HOST 2023 Microelectronics Security Challenge: Supply Chain Security Track

Navid Asadi, Yousef Iskander, Mohamed El-Hadedy, and Eslam Tawfik
Emails:nasadi@ufl.edu, yousefi@microsoft.com, mealy@cpp.edu, and tawfik.10@osu.edu

Overview: The lack of traceability in the globalized electronics supply chain results in the infiltration of various counterfeit electronic parts. Risks include recycled, remarked, overproduced, cloned, out-of-spec/defective, or tampered parts and pose a severe threat to the security of our critical infrastructure. Among these, recycled, remarked, and cloned parts constitute the most frequent incidents. Over the years, a class of solutions has been proposed to mitigate the widespread infiltration of these fake parts.

Although physical inspection methods have gained a lot of attention due to their flexibility across components (analog, digital, memory, FPGAs, etc.) and non-invasive nature, there are other techniques worth exploring. We propose a competition to explore methods of anomaly detection in electronics.

This challenge requires the competitors to develop a highly-accurate, automated method to identify counterfeit ICs or components. Compitetors wishing to utilize image analysis may use the provided dataset as their test, however it is also encouraged to build their own datasets and provide detailed description. Data set shall be limited to passive components and/or LSI (low scale integrated) chips. Even though the provided data set targets image processing methods, other modalities and techniques are highly encouraged.

Evaluation reference success rates are given in the following table.

Accuracy Range	**Competition Ranking Categories**
80%-100%	Gold
More than or equal to 70%, but less than 80%	Silver
More than or equal to 60%, but less than 70%	Bronze
More than or equal to 50%, but less than 60%	Qualified, but no specified ranking
Less than 50%	Disqualified

Sample Image Dataset:

Details on sample image data set are provided in a readme.txt file within the competition folder.

Submission Criteria:

- **Report:** An accompanying narrative, with a maximum page count of two (2) pages is required (excluding references if included). Competitors should provide a candid overview of their approach, any challenges encountered, limitations of their approach, future work, and how the objectives of their approach were achieved.
- **Technical Submission:** The participants are required to submit a zip file containing codes, sample submission, demo, and presentation. The file name should be "team_name_HOST_2023_SCS.zip using here.
- **Code "if exist":** Can be in any language, i.e., Python /R/Java/C++ etc.
    - A GitHub repository containing all necessary codes/libraries/helper functions to train, test, and visualize with a complete and comprehensive README file to implement on the hold-out test data.
    - If the README file and Demo video (see below) don't work/cannot help in successful implementation as claimed in the presentation (see below) and demo (mentioned later), the competitor will receive a penalty.
- **Sample submission:** a 'sample_submission.csv' file containing two columns –
    - id - Unique identifier for each sample test image as in 'test.csv'
    - predicted_label – 0 (if the prediction is 'authentic' for a certain sample test image), 1 (if the prediction is 'counterfeit' for a certain sample test image)
- **Demo:** a demo video either submitted or hosted on a site (preferred) such as Dropbox, YouTube, Google Drive, etc. (upload in here) to demonstrate how to run the developed system (train, test, and visualize).
    - Time limit: minimum - 5 mins, maximum - 15 mins, recommended – 10 mins
- **Presentation:** A PowerPoint presentation of a **minimum 5 to maximum 15 slides** in format to show the outcome (must include the method, results, and discussion). This presentation can be based entirely off the report and does not need unique content.

Evaluation Criteria:

Total: 100 pts

- **Report: 10** (evaluated based on clarity)
- **Training Strategy (e.g., Cross-validation, Data augmentation, Pre-processing, etc.) - 20 pts**
- **Algorithm/Model Complexity – 20 pts**
- **Model's Generalizability/Robustness - 10 pts**
  (To clarify, it will be examined how consistent the model's performance is over different dataset distribution and/or adversarial examples)
- **Time performance – 20 pts**
- **Scalability – 20 pts**

Other resources:

- **More about counterfeit IC detection:**
  - https://link.springer.com/chapter/10.1007/978-3-030-62609-9_2
- **Model's Performance Metrics:** https://neptune.ai/blog/evaluation-metrics-binary-classification
- **Model's Generalizability/Robustness :**
  - https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7780854&tag=1
  - https://proceedings.neurips.cc/paper/2020/hash/61d77652c97ef636343742fc3dcf3ba9-Abstract.html
- **Model's scalability:**
  - https://www.codementor.io/blog/scaling-ml-6ruo1wykxf
  - https://www.codementor.io/blog/scalable-ml-models-6rvtbf8dsd
  - https://neptune.ai/blog/how-to-scale-ml-projects
- **Model's explainability:**
  - https://neptune.ai/blog/explainability-auditability-ml-definitions-techniques-tools