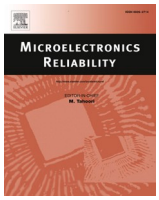
Microelectronics Reliability 168 (2025) 115652

Contents lists available at ScienceDirect

Microelectronics Reliability

journal homepage: www.elsevier.com/locate/microrel



Research paper

# Electronics authentication using electrical measurements and machine learning☆

S. Carta [a], A. Urru [b], M. Musa [b], P. Andronico [b], G. Mura [a,*]

[a] Department of Electrical and Electronic Eng., University of Cagliari, Cagliari, Italy
[b] Nurjana Technologies srl, Via Mario Betti 27/29, Elmas, Cagliari, Italy

ARTICLE INFO

*Keywords:*
Counterfeit electronics
Fake electronics
Electrical measurements
Non-destructive detection
Machine-learning algorithms
Fake amplifiers

ABSTRACT

The problem of counterfeiting in electronics is not recent but still critical today. Identifying counterfeit devices can be a complex task since not all suspicious items are necessarily inauthentic. The paper deals with the non-destructive detection of counterfeiting in electronics by using only electrical measurements. This approach paves the way for machine learning classification-assisted counterfeit detection through electrical measurements. Physical de-processing provides the final confirmation.

## 1. Introduction

Counterfeiting in the electronics industry is a major issue that can lead to serious problems such as personal injuries, mission failures, and reduced system reliability. Although the problem of counterfeit electronics has existed for some time, it remains a critical issue today [1–5].

It is essential to abstain from purchasing from unauthorized distributors to avoid the risk of counterfeit parts. However, when obsolescence forces the need to obtain parts from other sources, i.e. when manufacturers and their authorized wholesalers no longer provide them, problems can arise in avoiding counterfeit parts. This is especially true when replacing components that were made several years ago.

Many different techniques can be used to address various types of counterfeiting, and detection and avoidance methods are continually evolving [6–8] to stay ahead of counterfeiters who may adapt their strategies.

There is an increasing need for affordable and non-destructive methods of detecting counterfeit parts mixed in the same delivery packaging without wasting material or incurring high costs. Moreover, developing a unique detection method that comprehensively captures the entire taxonomy is complex. In recent years, extensive research efforts have focused on automating the detection process by using machine learning algorithms [9]. For instance, in [10], the packaging encapsulant material is chemically characterized to detect counterfeits. In [11], x-ray computed tomography, image processing, and machine learning algorithms are used to detect die-face delamination in a 3D image. Additionally, scratches are identified through artificial neural networks on an IC packaging image acquired using an optical microscope [12]. In [13], counterfeit ICs are detected through a one-class support vector machine classifier trained using only parametric measurements of brand-new devices in production. Terahertz signals and terahertz time-domain spectroscopy-based machine learning approach is conducted to demonstrate the capabilities of this non-destructive physical inspection method for counterfeit IC detection [14,15].

Published approaches cannot detect accurately all the types of counterfeits, but they partially have the potential to prevent fakes.

Electrical measurements represent an important non-destructive step in the verification process because they can determine whether the devices are functionally conformed to the datasheet and are conclusive in identifying the failure modes in defective units.

Our research compared the electrical characteristics of a wide variety of real (not simulated) devices acquired from the grey market with a large set of genuine devices sourced from an authorized distributor. In the proposed case, our analysis revealed that machine learning-assisted electrical measurements can be a highly effective way to authenticate electronic products when low-cost, non-destructive acceptance testing is required.

☆ This article is part of a special issue entitled: ESREF 2024 published in Microelectronics Reliability.

* Corresponding author.
*E-mail address:* giovanna.mura@unica.it (G. Mura).

https://doi.org/10.1016/j.microrel.2025.115652
Received 8 November 2024; Received in revised form 23 January 2025; Accepted 26 February 2025
Available online 12 March 2025

## 2. Experimental

### 2.1. Devices under test

The devices under test are some LMxxx power amplifiers designed for low-voltage consumer applications and provided in a plastic dual-in-line package. They serve specifically as a valuable example for demonstration purposes. Although these devices may not appear engaging, they are a suitable proof-of-concept for analysis. Several times during the COVID-19 pandemic, they were in short supply, and since then, numerous counterfeits have been readily available on the grey market. As noted in [16,17], destructive physical inspection detected fraudulent copycats of the original devices in previous works. This kind of device has also been modified over the years by the original manufacturer in terms of plastic package moulding compound and lead frame [18]. This aspect makes external inspection (in terms of optical microscopic and chemical analysis) and x-ray analysis unsuitable and unreliable for counterfeit detection.

Our work efficiently identifies fake devices using a non-destructive analysis based on electrical measurements and machine learning algorithms, providing a practical and reliable method for counterfeit detection.

Generally, electrical measurements ensure that the devices meet determined requirements and detect failure modes in case of fault, addressing the failure analysis [19–22].

The Aerospace standard AS6171 [23] provides the best guidance on the sequence of electrical tests, inspections, and requirements for suspect counterfeit part detection. The type of tests should be defined by the risk level and commodity type as reported in the standard general requirement.

Our work exploits machine learning algorithms better to analyse the electrical differences between original and fake devices. Finally, the destructive examination is only devoted to confirming the results derived from the classification.

### 2.2. Electrical measurements

The devices under test are purchased from an official distributor (O) and different unofficial sellers.

The electrical measurements, in terms of the quiescent supply current vs. the supply voltage, were acquired by means of an Agilent B1500A semiconductor parameter analyser in the range between 4 V and 12 V. Specifically, the quiescent current at $V_S = 6$ V and $V_I = 0$ V, where $V_S$ is the supply voltage and $V_I$ is the input voltage, is considered acceptable if it is between 4 and 8 mA.

The measurement setup and the acquired measurements for the set of original devices (O) are proposed in Fig. 1.

In addition, bandwidth measurements were acquired with supply

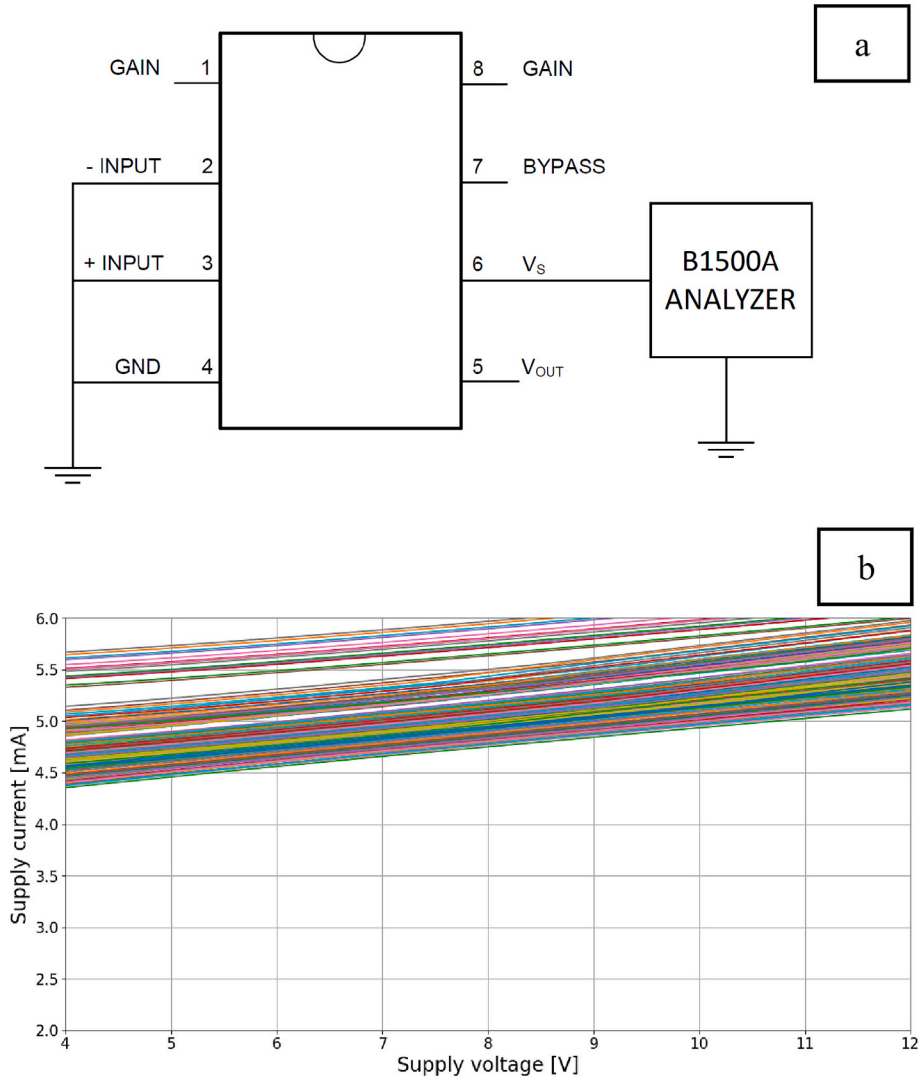



**Fig. 1.** (a) Setup for the quiescent current measurement and (b) quiescent current measurements from original devices.

voltage at $V_S = 6$ V using the Analog Discovery Network Analyser in the frequency range between 100 Hz and 1 MHz. Gain voltage measurements are obtained at f = 1 kHz in the same condition. In Fig. 2, the measurement setup and the acquired measurements for the set of original devices are presented.

Electrical measurements are summarized in Table 1. The table reports both electrical measurements performed on the set of original devices (O) and the corresponding typical values, as specified in the datasheet. Regarding trends and values, the data results for all the devices are approximately in agreement with the datasheet, except for the cut-off frequency, that appears to be around the double of the attended value. It is generally expected that a device's performance could differ from those reported in the datasheet. Additionally, for customer applications, the cut-off frequency indicated in the datasheet and the values obtained from measurements tend to be significantly higher than those relevant to the frequencies of interest.

Electrical characterization can help identify suspicious components, but the analyst should also keep in mind that a slight variability from the typical values proposed in the datasheet does not necessarily indicate a counterfeit part.

This can be due to unreported changes in the manufacturing process at the fabrication plant or to lot-related variability of the process. This experimental evidence suggests measuring the devices rather than relying solely on the datasheet is crucial.

Machine learning-based classifiers were considered to better analyse the data. The performed electrical measurements provide the input features.

### 2.3. Machine learning-based approach

A study was conducted to determine the most appropriate approach for building a classifier based on machine learning techniques to distinguish between original and counterfeit devices. In total 233 original and 318 counterfeit devices were measured for the study. Original devices (O), sourced from authorized distributors, belong to different production lots, while counterfeit devices sourced from grey market correspond to three different kinds of copycats of the original. Since the counterfeit devices belong to different types, while the originals belong to only one, we decided to unbalance the dataset by including a larger quantity of counterfeit devices. The study was structured into essentially three phases: gathering the dataset, analysing it, training and validating the machine learning algorithms.

The first phase involved characterising the devices and extracting features, as described in the previous section. The slope of the quiescent supply current vs. supply voltage characteristic, not included in the datasheet values, was considered as an additional feature. Such a parameter is not of interest to the device user and is not related to issues concerning the application in which the device is meant to operate; it depends on the amplifier's layout and process, so it was considered helpful for authentication.

In the second phase, the features' distribution and correlation were analysed, allowing us to determine whether certain features could be discarded or not. The third phase focused on selecting the algorithm, by limiting the analysis to a supervised approach.

During the second phase, all features were pairwise analysed, and some scatter plots are shown in Fig. 3. As shown in the figures, the features were normalized by applying the Robust Scaler, removing the median and scaling the data according to the Interquartile Range (the

**Table 1**
Typical values declared in datasheet and measured values for the set of original devices.

| Electrical characteristics | | Datasheet | O |
|---|---|---|---|
| Quiescent current | [mA] | 4 | 4.90 (±0.25) |
| Voltage gain | [dB] | 26 | 27.0 (±0.1) |
| Cut-off frequency | [kHz] | 300 | 605 (±30) |

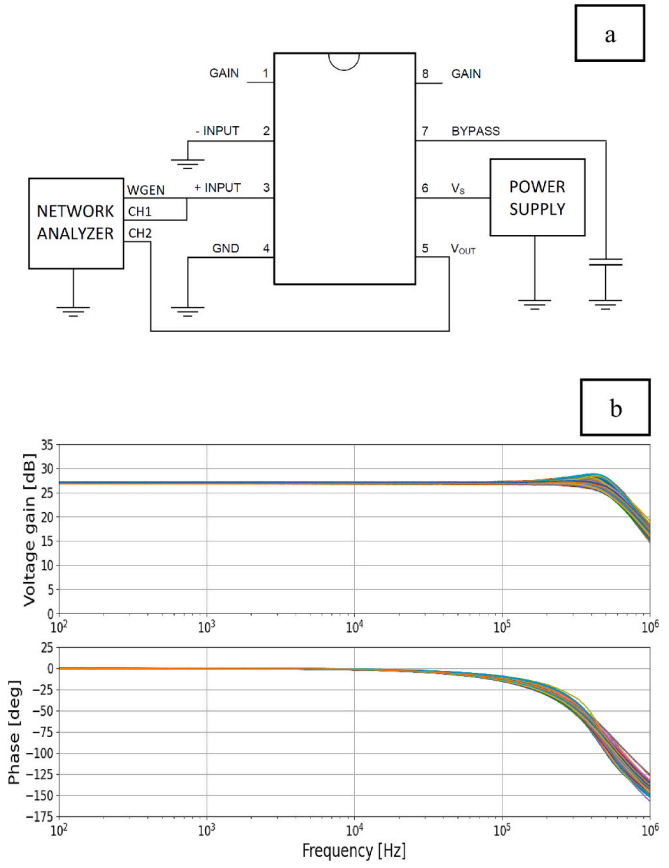



**Fig. 2.** (a) Setup for the bandwidth and gain measurements and (b) frequency response measurements from original devices.

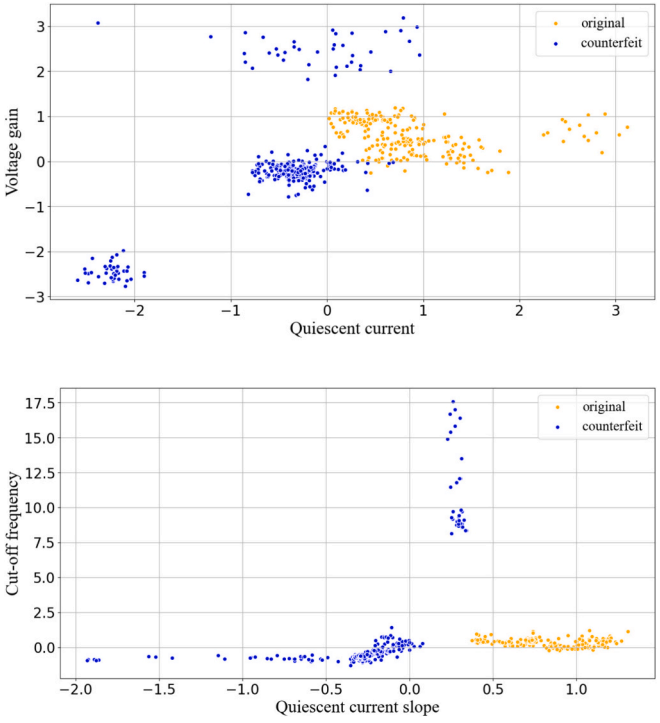



**Fig. 3.** Scatter plots for some of the feature's combinations (refer to the labels in the axis).

range between the 1st quartile and the 3rd quartile). Using the median and the interquartile range is a robust approach in the presence of outliers. Interestingly, for some combinations of features, the classes are perfectly separated, particularly for those containing the current slope. The algorithms selected, which ultimately fell on both KNN (k-nearest neighbours) and linear SVM (support vector machine), are briefly described in the following [24]. Both the models work well for small-sized datasets, although SVM exhibits greater flexibility and adaptability compared to KNN in general.

In KNN classification, the assigned class is the one most represented among the classes of the $k$ nearest points to the sample. The algorithm estimates the (posterior) probability that a sample belongs to a class as defined in Eq. (1).

$$P(\omega_i|\boldsymbol{x}) = k_i/k \tag{1}$$

Here $k_i$ is the number of neighbours belonging to class $\omega_i$ in an n-dimensional space region R, and $k$ is the number of $k$ closest elements (the number of neighbours, called prototypes) from the training dataset to the data point $\boldsymbol{x}$, within region R. The class of $\boldsymbol{x}$ is assigned based on the highest posterior probability, which is the class most represented among the $k$ prototypes.

The SVM is a versatile algorithm capable of performing linear and non-linear classification. With an appropriate non-linear mapping to a sufficiently high dimension, data from two categories can always be separated by a hyperplane. The primary goal of SVM is to find the optimal hyperplane that separates different classes in the feature space with the maximum margin. In the study case, a linear SVM is sufficient for an efficient classification. By way of illustration, an example of binary classification using a linear SVM on randomly generated data is shown in Fig. 4. In the example, two clusters belonging to two different classes are represented. The training data points that become the support vectors are marked differently. The decision boundary is the straight, solid line.

During the third phase, KNN and SVM were studied to understand the optimal combination of parameters for different combination of features.

With the KNN, every combination of features that includes the current slope leads to a success rate of 100 % for all the parameters considered (accuracy, precision, recall, F-score), this is due to the perfect separation of data in multidimensional space and appears independent of the number of neighbours k considered.

With the linear SVM every combination of features that includes the current slope leads to a success rate equal to 100 % for all the parameters considered, with values of parameter C comprised between 1 and 10.

Results are summarized in Table 2, where a comparison of different feature combinations is proposed.

**Table 2**
KNN and SVM test performance comparison. First and third lines refer to the training with three features (excluding the slope), second and fourth lines to the training with three features including slope and with four features.

| ML models | Accuracy | Precision | Recall | F-Score |
|---|---|---|---|---|
| KNN $n = 11$ | 99.4 % | 98.8 % | 99.7 % | 99.3 % |
| KNN n = 11 | 100 % | 100 % | 100 % | 100 % |
| SVM C = 10 | 94.3 % | 92.5 % | 93.9 % | 93.2 % |
| SVM $1 \leq C \leq 10$ | 100 % | 100 % | 100 % | 100 % |

Our study showed that both the algorithms perform excellently on the devices of the same type of those used to train the models. Further investigations will be conducted in the future with a larger quantity of data available, since, given the small size of the dataset under analysis, it can only serve as a starting point. The validated algorithms can be used to evaluate suspected devices.

Devices (A, B, C, D, E) whose electrical characteristics are reported in Table 3 were then tested with the best-performing algorithms selected. The order chosen for the measurement disposition in the table is arbitrary and do not depend on the device's performances. Results from the classification are reported in Table 4.

It must be said that counterfeit devices can sometimes exceed the performances of the originals. In this case, devices A and C absorb less current than the originals and provide desirable higher gain and bandwidth parameters. This aspect can insidiously induce one to think the devices are originals, but not because an unknown manufacturer produces them, resulting in fraudulent activity. Nevertheless, better performance at the starting point does not ensure their equal or higher reliability, which is fundamentally related to high-quality materials and processes and standard reliability testing. Results in Table 4 show that the two algorithms classify devices B, C and E coherently, while devices A and D are classified differently. In these cases, a prudent strategy should prioritize the indication of “counterfeiting” given by at least one of the algorithms.

### 2.4. *Destructive physical analysis (DPA)*

Physical inspection generally offers higher confidence than pure electrical verification but needs analytical techniques, dedicated labs and expertise. The DPA for microscopic inspection [25] includes the destructive removal of the package used when examining the internal structure, which is generally definitive to determine if a suspected part is a counterfeit. Moreover, the DPA is generally destructive and irreversible. The chemical removal of the plastic package was performed by using hot nitric acid. The optical metallographic microscope analysis enables the layout comparison. The DPA proposed in Fig. 5 is conclusive

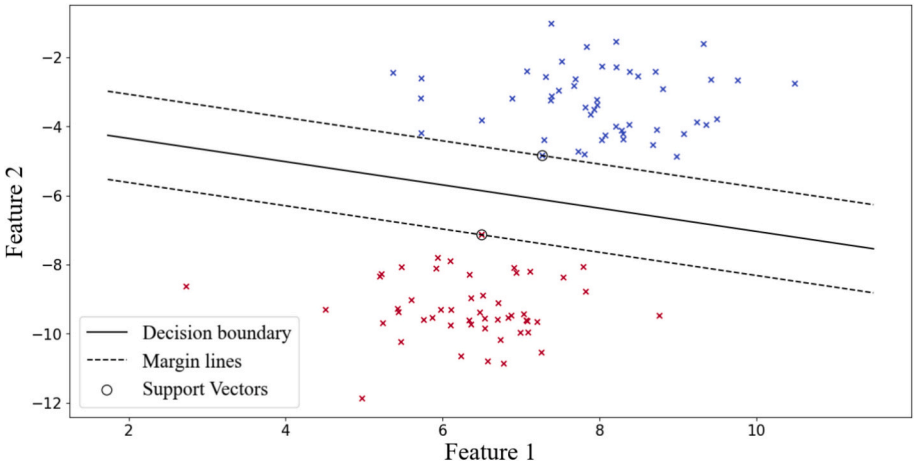



**Fig. 4.** Graphical example of boundary decision region construction through a linear SVM classifier.

**Table 3**
Typical and measured values for four different parameters.

| Electrical characteristics | | O | A | B | C | D | E |
|---|---|---|---|---|---|---|---|
| Quiescent current | [mA] | 4.90 (±0.25) | 3.70 | 4.60 | 3.72 | 4.96 | 4.73 |
| Slope | [$\mu\Omega^{-1}$] | 103 (±8) | 87.5 | 93.6 | 81.7 | 102 | 66.9 |
| Voltage gain | [dB] | 27.0 (±0.1) | 27.6 | 27.1 | 26.2 | 26.9 | 26.9 |
| Cut-off frequency | [kHz] | 605 (±30) | 901 | 583 | 1479 | 215 | 598 |

**Table 4**
Original (o) and counterfeit (c) classification.

| ML models | A | B | C | D | E |
|---|---|---|---|---|---|
| KNN | o | o | c | c | c |
| SVM | c | o | c | o | c |

for the authentication. Considering the layouts and internal markings, only type B is original, while A, C, D and E are merely copycats, so, in this evaluation, they can be considered counterfeit devices.

## 3. Conclusion

Our work considers the importance of non-destructive counterfeit detection and proposes an evaluation based on pure electrical measurements and simple machine learning algorithms.

The device under study is just an example for demonstration purposes. A wide variety of counterfeiting types are available in the market and original manufacturer has introduced a relevant number of modifications that make some detection techniques useless.

The destructive physical analysis confirms that both algorithms can perform well on devices of the same type of those used in the training phase (resulting from test scores). Thus, original devices are correctly classified as original (device B), and counterfeit devices of the same kind as those used in the training phase are correctly classified as counterfeits (device C). Devices A, D, and E are counterfeit devices, different from those used in the training phase. From a performance perspective, A and C exhibit better electrical characteristics, consuming less current while providing higher gain and bandwidth compared to the original products. Although they feature a similar manufacturer logo that may give the false impression that they are originals, these items are actually produced by an unidentified manufacturer. As a result, both the production process and the reliability testing do not meet the standards expected by consumers. In addition, considering the conformity to the original values in devices A, C, and D, the cut-off frequency is suitable for discriminating between originals and fakes. Still, the cut-off frequency in E is not a reliable discriminator compared with the feature "slope." Indeed, variations in an electrical parameter, even if this one is not an essential attribute, could indicate counterfeiting. The algorithms based on the set of 4 features, individually or in combination, consistently detect a greater number of different counterfeit parts.

These results also open the possibility of training new algorithms for emerging types of counterfeits.

The proposed method can detect different copycats, remarked and out-of-spec/defective devices.

For this kind of devices, the electrical testing can identify components with different performance levels and layouts that cannot be accurately detected by using other non-destructive inspection methods [23]. Considering the slight differences detected in originals from different production lots, the approach could, in principle, detect even overproduced devices. Future activity aims to inspect whether even aged/recycled devices are easily detectable with this approach.

Moreover, this approach could pave the way toward quality inspections where lot acceptance verifications are mandatory to avoid failures from innocuous/unreported manufacturing process changes.

## CRediT authorship contribution statement

S. Carta: Conceptualization; Data curation; Formal analysis; Investigation; Methodology; Software; Validation; Visualization; Writing - original draft; Writing - review & editing.

A. Urru: Conceptualization; Data curation; Formal analysis; Methodology; Software; Writing - original draft; Writing - review & editing.

M. Musa: Conceptualization; Project administration; Supervision; Validation.

P. Andronico: Conceptualization; Project administration; Supervision; Validation; Funding acquisition.

G. Mura: Conceptualization; Data curation; Formal analysis; Methodology; Project administration; Funding acquisition; Resources; Software; Supervision; Validation; Visualization; Writing - original draft; Writing - review & editing.

## Declaration of competing interest

The authors declare that they have no known competing financial

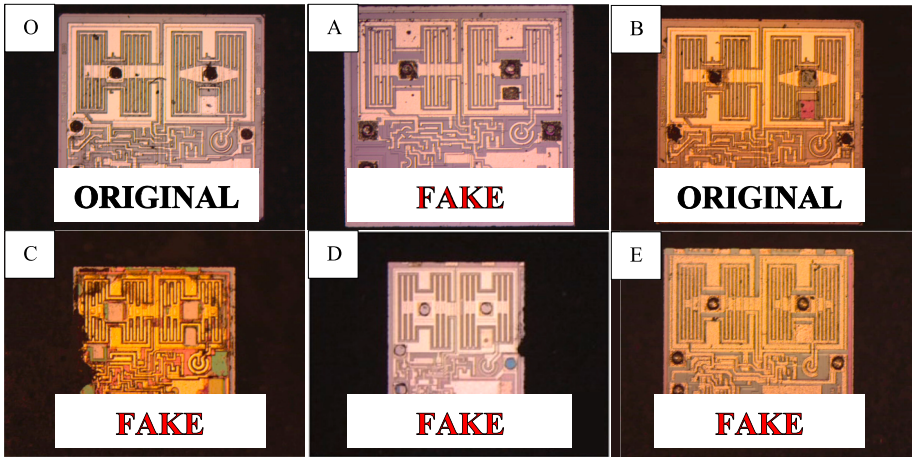



**Fig. 5.** Layout optical comparison after the physical de-processing of the plastic packages.

interests or personal relationships that could have appeared to influence the work reported in this paper.

## Acknowledgements

This work has been partially founded by “Fondazione di Sardegna” under project “DACE – Detection and Avoidance of counterfeit electronics”, CUP: F73C22001310007 and partially founded by “Regione Sardegna- Aiuti per progetti di ricerca e sviluppo -Settore ICT” under the project “NoDeCI- Non-Destructive Counterfeit Identification”.

## Data availability

Data will be made available on request.

## References

[1] S. Bastia, Next generation technologies to combat counterfeiting of electronic components, IEEE Trans. Comp., Packaging Tech. 25 (1) (2002) 175–176, https://doi.org/10.1109/6144.991192.
[2] J. Stradley, et al., The electronic part supply chain and risks of counterfeit parts in defense applications, IEEE Trans. Comp., Packaging Tech. 29 (3) (2006) 703–705, https://doi.org/10.1109/TCAPT.2006.882451.
[3] H. Akhavantaheri, An enterprise network model for understanding and disrupting illicit counterfeit electronic part supply chains, IISE Trans. 56 (3) (2024) 257–268, https://doi.org/10.1080/24725854.2023.2172631.
[4] G. Mura, Reliability concerns from the gray market, Microel. Reliab. 88–90 (2018) 1–4, https://doi.org/10.1016/j.microrel.2018.06.098.
[5] G. Mura, The threat of counterfeit electronics to the development of CubeSats, Int. Symp. ELMAR (2024) 223–226, https://doi.org/10.1109/ELMAR62909.2024.10694162.
[6] O. Aramoon, et al., Impacts of machine learning on counterfeit IC detection and avoidance techniques, Int. Symp. on Quality Electronic Design (2020) 352–357, https://doi.org/10.1109/ISQED48828.2020.9136972.
[7] K. Nyako, et al., Building trust in microelectronics: a comprehensive review of current techniques and adoption challenges, Electronics 12 (22) (2023) 4618, https://doi.org/10.3390/electronics12224618.
[8] D. Richman, et al., Analysis of standards-based counterfeit microelectronics detection methods, IEEE Access 13 (2025) 7691–7704, https://doi.org/10.1109/ACCESS.2025.3526518.
[9] Shankar S. Udaya, et al., A review on machine learning based counterfeit integrated circuit detection, Eng. Res. Express 5 (2023) 042002, https://doi.org/10.1088/2631-8695/ad0023.
[10] C. Xi, et al., Machine learning assisted counterfeit IC detection through non-destructive infrared (IR) spectroscopy material characterization, Electronic Comp. and Tech. Conference (2022) 2249–2255, https://doi.org/10.1109/ECTC51906.2022.00355.
[11] B. Ahmadi, et al., Automated detection of counterfeit ICs using machine learning, Microel. Reliab. 88–90 (2018) 371–377, https://doi.org/10.1016/j.microrel.2018.06.083.
[12] N. Asadizanjani, et al., Counterfeit electronics using image processing and machine learning, J. Phys. Conf. Ser. 787 (1) (2016) 012023, https://doi.org/10.1088/1742-6596/787/1/012023.
[13] K. Huang, et al., Parametric counterfeit IC detection via support vector machine, IEEE Int. Symp. on Defect and Fault Tolerance in VLSI and Nanotech. Systems (2012) 7–12, https://doi.org/10.1109/DFT.2012.6378191.
[14] J. True, et al., Terahertz based machine learning approach to integrated circuit assurance, Proc. of IEEE ECTC (2021) 2235–2245, https://doi.org/10.1109/ECTC32696.2021.00351.
[15] X. Chengjie, et al., Enhancing counterfeit detection of integrated circuits through machine learning-assisted THz-TDS analysis, in: Terahertz, RF, Millimeter, and Submillimeter-Wave Technology and Applications XVII, 2024, https://doi.org/10.1117/12.3003766.
[16] G. Mura, et al., Analysis of counterfeit electronics, Microel. Reliab. 114 (2020) 1–4, https://doi.org/10.1016/j.microrel.2020.113793.
[17] G. Mura, et al., Analysis of fake amplifiers, Proc. of ICM 131–134 (2021) 173136, https://doi.org/10.1109/MIEL52794.2021.9569080.
[18] G. Mura, et al., Electronic components authentication via physical analysis, Proc. of IEEE MIEL 177483 (2023), https://doi.org/10.1109/MIEL58498.2023.10315874.
[19] S. Frank, et al., Electrical characterization, in: L.C. Wagner (Ed.), Failure Analysis of Integrated Circuits 494, Springer, 1999, https://doi.org/10.1007/978-1-4615-4919-2_2.
[20] M.J. Deen, F. Pascal, Electrical characterization of semiconductor materials and devices, in: Handbook of Electronic and Photonic Materials, Springer, 2017, https://doi.org/10.1007/978-3-319-48933-9_20.
[21] G. Mura, M. Vanzi, The interpretation of the DC characteristics of LED and laser diodes to address their failure analysis, Microel. Reliab. 50 (2010) 471–478, https://doi.org/10.1016/j.microrel.2010.01.035.
[22] M. Vanzi, et al., Extended modal gain measurement in DFB laser diodes, IEEE Photonics Tech. Lett. 29 (2017) 7762038, https://doi.org/10.1109/LPT.2016.2633440.
[23] SAE International, Techniques for suspect/counterfeit EEE parts detection by electrical test, Methods AS6171/7 (2016).
[24] A. Geron, Hands-on Machine Learning with Scikit-Learn, Keras and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems, 2019.
[25] SAE International, Techniques for suspect/counterfeit EEE parts detection by delid/decapsulation physical analysis test, Methods AS6171/4 (2016).