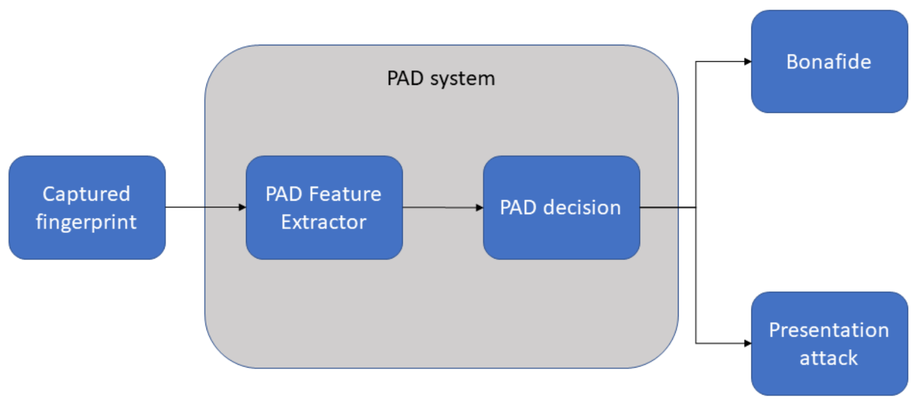
Robust algorithms for fingerprint presentation attack detection

NTNU

Objective

- Development of robust fingerprint presentation attack detection algorithm for both contact and contactless fingerprint
- Develop novel digital fingerprint presentation attack instruments based on both hand-crafted and deep learning techniques like Generative Adversarial Networks
- Development of fingerprint verification and presentation attack detection algorithms suitable for embedded devices



Research Questions

- How to generate high quality digital fingerprint/photo attacks with smooth texture using hand-crafted or deep learning (e.g. GAN) based approach?
- Does the fingerprint patch-based approach using hand crafted/deep learning can be used to detect fingerprint presentation attacks?
- Does the fingerprint algorithms developed based on multi modal capture using multi-spectral sensors can improve the robustness of both verification and presentation attack detection?

Approach

- Through modification to the GAN model and optimization policy, the algorithm can generate a more realistic fingerprint with warping and distortion.
- Use the embedded device to collect as much data as possible to prepare for development of fingerprint verification system. Then experimented with several SOTA FPAD method.
- Measuring the fingerprint matching performance by using different capture devices.
- Generalization on the capability for detect the unknown attacks.

PONE BIOMETRICS

NTNU

The Research Council of Norway

Hailin Li
hailin.li@ntnu.no

Raghavendra Ramachandra
raghavendra.ramachandra@ntnu.no

Prof Dr. Patrick Bours
patrick.bours@ntnu.no

Norwegian University of Science and Technology – Norwegian Biometrics Lab