MASTER THESIS

PRESENTATION ATTACK DETECTION FRAMEWORK FOR SMARTPHONES

OBJECTIVE & GOALS:

The presentation attack is nothing but an attempt to deceive biometric system by presenting a fake biometric characteristic to its sensors, and many such examples can be found where a successful attack has been carried out. Hence, there is a need for countermeasures to detect and deter these attacks to reduce the risk of identity frauds using such biometric systems. The work is a part of SWAN (Secured access over Wide Area Network) project and aims at getting a better understanding of Presentation Attack Detection (PAD) for multibiometrics in the smartphone environment. We can expect to formulate a secure smartphones based biometric system. By combining the information from multiple biometrics (e.g. Face, Eye, Finger photo) and incorporating PAD schemes

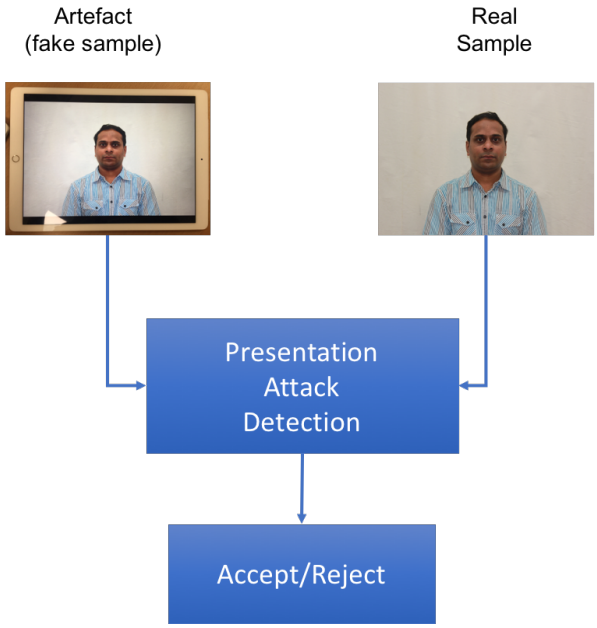

Fig. 1: Presentation Attack Detection

TASKS:

- Apply image/signal analysis, machine learning techniques to identify the presentation attacks such as display, print and video attack.
- Assessment of the devloped algorithms through performance evaluation as per standards

PREREQUISITES:

- Interest in image and signal analysis, biometrics
- OpenCV, C/C++
- Familiar with iOS/Android development

CONTACT:

- Pankaj Wasnik (pankaj.wasnik@ntnu.no)
- Dr.Raghavendra Ramachandra(raghavendra.ramachandra@ntnu.no)
- Prof. Christoph Busch(christoph.busch@ntnu.no)

NOTE: Highly qualified foreign students can get financial support to cover cost of an internship