CSE341/541: Advanced Biometrics

Assignment:#2 Deadline: 1 April 2018 (UTC-12)

Note: Plagiarism of any kind is not allowed.

AR Database: https://drive.google.com/open?id=1TRY9Po5StBz5aMaX78yR4B3_ftdYwyml

Report/compare the performance of your algorithms using ROC, CMC, Equal Error Rate (EER), Half Total Error Rate (HTER), False Positive, False Negative, True Positive, and True Negative metrics (based on the appropriate parameters for following questions).

Q1. Implement any **deep learning based face detection and recognition technique** discussed in class. (Use AR face database).

Q2. Implement **any one** of the following face presentation attack detection algorithms on SMAD Database [1]. While reporting the results, you should have followed the correct database protocol. Compare the performance of your implementation with the findings published in the corresponding paper.

Algorithms for implementation:

A. **Face Anti-Spoofing Based on General Image Quality Assessment** (http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6976921)
B. **Face Spoof Detection With Image Distortion Analysis** (http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7031384)
C. **Face Spoofing Detection Using Colour Texture Analysis** (http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7454730)
D. **Face Anti-Spoofing with Multifeature Videolet Aggregation** (http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7899772)

[1] **SMAD Database paper**: Detecting Silicone Mask-Based Presentation Attack via Deep Dictionary Learning (http://ieeexplore.ieee.org/document/7867821/)

Dataset Division:

Videos from each class are equally distributed in five non-overlapping folds. In each iteration, three folds are used for training the PAD algorithm while the other two are used as the test set. The training folds can be used for parameter optimization and as validation or development set. This train-test split is randomly repeated five times for cross validation and performance evaluation.

To demonstrate the performance of presentation attack detection algorithms, this study proposes two protocols: frame-based and video-based. The performance obtained by classifying all the individual frames as genuine or attacked is referred to as the *frame based approach*, while the *video based approach* classifies entire video samples into two classes.

Bonus + Paper:

You can propose any novel algorithm (in place of above mentioned existing algorithms) and if that achieves state-of-the-art performance on SMAD database (i.e., EER < 12.3%), bonus marks will surely be provided and a possible paper submission too.