Low-cost Remarked Counterfeit IC Detection using LDO Regulators

Sreeja Chowdhury[1], Fatehmeh Ganji[1], and Domenic Forte[1]

[1]Florida Institute of Cybersecurity Research, University of Florida
{sreejachowdhury, fganji}@ufl.edu, dforte@ece.ufl.edu

***Abstract*— Remarked and recycled counterfeit integrated circuits (ICs) form a vast majority (≈80-90%) of the total number of counterfeit IC instances. Although different types of test strategies have been developed for recycled IC detection, techniques that detect remarked ICs are limited. In this paper, we develop a method to detect false remarking of commercial grade chips into industrial/automotive grade by distinguishing power supply rejection ratio (PSRR) of commercial and automotive grade low drop-out (LDO) regulators from four different vendors. In this process, we use supervised and unsupervised machine learning (ML) methods on PSRR measurements. Our results show a best-case accuracy of 90% for both commercial and industrial LDOs with supervised ML. On the other hand, unsupervised ML can detect commercial and industrial LDOs with a best-case accuracy of 75% for both types.**

I. Introduction

Globalization and extensive use of electronic integrated circuits (ICs) have exponentially increased the complexity of electronic supply chain. The diversity of vendors and components of a single chip has heightened the risks of IC counterfeiting. A counterfeit IC 1) is an illegitimate part; 2) is not produced by the original component manufacturer (OCM) or produced by unauthorized third-party vendors; 3) does not comply to the OCM's design and performance standards; 4) has been used before and sold to consumer as "new"; 5) is defective or off-specification 6) has false markings, etc. There are various types of counterfeit ICs reported as described by the taxonomy in [1]. Among them, recycled and remarked counterfeits are most popular and cumulatively contribute to $\approx 80\% - 90\%$ of the total counterfeits [2]. In this paper, we focus only on remarked counterfeit ICs and methods to identify them. Remarked ICs are parts whose original markings have been removed and replaced by false markings from unauthorized vendors. A specific type of remarking involve replacing consumer grade markings with automotive grade by rogue third party distributors. This endangers the performance of military and automotive grade equipments and threatens national security. News articles in [3] and [4] claim that Intel microprocessor chips have been falsely remarked as military and sold to undercover agents for use in military helicopters. Thus, remarked IC detection is a critical issue and demands specific detection strategies.

The dire necessity to detect counterfeit ICs has led to several specialized testing procedures in past years including physical inspection, electrical testing and aging based fingerprinting [1]. Unfortunately, these techniques are not applicable to all types of counterfeit ICs. A limited number of test strategies have been developed so far to detect remarked counterfeit ICs. In [5], the authors generate electromagnetic (EM) fingerprints to detect cloned and remarked ICs of 8051 microprocessors with a 99% accuracy. Despite stellar accuracy, the implementation requires expensive set up like EM probes and specialized mixed signal oscilloscopes. Another image processing based approach was implemented in [6], where the authors recorded a 100% accuracy over 14 samples including both counterfeit and authentic ICs. The process, however, utilizes only the physical inspection method and does not have any relationship with the electrical performance/parameters of the chips. Compared to them, our approach is completely different and utilizes the electrical performance perspective of the chips.

Compared to the above state-of-the-art techniques in remarked IC detection, our method focuses on a single element, i.e., an LDO, which is a universal element within the power supply of any IC or system on chip (SoC). We utilize the specifications PSRR of LDOs to serve our purpose. The major contributions of the paper are summarized below. 1) We develop an automatic remarked IC detection strategy. Our technique measures PSRR at different operating voltage and temperature levels of commercial and automotive grade LDOs from four different vendors. 2) Our method detects that a commercial grade LDO of a corresponding vendor and its analogous automotive grade version behave differently with respect to input voltage variation. 3) We utilize the above difference in behaviour among the two different grades of LDOs and feed them to machine learning (ML) algorithms to automatically detect respective grades. 4) According to our results, through applying our framework, commercial and industrial LDOs can be differentiated with a high level of accuracy (up to approximately 95%). Compared to other approaches defined in the literature, the equipment cost for our proposed method is relatively low. To record PSRR curves of LDOs, we only need a spectrum analyzer and power supply with an approximate total cost of $2000.

The remainder of the paper is structured as follows. Section II provides preliminary information regarding LDOs. Section III describes the proposed methodology used for remarked detection, whereas Section IV contains experimental and ML results. Finally, Section V concludes the paper with possible future works.

II. LDO Preliminaries

An LDO is a type of linear regulator, which can regulate output voltages to values very close to the supplied input voltage. The input to output differential voltage, at which the LDO fails to regulate the output is defined as the drop-out voltage. The structure of a generic LDO is provided in the block diagram shown in Figure 1. An LDO consists of an error amplifier (EA), an NMOS or PMOS pass transistor (PT) and a resistor divider forming a negative feedback loop. The EA is fed with a constant reference voltage (V_{ref}) by a bandgap circuit and in turn controls the PT through the feedback loop and the resistor divider circuit. The EA tracks the error between the output and V_{ref} and accordingly regulates the gate voltage of PT. The PT acts as a variable resistor and adjusts the output current to further control the output voltage at the desired level.

LDOs are essential components in the power supply of most ICs. They provide a ripple-free, stable fixed output

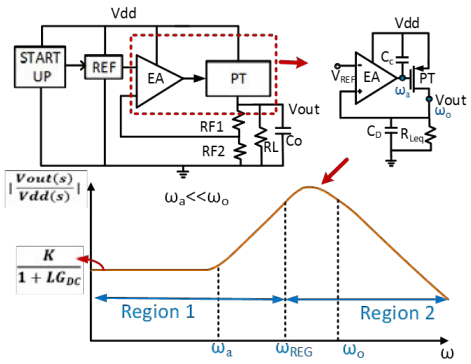

Fig. 1: Block diagram of a low drop-out (LDO) regulator and its associated PSRR curve (linear scale).

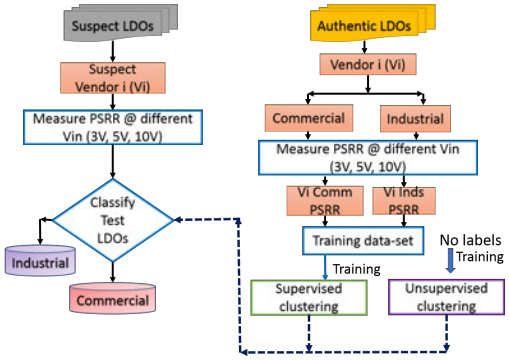

Fig. 2: Flow chart of the our methodology to detect remarked ICs.

voltage; isolating it from the input noise. An LDO has several important performance specifications and the power supply rejection ratio (PSRR) is one of them. PSRR is a quantitative measure of the attenuation of input ripples by the LDO at it's output. These ripples can originate from various parts of the circuit, like DC/DC converters or shared power supplies of other circuit blocks. PSRR is expressed as $PSRR = 20\log(\frac{v_{out}}{v_{in}})$, where v_{out} and v_{in} refer to magnitudes of input and output ripples. In Figure 1, the PSRR of LDO is divided into two distinct regions (region 1 and region 2). Region 1 covers the low and mid frequency range till the regulator bandwidth frequency (ω_{reg}), where PSRR primarily depends on the loop gain (LG) of the regulator. Region 2 starts after ω_{reg}, where PSRR is independent of LG and is dominated by output parasitics, PCB impedance, etc.

III. Proposed Methodology

Here, we propose detection of remarked LDOs by investigating PSRR curves pertaining to different grades. We have selected LDO as a case study because it is a common element in the power supply of most ICs. Our method can be generalized for other SoCs/PCBs containing LDOs. The following assumptions in relation to the proposed method must be noted: 1) Our method is applicable only to detect remarked ICs with fraudulent grades, like a commercial IC falsely remarked as industrial grade. 2) We assume that the subject matter expert (SME) has access to the output pin of the LDO. 3) We implement the proposed idea on standalone LDOs as a proof of concept but if the LDO output pin is accessible, the method can be applied to embedded LDOs in SoCs/PCBs.

A. PSRR Variations: Industrial vs. Commercial LDOs

The major difference between a commercial and industrial grade LDO is in specifications. The industrial grade LDOs mostly work at higher range of input voltage (V_{IN}) and sometimes wider temperature ranges. The output current (I_{OUT}), drop-out voltage (V_{DO}) and PT layout and size may also differ. Analytically, PSRR of a generic LDO can be expressed as follows:

$$PSRR = \frac{v_{out}(s)}{v_{dd}(s)} = \frac{K}{(1+\frac{s}{\omega_o})(1+LG(s))} \text{ s.t. } K = \frac{R_{Leq}}{R_{Leq}+r_{dsP}} \quad (1)$$

In the above formula, $LG = f(A_{EA}, A_{PT})$ is the loop-gain of the LDO feedback loop, and A_{EA} as well as $A_{PT} = f(V_{DO}, V_{HR}, I_{OUT})$ are the individual gains of EA and PT, respectively. The V_{DO} for an LDO depends on various factors like the LDO architecture, V_{IN}, the junction temperature (T_J), PT size, I_{OUT} etc. [7] and thus can be expressed as function of the above variables, i.e., $V_{DO} = f(V_{IN}, T_J, I_{OUT}, PT_{size})$. Moreover, R_{Leq} is the output equivalent resistance at V_{OUT} (see Figure 1) and r_{dsP} is the small signal output resistance of PT. PSRR improves with increase in the input to output differential voltage or the headroom voltage (V_{HR}). With lower V_{IN} (nearing V_{DO}) specifically at higher I_{OUT}, A_{PT} reduces as PT shifts to triode region from saturation region, reducing the LG. This improvement in PSRR can be seen for vendor 1 (V1) and vendor 4 (V4), when we change V_{IN} from 3V to 10V and 5V, respectively (see Figures 3a and 4a). Thus, from these equations, the dependency of PSRR on factors mentioned above, including V_{DO}, V_{IN}, I_{OUT}, T_J, the EA as well as PT architectures etc., can be verified.

Since industrial and commercial LDOs have varied specifications, from the above equations, it can be concluded that: 1) the PSRR of a commercial LDO may be entirely different than it's industrial version at normal operating T_J and V_{IN}, and 2) if the prior condition in Equation (1) is not satisfied, then the change of PSRR with respect to external conditions (V_{IN}, T_J) for commercial LDOs can be different than that of industrial LDOs. Thus, we propose segregation of industrial and commercial grade LDOs by inspecting their corresponding PSRRs at different voltage and temperature conditions. In case of our chosen vendor samples, the commercial LDO and the analogous industrial version had the same range of operating T_J but different range of V_{IN} and V_{DO}. Thus, the changes in PSRR with respect to V_{IN} for commercial LDOs differed from that of their industrial variant, while the temperature effects on PSRR for both commercial and industrial ones were similar. So, we collected PSRR of both commercial and industrial grade LDOs at different V_{IN} and fed them to supervised and unsupervised ML algorithms to separate them automatically.

For two of the vendors (V2 and V3), the PSRR curve of the commercial grade differed from it's industrial version at $25°C$ and $V_{IN} = 3V$ as shown in Figures 3b and 4a respectively. This is because industrial LDOs of V2 and V3 have higher V_{IN} range and higher V_{DO} compared to the corresponding commercial LDO. In contrast, for V1, the industrial and commercial version has exactly similar specification except the industrial part has only a higher V_{IN} range. The commercial part can work till V_{IN} =10V, whereas the industrial one can go up to 13.5V. Thus, though at 3V and $25°C$ the industrial PSRR is exactly same as commercial one as shown in Figure 3a, at 10V the industrial grade has a better PSRR. The most difficult case is with V4 where the industrial has slightly better PSRR compared to commercial

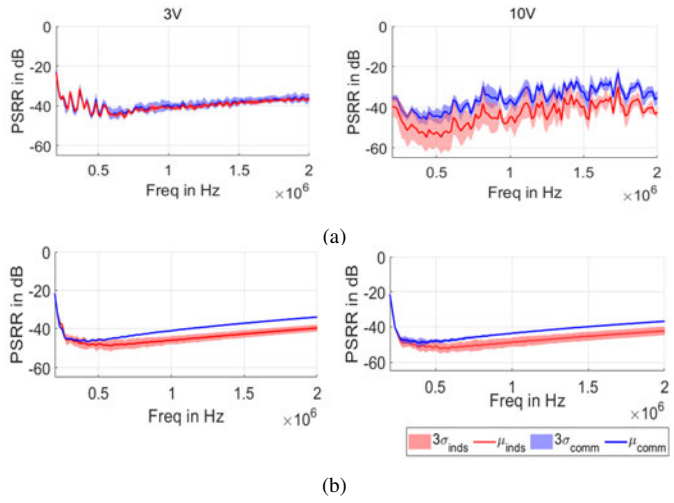

Fig. 3: PSRR of LDOs from (a) vendor 1 (V1) and (b) vendor 2 (V2) at $25°C$ and operating at $V_{\text{IN}} = 3V$ (left) and $V_{\text{IN}} = 10V$ (right).

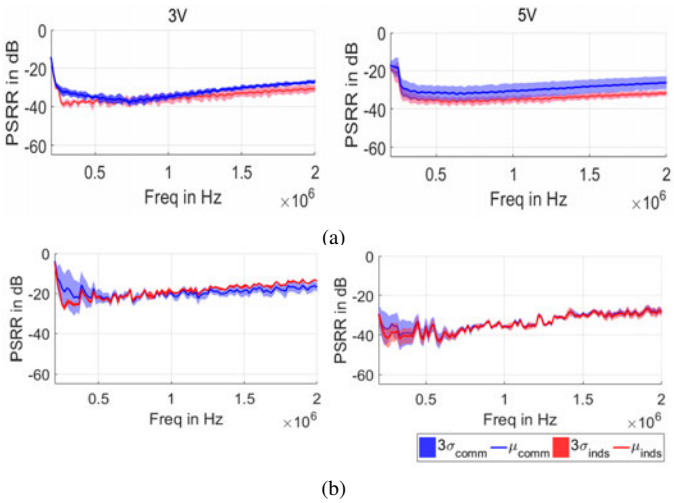

Fig. 4: PSRR of LDOs from (a) vendor 3 (V3) and (b) vendor 4 (V4) at $25°C$ and operating at $V_{\text{IN}} = 3V$ (left) and $V_{\text{IN}} = 5V$ (right).

at $V_{\text{IN}} = 3V$ and lower frequency. But due to the increase in process variation, it is difficult to distinguish at higher V_{IN}.

B. Our Proposed Framework

To detect remarked ICs, we follow the flow described in Figure 2. At first, samples of authentic commercial and industrial LDOs are chosen from each vendor. The PSRR for these samples are collected at different environmental conditions. The environmental conditions are chosen keeping in mind the spec sheets of the different grades used. In our case, the commercial and industrial varieties had different V_{IN} range. Thus, PSRR data is collected corresponding to different pre-selected V_{IN} levels. The PSRR data also varies due to the frequency of input signal as discussed in Section II. Since, for high frequencies the PSRR is mainly dependant on the output and PCB parasitics, it may vary from one test setup to another. Thus we chose the low and mid frequency region to ensure similarity in test results across various test structures. Taking into view the above criteria, a frequency range of 1Hz-2MHz was chosen. To test whether a suspect LDO is remarked or not, we measure the PSRR of the suspect LDOs every 5 kHz, over the above-mentioned frequency range and across the pre-decided V_{IN} values. This set of data is fed to a ML algorithm to classify commercial and industrial LDOs. Depending on the availability of the labels of LDOs (i.e., industrial or commercial), supervised or unsupervised algorithms are adopted. The details regarding the ML algorithms are provided in Section III-C.

C. Data Analysis through ML

The process of analyzing the data collected by measuring the PSRR begins with its representation as a time series. As has been demonstrated in [8], the order and irregularities (e.g., the impact of environmental noise) that are present in the collected data enable us to represent the data as a time series. The former property is the result of how we measure the PSRR values, namely at different voltages and frequencies, with predefined steps and over well-chosen ranges. Consequently, the problem of distinguishing between industrial and commercial devices can be seen as a sequence labeling problem with time series-like sequences, which can be tackled by applying a state-space model (SSM). Additionally, it is common practice to assume that the measured data is generated under the impact of *hidden* parameters that follow Gaussian distributions. In other words, in our scenario, we assume that a set of hidden parameters has an influence on the PSRR-related characteristics of the device, and their impacts can be modeled by Gaussian-distributed variables. These variables are then helpful to differentiate a commercial device from an industrial one. To learn these variables, we take two approaches discussed as follows.

1) *Supervised classification:* In this case, the labels (i.e., industrial and commercial) associated with a set of the LDOs are available. After the algorithm learns the parameters that account for exhibiting the characteristics of industrial and commercial LDOs, unseen LDOs are given to it to classify. The accuracy of this classification shows how well the model (i.e., hidden parameters and their relationships) learned by the algorithm can be generalized to other LDOs manufactured by the same vendor. As for the supervised classification algorithm, we apply the K-nearest neighbor (KNN) algorithm known to learn Gaussian SSMs effectively.

2) *Unsupervised clustering:* Besides the supervised classification, we go a step further and widen the scope of our study by considering a case, where the labels are not available. In this case, only (at least) one golden LDO (known industrial or commercial, chosen by a subject matter expert) must be provided. An unsupervised algorithm is given the PSRR measured from an unseen LDOs and the golden LDO. The algorithm then attempts to determine whether the unseen LDO is industrial or commercial, depending on a slight difference between the characteristics of the golden LDO and the unseen one. To this end, we employ the k-means algorithm, commonly applied in various studies.

Feature Selection Techniques: Features are individual, measurable properties that are observable during the measurement. For instance, in our scenario, PSRR values measured at different frequencies and voltages are the features composing each observation, i.e., an example. When analyzing the data, irrelevant and redundant features that could be involved in the examples reduce the prediction accuracy significantly. To tackle this problem, feature selection methods have been devised and incorporated into the ML frameworks [9]. In particular, when the features exhibit a high correlation, i.e., solely some of the features are sufficient to describe the data, feature selection techniques can be indeed

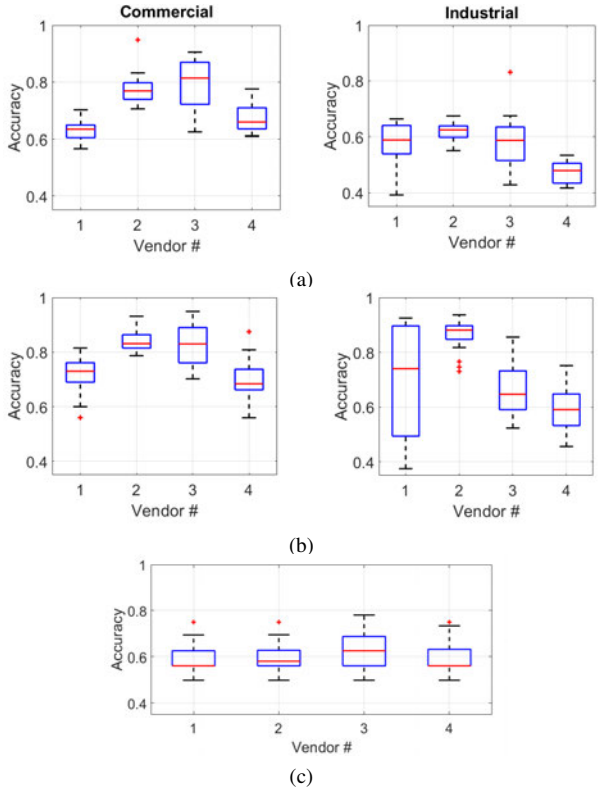

Fig. 5: Detection accuracy of commercial and industrial LDOs: (a) KNN algorithm without feature selection, (b) KNN algorithm with feature selection, (c) k-means clustering algorithm, in this case, the clusters corresponding to the industrial and commercial LDOs exhibit the same accuracy, see Section IV.

helpful. Among several possible feature selection methods, in this paper, we apply the neighborhood component analysis (NCA). The reason behind this is that NCA has been first developed to increase the accuracy of the KNN algorithm by improving the process of defining the nearest neighbors of a test point [10]. To this end, the class labels, in addition to input features, are used to find the relevant features that can describe the relationship between the inputs and the labels.

To sum up this section, we stress that the ML algorithms included in our framework are chosen carefully to model the data as accurate as possible. If, instead of such a systematic, precise approach, an arbitrarily-chosen method is employed to improve the accuracy of learning a given set of data, that approach cannot be generalized to other instances of the devices. This is in contrast to our techniques tailored to the specific nature of the data collected from the LDOs.

IV. Result and Discussion

This section introduces our experimental setup and presents the results achieved by applying the ML algorithms discussed in Section III-C.

Experimental Setup: In our experiments, the PSRR values are collected from industrial and commercial LDOs manufactured by four different vendors (V1, V2, V3, and V4). In our set of LDOs, from each of the manufacturers, we have 32 industrial and commercial (16 each grade) LDOs. PSRR is measured at V_{IN} =3V, 5V and 10V for V1 and V2. For V3 and V4, the maximum V_{IN} is 5.5V, hence, the measurement is done at 3V and 5V. The measured data, described in Section III-B, is fed into ML algorithms embedded in the Matlab software package [11]. To this end, for each LDO, the PSRR values measured at different voltage levels are concatenated together to prepare a single example.

Supervised Learning: Figure 5 illustrates our results obtained by applying the KNN algorithm. In our experiments, we set $k = 16$ to ensure that the maximum number of LDOs with the same grade can be considered by the algorithm. Moreover, the accuracy levels depicted in Figure 5 is achieved through a 10-fold cross-validation method, i.e., the algorithm is run 10 times. In each round, the training process is carried out on 9 folds (i.e., portions) of the dataset and tested on the remaining fold, and therefore, folds are chosen uniformly, and the accuracy is computed with less bias [12]. The boxplot shown in Figure 5a demonstrates that if the raw data (i.e., without using the feature selection method) is given to the KNN, the maximum accuracy of the classification is 90% and 83% for commercial and industrial LDOs, respectively. We further examined whether applying the feature selection technique can improve the accuracy, as explained in Section III-C. The results presented in Figure 5b confirm this, namely the accuracy is up to 95% and 92% for commercial and industrial LDOs, respectively.

Unsupervised Learning: Under this scenario, the labels (i.e., the grades) associated with the LDOs are not available, and the clustering relies on the data acquired from the golden LDO, i.e., an industrial or commercial one. Although this case can be interesting as we require a fewer number of known LDOs, from the point of view of ML, it is more challenging to deal with. In our study, as mentioned before in Section III-C, we apply the k-means algorithm, incorporated with the Silhouette method to validate the consistency within clusters. Besides, we first examine, which distance metric can provide better separation between clusters. According to our observation, the Euclidean distance metric is chosen, and the algorithm is further supported by the re-sampling technique to find lower, local minima of the Euclidean distances between examples. To remove the effect of noisy examples, the centroids of the clusters are determined at the first stage, and then used to re-cluster the data. The results of running the k-means algorithm on our data are shown in Figure 5c. Note that the accuracy of clustering both of the industrial and commercial LDOs is the same as we force the k-means algorithm to deliver two clusters. Compared to the results of supervised classification, the accuracy of making a decision on whether an unseen LDO is industrial or commercial is slightly reduced to approximately 75% (at most); however, in this case, no labeled data is needed. In summary, the key observation made and confirmed by our results in this section is that even in the absence of a sufficiently large set of labeled devices, it is still possible to group the devices with the same grade together, with relatively high accuracy (approximately, 75%).

V. Conclusion and Future Work

We proposed an automated, low-cost test strategy to detect remarked LDOs by observing PSRR at different voltage levels. We further showed that LDOs with different grades (i.e., commercial and industrial) can be differentiated by applying supervised and unsupervised ML algorithms. Through our methodology, we demonstrate the accuracy of up to 95% and 75% for supervised and unsupervised cases, respectively. In future, we plan to extend our framework by incorporating other external conditions, e.g., output current etc., and consider LDOs fabricated by diverse manufacturers.

REFERENCES

[1] U. Guin, D. Dimase, and M. Tehranipoor, "Counterfeit integrated circuits: Detection, avoidance, and the challenges ahead," *J. Electron. Test.*, 2014.

[2] L. Kessler and T. Sharpe, "Faked parts detection," 2010. [Online]. Available: http://publish-it-online.com/article/Faked+Parts+Detection/411055/39826/article.html

[3] D. of Justice, "New york man admits supplying falsely remarked computer chips used in u.s. military helicopters," https://www.justice.gov/usao-ct/pr/new-york-man-admits-supplying-falsely-remarked-computer-chips-used-us-military, 2015, [Online; Last accessed Oct. 11 2019].

[4] L. Cairns, "Electronics counterfeiters get their day in court," https://epsnews.com/2016/01/15/electronics-counterfeiters-get-day-court/, 2016, [Online; Last accessed Oct. 11 2019].

[5] A. Stern, U. Botero, B. Shakya, H. Shen, D. Forte, and M. Tehranipoor, "Emforced: Em-based fingerprinting framework for counterfeit detection with demonstration on remarked and cloned ics," in *2018 IEEE International Test Conference (ITC)*, 2018.

[6] P. Ghosh and R. S. Chakraborty, "Recycled and remarked counterfeit integrated circuit detection by image-processing-based package texture and indent analysis," *IEEE Transactions on Industrial Informatics*, April 2019.

[7] A. Paxton, "Ldo basics: Chapter 1 dropout," http://www.ti.com/lit/ml/slyy151a/slyy151a.pdf, [Online; Last accessed Oct. 15 2019].

[8] S. Chowdhury, F. Ganji, T. Bryant, N. Maghari, and D. Forte, "Recycled analog and mixed signal chip detection at zero cost using ldo degradation," https://www.researchgate.net/publication/336146643_Recycled_Analog_and_Mixed_Signal_Chip_Detection_at_Zero_Cost_Using_LDO_Degradation, 2019, [Online; Last accessed Oct. 10 2019].

[9] G. Chandrashekar and F. Sahin, "A survey on feature selection methods," *Computers & Electrical Engineering*, vol. 40, no. 1, pp. 16–28, 2014.

[10] J. Goldberger, G. E. Hinton, S. T. Roweis, and R. R. Salakhutdinov, "Neighbourhood components analysis," in *Advances in neural information processing systems*, 2005, pp. 513–520.

[11] MATLAB, *Version 9.4.0.813654 (R2018a)*. The MathWorks Inc., 2018.

[12] M. Kuhn and K. Johnson, *Applied predictive modeling*. Springer, 2013, vol. 26.