Computer Vision

Ferm et al. (2022) focused on the impact of AI on data privacy, particularly from a consumer perspective. They examined how AI technologies collect data and the resulting inherent privacy concerns. The authors refer to types of AI) like NLP, ML, and deep learning, while showcasing their applications and privacy implications. Through case studies that involve computer vision, including Clearview AI and Hello Barbie, the authors illustrate real-world scenarios of privacy breaches, underscoring the urgent need for transparent and ethical data handling practices in the AI domain. Harichandana et al. (2022) proposed a novel framework to detect sensitive content in images, particularly focusing on individuals with disabilities, to prompt photographers to receive consent before capturing or sharing such images. The system leverages object detection and eye-gaze detection techniques, utilizing a custom-curated dataset for training. The research emphasizes ethical considerations in digital photography, aiming to protect the privacy of vulnerable individuals. It demonstrates the feasibility of implementing a lightweight, efficient privacy-preserving AI system on resource-constrained devices. Liu et al. (2019) presented a new framework and algorithms designed to safeguard image privacy against both human observers and AI systems. They integrated adversarial image perturbation that is effective against AI, with obfuscation techniques aimed at human adversaries. Through experiments, the authors demonstrate the effectiveness of their methods across different types of attackers, addressing the heightened privacy risks posed by the advancement of AI in analyzing multimedia data.

References

Ferm, L.-E. C., Quach, S., & Thaichon, P. (2022). Data privacy and artificial intelligence (AI): how AI collects data and its impact on data privacy. In *Artificial Intelligence for Marketing Management* (pp. 163--174). Routledge. Retrieved from https://www.taylorfrancis.com/chapters/edit/10.4324/9781003280392-13/data-privacy-artificial-intelligence-ai-lars-erik-casper-ferm-sara-quach-park-thaichon

Harichandana, B., Agarwal, V., Ghosh, S., Ramena, G., Kumar, S., & Raja, B. R. (2022). PrivPAS: A real time Privacy-Preserving AI System and applied ethics. *2022 IEEE 16th International Conference on Semantic Computing (ICSC)* (pp. 9--16). IEEE. doi:https://doi.org/10.1109/ICSC52841.2022.00010

Liu, B., Xiong, J., Wu, Y., Ding, M., & Wu, C. M. (2019). Protecting multimedia privacy from both humans and AI. *2019 IEEE international symposium on broadband multimedia systems and broadcasting (BMSB)* (pp. 1--6). IEEE. doi:https://doi.org/10.1109/BMSB47279.2019.8971914