Motivation

Face biometric systems are a popular but exploitable instrument for user authentication. Attackers try to cheat such systems with different attacks, including the presentation of printouts and videos that portray legitimate users. Robust authentication systems therefore depend on additional liveness detection methods that indicate the presence of such attacks. For optimal applicability and efficiency, such methods should work with ordinary optical sensors and neither rely on special user actions, nor on resource-intensive algorithms.

Goals

The aim of this project is to implement a machine learning-based system as a primary method for face presentation attack detection. The system will utilize spatial and temporal features and a self-attention module for fine-grained image discrimination on the pixel-level. The effectiveness of this approach should then be evaluated with existing liveness detection methods. When deployed in the real-world, the system will mitigate the risk of illicit access to systems protected by face authentication.

Requirements

- Programming experience in Python and Tensorflow (or PyTorch)
- Prior knowledge about Machine Learning
- Basic knowledge about Linux

We offer

- An interesting topic with strong demand by many real-world applications
- Frequent meetings and writing support during the thesis
- A friendly and encouraging work atmosphere
- A deep understanding of machine learning for liveness detection

Duration

10 weeks

Contact

Moritz Finke, B.Sc.  
moritz.finke@uni-wuerzburg.de
Informatikgebäude, 1.OG, Room A118  
go.uniwiue.de/finke

Please provide a short motivation and an overview of your study grades when contacting by mail.