Politecnico di Torino

ScuDo
Scuola di Dottorato ~ Doctoral School
WHAT YOU ARE, TAKES YOU FAR

Doctoral Dissertation
Doctoral Program in Computer Engineering (37^{th}cycle)

Tackling Data Challenges in Computer Vision

By

Luca Piano

******

Supervisor(s):
Prof. Fabrizio Lamberti, Supervisor
Prof. Morra Lia, Co-Supervisor,
Prof. Chiaberge Marcello, Co-Supervisor

Doctoral Examination Committee:
Prof. Lucile Sassatelli, Université Côte d'Azur (Referee)
Prof. Lorenzo Seidenari, University of Florence (Referee)

Politecnico di Torino
2025

Summary

Deep learning (DL) has transformed computer vision (CV), enabling significant advancements in tasks such as image recognition, segmentation, and generation. These breakthroughs are largely driven by the availability of large, diverse datasets that allow AI models to become more robust and generalizable. However, many existing datasets are large and uncurated, often containing privacy-sensitive or biased information, which raises ethical and regulatory concerns. Synthetic data, generated through methods like computer graphics (CG) and diffusion models (DMs), provides a scalable and controllable solution to these issues, helping to address biases and privacy risks while improving model performance. Furthermore, integrating domain knowledge into the training process can boost model robustness and adaptability, leading to more ethical and efficient AI applications.

This research focuses on three main areas. The first research area focuses on using synthetic data to address data scarcity in object re-identification (ReID). This includes leveraging CG to create diverse datasets that help deep neural networks (DNNs) learn robust representations, especially in challenging real-world conditions like variations in lighting, weather, occlusion, and long-term changes in object appearance. Specifically, the research explores the novel task of re-identifying damaged objects, using bicycles as a case study. The synthetic dataset, BBBicycles, is introduced as the first dataset for damaged object ReID, aiming to improve model performance by providing varied examples of deformations, damages, and missing parts, which are difficult to capture in real-world data.

The second area delves into the use of generative models, particularly DMs, to address challenges in data privacy and utility. This research focuses on using DMs to generate synthetic data that protects privacy while maintaining the usability of the data for various applications. The research explores how DMs, when controlled using auxiliary networks, can enhance anonymization capabilities, ensuring that personal data is unidentifiable while retaining critical information. By leveraging prior knowledge within these models, the research aims to make the anonymization process more efficient and accessible, thus mitigating privacy risks in sensitive domains like healthcare, security, and autonomous systems. This approach seeks to improve privacy protection not only for individuals but also for background elements, offering a more comprehensive solution to data privacy concerns.

The third area focuses on addressing overinterpretation in image classifiers, which can lead to faulty predictions when models rely on semantically meaningless patterns, often found in small areas of an image. This research explores a novel approach to reduce classifiers' confidence in these irrelevant patterns, without requiring explicit human annotations. By fine-tuning the classifier with this technique, the study aims to minimize the reliance on such patterns, improving alignment with human perceptions, enhancing robustness against domain shifts, and increasing resistance to adversarial attacks.

In conclusion, the dissertation presents advances in DL methodologies for CV, with a focus on synthetic data generation, model robustness, and efficient learning strategies. Explores the potential of synthetic datasets to address challenges such as data scarcity, privacy concerns, and dataset biases. The research also introduces a technique to improve the robustness of DNNs against adversarial attacks and domain shifts. Despite progress, the dissertation highlights ongoing challenges, such as bridging the synthetic-to-real domain gap and optimizing robustness strategies across diverse tasks.