Multi-Objective Counterfeit Circuit Detection

Sukhwan Jung*, Courtney Foots‡, Faith Nice§, Ina Edstrom¶, Aviv Segev†
Department of Computer Science
University of South Alabama
Mobile, USA
*shjung;†segev@southalabama.edu, ‡cef1622;§fn1822;¶ije1922@jagmail.southalabama.edu

***Abstract*—Counterfeit circuits pose disproportional dangers to the systems they are installed in. The authors propose a machine learning approach to counterfeit detection, identifying optimal testing conditions where the effects of circuit variations are minimized. An optimal set of temperatures was identified over a variety of simulated circuits where the variations between authentic circuits are minimized while maximizing the differences against the counterfeits. Intel models and their Soviet clone counterparts were tested afterward in temperatures bordering a normal operational range. Significant differences were observed between authentic and counterfeit circuits, leading to low-cost and high-coverage counterfeit detection.**

***Index Terms*—Integrated Circuit Counterfeit Detection, Machine Learning, Multi-Objective Optimization**

I. Introduction

Counterfeit microelectronics are integrated circuits that are engineered to pass off as being authentic. With circuits having yearly global market revenue exceeding 100 billion dollars and growing, counterfeit circuit detection is increasingly becoming crucial for circuit manufacturers and consumers in the automotive industry, healthcare, military, and government infrastructures. Non-destructive visual inspection methods such as X-ray and scanning acoustic microscopy (SAM) [1] are used as basic approaches. Electrical inspections can also be done by measuring voltage disparities and functioning tests [2]. More detailed evaluations are often done through destructive approaches such as Microblast analysis [3], scanning electron microscopy (SEM) [4], or burn-in test [5] as they have a high accuracy of detecting counterfeits at the cost of a tested circuit. While such methods provide a high degree of precision in identifying counterfeits, they are often destructive, expensive, time-consuming, circuit-specific, or open to manual interpretations without objective measurement. Only a small portion of samples can be tested to preserve economic viability on a large scale, which makes it more difficult to detect counterfeits that are rare in the population to begin with.

The paper aims to propose a non-destructive, cheaper, faster, and general approach to counterfeit detection by utilizing an electrical testing method, mediating variations in the circuits' electronic signals by identifying optimal testing environment variables. Machine learning based counterfeit circuit detection has recently been gathering more attention for its automation capabilities [6], and multi-objective optimization with evolutionary algorithms is used to satisfy both, often conflicting, goals. The use of the evolutionary algorithm has been proposed for its flexible, derivative free nature [7] removing the need for gradient analysis and function continuity dependencies from real-world problems [8]. The proposed method generates measurable, objective testing conditions enabling larger scale testing by minimizing the effect of circuit variations.

Once the optimal testing conditions are found, they are validated with Intel's integrated circuits and their clones manufactured by the Soviets during the Cold War. They are used as their identities are readily known. Significant differences between an authentic pair and an authentic-counterfeit pair would indicate that counterfeits can be detected.

II. Simulated Multi-Objective Optimization

A machine learning model is trained on parametric test results between the authentic and the counterfeit circuit. Two circuit designs - resistor, inductor, and capacitor circuit (RLC circuit) and non-inverting amplifier circuit - were used for a controlled testing environment to detect a possible range of parametric testing conditions for counterfeit detection.

The NSGA II algorithm is used with input voltage $1 \leq x_0 \leq 20$ and temperature $0 \leq x_1 \leq 100$ as testing conditions, going up to 20 generations with 5 populations using 0.9 and 1.0 crossover and polynomial mutation probabilities. Two objective functions $f_1(x) = |a_1(x) - a_2(x)|$ and $f_2(x) = -1 * |a_1(x) - s(x)|$ [9] are used, a_1, a_1, and s respectively representing two authentic circuits and one counterfeit circuit. The optimization goal is to minimize both objectives. Non-dominated solutions go through a 2-degree polynomial regression using each solution's intersection vector to the Pareto front. The regression formula is then iterated to pull each local solution point towards the front, reducing the overall distance to the Pareto-optimal front.

The final results of this formulation would be a Pareto front of optimal solutions, defined as testing conditions that produce the maximum parametric difference between the authentic and suspected circuits while minimizing differences between the authentic circuits. It should be noted that typically the full set of most optimal solutions is desired when utilizing a multi-objective optimization algorithm with conflicting objective functions. However, this is not necessarily the case in this domain. A single test condition with significant parameter output differences is sufficient for counterfeit circuit detection to work as the specific test conditions are not the desired result themselves. The identified input variable combination does not need to result in the most significant differences, and the complete set of all testing conditions that produce a

978-1-6654-8768-9/22/$31.00 ©2022 IEEE

significant difference in performance is not needed as well. Any performance difference that is larger than the threshold of acceptable results as defined by the user would suffice in determining if the suspected circuit is, in fact, counterfeit.

III. Results and Conclusion

The proposed method was run with RLC circuits and Non-Inverting Amplifiers over ten generations with three randomly selected test conditions, resulting in a total of 23 different conditions. The differences between authentic circuits were minimized while the differences against counterfeits are maximized, showing $max(f_1) = 0.05V$ and $max(f_2) = 0.2V$ for RLC circuits and $avg(f_1) = 0.01V$ and $avg(f_2) = 4.0V$ for Non-Inverting Amplifiers. Nearly all solutions came from stress test conditions such as extreme heat or cold, which were the main contributor to the optimized counterfeit detection.

The experiments with multi-objective optimization showed that counterfeit detection can be done by exposing the circuits to intense temperatures. Three sets of Intel (*authentic*) and Soviet clone (*counterfeit*) circuits were tested. Microprocessors (Intel 8086, K1810VM86) and GPIB controllers (Intel 8292, KR580VG92) first validated the effect of cold temperatures. While the output differences averaged around 13.86% at room temperatures for microprocessors, extreme voltage differences were observed when they were chilled; four out of 40 pins showed 476 to 667 times larger output for counterfeits. Counterfeit GPIB controllers showed higher variance when chilled with +0.18 to -0.39V, while the authentic circuits were mostly unchanged with two pins showing $> 0.2V$.

Fig 1 visualizes 10-step moving averages of the output voltage over temperatures using two address multiplexer (Intel 3242, KR580VT42) pairs, showing that differences can be seen within normal operational ranges on P4. Significant differences can be observed in chilled, normal, and heated environments; the results indicate that counterfeit detection can be done in non-stressed conditions in specific temperature ranges. Identifying such ranges with low variances, however, requires experiments over the whole temperature spectrum.

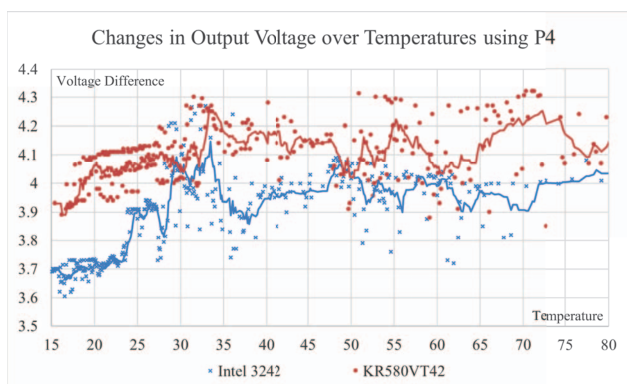

Fig. 1. Automatic temperature measuring for P4 in Intel 3242 and KR580VT42, with trendlines of 10 moving average periods. The X-axis represents temperature from 15 to 80$°C$.

The multi-objective optimization was able to identify optimal test conditions with the given two environmental variables; testing at a certain temperature range can be used to mitigate variations in the circuits and allow reliable counterfeit detection with parametric tests. Low temperature resulted in significant disparities between authentic and counterfeits in multiple experiments, either by revealing significant differences between the two circuit models at lower temperatures or with distinct reactions to the temperature changes. Temperatures bordering the higher end of the operational range also resulted in significant differences between the circuits, both in average voltage and variance of the outputs.

The proposed model is independent of any circuit-specific functional or structural knowledge and can be applied to automated industrial-grade counterfeit detection equipment with relatively less cost, compared to currently available machines which often require knowledge about circuit specifications or manual interpretations. The multi-objective optimization process can be used to incorporate more environmental, physical, and electrical properties to build more accurate counterfeit detection testing conditions in general; or it can be used to identify model-specific conditions for large-scale batch detection. Future works include automated physical experiments and testing the industrial applications of the proposed method on modern circuits using basic parametric evaluations. The goal is to detect more environmental variables and their conditions for successful counterfeit detection and to show that the proposed method is capable of detecting different kinds of counterfeits in more advanced circuits.

Acknowledgment

Effort sponsored by the U.S. Government under Other Transaction number W9124P-19-9-0001.

References

[1] Z. Yu and S. Boseck, "Scanning acoustic microscopy and its applications to material characterization," *Reviews of modern physics*, vol. 67, no. 4, p. 863, 1995.

[2] P. Mazumder and K. Chakraborty, *Testing and testable design of high-density random-access memories*. Kluwer academic publishers, 1996.

[3] U. Guin, K. Huang, D. DiMase, J. M. Carulli, M. Tehranipoor, and Y. Makris, "Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1207–1228, 2014.

[4] J. I. Goldstein, D. E. Newbury, J. R. Michael, N. W. Ritchie, J. H. J. Scott, and D. C. Joy, *Scanning electron microscopy and X-ray microanalysis*. Springer, 2017.

[5] L. M. Leemis and M. Beneke, "Burn-in models and methods: a review," *IIE transactions*, vol. 22, no. 2, pp. 172–180, 1990.

[6] A. Stern, U. Botero, F. Rahman, D. Forte, and M. Tehranipoor, "Emforced: Em-based fingerprinting framework for remarked and cloned counterfeit ic detection using machine learning classification," *IEEE transactions on very large scale integration systems*, vol. 28, no. 2, pp. 363–375, 2019.

[7] K. Deb, A. Pratap, S. Agarwal, and T. Meyarivan, "A fast and elitist multiobjective genetic algorithm: Nsga-ii," *IEEE transactions on evolutionary computation*, vol. 6, no. 2, pp. 182–197, 2002.

[8] C. Jung, W. C. Yoon, R. Datta, and S. Jung, "Knowledge base driven automatic text summarization using multi-objective optimization," *International journal of advanced computer science and applications*, vol. 12, no. 8, pp. 836–849, 2021.

[9] M. D. Intriligator, *Mathematical optimization and economic theory*. SIAM, 2002.