Mini-project #1: Fingerprint Spoof Detector using Bayes Classifier
Possible Points: 30

Abstract: Fake fingers can be easily fabricated using commonly available materials, such as latex, silicone and gelatine, with the fingerprint ridges of an individual engraved on it. These fake fingers can then be used by an adversary to launch a spoof attack by placing them on a fingerprint sensor and claiming the identity of another individual.
A fingerprint spoof detector is a pattern classifier that is used to distinguish a live finger from a fake (spoof) one in the context of an automated fingerprint recognition system. Most liveness detectors are learning-based and rely on a set of training images. Consequently, the performance of a liveness detector significantly degrades upon encountering spoofs fabricated using new materials not used during the training stage.

Project: The aim of this project is to design a spoof detector using Naïve Bayes classifier. The following steps are required to be performed:

Step 1: Train the Naïve Bayes classifier using training set of live and fake fingerprint images fabricated using latex material.

- Use: featureMat_liv_train_bioLBP.mat and featureMat_Latex_train_bioLBP.mat along with the target variable.

Step 2: Test the classifier on test set of featureMat_liv_test_bioLBP.mat and featureMat_Latex_test_bioLBP.mat.

Step 3: Compute loss and re-substitution error of the classifier.

Step 4: Test the classifier on test set of featureMat_liv_test_bioLBP.mat and featureMat_Latex_test_bioLBP.mat and featureMat_Gelatine_test_bioLBP.mat

Step 5: Re-compute the loss and re-substitution error of the classifier.

Step 6: Change the prior of the classes to [0.6 0.4] and perform Step 2 and 3.

Comment on all the observations in a one-page report.

Recommended Reading:

A. Rattani and A. Ross, "**Automatic Adaptation of Fingerprint Liveness Detector to New Spoof Materials**", *Proc. of International Joint IEEE Conference on Biometrics (IJCB)*, (Clearwater, Florida, USA), September 2014.