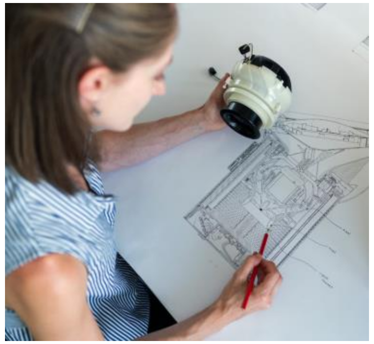
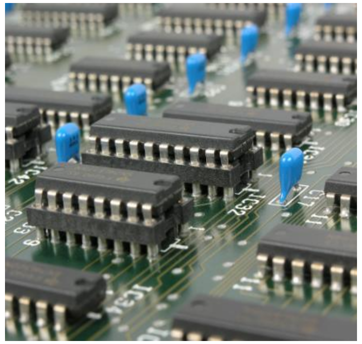
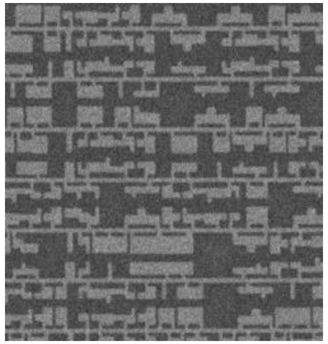
UF Herbert Wertheim College of Engineering
Florida Institute for National Security (FINS)
UNIVERSITY *of* FLORIDA

IC SEM RE Tutorial using AI Part 4: Supervised Machine Learning

Olivia Dizon-Paradis, Ronald Wilson, Domenic Forte, Damon Woodard







Florida Institute for National Security (FINS)

Objective

- Hardware Reverse Engineering Project using AI
  - Hands-on tutorial
  - Practical application in hardware assurance
  - Resume-builder / professional development
- Last Time:
  - Introduced Unsupervised Machine Learning
  - Improved upon previous code pipeline
- This lecture:
  - Introduce Supervised Machine Learning
  - Improve upon previous code pipeline

Refer to the prerequisites and documentation!

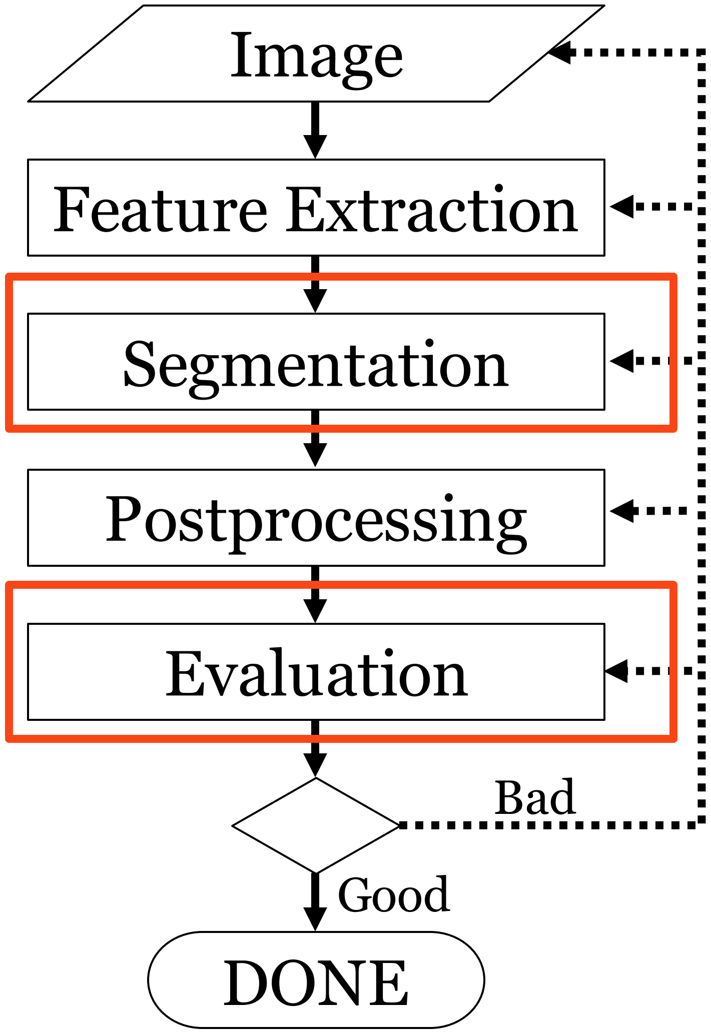
Recap

- Unsupervised

  Learns <u>without</u> ground truth

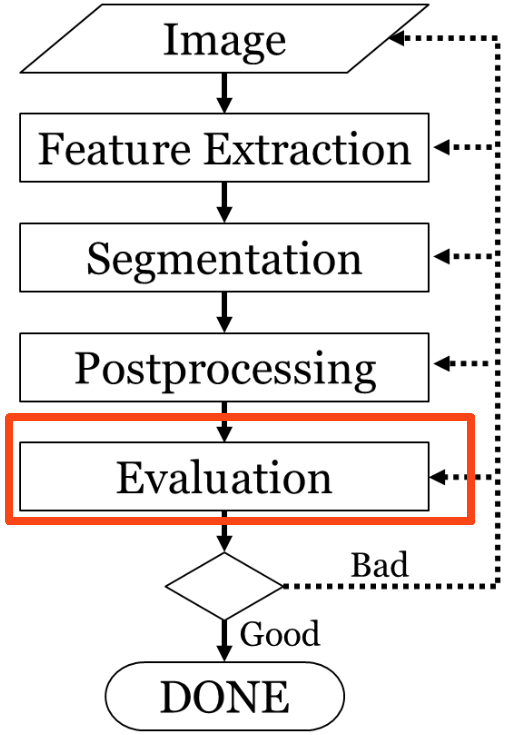
- Supervised:

  Learns <u>from</u> ground truth



Training vs. Testing Data

- Train/Test Split
- Overfitting Problem
- Training data must be:



Image

Feature Extraction

Segmentation

Postprocessing

Evaluation

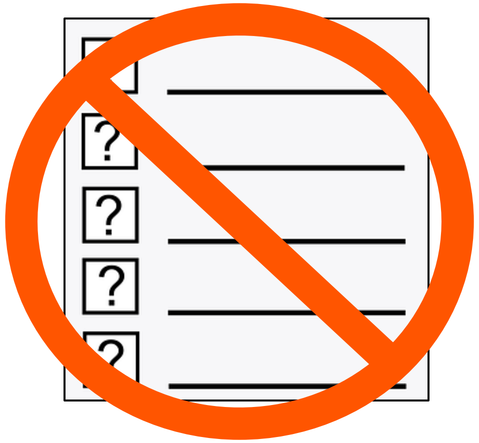
Bad

Good

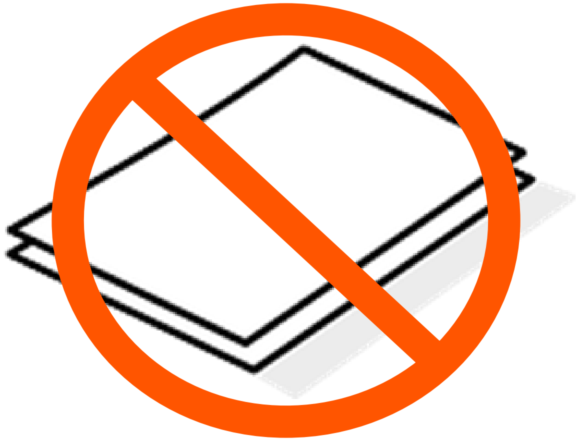
DONE

Representative

Correct

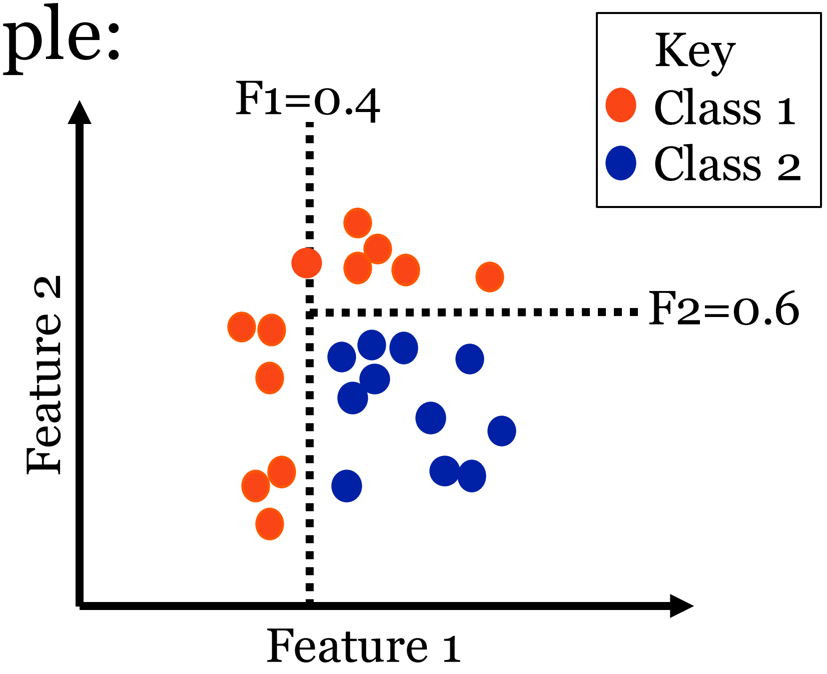


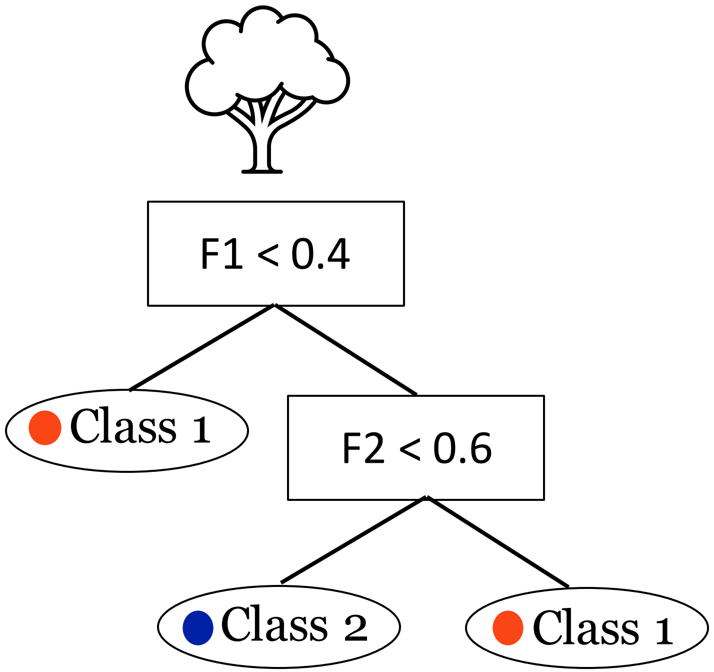
Sufficient

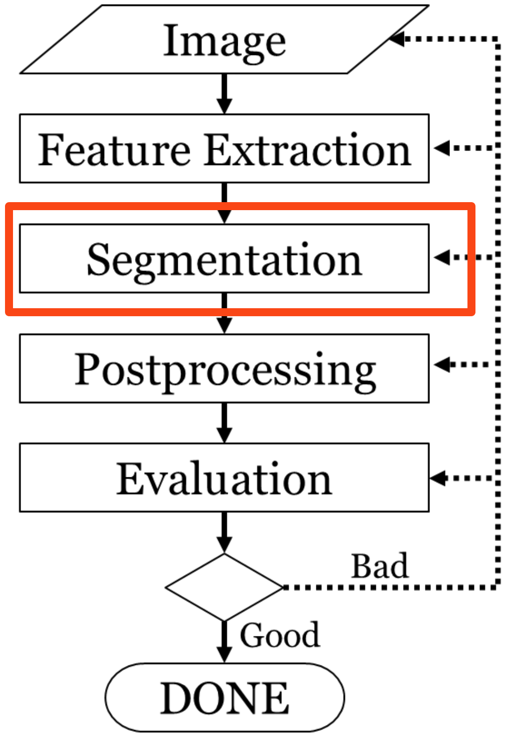


Segmentation Method 4: Decision Tree Classifier

- Supervised ML technique
- Uses simple decision rules in a hierarchy
- Needs: training data
- Example:

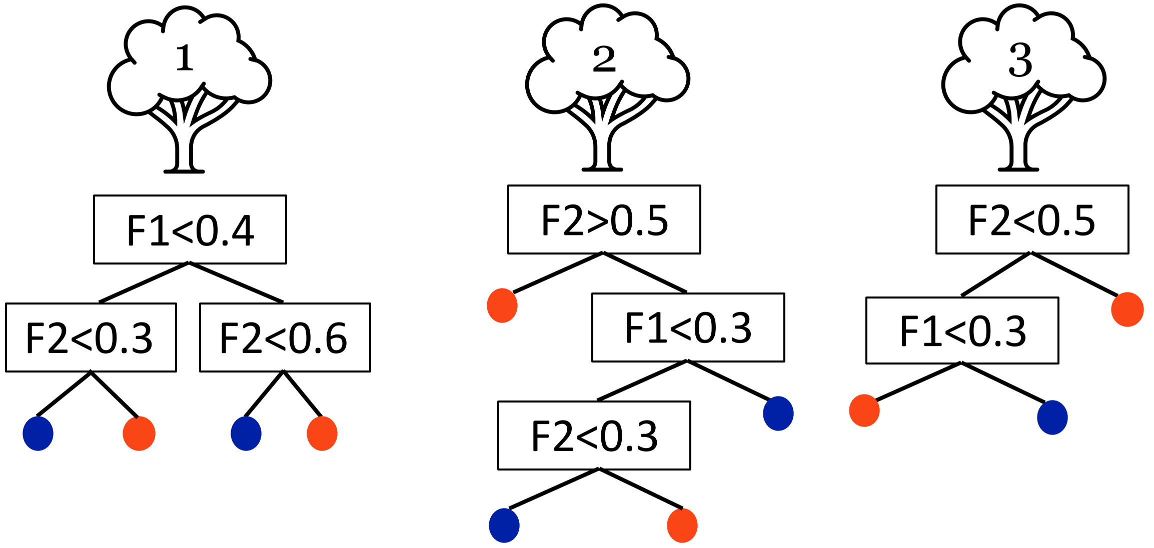






Segmentation Method 5: Random Forest Classifier

- Supervised meta-ML technique
- Uses an ensemble of decision trees
- Needs: training data, number of estimators
- Example:

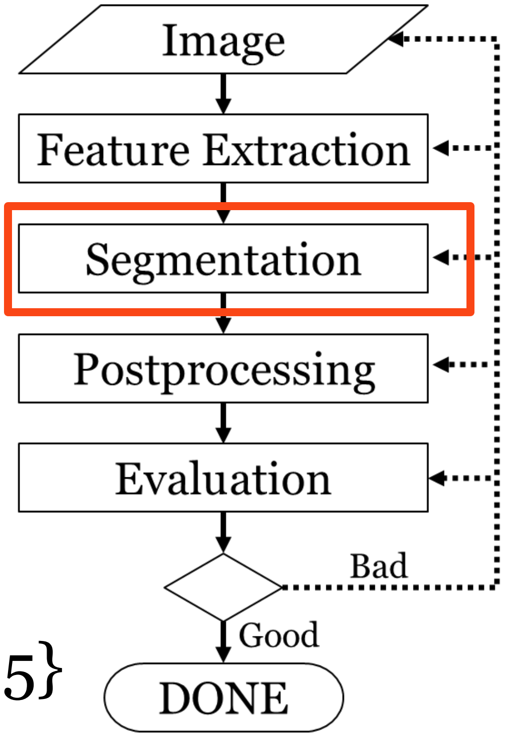


Key
● Class 1
● Class 2

Test Data Point: {0.55, 0.55}

- Tree 1: ● Class 2
- Tree 2: ● Class 1
- Tree 3: ● Class 1

Forest: ● Class 1



Improvements

- Evaluation
  - K-fold cross-validation
- Segmentation
  - Parameters
  - Other Classifiers: Nearest Neighbors, Support Vector Machines (SVM), Naïve Bayes
  - Other ensemble methods: AdaBoost, Gradient Boosting

Experiment!

Key Takeaways

1. Introduced Supervised Machine Learning
2. Evaluation: Train/Test Split
3. Segmentation: Decision Trees and Visualization
4. Segmentation: Random Forest and Ensemble Methods
5. Extensions

Thank you for your time!