器中设定的隐私偏好使用隐私策略库中的不同的隐私策略处理隐私，该模型有效解决了 LiuLifelog 数据集中的隐私问题和用户个性化隐私问题。而后本文根据 Lifelog 图片数据的特性进一步研究了一项针对 Lifelog 图片数据的隐私保护策略 SPP (Scene privacy policy)。

本文的章节总共分为 6 节，本节为引言。第二节介绍了我们的生活日志系统和作者 13 年间收集的 LiuLifelog 数据集，介绍了数据集的特点。第三节阐述了 LPPM 模型的整体架构和针对图片隐私提出的隐私策略。第四节通过实验对 SPP 图片隐私策略进行验证。第五节建立原型系统，用以验证 LPPM 模型的效果。最后一节对实验和模型进行总结，并展望未来的研究方向。

2. 相关工作

2.1. LiuLifelog Project

从 2011 年开始我们发起了一个 LiuLifelog 项目，同时为了构建丰富的 Lifelog 数据集，我们开发了一款生活日志系统。它由 Lifelog 上传 app 和后台数据管理系统组成，该系统用于我们团队内部上传数据，并在内部分享这些数据。到目前为止共有 22 名成员加入了我们，为整个项目提供了 4 万多条数据。读者可以通过访问网站(http://www.lifelog.vip/)查看我们用这些数据做出的研究。同时，我们还提供了可安装在手机上的应用程序。我们期待更多的人加入我们，开始上传他们的生活记录。

2.2. LiuLifelog 数据集

LiuLifelog 数据集不但数据类型多样，涵盖图片、视频、音频、位置、文本等类型，而且数据集的收集时间长且具有较高的连续性。例如我们团队有一名参与者从 2011 年开始每天不间断的上传至少一条记录，充分展现了个人生活在不同时间段的变化和趋势。此外，LiuLifelog 数据集贡献者较多，覆盖不同年龄层，这使得研究者能够从多角度分析不同年龄群体的生活方式和行为模式，是进行 Lifelog 研究的理想数据集。我们团队一直使用该数据集进行 Lifelog 领域的相关研究，但由于隐私原因，暂时无法公开数据。例如在公园、街道、车站、机场等公共空间拍照时，照片中可能会包含其他旁观者的形象，这涉及到他们的隐私问题。

在图 1 中展示了一些风景、游玩、运动、饮食类型的 lifelog 数据，这些数据均为可公开的内容，不包含需要隐私遮挡的部分。

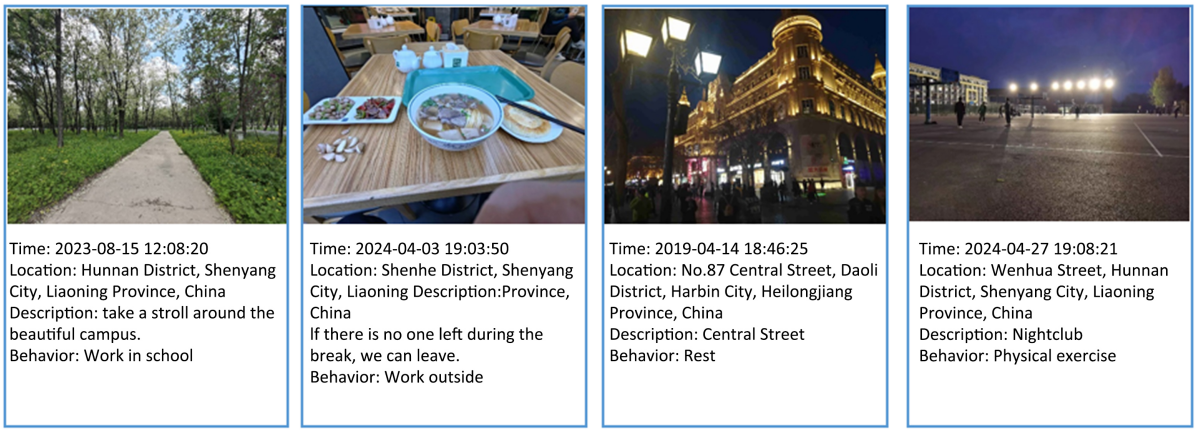

Figure 1. Lifelog data examples
图 1. Lifelog 数据示例

3. LPPM 模型

3.1. 模型的整体架构

为了解决 Lifelog 数据集公开的问题，我们考虑从数据公开时的隐私处理入手，提出了一个 LPPM 隐私保护模型。该模型包括隐私处理模块共包含用户、隐私偏好管理器、数据处理器、隐私处理引擎、隐私策略库、算法库六个主体。模型的整体架构如图 2 所示。

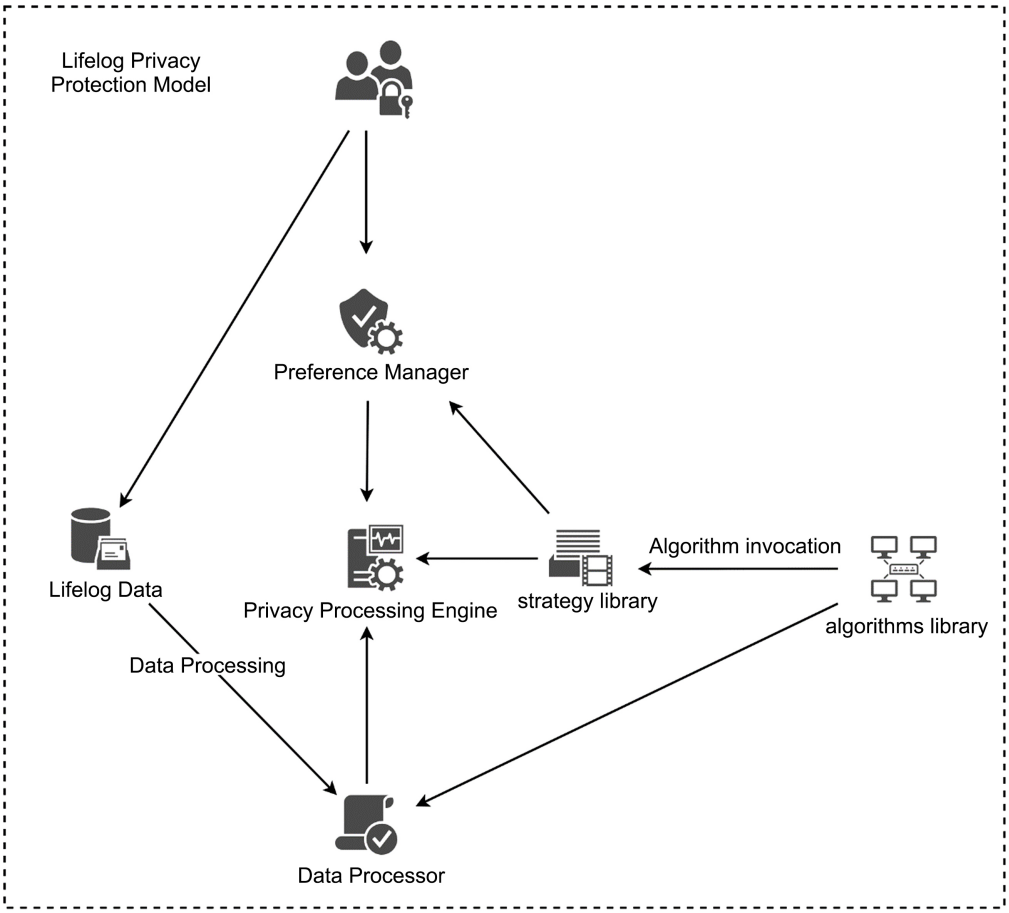

Figure 2. Lifelog privacy protection model
图 2. Lifelog 隐私保护模型

在图 2 Lifelog 隐私保护模型中，用户作为模型的参与者可以上传个人的 Lifelog 数据并在隐私偏好管理器中设定自己的隐私策略，控制个人 Lifelog 数据的隐私保护程度。

隐私偏好管理器负责记录用户选择的隐私策略，并允许用户可以对策略进行组合使用。对不同形式的数据用户可以选择不同的隐私策略例如：针对图片的隐私处理策略，用户可以使用隐私区域遮挡和模糊处理两种策略进行隐私保护，针对位置的隐私处理可以使用模糊位置和延迟位置公开的策略进行隐私保护。隐私偏好管理器，解决了不同用户对隐私程度要求不同的问题，提供了个性化的隐私保护方式。

数据处理器主要职责是对 Lifelog 数据进行预处理，数据处理器首先会根据数据的类型进行分类处理将其分为文本、图片、视频、GPS、音频，然后调用算法库中与该数据类型对应的特定算法，执行数据格式转换、编码转换、去重等预处理操作。数据分类处理降低了数据类型不同时的隐私处理复杂度，为解

决多种形式的 Lifelog 的隐私问题提供了基础，同时统一的数据格式提高了隐私处理的效率。

策略库是一个存储和管理隐私处理策略的集合，分别为 Lifelog 中的文本、图片、视频、音频、GPS 类型的隐私处理提供了相应类型的多种策略，以满足不同用户和隐私处理的需求。例如，对于文本的隐私策略有基于规则库的敏感词汇匿名化处理，文本加噪，语义变换等多种策略。通过这些策略的应用，确保经过处理的 Lifelog 数据符合用户和相关法规的要求。

算法库是整个模型的核心组成部分，负责存储与数据预处理和隐私策略相关的各种算法，例如加密算法 FF1、RSA、AES 等和位置模糊算法 Geo-Indistinguishability、Spatial Cloaking 等。数据处理器依靠算法库中的算法对数据进行预处理，隐私策略的具体实现依赖于算法库中的算法。

隐私处理引擎是模型的调度中心，负责整个模型各部分的调度。它首先接收数据处理器处理的数据结果，然后从隐私偏好管理器中获取用户的设定隐私策略。接着隐私处理引擎调用策略库中的相应策略，并将数据交由相应的算法进行处理。

3.2. SPP 图片隐私保护策略

图片隐私保护的目标是将图片中的敏感信息遮挡起来，但是并不是所有的图片都要执行一样的标准。举例来说，对于一张脏乱的卧室照片，由于其包含大量私人信息，可能需要完全遮挡房间的内容，以防止私人信息泄露；而在街道、游乐园、车站这些公共场合的图片中，仅需遮挡人脸、车牌等个人识别信息即可，因为这些场景中的敏感信息相对较少。

为了在图片的可用性和隐私保护之间取得平衡，考虑到不同场景下需要进行遮挡的敏感信息不同，为此我们提出了一种基于场景分类的图片隐私策略 SPP。如表 1 所示，我们分析了我们的 Liulifelog 数据集，将场景分为高隐私场景例如家庭场所中等私人空间，中隐私场景例如工作场所、会议室等半开放空间，低隐私场景例如公园、街道等完全开放空间。

Table 1. Image privacy scenarios
表 1. 图片隐私场景

高隐私场景	中隐私场景	低隐私场景
家庭场所	办公室	公园、街道、购物中心
私人汽车内	实验室	车站、机场
医院病房	会议室	超市
……	……	……

SPP 策略首先对 Lifelog 图片采用图片分类的方式进行场景分类，对高隐私场景的图片采用整体像素全部设为黑色的不可恢复遮挡的方法，对中、低隐私的图片继续使用目标检测算法检测隐私，然后对目标检测出的隐私目标采用选择性区域像素全部设为黑色的不可恢复遮挡方式进行处理后公开发布。通过这种基于场景分类的图片隐私策略，我们可以更精确地保护图片中的隐私，这种策略不仅提高了隐私保护的效率，还避免了过度遮挡带来的不便。

4. 实验结果与分析

4.1. 实验目的

为了验证本文提出的 SPP 图片隐私保护策略，我们采用了 YOLOv8 算法模型进行场景分类和隐私目

标检测实验。通过 YOLOv8 识别图片中的场景和隐私目标后，根据识别结果进行隐私保护。YOLOv8 同时具备目标检测和图片分类功能，并且相比于其他深度学习模型在速度、实时性和稳定性等方面更具优势，因此我们选择 YOLOv8 进行场景分类和隐私目标检测实验。

4.2. 数据预处理

我们共使用了场景分类和隐私目标检测两个数据集进行实验，数据集中的图片来源于 LiuLifelog 数据集、个人拍摄以及网络。其中场景分类数据集包含 6302 张图片，其中包含 1009 张会议室场景图，1190 张办公室场景图，1450 张家庭室内场景图，1326 张公园场景图，1327 张交通街道场景图。实验将场景分类数据集随机划分为训练集和验证集，比例为 8:2。隐私目标检测数据集中包含了我们标注的 1029 张图片共涵盖了人脸、车牌、屏幕、文档、地标、二维码、身份证件 7 个类别。本次实验将目标检测数据集也随机划分为训练集和验证集，比例为 8:2。

4.3. 实验方式和评价指标

我们使用 YOLOv8-cls 分类模型对场景分类数据集中的图片进行了训练，得到一个训练好的分类模型用于场景分类。随后，我们使用 YOLOv8-s 目标检测模型对隐私目标检测数据集进行了训练，得到一个训练好的目标检测模型用于隐私目标检测。首先，我们通过 YOLOv8-cls 分类模型区分不同的场景。对于高隐私场景(如家庭室内场景)，我们对整个场景进行遮挡；对于中隐私场景(如会议和工作场景)，我们通过 YOLOv8 目标检测模型找到图片中的人脸、屏幕、文档、二维码和身份证件，然后进行遮挡；对于低隐私场景(如公园、街道场景)，我们同样采用目标检测找到图片中的人脸、车牌和地标，然后进行遮挡。

我们针对于图片场景分类和隐私目标检测的效果，分别使用准确度(Accuracy)、精确率(Precision)、召回率(Recall)、F1 分数和平均精确度均值(mAP@0.5)作为评价指标，评价 yolov8 算法在图片场景分类和隐私目标检测方面的有效性。

4.4. 实验结果和评估

图片场景分类的评估指标主要为图片的分类准确度(Accuracy)，同时采用精确率(Precision)、召回率(Recall)和 F1 分数来分析实验结果。

我们采用的 YOLOv8s-cls 分类模型在场景分类数据集上经过 300 轮训练后，其评估指标结果见表 2。训练后模型的所有类别最好的分类准确度(accuracy_top1)达到了 0.931，这证实了该模型在图像隐私检测方面的有效性。

Table 2. YOLOv8 classification model's classification results on the scene classification dataset
表 2. YOLOv8 分类模型在场景分类数据集分类结果

类别	精确度	召回率	F1 分数
home	0.951	0.934	0.942
office	0.876	0.924	0.899
conference	0.911	0.920	0.914
park	0.976	0.929	0.952
street	0.929	0.939	0.934

隐私目标检测的评估指标主要为目标检测的平均精确度均值(mAP@0.5)，同时采用精确率(Precision)、召回率(Recall)和 F1 分数来分析实验结果。

我们采用的 YOLOv8s 目标检测模型在隐私检测数据集上经过 500 轮训练后，其评估指标结果见表 3。训练好的 YOLOv8 目标检测模型，在所有类别中，平均精确度均值(mAP@0.5)达到了 0.885。这证实了该模型在图像隐私检测方面的有效性。

Table 3. The detection results of the YOLOv8s object detection model on the private dataset
表 3. YOLOv8s 目标检测模型在隐私数据集检测结果

类别	精确度	召回率	F1 分数
人脸	0.856	1	0.922
二维码	0.733	0.936	0.822
车牌	0.878	0.867	0.872
文档	0.721	0.898	0.800
屏幕	0.667	0.878	0.758
地标	0.962	0.862	0.909
身份证件	0.900	0.947	0.923

为了展示 SPP 策略真实应用的效果，我们在图 3 中展示了一些隐私保护的效果。通过对比原始图像和处理后的图像，可以清晰地观察到隐私保护的遮挡效果。

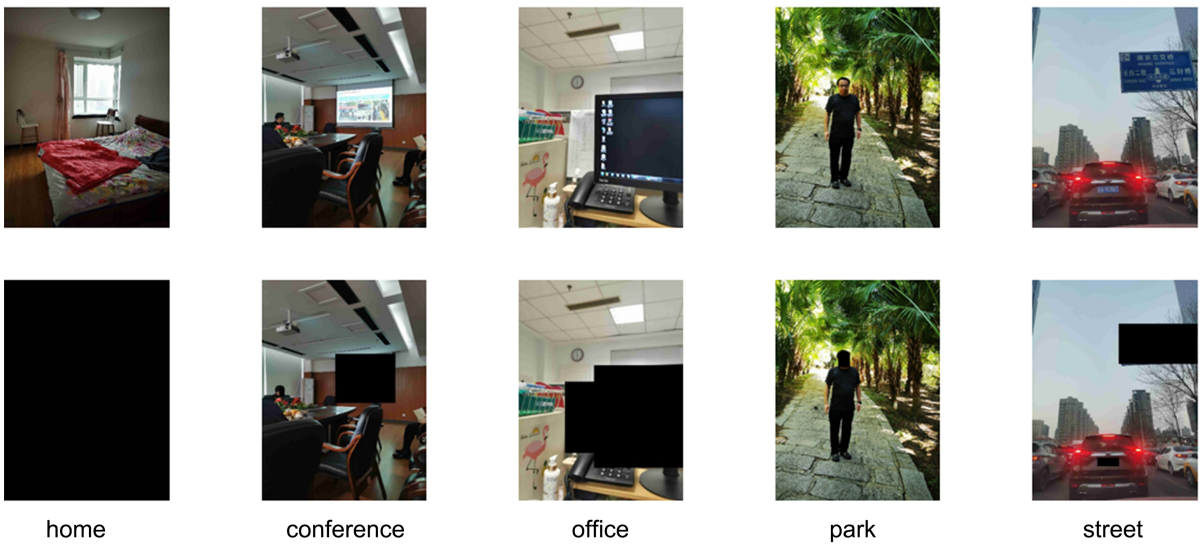

Figure 3. Image privacy processing effect comparison chart
图 3. 图片隐私处理效果对比图

在图 3 中，在卧室的家庭场景图中，图像中的所有内容都被完全遮挡，使得任何私人信息都无法被识别。在会议场景图中我们遮挡了人脸、屏幕以保护参与者的隐私和会议信息。在该工作场景图中我们

遮挡了屏幕和文档，以防止泄露敏感的工作资料。在公园场景图中我们遮挡了出现的人脸，防止泄露个人和“第三者”的肖像隐私。在街道场景图中我们遮挡了路标和车牌，防止泄露个人车牌和个人位置信息。

5. 模型验证

我们开发了一个基于 Python 的原型系统，用于验证 LPPM 模型。该系统已经作为开源项目发布在 Github 上(https://github.com/wyx17623/LPPM)，读者可以通过访问网站(http://www.lifelogwyx.asia)去体验系统的功能。原型系统目前仅实现了 Lifelog 图片类型的处理，研究人员可以下载测试图片数据，测试系统的功能。该项目提供了一个完整的框架，用于验证 LPPM 模型的表现，我们希望能够吸引更多的开发者和研究者参与其中，共同推动 Lifelog 隐私保护的发展。

原型系统内置了 SPP 隐私策略、ROI 隐私策略、None 隐私策略等策略，以提供不同级别和方式的隐私保护，研究人员可以设定个人隐私偏好，使用这些策略处理图片。接下来我们以这三种策略为例，展示它们的隐私保护效果，如图 4 所示。

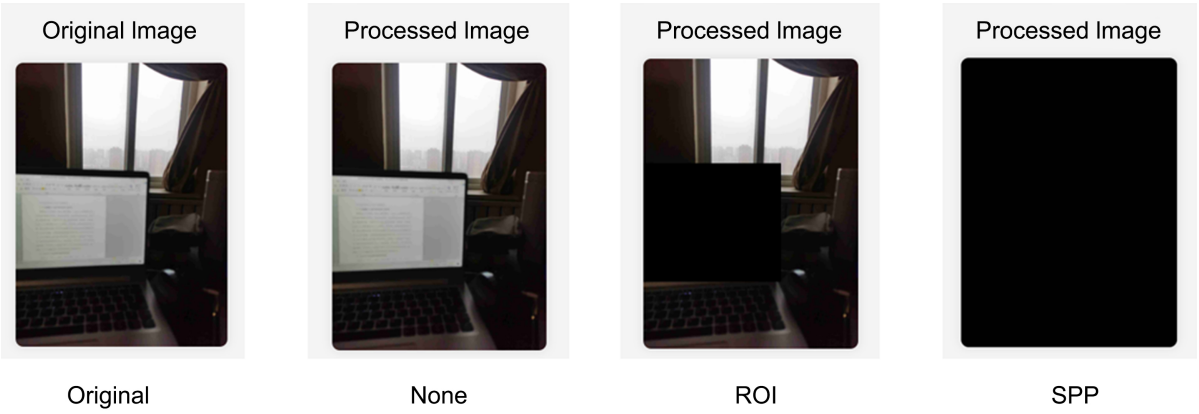

Figure 4. The effects of different privacy policies
图 4. 不同的隐私策略效果图

我们选择了不同的策略对一张卧室图片进行隐私处理，None 隐私策略是不使用任何隐私策略，直接展示原始图片，ROI 隐私策略是仅对所有隐私目标区域进行遮挡处理，SPP 策略是基于场景隐私保护的策略，对高隐私的卧室场景全部遮挡。通过该原型系统，我们验证了 LPPM 模型的可行性。

6. 结论与展望

隐私问题一直困扰着 Lifelog 研究者公开和共享他们的数据集和研究成果，由于目前 Lifelog 数据形式多样，并且每个人对隐私保护的要求不同。为了应对多种数据格式和个性化隐私保护带来的隐私挑战，我们提出了一个名为 LPPM (Lifelog Privacy Protection Model)的隐私保护模型。该模型从 Lifelog 数据公开的角度出发，综合考虑了多种形式的 Lifelog 数据及个人隐私偏好，解决了不同数据类型的 Lifelog 隐私处理和用户个性化隐私的问题。Lifelog 数据包括文字、视频、音频和图片等多种形式，而我们重点研究了图片的隐私保护问题。我们针对 Lifelog 图片数据提出了基于场景的隐私保护策略，实现了在图片的可用性和隐私保护之间的平衡。我们处理了 LiuLifelog 数据集中的部分图片，结果表明，经过 LPPM 模型的处理，大多数隐私数据都得到了有效掩盖，使我们的 Lifelog 数据集达到了可以公开的程度，用户现在可以在网络上访问我们的数据集，而无需担心隐私泄露。

尽管我们提出的模型在图片隐私保护方面取得了显著成效，但未来的研究仍需进一步提升隐私保护的精确性和全面性。我们计划在更精确的识别算法、视频数据的隐私处理、多模态数据融合以及用户控制和透明度方面进行深入研究，确保图片中所有敏感信息都能被准确识别和处理，并扩展至视频数据中，通过优化隐私保护策略，进一步提升 Lifelog 数据隐私保护的有效性和可靠性，促进 Lifelog 研究的公开与共享，推动该领域的发展。

基金项目

辽宁省教育厅自然基金项目(LJKZ0595)。

参考文献

[1] Rawassizadeh, R. (2012) Towards Sharing Life-Log Information with Society. *Behaviour & Information Technology*, **31**, 1057-1067. https://doi.org/10.1080/0144929x.2010.510208

[2] Wolf, K., Schmidt, A., Bexheti, A. and Langheinrich, M. (2014) Lifelogging: You're Wearing a Camera? *IEEE Pervasive Computing*, **13**, 8-12. https://doi.org/10.1109/mprv.2014.53

[3] Yen, A., Huang, H. and Chen, H. (2019) Personal Knowledge Base Construction from Text-Based Lifelogs. *Proceedings of the 42nd International ACM SIGIR Conference on Research and Development in Information Retrieval*, New York, 21-25 July 2019, 185-194. https://doi.org/10.1145/3331184.3331209

[4] Rossetto, L., Inel, O., Lange, S., Ruosch, F., Wang, R. and Bernstein, A. (2023) Multi-Mode Clustering for Graph-Based Lifelog Retrieval. *Proceedings of the 6th Annual ACM Lifelog Search Challenge*, New York, 12-15 June 2023, 36-40. https://doi.org/10.1145/3592573.3593102

[5] Climent-Pérez, P., Spinsante, S., Mihailidis, A. and Florez-Revuelta, F. (2020) A Review on Video-Based Active and Assisted Living Technologies for Automated Lifelogging. *Expert Systems with Applications*, **139**, Article 112847. https://doi.org/10.1016/j.eswa.2019.112847

[6] Ziaei, A., Sangwan, A., Kaushik, L. and Hansen, J.H.L. (2015) Prof-Life-Log: Analysis and Classification of Activities in Daily Audio Streams. 2015 *IEEE International Conference on Acoustics, Speech and Signal Processing* (*ICASSP*), South Brisbane, 19-24 April 2015, 4719-4723. https://doi.org/10.1109/icassp.2015.7178866

[7] Liu, G., Rehman, M.U. and Wu, Y. (2021) Toward Storytelling from Personal Informative Lifelogging. *Multimedia Tools and Applications*, **80**, 19649-19673. https://doi.org/10.1007/s11042-020-10453-z

[8] Liu, G., Zheng, Q., Niu, S. and Ma, J. (2024) Research and Application of the Global Positioning System (GPS) Clustering Algorithm Based on Multilevel Functions. *Journal of Computational Methods in Sciences and Engineering*, **24**, 357-368. https://doi.org/10.3233/jcm-237061

[9] Gurrin, C., Smeaton, A.F. and Doherty, A.R. (2014) Life-Logging: Personal Big Data. *Foundations and Trends in Information Retrieval*, **8**, 1-125. https://doi.org/10.1561/1500000033

[10] Spiess, F., Gasser, R., Heller, S., Rossetto, L., Sauter, L., van Zanten, M., *et al*. (2021) Exploring Intuitive Lifelog Retrieval and Interaction Modes in Virtual Reality with vitrivr-VR. *Proceedings of the 4th Annual on Lifelog Search Challenge*, Taipei, 21 August 2021, 17-22. https://doi.org/10.1145/3463948.3469061

[11] Ninh, V.T., Le, T.K., Zhou, L., Piras, L., Riegler, M.A., Halvorsen, P., *et al*. (2020) Overview of Image CLEF Lifelog 2020: Lifelog Moment Retrieval and Sport Performance Lifelog. 2020 *CEUR Workshop Proceedings*, Luxembourg, 3-4 December 2020, Article 2096.

[12] Liu, G., Rehman, M.U. and Wu, Y. (2021) Personal Trajectory Analysis Based on Informative Lifelogging. *Multimedia Tools and Applications*, **80**, 22177-22191. https://doi.org/10.1007/s11042-021-10755-w

[13] Duy Dinh, T., Nguyen, D. and Tran, M. (2018) Social Relation Trait Discovery from Visual Lifelog Data with Facial Multi-Attribute Framework. *Proceedings of the 7th International Conference on Pattern Recognition Applications and Methods*, Madeira, 16-18 January 2018, 665-674. https://doi.org/10.5220/0006749206650674

[14] Mafrur, R., Nugraha, I.G.D. and Choi, D. (2015) Modeling and Discovering Human Behavior from Smartphone Sensing Life-Log Data for Identification Purpose. *Human-Centric Computing and Information Sciences*, **5**, Article No. 31. https://doi.org/10.1186/s13673-015-0049-7

[15] Chung, S., Jeong, C.Y., Lim, J.M., Lim, J., Noh, K.J., Kim, G., *et al*. (2021) Real-World Multimodal Lifelog Dataset for Human Behavior Study. *ETRI Journal*, **44**, 426-437. https://doi.org/10.4218/etrij.2020-0446

[16] Kim, J.W., Lim, J.H., Moon, S.M. and Jang, B. (2019) Collecting Health Lifelog Data from Smartwatch Users in a Privacy-Preserving Manner. *IEEE Transactions on Consumer Electronics*, **65**, 369-378.

https://doi.org/10.1109/tce.2019.2924466

[17] Jalal, A., Quaid, M.A.K., Tahir, S.B.U.D. and Kim, K. (2020) A Study of Accelerometer and Gyroscope Measurements in Physical Life-Log Activities Detection Systems. *Sensors*, **20**, Article 6670. https://doi.org/10.3390/s20226670

[18] Ksibi, A., Alluhaidan, A.S.D., Salhi, A. and El-Rahman, S.A. (2021) Overview of Lifelogging: Current Challenges and Advances. *IEEE Access*, **9**, 62630-62641. https://doi.org/10.1109/access.2021.3073469

[19] Jacquemard, T., Novitzky, P., O'Brolcháin, F., Smeaton, A.F. and Gordijn, B. (2013) Challenges and Opportunities of Lifelog Technologies: A Literature Review and Critical Analysis. *Science and Engineering Ethics*, **20**, 379-409. https://doi.org/10.1007/s11948-013-9456-1

[20] Ahmad, I., Farzan, R., Kapadia, A. and Lee, A.J. (2020) Tangible Privacy. *Proceedings of the ACM on Human-Computer Interaction*, **4**, 1-28. https://doi.org/10.1145/3415187

[21] Elagroudy, P., Khamis, M., Mathis, F., Irmscher, D., Sood, E., Bulling, A., *et al*. (2023) Impact of Privacy Protection Methods of Lifelogs on Remembered Memories. *Proceedings of the* 2023 *CHI Conference on Human Factors in Computing Systems*, Hamburg, 23-28 April 2023, 1-10. https://doi.org/10.1145/3544548.3581565

[22] Price, B.A., Stuart, A., Calikli, G., Mccormick, C., Mehta, V., Hutton, L., *et al*. (2017) Logging You, Logging Me. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, **1**, 1-18. https://doi.org/10.1145/3090087

[23] Yen, A., Huang, H. and Chen, H. (2021) Ten Questions in Lifelog Mining and Information Recall. *Proceedings of the* 2021 *International Conference on Multimedia Retrieval*, Taipei, 21-24 August 2021, 511-518. https://doi.org/10.1145/3460426.3463607

[24] Ferdous, M.S., Chowdhury, S. and Jose, J.M. (2016) Privacy Threat Model in Lifelogging. *Proceedings of the* 2016 *ACM International Joint Conference on Pervasive and Ubiquitous Computing*: *Adjunct*, Heidelberg, 12-16 September 2016, 576-581. https://doi.org/10.1145/2968219.2968324

[25] Gurrin, C., Albatal, R., Joho, H. and Ishii, K. (2014) Digital Enlightenment Yearbook 2014. IOS Press, 49-73.

[26] Gupta, R., Crane, M. and Gurrin, C. (2020) Considerations on Privacy in the Era of Digitally Logged Lives. O*nline Information Review*, **45**, 278-296. https://doi.org/10.1108/oir-04-2018-0119

[27] Steil, J., Koelle, M., Heuten, W., Boll, S. and Bulling, A. (2019) PrivacEye: Privacy-Preserving Head-Mounted Eye Tracking Using Egocentric Scene Image and Eye Movement Features. *Proceedings of the* 11*th ACM Symposium on Eye Tracking Research & Applications*, Colorado, 25-28 June 2019, 1-10. https://doi.org/10.1145/3314111.3319913

[28] Chowdhury, S., Ferdous, M.S. and Jose, J.M. (2016) Exploring Lifelog Sharing and Privacy. *Proceedings of the* 2016 *ACM International Joint Conference on Pervasive and Ubiquitous Computing*: *Adjunct*, Heidelberg, 12-16 September 2016, 553-558. https://doi.org/10.1145/2968219.2968320

[29] Hoyle, R., Templeman, R., Anthony, D., Crandall, D. and Kapadia, A. (2015) Sensitive Lifelogs. *Proceedings of the* 33*rd Annual ACM Conference on Human Factors in Computing Systems*, Seoul, 18-23 April 2015, 1645-1648. https://doi.org/10.1145/2702123.2702183

[30] Chertchom, P., Tanimoto, S., Ohba, H., Kohnosu, T., Kobayashi, T., Sato, H., *et al*. (2017) A Lifelog Data Portfolio for Privacy Protection Based on Dynamic Data Attributes in a Lifelog Service. In: *Studies in Computational Intelligence*, Springer, 107-120. https://doi.org/10.1007/978-3-319-62048-0_8

[31] Kim, J.W., Moon, S., Kang, S. and Jang, B. (2020) Effective Privacy-Preserving Collection of Health Data from a User's Wearable Device. *Applied Sciences*, **10**, Article 6396. https://doi.org/10.3390/app10186396