Deep Tree Learning for Zero-Shot Face Anti-Spoofing

Yaojie Liu, Joel Stehouwer, Amin Jourabloo, Xiaoming Liu
Department of Computer Science and Engineering, Michigan State University, MI

Introduction

• Empower the machine to detect unknown/unseen attacks
• Enlarge the study from 2 types to 13 types
• Collect the first database for Zero-shot Face Anti-spoofing

Convolutional Residual Unit (CRU)

- 3x3 convolution layer w/ 40 channels
- residual connections
- max pooling

Supervised Feature Learning (SFL)

- Classification Supervision
  \[ \mathcal{L}_{\text{class}} = \frac{1}{N} \sum_{i=0}^{N} \left( -y_i \log \hat{y}_i + (1 - y_i) \log (1 - \hat{y}_i) \right) \]
- Pixel-wise Supervision
  \[ \mathcal{L}_{\text{pixel}} = \frac{1}{N} \sum_{i=0}^{N} \| M_i - D_i \|_2 \]

Overall Architecture

- Motivations?
  • Different spoof attacks require different features/cues to distinguish
  • Leverage the knowledge from known attacks
- Deep Tree Network
  • Learn homogenous features in early stage/ distinct features in later stage
  • Unsupervised to build the tree: splitting on the direction of largest data variation
  • Supervised to learn the features at the leaf node
  • End-to-end training

Tree Routing Unit (TRU)

- Tree routing function:
  \[ v(x) = (x - \mu)^T \gamma \quad \| \gamma \| = 1 \]
- To make the \( v \) to be the largest projection base:
  \[ \arg \max_{\gamma} \lambda = \arg \max_{\gamma} v^T X_S X_S \gamma \]
- Tree unique loss:
  • balance the training data for each split

Data and Experimental Results

- Stasts of the Spoof in the Wild II database for ZSFA
- Leave-one-out testing protocols and performance comparison

Find more details and source code:

Find more details and source code: