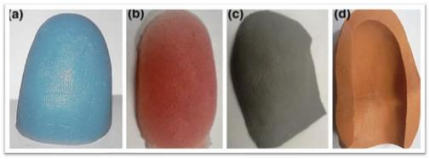
# Adversarial perturbation detection

Liveness detection consists in the recognition of real fingerprints from artificial replicas, used to try to bypass a biometric-based authentication system. Fake fingerprints could be made using several materials, including latex, wood glue, gelatin, etc.




Artificial finger replicas made using GLS (a), Ecoflex (b), Liquid Ecoflex (c) and Modasil (d).

When the liveness detector is based on Convolutional Neural Networks (CNN), it is possible to leverage adversarial perturbation to craft a noise able to make a fake fingerprint recognised as live.


The Data Mining contest for the academic year 2020/2021 addresses the detection of Adversarial Fingerprints, namely fake fingerprints modified by means of adversarial perturbation with the aim of misleading a CNN-based liveness detector.

# Contest Rules

Each student (team) has to predict if the fingerprint is clean or adversarially perturbed (thus, this is a binary classification problem). The aim is to set up one or more prediction models using data analysis and Data Mining techniques trained on the training dataset. The following steps have to be conducted and documented:

1. Business and Data Understanding
2. Data Preparation
3. Modeling

Each participant is free to add new features, to modify the current features and to use external tools (i.e. Weka, Knime, MatLab, etc.), taking care to accurately describe each performed step in a final report.

For examination purposes, it is MANDATORY to provide a report describing the steps followed in order to reach the development of the final model.

# Evaluation criterion

The evaluation metric for this competition is the Accuracy (Acc). The Accuracy is the percentage of correctly classified instances with respect to the total evaluated instances.

**Acc=True Positive+True Negative / # Evaluated Instances**