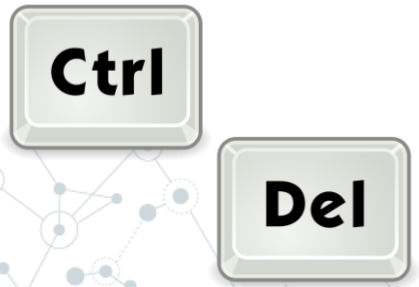
UNIVERSITÄT PADERBORN

Machine Unlearning for Face Recognition

Responsible AI for Biometrics Group

Dr.-Ing. Philipp Terhörst

Rouqaiah Al-Refai



Winter Semester 2025/26

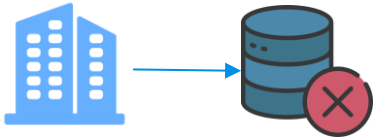
UNIVERSITÄT PADERBORN

Motivation

User A shares face images with a company for authentication.

Later, the user revokes consent and requests **data removal** (GDPR).

Data is deleted from the database, and model retrained.



Problem: retraining from scratch is **costly** and **slow** especially for face recognition systems.

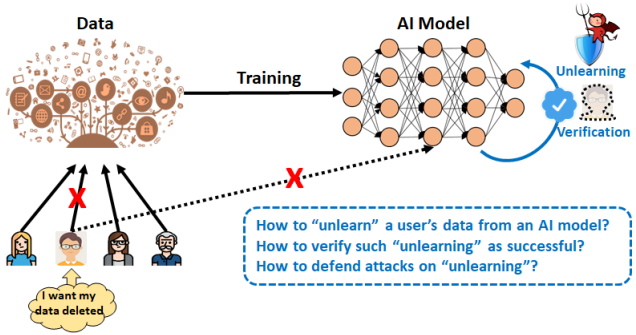
Possible solution: Machine Unlearning for Face Recognition.

What is Machine Unlearning?

Removing the influence (**forgetting**) of **undesirable data points** and the associated **model capabilities** while preserving the **model utility** on unrelated information, all without the need for costly and prolonged **retraining**.

Main goals of MU research:

- Computation Efficiency
- Forgetting Quality
- Preserved Model Utility



Qu, Youyang, et al. "Learn to unlearn: A survey on machine unlearning.", 2023

UNIVERSITÄT PADERBORN

Machine Unlearning Types

How is Machine Unlearning achieved?

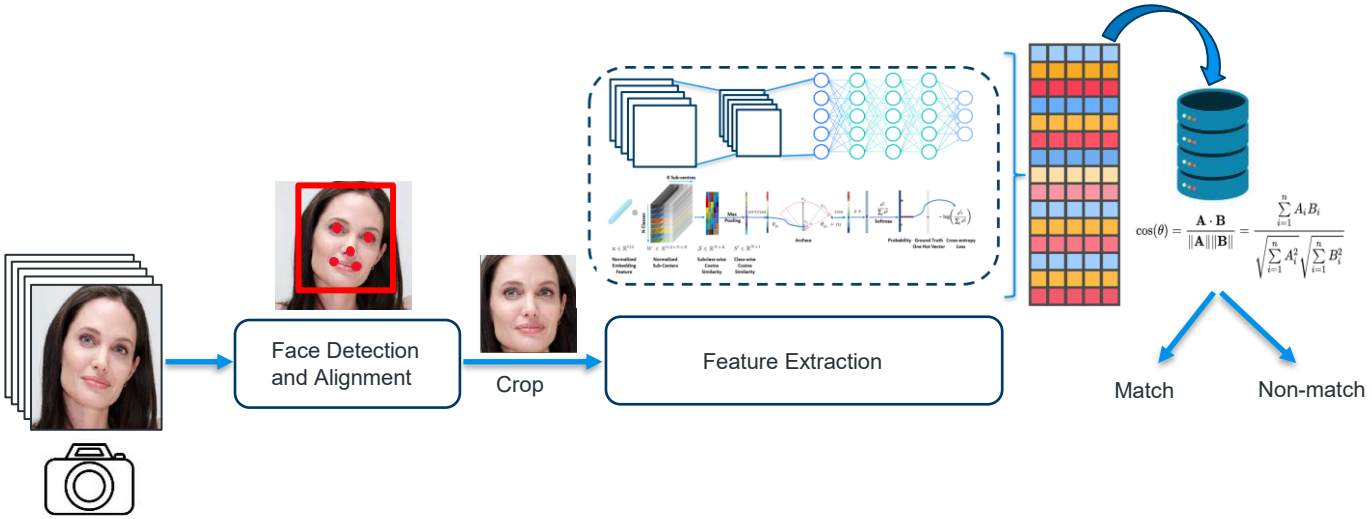
Exact MU

- Retrain-based, guarantees removal (e.g., SISA shard and aggregate retraining)
- Reliable but computationally expensive and inflexible

Approximate MU

- Removes influence via selective parameter updates or architecture constraints.
- Faster, more scalable
- Hard to verify forgetting

Face Recognition Pipeline

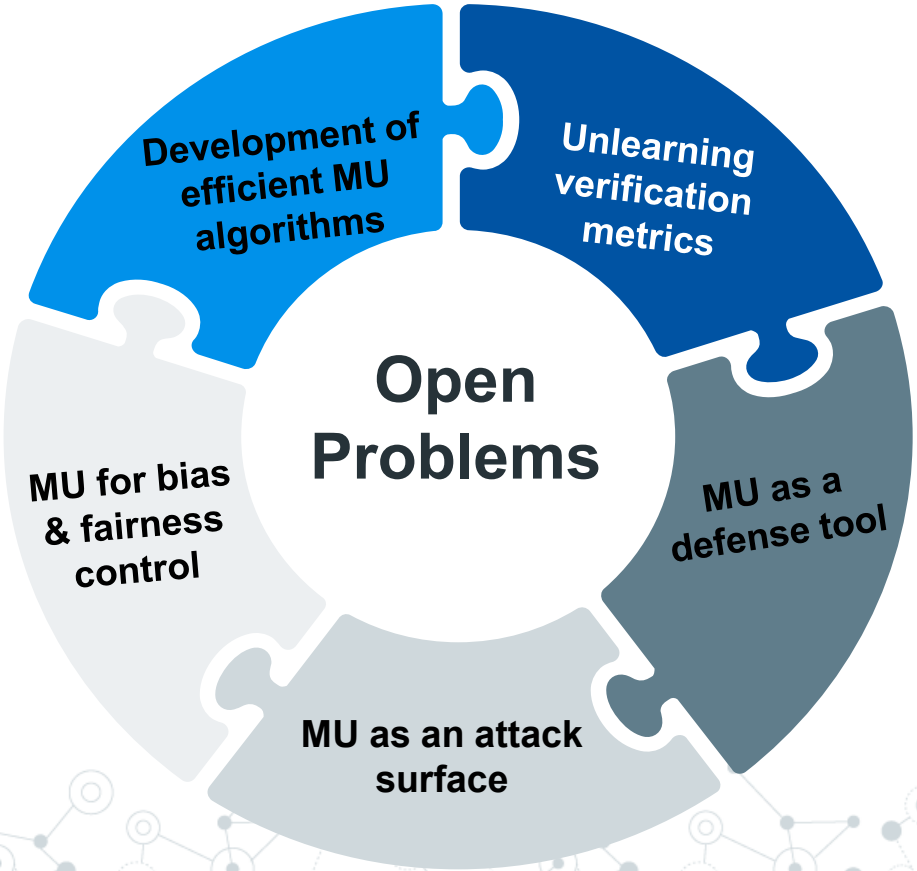


Challenges:

- Large-scale models & datasets
- Representation learning task
- Similarity-based decision making

UNIVERSITÄT PADERBORN

Machine Unlearning for FR



UNIVERSITÄT PADERBORN

Project Group Overview

Main goal:

Developing and implementing efficient machine unlearning algorithms capable of removing individual or group of identities and their influences without needing to retrain the model from scratch with every request for data removal.

What can this project group do?

Explore and implement methods for Machine Unlearning in Face Recognition.

Investigate research extensions: backdoor forgetting, bias removal, MU privacy risks.

Produce suitable and efficient unlearning verification metrics for evaluation.

Project Structure and Details

How will we work?

Project Part 1

- General research about machine unlearning and face recognition
- Topic selection and deep literature review
- Baseline model set-up/implementation

Project Part 2

- Specific approach implementation and refinement
- Approach experiments, analysis and evaluation
- Report and final presentations

Tools and Resources

What do you need:

- Interest in **biometrics**, motivation to work and enthusiasm.
- Programing skills preferably in **python**
- Knowledge in **machine learning** / **deep learning**
- Knowledge in libraries such as **OpenCV, pytorch, tensorflow** is a plus

How can I know more, see the following:

Bourtoule, L., Chandrasekaran, V., Choquette-Choo, C. A., Jia, H., Travers, A., Zhang, B., ... & Papernot, N. (2021, May). Machine unlearning. In *2021 IEEE symposium on security and privacy (SP)* (pp. 141-159). IEEE.

Foster, J., Schoepf, S., & Brintrup, A. (2024, March). Fast machine unlearning without retraining through selective synaptic dampening. In *Proceedings of the AAAI conference on artificial intelligence* (Vol. 38, No. 11, pp. 12043-12051).

Zhang, H., Nakamura, T., Isohara, T., & Sakurai, K. (2023). A review on machine unlearning. *SN Computer Science*, *4*(4), 337.

Team and Contact

Dr.-Ing. Philipp Terhörst
Supervising professor

Rouqaiah Al-Refai
Project group supervisor
Rouqaiah.al.refai@uni-paderborn.de