Submission Instructions for LivDet-Iris 2023
Part 2 – "Algorithms-Independently-Tested"

1. Participants of Part 2 need to send iris liveness detection algorithm to the following email address: ***purnaps@clarkson.edu***

2. Installation Requirements:

- Windows 11 OS (64-bit)
  - Executable file (.exe) or similar executable for Windows OS.
- Ubuntu OS **(version 20.04 only)**
  - Necessary software packages, versions and installation instructions for Ubuntu.
  - All necessary software modules for installation must be provided.
  - Algorithms should be able to process common image formats (PNG, JPG, JPEG, BMP).
  - Only CPU versions of the algorithms will be accepted for evaluation.

Algorithm Output

The algorithm output file must be a .txt file with rows including the image filename, the corresponding liveness score for the image, and the corresponding image processing time presented to the algorithm.

The liveness score for the processed image is a posterior probability of the live class given the image or a degree of liveness, normalized in the range 0 and 100 (100 is the maximum degree of liveness, 0 means that the image is fake). In the case that the algorithm does not process the image properly, the correspondent liveness score must be -1000 (failure to enroll).

The image processing duration (in seconds) is the duration required for the data capture subsystem and comparison subsystem to acquire and process a sample, inclusive of PAD subsystem processing duration

Performance Evaluation of Algorithms Submitted to LivDet-Iris 2023 Part 2 -- "Algorithms-Independently-Tested"

Laboratory staff will attempt to evaluate the algorithm with iris samples (both live and spoof) to collect performance scores. ***The submitted algorithms must have the capability to process (640*480) grayscale iris images.***

The parameters adopted for the performance evaluation of each successfully submitted algorithms will be the following:

Attack presentation classification error rate* (APCER): the proportion of attack presentations using the same PAI species incorrectly classified as bona fide presentations at the PAD subsystem in a specific scenario

Bona fide presentation classification error rate (BPCER): the proportion of bona fide presentations incorrectly classified as presentation attacks at the PAD subsystem in a specific scenario

Attack presentation non-response rate (APNRR): the proportion of attack presentations using the same PAI species that cause no response at the PAD subsystem or data capture subsystem

Weighted Average of APCER (APCER-Average): the average of APCER across all PAIs, weighted by the sample counts in each PAI category

Average Classification Error Rate (ACER): the average of APCERaverage and BPCER. (Only for the purpose of competition ranking)

Algorithm processing duration (A-PD): the duration required for the algorithm to acquire and process a sample, inclusive of PAD subsystem processing duration

Definitions

Presentation Attack (PA)**: presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system

Presentation Attack Instrument (PAI): biometric characteristic or object used in a presentation attack

*Rates are based on the assumption of a threshold of 50.0. Quality and match scores will be computed based on the collected images to support efforts to maintain fairness between the submitted systems

**In the case here, PAI species are the known and unknown spoof recipes that will be used in this competition.

Declaration of the Winner

The winner of the Part 2 competition category will be awarded based on minimum overall classification error. One winner in Part 2 will be awarded.