Hardware Trust and Assurance through Reverse Engineering:

A Tutorial and Outlook from Image Analysis and Machine Learning Perspectives

ULBERT J. BOTERO*, [1]
RONALD WILSON*, [1]
HANGWEI LU, [1]
MIR TANJIDUR RAHMAN, [1]
MUKHIL A. MALLAIYAN, [1]
FATEMEH GANJI†, [2]
NAVID ASADIZANJANI, [1]
MARK M. TEHRANIPOOR, [1]
DAMON L. WOODARD, [1]
DOMENIC FORTE, [1],
1 Florida Institute for Cybersecurity Research, University of Florida, and 2 Worcester Polytechnic Institute

In the context of hardware trust and assurance, reverse engineering has been often considered as an illegal action. Generally speaking, reverse engineering aims to retrieve information from a product, i.e., integrated circuits (ICs) and printed circuit boards (PCBs) in hardware security-related scenarios, in the hope of understanding the functionality of the device and determining its constituent components. Hence, it can raise serious issues concerning Intellectual Property (IP) infringement, the (in)effectiveness of security-related measures, and even new opportunities for injecting hardware Trojans. Ironically, reverse engineering can enable IP owners to verify and validate the design. Nevertheless, this cannot be achieved without overcoming numerous obstacles that limit successful outcomes of the reverse engineering process. This paper surveys these challenges from two complementary perspectives: image processing and machine learning. These two fields of study form a firm basis for the enhancement of efficiency and accuracy of reverse engineering processes for both PCBs and ICs. In summary, therefore, this paper presents a roadmap indicating clearly the actions to be taken to fulfill hardware trust and assurance objectives.

CCS Concepts: • **Security and privacy → Malicious design modifications**; **Hardware reverse engineering**.

*Ulbert J. Botero and Ronald Wilson contributed equally to this research.
†Corresponding author. Fatemeh Ganji was with Florida Institute for Cybersecurity Research, University of Florida, when this study has been done.

Authors' addresses: Ulbert J. Botero, jbot2016@ufl.edu[1]; Ronald Wilson, ronaldwilson@ufl.edu[1]; Hangwei Lu, qslvhw@ufl.edu[1]; Mir Tanjidur Rahman, mir.rahman@ufl.edu[1]; Mukhil A. Mallaiyan, mukhil.mallaiyan@ufl.edu[1]; Fatemeh Ganji, fganji@wpi.edu[2]; Navid Asadizanjani, nasadi@ece.ufl.edu[1]; Mark M. Tehranipoor, tehranipoor@ece.ufl.edu[1]; Damon L. Woodard, dwoodard@ece.ufl.edu[1]; Domenic Forte, dforte@ece.ufl.edu[1],
1 Florida Institute for Cybersecurity Research, University of Florida, 601 Gale Lemerand Dr, Gainesville, FL, 32611, 2 Worcester Polytechnic Institute, 100 Institute Road, Worcester, MA, 01609-2280.

XXXX-XXXX/2020/10-ARTXXX $15.00
https://doi.org/XXX

Additional Key Words and Phrases: Hardware Counterfeiting, Hardware Trojan, Imaging, Image Processing, Integrated Circuits, Machine Learning, Printed Circuit Boards, Reverse Engineering, Trust and Assurance.

ACM Reference Format:
Ulbert J. Botero, Ronald Wilson, Hangwei Lu, Mir Tanjidur Rahman, Mukhil A. Mallaiyan, Fatemeh Ganji, Navid Asadizanjani, Mark M. Tehranipoor, Damon L. Woodard, and Domenic Forte. 2020. Hardware Trust and Assurance through Reverse Engineering: : A Tutorial and Outlook from Image Analysis and Machine Learning Perspectives. XX, X, Article XXX (October 2020), 54 pages. https://doi.org/XXX

1 INTRODUCTION

Outsourcing of integrated circuit (IC) and printed circuit board (PCB) design, fabrication, packaging, and testing has dramatically reduced product development time and cost. In doing so, this has enabled the widespread availability of microelectronics, which has indeed transformed modern life. However, unintended consequences include malicious design alteration (i.e., hardware Trojan insertion [136, 160]) and the rise of the counterfeit electronics industry [187]. Reverse engineering (RE) is widely applied for educational purposes and for detecting Intellectual Property (IP) infringement, but it can play an even more significant role in hardware trust and assurance. RE of electronic chips and systems refers to the process of retrieving an electronic design layout and/or netlist, stored information (memory contents, firmware, software, etc.), and functionality/specification through electrical testing and/or physical inspection. Although RE is often presented in a negative light (e.g., illegal cloning designs and/or disclosing sensitive information to a competitor or adversary), it is sometimes the only foolproof way to detect malicious alteration and/or tampering by semiconductor foundries, find vulnerabilities present in commercial-off-the-shelf (COTS) chips and avoid them, and replace obsolete (i.e., no longer manufactured) hardware.

As for attaining trust and assurance, existing techniques are limited and/or ineffective. For example, run-time monitoring techniques increase the resource requirements – power consumption, memory utilization, and area overhead on ICs/PCBs – due to on-chip/board sensors used to detect anomalous activities. In test time methods, the challenge is to generate test vectors that trigger stealthy, well-placed hardware Trojans in billion-transistor chips. Similarly, in side-channel signal analysis approaches, inescapable process variations, and the measurement noise undermine the probability of detecting small Trojans [89]. As a result, the confidence level in detecting Trojans using the aforementioned techniques is quite low [28, 138, 186]. Hence, RE has been gaining more attention in recent years and experiencing community-wide acceptance as an effective approach, in particular, for hardware Trojan detection [12, 45].

In the area of IC counterfeit detection and avoidance, the current best practice requires the use of either classification by subject matter experts (SME), procuring lifetime buys for long-term system maintenance, or acquiring components from untrusted distributors in a supply chain, which potentially involves grey market distributors. Each of these options is non-ideal. The large quantities of components that SME counterfeit analysts are required to analyze and manually classify makes this current practice very inefficient and costly. As for life-of-type buys, it is impractical and almost impossible to predict the lifetime of every component in a design, in anticipation of obsolescence and failure. Overestimation of the lifetime leads to procuring more components than necessary, and consequently, the waste of resources. Underestimation of the lifetime results in non-ideal situations, such as redesign or procurement through grey market distributors necessitated earlier than desired.

For PCBs, counterfeiting and Trojan insertion is a similarly prevalent problem. While there are existing chip-level integrity validation approaches, as mentioned above, they are not readily adaptable to PCBs, which is a cause for concern. In response to this concern, a common method for preventing and protecting against PCB counterfeiting is to take advantage of intrinsic characteristics of PCBs making each and every of them (quite) unique [218]. Additionally, [85] has explored using

unique patterns seen in images of surface vertical interconnect access (via) as fingerprints of design to overcome the problem of counterfeit PCB distribution. While both of these approaches can help us to improve reliability and assurance of a PCB after manufacturing, these techniques would still have to face difficulties in detecting small Trojans, similar to that seen in the October 2018 Bloomberg Businessweek article, entitled "The Big Hack" [160]. In October 2018, it was claimed that unauthorized microchips were found in the products of a manufacturer that provided Apple, Amazon, and even the US government with specialized servers [136]. As reported in [136], security experts suspected that the assembly facility owned by Supermicro might have implanted the chip, which could serve as a backdoor for spying information exchanged over networks equipped with the altered PCBs of servers. Such an attack, i.e., adding an extra chip maliciously, severely affects the confidentiality and integrity of a system. More importantly, the survivability of this system is strongly influenced due to the typically high degree of complication and obstacles involved in revealing the existence of such threats and recovering the system from them. This can further highlight the strong demand for the verification of the security of the physical systems.

According to the above discussion, today more than ever, there is a significant need for fast and fully automated RE, imposed by industries, and especially for security-critical applications. The RE process comprises delayering, imaging, annotation, and netlist extraction. The current state-of-the-art practices are tedious, challenging, and expensive. They usually require a suite of cleanroom and microscopy equipment, very long imaging times, and manual or semi-automated post-processing steps for converting images to netlists. Despite this, recent advancements in failure analysis tools and delayering processes are opening up new dimensions in RE. As an example, plasma etching has achieved better control over ion-energy distribution, thereby improving selective and automation in delayering [154]. Furthermore, the introduction of non-destructive X-ray computed tomography (X-Ray CT) and ptychography in recent years can eliminate the process of delayering, and hence, can speed up the imaging time for the upper metal layers of an IC and an entire PCB. New scanning electronic microscopes (SEMs), such as multi-beam systems, have also been introduced to significantly speed up imaging of nanoscale samples. Nevertheless, they are not widely available and are still several times more expensive than standard SEMs. In addition, since such tools could yield petabytes of data in only a day, the research on automated and intelligent image analysis algorithms is an urgent need to reduce the time and cost of RE.

In this tutorial, we systematically study the current challenges that automated RE faces in order to be useful for providing trust and assurance. Existing surveys on RE focus on different aspects, e.g., Keshavarz et al. have presented examples of image-based RE applications and discussed hardware attacks in detail [97], while Fyrbiak et al. have summarized the process of accessing gate-level netlist from three system models and discussed the evaluation strategies [60]. Compared to our work, they have explored neither the challenges during a typical RE process from an imaging perspective nor considered the possibility of applying machine learning approaches in this context. Our tutorial further describes a typical workflow of RE, and then investigates the possibilities and limitations of processes incorporated in such a workflow from the RE perspective. More precisely, we explain inherent differences between natural images, which virtually all the well-developed image processing algorithms are designed for, and images taken to conduct RE on a hardware device. To this end, we give an exhaustive overview of numerous obstacles to applying common methods originating in image processing and machine learning. In particular, we place emphasis on the need to incorporate domain knowledge to overcome them. Several examples of such issues are given and reviewed in detail. In summary, this tutorial aims at providing an outlook on how to improve RE so that it can better handle detection and avoidance tasks in the context of hardware trust and assurance.

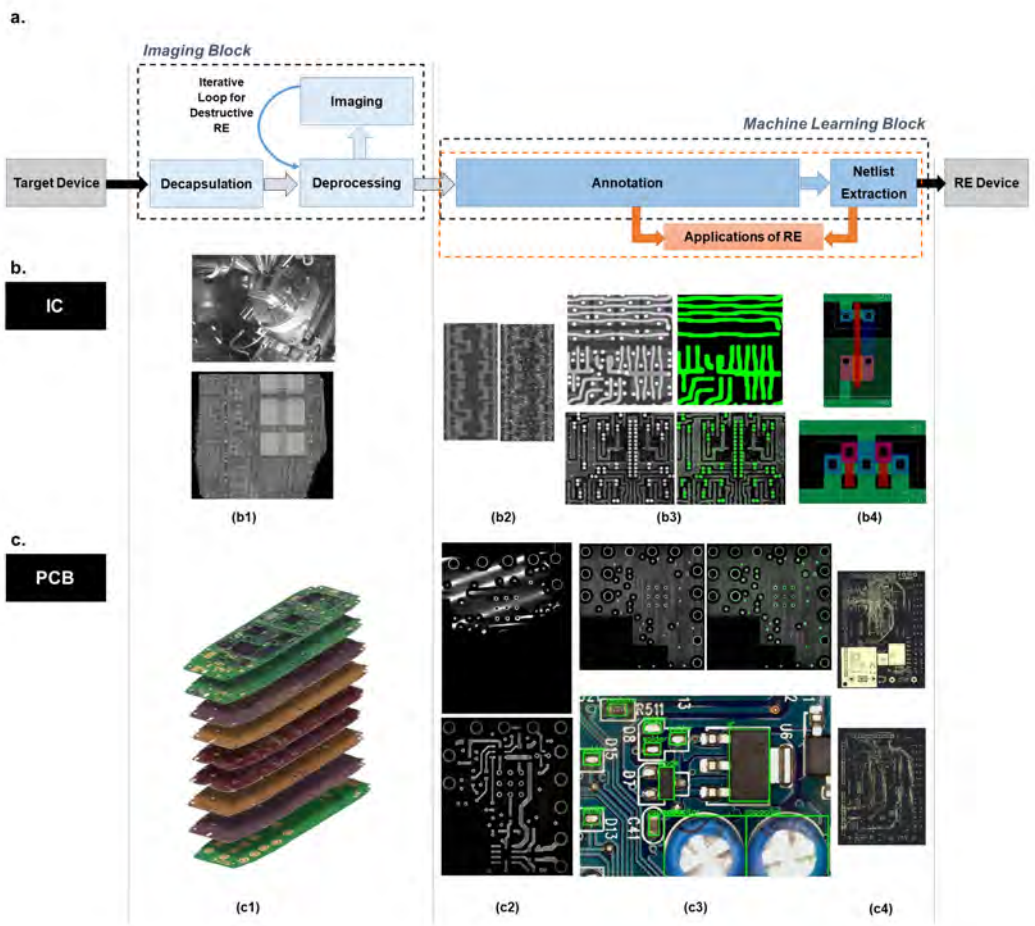


Fig. 1. Our systematic overview of an RE process, which can be performed on ICs and PCBs, its challenges and possibilities. (a) A typical workflow of RE encompassing various stages. Two main blocks of such a workflow are: Image Analysis (see Section 4) and Machine Learning (see Section 5). Moreover, we discuss how the outputs of the machine learning-related block can enable us to provide hardware-based trust and assurance, as an application of RE (for a general view, see Section 2). Inherent challenges facing us in both cases of ICs and PCBs are further discussed in Section 4- 5. (b) RE workflow for IC: (b1) Deprocessing of the IC [149], (b2) Example of noise removal in the active region using different imaging parameters, (b3) Segmentation and extraction of polysilicon structures and vias in an IC [34, 35], (b4) Netlist of extracted logic cells. (c) RE workflow for PCB: (c1) Image depicting a multi-layered PCB [193]. Depending on the number of the layers in a PCB, different types of RE techniques should be considered. Irrespective of this, these challenges are inevitable: (c2) Example for misaligned layer and reconstructed image, (c3) Segmentation and extraction of vias for X-rayed PCB and labelled components on the surface of an optically imaged PCB, (c4) Segmented layout of PCB layers with connected and not-connected vias [7].

A brief overview and the organization of the tutorial: Beyond providing a taxonomy of approaches proposed to address trust and assurance issues, Section 2 describes how automated RE can enable us to solve those problems more effectively. Section 3 provides a high-level overview of the challenges with RE. Section 4 discusses the issues impeding the RE workflow from an imaging

perspective (see the imaging block in Figure 1). This section is complemented by Section 5 with an in-depth discussion from a machine learning and image analysis point of view along with a brief discussion on the application of deep learning in RE, as illustrated in the machine learning block in Figure 1. Section 5 further demonstrates how various applications of RE, such as counterfeit and Trojan detection, can leverage the information retrieved through feature extraction and analysis. Section 5 also briefly discusses counter RE approaches implemented in contemporary hardware. As this tutorial aims at pointing to a new outlook, Section 6 is devoted to future research directions. Finally, we conclude by pointing out the issues addressed in the tutorial.

2 APPLICATIONS OF RE FOR TRUST AND ASSURANCE

Semiconductor technology has become an integral part of our everyday lives, as ICs and embedded systems have been becoming ubiquitous. The spectrum of the applications of these devices and systems covers various areas including, but not limited to, household appliances, critical infrastructures (i.e., commercial facilities sector, government facilities, energy sector, etc.), and military systems. Regardless of these applications, their trustworthiness and reliability must be assured. This section aims to explain how automated RE can address this concern by providing an added degree of precision for the analysis and evaluation, applied at different development stages in electronics industries. We further elaborate on the applications of (automated) RE, namely Trojan detection and obsolescence replacement.

2.1 Trojan Detection and Counterfeit Avoidance

Counterfeit and tampered electronics pose serious threats to hardware-based trust and assurance. In particular, cloned chips and hardware Trojans can violate the security requirements of root-of-trust, thereby reducing confidentiality, integrity, and availability. For ICs, cloning is the process of copying and unauthorized production of a design without having legal IP rights. Moreover, any malicious modification of the structure, functionality, or parameters of the chip that causes the device to operate outside of its specification can be identified as a hardware Trojan. Furthermore, the root-of-trust can be compromised at the system level. PCBs give another opportunity for an attacker to tamper, clone, counterfeit, and insert a hardware Trojan. In fact, since PCBs lie at the heart of an electronic system and integrate several components to achieve the desired functionality, it is increasingly important to guarantee a high level of trust and reliability at such an integration stage. The aforementioned incident allegedly at Supermicro serves as an example (see Section 1). Advances in the RE automation process can enable us to shorten the time to identify these types of threats at multiple levels of an electronic system [7, 156].

The importance of applying RE for addressing trust and assurance-related issues are twofold, namely detection and avoidance (see Figure 2). When it comes to avoidance, we are interested in approaches that can prevent counterfeit parts from entering the supply chain. For this purpose, it is crucial to develop relatively less costly and time-consuming counterfeit detection methods [71]. Therefore, due to this close connection between avoidance and detection, in this tutorial, our primary focus of interest is detection methods. In the detection process, the incoming electronic components undergo a physical or electrical inspection process to examine authenticity. As RE is an interior, physical-inspection-based approach, to decide whether a chip/system is cloned or to detect a Trojan, one should rely on the availability of golden data. Golden data can be images from a known authentic chip or PCB, bill of materials (BoM), schematic, layout, or device, whose functionality, structural and electrical parametric signatures are available for comparison.

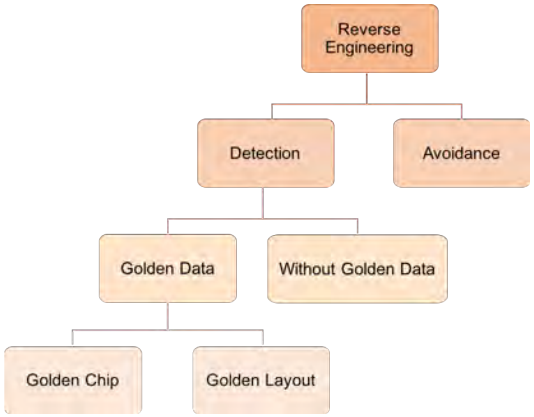


Fig. 2. Taxonomy of approaches for addressing trust and assurance issues through RE.

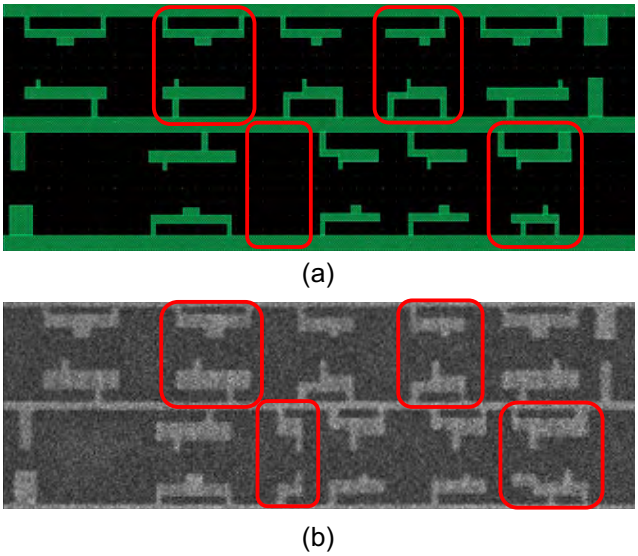


Fig. 3. (a) Layout of smart card chip (b) SEM image of the corresponding area. (Circled areas shows the effect of a modification or insertion of the logic cell.)[197]

For example, a layout[1] is determined as *golden* if the IP holder and System-on-Chip (SoC) designer/PCB manufacturer are authorized and trusted[2] [197]. A golden layout or design can provide a benchmark for assessing the functionality of the chip or analyzing its physical structure. The designer's layout (see Figure 3(a)) can be compared to the SEM image taken from the respective

[1]After performing the translation of a specification into a behavioral description (typically in a hardware design language (HDL)), this description is synthesized to generate a design implementation of logic gates, i.e., netlist. This netlist is used to produce a layout (GDSII file) by conducting placement/routing. To fabricate ICs, this GDSII is sent to a foundry by the design house.

[2]A trusted party is defined as one committed to ensuring a proper IC design/fabrication flow (i.e., does not insert Trojans, protects IP confidentiality, etc.). An untrusted party cannot ensure such a proper flow or performs malicious activities intentionally.

manufactured design (see Figure 3(b)), to determine possible Trojan insertions. However, it does not provide any reference for side-channel parametric profiles, e.g., power, path timing, electromagnetic signature, photonic emission, etc., which can only be characterized by using a fabricated chip or board. Additionally, a device is considered *golden*, when either it is fabricated from a golden layout in a trusted facility or its functionally and physical characteristics are verified through full-blown RE [186]. The primary concern regarding fabricating a golden sample in a trusted facility is a prohibitively costly process. Besides, the parametric profile of the golden device is different from the same parametric profile of devices produced in another facility for the same technology node, even within the same fabrication facility.

Nevertheless, common test methodologies may not always be helpful for detecting Trojans [88]. In this context, an RE approach can also be employed to detect extra insertions and deletions [172, 196]. Note that although IC camouflaging[3], especially dummy contact-based IC camouflaging, can impair the effectiveness of *malicious* RE of ICs, the designer can greatly benefit from an automated RE along with a golden chip or layout to deal with such cases. Yet the challenges with RE-based approaches are the SME involvement and the execution time (see Section 2.2).

For PCBs, due to the minute details involved in the Trojan insertion process, the availability of golden data to facilitate full-blown PCB RE is even more pressing. The modern nature of PCB designs, being multi-layered, provides a variety of Trojan insertion possibilities that are nearly impossible to prevent without full-blown RE. Specifically, an attacker can take advantage of unused pins, multiple layers, and hidden vias in the design to alter connections throughout the internal layers/ hidden vias, as well as the properties of these connections. Altering traces in the internal layers can make no structural difference, but produces undesired functionality under certain conditions. Such alterations include modifying the mutual coupling capacitance, characteristic impedance, and loop inductance [63] as well as adding ultra-low areas, and power components in the internal layers. Moreover, the chances of detecting these modifications via exhaustive testing are low since malicious functions are barely triggered during in-circuit and boundary-scan-based functional tests. With a full-blown RE, the design dimensions going down to the trace widths and spacing can be extracted and compared for tamper detection and to give the IP holder an available golden sample. If the attacker alters the design structure, by comparing the designed and extracted netlists, the detection can be less challenging, and the full-blown RE can be more effective (for more details see Section 2.2).

In general, the detection techniques have progressed at a fast pace, due in part to advancements in artificial intelligence, and in particular, machine learning. Techniques originating from machine learning have been widely employed in hardware security. For instance, machine learning algorithms have been applied for Trojan and IC counterfeit detection; for a comprehensive survey, see [54]. Nevertheless, when it comes to approaches leveraging the strengths and capabilities of both reverse engineering and machine learning methods, e.g., [10, 11], less effort has been made to develop such approaches. Only recently, as a result of the advancements in image analysis incorporated with the developments of techniques relying on SEM, X-Ray CT, and optical imaging, more reliable, faster and automated hardware Trojans detection methods have been developed, being also useful for detecting cloned chips/systems. Such a process generally involves several steps, namely image pre-processing, feature extraction, and classification.

Image pre-processing influences the accuracy of perceptual feature extraction through noise reduction, edge enhancement, segmentation, etc. As the name implies, feature extraction deals with extracting salient features from the images of in the electronic component, acquired by using the

[3]A technique that can be employed to mask the circuit functionality by synthesizing circuits with logic cells, which look similar, but can have different functionalities.

SEM/X-ray CT/optical microscope. Those features are represented as inputs for machine learning algorithms, e.g., neural network, support vector machine (SVM) or clustering approaches, which can determine modifications in the function or the structure in the system. However, to benefit from advances in machine learning, relatively large sets of data are necessary to train machine learning algorithms. Especially for deep learning methods, a vast number of data samples are required to achieve an acceptable level of performance.Nonetheless, advanced methods, e.g., Trojan Scanner [197], can direct trust and assurance-related studies towards partial RE-based hardware Trojan detection methods.

In the presence of data derived from a golden sample, different methodologies, e.g., the structural test comparison between a suspected sample and the golden sample/layout, can be deployed to identify cloned devices [71]. Over the years, to address the availability of neither a golden chip/layout nor a sufficiently large training dataset when dealing with protecting chips/systems, different avoidance methodologies like the secure split-test, physically unclonable functions, and lightweight on-chip sensors have been proposed for countefeit detection and avoidance[71]. In line with this, the fast and automated RE can enable us to establish a secured supply chain comprised of a trusted manufacturing facility and distribution for the security-critical applications. Such improvement offers effective measures for the avoidance of cloned or Trojan-infected chips.

2.2 Obsolescence

In addition to Trojan detection and counterfeit avoidance, an RE-based method also provides trust and assurance for the obsolete or near-term life technologies and components. These technologies, usually referred to as legacy electronics/systems, are prominent in many critical systems. Typically the production cycle for electronics is under pressure from the fast-paced consumer electronics industry, where the next generation of devices with improved properties is expected and adopted in the course of the following calendar year. Yet, the opposite is the case in military and government electronic systems that go through longer development cycles and deployment. These systems are designed to be in operation for decades [181]. However, since these systems are deployed for increasingly longer periods, the cost of maintenance begins to increase due to needed parts becoming obsolete. The long life span of these components and systems opens up new possibilities for malicious activities including security concerns and vulnerabilities. Most notably, diminishing manufacturing sources for obsolete components can force original equipment manufacturers (OEMs) to purchase from untrustworthy distributors. This has been identified as a known source for recycled, remarked, or counterfeit components/systems and consequently, a pressing concern for governments, as reported by, e.g., the United States Senate [42].

Although a full system redesign is an option to address this concern, it is impractical due to the associated costs and manpower [181]. In particular, if previous design information that would be used for the redesign is no longer available or scarce, performing RE to acquire the needed design information can result in destroying the only available samples. This is often the case in legacy systems, where previous designs are lost over time through company migrations/transitions or components are obsolete and discontinued. These concerns are present for both of the IC and PCB levels, but can be addressed thanks to advances in image analysis and machine learning.

2.2.1 IC Level Upgrades. As an interdisciplinary field including several key components from image analysis and machine learning fields of study, automated RE enables us to replace obsolete technologies and provide additional trust and assurance in hardware security. With respect to the ability of automated RE to segment, identify, and interpret different properties of IC layouts, it is possible to not only deconstruct the netlist of a device, but also reconstruct it. By identifying various components on a layout and comparing them with the standard cells, the functionality and netlist

of an IC can be deconstructed. Afterward, this information can be used either to analyze possible faults in the layout or for reproduction, if the reverse-engineered device is obsolete and no longer in distribution. Furthermore, once the functionality is deduced and the netlist is reconstructed, any desired upgrades (additional logic, security primitives, etc.) can be added to the design and the new upgraded design and layout are ready for fabrication [21].

2.2.2 PCB Level Upgrades. The above-mentioned advances enable us to offer the maintenance or replace obsolete or rare PCBs as well. In a similar fashion to ICs, automated RE can be used on PCBs to identify key components, traces, vias, and layers to reconstruct the design and netlist [133]. Coupling these techniques with advances in non-destructive RE via X-Ray CT [7] leads to an all-encompassing process that completely removes the traditionally needed SME. This is especially useful for PCBs, whose design information has been mishandled or with scarce supply. This can be explained by the fact that traditional RE may result in the destruction of samples undergoing the process [69]. Providing a substantial cost and efficiency savings achieved through this gathered design information, it is now possible to perform design-to-manufactured product validation, product-to-product comparison, and the ability to upgrade past designs. All of these provide an added level of trust and assurance to the systems that require the utmost attention to security.

2.3 Limitations of RE

Upon completion of the workflow shown in Fig. 1, gate-level connectivity, i.e., netlist, of the IC, can be extracted. However, the design hierarchy and the intend of the circuit blocks are still missing from the netlist. RE from the gate-level netlist to abstraction level - register-transfer level (RTL) and behavior (architectural) level is not a straightforward task since at the pre-silicon stage, each design undergoes extensive optimization performed by computer-aided-design (CAD) tools. CAD tools perform its optimization at the gate-level netlist by flattening the netlist, which results in loss of high-level design data, i.e., hierarchy and module information. Further, logic synthesis for logic minimization, technology mapping, sharing logic, and functional blocks increase the complexity in extracting RTL and behavior abstraction. In recent years, several formal verification methods, for example, Boolean Satisfiability Function (SAT) [182], Binary decision diagram (BDD) [211], and Quantified Boolean Function (QBF) [118], have been used to identify the control logic and generate finite-state machine transition graph for extracting functional modules, e.g., registers, multiplexers, or modules like Arithmetic-Logic Unit (ALU), interfacing circuit, from the extracted GDSII file of the device.

Alike behavior extraction of an IC, information retrieval from non-volatile memory (NVM) and physical unclonable functions (PUFs) is challenging. The NVM, such as Flash and EEPROM, stores charges as a medium of keeping the information safe during the power-off state of the device. However, reverse engineering the FLASH and EEPROM without disturbing the charge, even with the most sophisticated FA tools, is proved to be difficult [47]. Unlike charge-based NVM, one-time programmables like E-fuse and anti-fuse can be reverse engineered using SEM and transmission electron microscopy (TEM) [155]. Though PUF is considered as a secured key-storage, the key stored in PUF is considered lost during destructive RE.

3 REVERSE ENGINEERING AND ASSOCIATED CHALLENGES

Research and development in most domains are typically fueled by academic interest, commercial gain, and governmental entities for national interest matters. With RE being opposite to the mainstream workflow for hardware design and manufacturing, research interest in it has been minimal. An exemplary instance of this fact could be observed in technical surveys with less focus

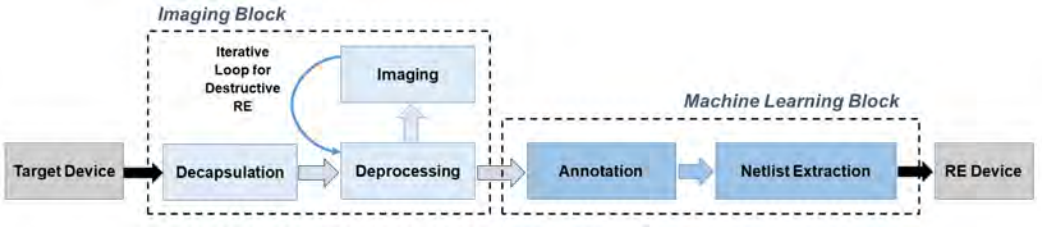


Fig. 4. A typical RE workflow with demarcations for both image analysis and machine learning applicable blocks

on complete RE, in contrast to one of most relevant domain, i.e., applications of ML in hardware security [54]. In addition, for hardware assurance, several studies considered RE as a last resort due to its overall complexity and costs. With the recent commercial interest in RE, stemming from the need for IP protection, it is necessary to devote more effort to research. In this regard, Lippmann et al. have suggested that given enough time and resources, RE can recover the building blocks of any given IC with up to 99% accuracy [124]. This estimate includes accounting for the possibility of countermeasures designed to thwart the performance of RE. From the perspective of commercial entities associated with hardware development and design, the goal is not to get designs to be completely RE-proof but to delay the process long enough to introduce completely novel designs and technologies. Due to this inherent conflict of interest, the amount of data available is limited as compared to other fields and, hence, limits the effectiveness of data-driven approaches such as machine learning in RE. Furthermore, compared to other relevant domains, e.g., failure analysis, techniques applied in the context of RE could not keep pace with the evolution of technology.

To address these, RE should be performed as a highly modular process with a well-established workflow with a typical, practical example shown in Figure 4. This workflow has been tried and tested in a variety of works [45, 86, 151, 166, 193]. Typically, the development of a complex systematic approach, like RE, is initiated by drawing up a high-level overview of the problem. The lower level details are separated into modules for independent research and development depending on their overall contribution to an effective solution for the problem. However, in the case of RE, this process is reversed. For instance, imaging for ICs was predominantly used for fault and yield analysis in the forward manufacturing workflow, but was later adapted for RE. As a result of such an adoption, development of modules have become unbalanced, which leads to process bottlenecks and missing links between established modules. The sequential nature of the workflow further exacerbates this problem, i.e., the errors accumulate at each layer, making the final result erroneous and unsuitable for the intended purpose.

To make the RE workflow more clear to the readers, the next sections elaborate on existing approaches associated with each module in the RE workflow, their inherent assumptions, potential drawbacks, and, finally, avenues of further research and development for the hardware assurance community.

4 INHERENT CHALLENGES ASSOCIATED WITH IMAGING ELECTRONIC COMPONENTS AND SYSTEMS

As depicted in Figure 4, the imaging block encompasses all the steps involving physical interaction with the ICs and PCBs providing an effective demarcation between the hardware and software aspects of RE. The imaging block comprises of three key steps of the RE process: decapsulation, deprocessing, and imaging. This section describes these steps in detail for ICs and PCBs.

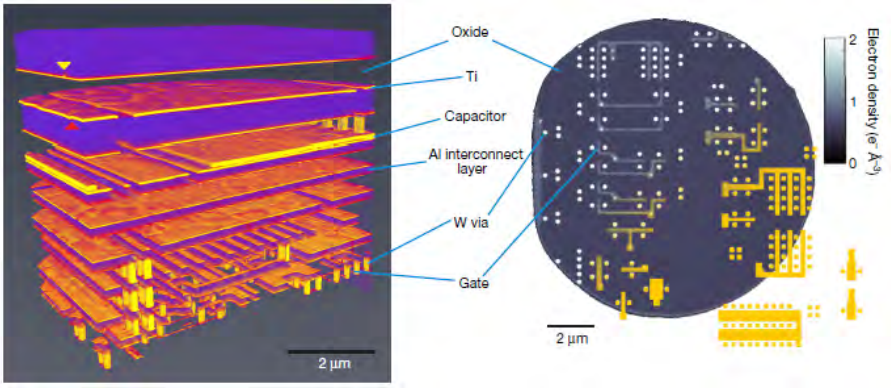


Fig. 5. Non-destructive imaging using X-Ray CT [81]

4.1 Problems Associated with Handling IC Images

The first step in the RE workflow is called decapsulation, taken to remove the protective enclosure surrounding the silicon die. The process of removal typically includes mechanical force and etching with acid. The various tried and tested recipes, like fuming nitric acid, can be found in literature [178]. This is then followed by deprocessing, and imaging steps, as explained below.

4.1.1 Deprocessing. This is a decisive step in the RE workflow. Depending on the imaging modality available, the sample preparation varies. There are two major approaches: non-destructive and destructive imaging.

Non-destructive imaging: In the context of electronics, this type of imaging is predominantly used for fault analysis. In this regard, scanning confocal electron microscopy has been used to image buried structures in thick IC samples [57]. X-ray based imaging has been used for counterfeit IC detection and fault analysis [109, 116, 127, 205]. Scanning optical microscope has been used for counterfeit IC detection, but this approach assumes access to IC design files [131]. However, a recent study shows promising results for RE [81]. The X-ray computed tomography (CT) technique has been able to effectively resolve features in an IC up to 14.6 nm. The CT reconstruction and a slice from the CT is shown in Figure 5.

However, this advantage comes with significant overhead in the image acquisition time frame. With advancements in X-ray imaging, non-destructive may become a significant tool for RE. All the methods stated in this section are non-invasive. On a similar note, imaging techniques such as photon emission microscopy have been used for probing and decoding functionality of live ICs in near-infrared (NIR) spectra. Although these methods do assist in RE and have been widely used for hardware assurance purposes, they cannot be exploited for full-scale RE.

Destructive imaging: A wide range of electron microscopy techniques is employed in destructive imaging. Unlike imaging techniques presented in the previous section, these techniques require extensive sample preparation. Images acquired using improperly processed samples can have a detrimental impact on the final result. Electron microscopy techniques such as Scanning Electron Microscopy (SEM), Transmission Electron Microscopy (TEM), Focused Ion Beam (FIB) [74], Helium Ion Microscopy (HIM) [147] and several other similar techniques are used. All of these techniques use active imaging where charge carriers are bombarded on the sample to generate a secondary response. SEM, being widely available and reasonably affordable, is the most common tool used for imaging ICs. TEMs are seldom used owing to their stringent sample preparation requirements as

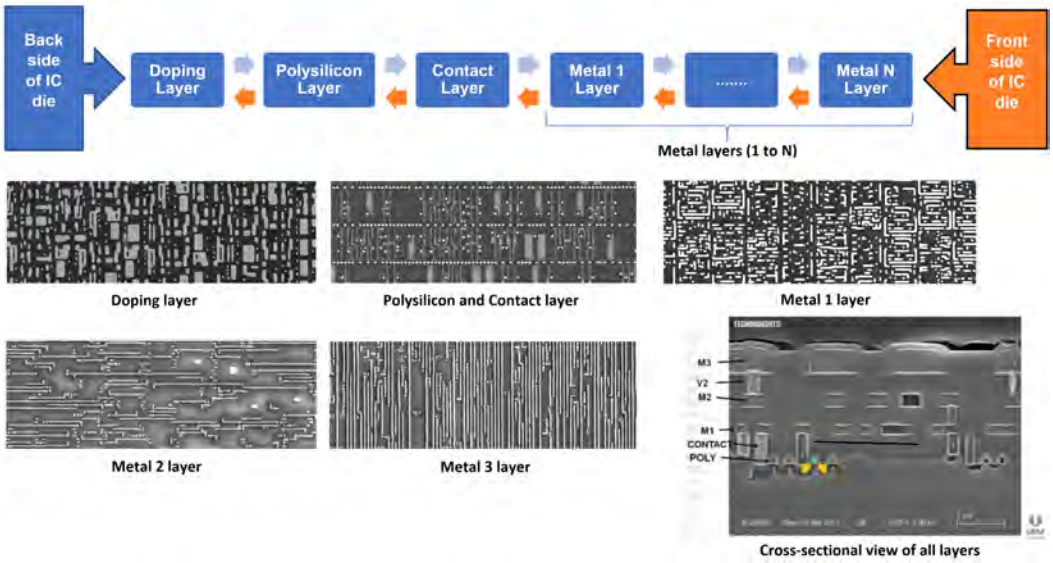


Fig. 6. The sequence of the layers in an IC along with their cross-sectional view [1, 151]

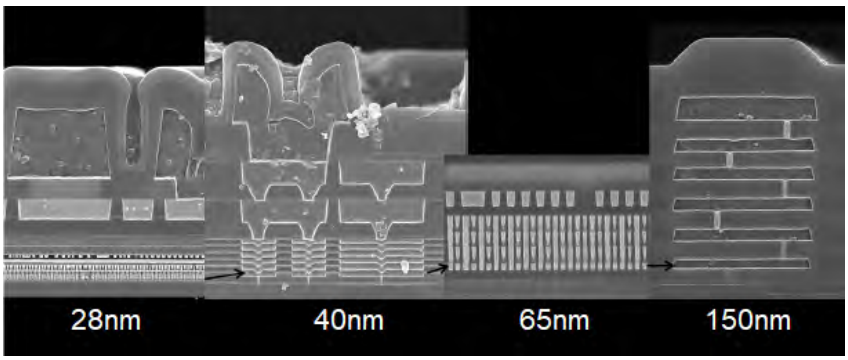


Fig. 7. Cross-sectional view of ICs in various node technologies [124]

compared to SEMs [109]. The typical cost associated with renting an SEM is around 100 euros for an hour [46].

Destructive imaging is one of the most commonly used approaches for RE. It requires the sample to be mounted onto a plate, and layers of specific thickness are removed at a time. This process is called delayering. This is an iterative process with its ultimate purpose of imaging various IC layers (see Figure 6). The depth of delayering and number of layers in the IC obtained using a cross-sectional image of the IC. The cross-sectional view is obtained by vertically slicing the IC die using a diamond saw followed by mechanical polishing [148]. After this, the IC die cannot be used for further processing. Note that when performing destructive deprocessing for RE, the layer thickness should be known apriori through, e.g., access to the IC design information. A cross-sectional view of some contemporary ICs are shown in Figure 7. The delayering process uses wet/dry chemistry to etch away material from the IC surface to expose each layer. This process is also done mechanically using a multi-axial Computed Numeric Control (CNC) mill. The acid

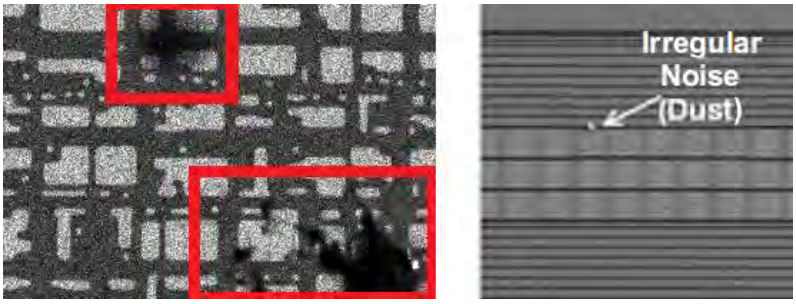


Fig. 8. Effects of inadequate care during the sample preparation process. Etch residue leftovers (left) and dust particle on the die (right) [82]

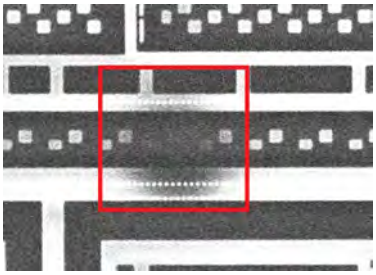


Fig. 9. Effect of uneven delayering. This maybe a result of improper mounting of the sample or inadequate polishing of the die surface

for etching the surface is selected depending on the material composition of the IC. A detailed description of the delayering process, including various etch chemistry, can be found in literature [46, 100, 101, 105].

At the slightly increased cost and deprocessing time overhead, a FIB can be used to delayer the sample more accurately. A FIB uses a focused ion beam to remove materials slowly with selections of gas chemistry [60, 202]. FIB is generally a preferred option for ICs using contemporary node technology because of their smaller feature sizes and fragile nature. It has been recommended that at least one die be provided for each layer in the IC [4]. In the case that the number of samples is not adequate, it would be safer to opt for a non-destructive approach. Moreover, to improve the time-complexity of RE, in situations where the emphasis is not on extracting all the elements in the IC, but on a certain aspect of the IC, a Region of Interest (ROI) -based approach is taken. RE, in this case, is only performed on the ROI of the IC. This significantly reduces the effort required for RE.

Because of the importance of image acquisition for RE, clear precautions should be taken for sample preparation. For instance, as shown in Figure 8, the etching process may leave some residue on the sample, or they may be dust particles on the imaging surface of the die. These should be cleaned thoroughly. Similar issues arise with milling and over-etching. Polishing must be carried to ensure a smooth sample surface for imaging. Earlier works in RE also provide cautionary reports on features from multiple layers being visible at the same time due to uneven delayering and improper mounting of the sample (see Figure 9). Delayering should be performed parallel to the die base for optimal results. For technology nodes smaller than 10 nm, difficulties in achieving

[4]Chipworks, currently TechInsights. Link: https://www.techinsights.com/

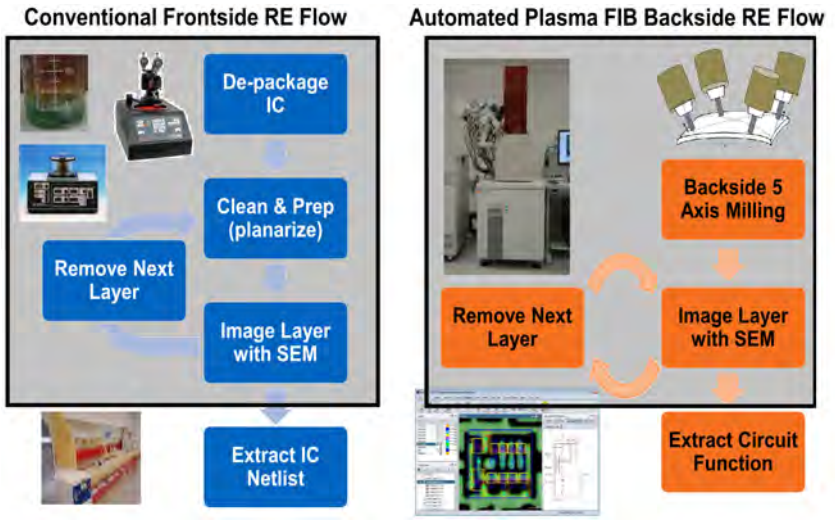


Fig. 10. Front-side vs. Back-side deprocessing workflow [149]

proper mechanical polishing and the tendency for surface damage have been reported in a case study [174].

In a typical RE process, the delayering operation is performed from the frontside of the IC. The frontside of the IC begins with the lowest metal layer in the structure. Being a well known approach, there are counter RE measures installed on ICs to prevent frontside RE [27]. Although this countermeasure can be bypassed by a skilled operator using existing delayering methods, critical damages to the IC under deprocessing could be caused [174]. An alternative to frontside RE is the backside RE. At present, there are no known countermeasures to backside RE [101]. Initially developed as an approach for live-probing an IC under test for fault analysis, backside deprocessing has also been utilized for IC RE. A complete workflow for both approaches is shown in Figure 10. Apart from the obvious advantage of safer sample deprocessing, the backside approach can also be fully automated [149]. A major drawback of backside deprocessing is the die warpage. With most of the bulk silicon substrate at the backside of the IC, deprocessing results in an increased mechanical stress on the die, causing it to warp. This phenomenon is shown in Figure 11. The sample preparation and delayering process typically take half a day to complete [47]. A detailed breakdown of the sample preparation time frame from a case study is shown in Table 1. The FIB was introduced earlier for safer deprocessing. Although it can be used for both frontside and backside deprocessing, it is predominantly used for backside deprocessing. As shown in Figure 7, in typical ICs, the frontside is packed with thick metal layers. Being a process designed for precise removal of materials, FIB editing takes a considerable amount of time to get through the thick metal layers. For backside deprocessing, the bulk of the silicon substrate can be removed using simple mechanical polishing after the thickness of the silicon substrate is identified using a cross-sectional view. The last few nanometers of the silicon substrate can be handled using FIB for precise and time-efficient deprocessing.

4.1.2 Imaging. Destructive RE is the most common approach in the RE community. Being an iterative procedure, as illustrated in Figure 4, delayering and imaging are done in an alternating fashion to acquire images of all layers in the IC. As mentioned earlier, SEM is the most common imaging modality used in RE, owing to its simplicity and ease of access. Consequently, we will

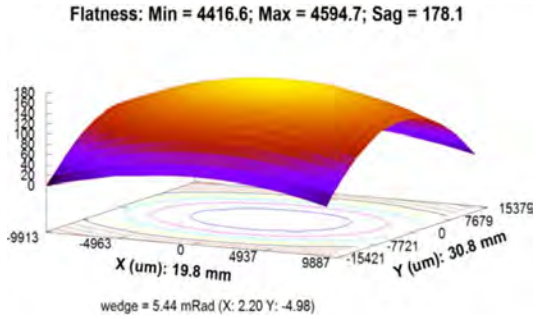


Fig. 11. Warpage in the silicon die due to the accumulation of mechanical stress. Delayering on a warped die can cause uneven delayering and pin-cushion effects [149]

Table 1. Breakdown of sample preparation on different layers for a 130nm node technology IC (Die Area: 558,000 μm^2 [100]

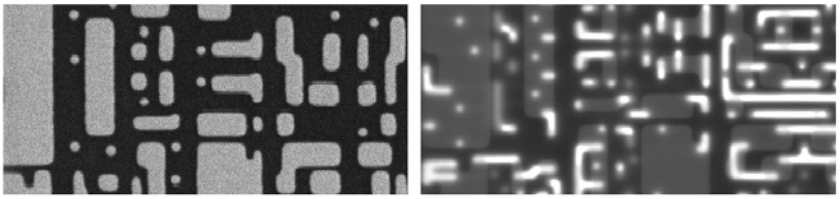
Layer Name →	Metal 2	Metal 1	Polysilicon	Active
Time (mins) →	232	199	26	42

be focusing on SEM in this tutorial. In SEM imaging, the following parameters are commonly fine-tuned depending on the features that need to be extracted:

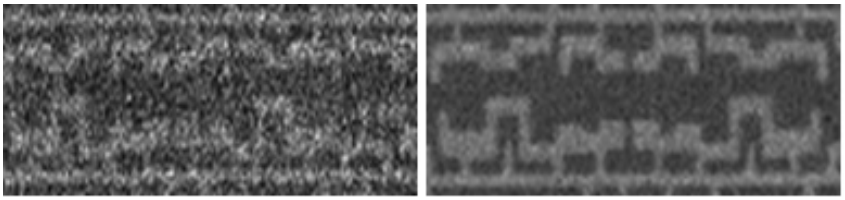
- *Excitation voltage:* The excitation voltage of the electrons controls the depth of penetration into the sample. A higher excitation voltage can show structures that are hidden below the visible surface (see Figure 12a).
- *Dwelling time:* This refers to the time that the scanning beam takes to measure the intensity value of a single pixel in the image. A longer dwelling time would give a better estimation of the true intensity of the value at the given position (see Figure 12b).
- *Field-of-View:* Commonly referred to as magnification. It refers to the size ratio between an object and its scaled projection. A high level of magnification enables us to take images of small features that cannot be seen at low magnification (see Figure 12c).
- *Resolution:* This parameter refers to the number of pixels in the image. Higher pixel count produces better images (see Figure 12d).

The time cost of taking images for a 130 nm IC is reported in Table 2 [197]. It can be observed that full-blown RE for a single layer, with high-quality image acquisition settings, takes over 30 days to complete.

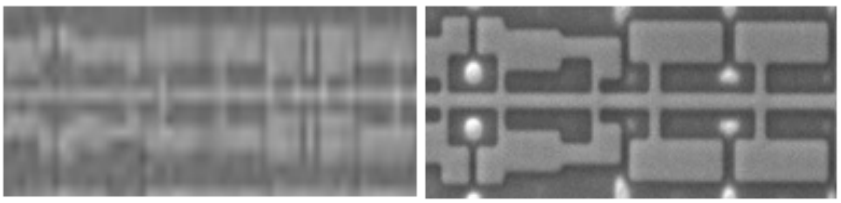
A rule of thumb in image acquisition is to use higher magnification, resolution, and dwelling time; however, these choices significantly affect imaging times. Imaging potential is typically kept low (≤5kV) to prevent interaction with underlying layers. For more control, a few more parameters can be adjusted [124]. The goal for imaging is to effectively resolve the features in the IC. For instance, in a case study, each pixel in the image corresponded to 10 nm in the actual IC [124]. If the smallest feature in the IC is smaller than the resolution capability of the SEM, the feature cannot be resolved effectively. With studies suggesting features spanning a few pixels in the image being a cause of concern for the hardware assurance community, a higher magnification is usually warranted. Approaches that can automatically, dynamically control the SEM magnification based on the smallest feature size in the current Field-of-View have been proposed to optimize the magnification selections for real-world applications [208].



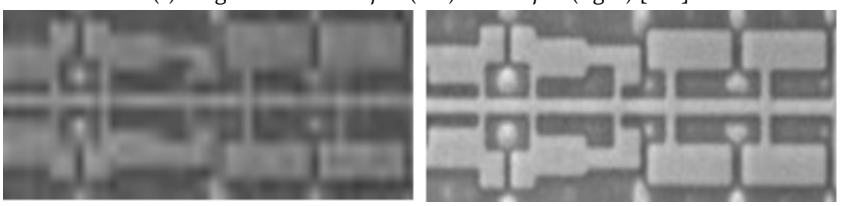
(a) Excitation voltages: the image acquired at 5 kV (left), which shows the surface-level features for the doping layer, and the image acquired at 15 kV (right) showing the same features of the doping layer along with the features of the contact/metal layers, present below the surface.



(b) Dwelling time: 3.2 μs/pixel (left) and 32 μs/pixel (right) [197].



(c) Magnification: 500 μm (left) and 20 μm (right) [197].



(d) Resolution: 512 x 512 (left) and 2048 x 2048 (right) [197].

Fig. 12. The impact of changing the imaging parameters.

There are some inherent drawbacks of utilizing electron microscopy for imaging IC structures. Some of them result from the physics behind the imaging modality, whereas other ones are inherent to the semiconductor structure and associated deprocessing. They are discussed below in detail:

- *Manufacturing process variations:* Due to the high accuracy of the imaging modality, any small variation in the manufacturing process would cause changes in the acquired image. The degree of influence of these variations depend on the precision/tolerance of the manufacturing process and the resolution of the imaging modality. These variations are utilized in hardware assurance techniques such as PUFs. Being naturally nondeterministic processes that may not necessarily be parametric, modeling these variations using statistical models is not recommended [166].
- *Topography of the material:* Areas with high roughness or edges between materials in the IC have larger escape areas for the secondary electrons [74, 170]. These cause intensity

Table 2. Time table of SEM imaging for an IC with the following characteristics: technology node: 130nm, and size: 1.5 mm x 1.5 mm [197]

Scanning Speed	Field of View Resolution	500um x 500um	20um x 20um
1 usec/pixel	512x512	9 sec	1 hr 33 min
1 usec/pixel	1024x1024	18 sec	3 hr 7 min
1 usec/pixel	2048x2048	54 sec	9 hr 22 min
10 usec/pixel	512x512	45 sec	7 hr 48 min
10 usec/pixel	1024x1024	3 min 18 sec	1 d 10 hr
10 usec/pixel	2048x2048	6 min 25 sec	5 d 12 hr
32 usec/pixel	512x512	1 min 30 sec	15 hr 0 sec
32 usec/pixel	1024x1024	6 min 30 sec	1 d 21 hr
32 usec/pixel	2048x2048	24 min 0 sec	11 d 1 hr
100 usec/pixel	512x512	4 min 48 sec	2 d 2 hr
100 usec/pixel	1024x1024	18 min 54 sec	8 d 4 hr
100 usec/pixel	2048x2048	1 hr 11 min	30 d 20 hr

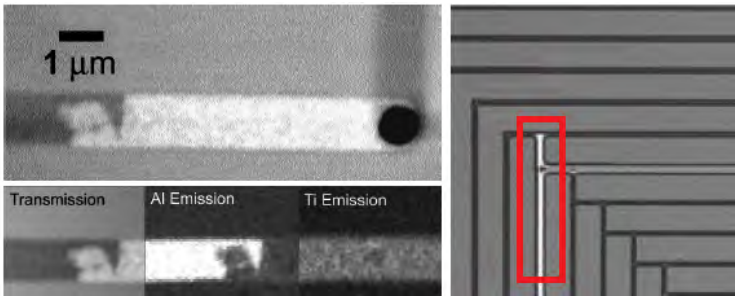


Fig. 13. Electron migration (left) due to accelerated life cycle conditions causing variations in intensities measured for the same material [57]. Charging effects (right) exhibited in insulating materials under SEM observation [82]

variations of the same material measured in different locations on the same IC die. This further emphasizes the need for polishing and planar surface on the deprocessed IC die.

- *Oxidation:* Delayering exposes the metallic structures in the IC to the atmosphere [174]. Oxidation of metallic surfaces causes fluctuations in the responses obtained for the same material at various points in the IC.
- *Electron-migration:* If the IC has been under use, there are chances of having electron migration and changes in the physical structure of the material [57]. This type of defect is usually found in metal interconnects, through which high-density currents flow (see Figure 13). This issue is predominantly studied in device failure analysis in estimating the lifetime of an IC [129].
- *Conductivity:* Insulating materials may charge positively and suppress the secondary electrons [74]. This leads to localized pockets of bright and dark regions in the image (see Figure 13). This issue can be offset by depositing thin layers of conductive materials such as carbon or platinum on the IC die surface [105, 152]. Moreover, if the material is considerably thin, the electrons can pass through so that the sensors cannot detect them [165]. It should also be noted that when using an active mode of imaging, radiation exposure over a long duration at a specific location causes a contamination layer to build up over the exposed region, preventing further emission of electrons for effective imaging [170].

Several other issues that are predominantly associated with electron microscopy are illustrated in Figure 14 as an exemplary case.

Fig. 14. Practical limitations of electron microscopy techniques. The raw image is shown on left and the middle one is corrupted with drift and vibration. Rightmost image is corrupted with all three noise sources (drift, vibration, and radiation dose). Context: Gold particles on carbon surface [39].

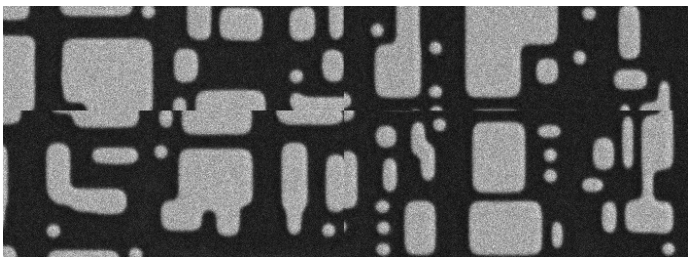


Fig. 15. Stitching error in the active layer due to improper image registration

- *Drift*: It is present in every EM modality and cannot be fully accounted for in every case. It occurs mainly due to random fluctuations in the scanning beam and mechanical creep induced by the staging platform of the SEM. Drift is more pronounced at a lower magnification that covers a larger Field-of-View [39].
- *External Environment*: Vibrations, even those that are barely perceptible, along with thermal expansions in the sample caused by slight temperature fluctuations in the environment, can significantly affect image quality [39].
- *Radiation dose*: This specific aspect of imaging is controlled by the dwelling time of the beam over a given pixel. In simple terms, longer dwelling times result in better images. With significant development in SEM imaging, especially in scan generators, it is possible to acquire significantly better images at lower dwelling times. However, there is a persisting interest in the community for low-dose imaging to reduce sample damage [64]. There have been several attempts to model the noise introduced by lower dose imaging in the microscopy community, but the influence of noise in recovering feature in semiconductor RE has not been studied in detail. Currently, there is a consensus agrees on modeling the noise as a Poisson-Gaussian process [55, 104, 145, 162, 177].

With regard to the last point, the noise from the electronic components of the SEM (e.g., amplifiers and scan generators) has been modeled as Additive White Gaussian Noise (AWGN), but its influence was found to be negligible as compared to that of emission noise [14, 192]. It has been suggested that the noise introduced by the imaging modalities can be used to hide hardware Trojans [166]. This is the motivation behind studying noise in SEM and acquiring good quality images for hardware assurance applications. The RE workflow has not been optimized for repeatability. Hence, there will always be unforeseen circumstances during the RE process that would require human interaction to resolve.

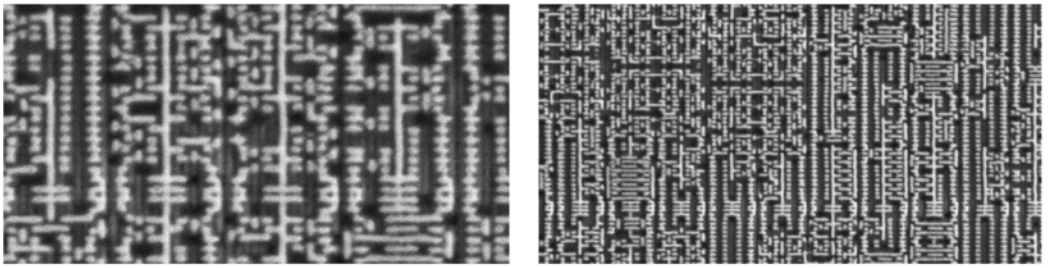


Fig. 16. SEM images acquired from a FinFET IC utilizing 14nm node technology. Field-of-View has been varied in both images to display contrast in feature sizes. Left: 5μm, Right: 15μm.

In addition to the above issue, when employing SEM, caution regarding the following problems should be used.

Stitching process: In most cases, the Field-of-View provided by SEM does not cover the entire ROI. This typically results in multiple images to be collected and stitched together to form a complete image. In typical applications, the stitching process involves taking two images with a certain overlap. The degree of overlap is decided by the operator and remains fixed for the entire image acquisition phase. Similarity measures like normalized cross-correlation [124] or features like Scale Invariant Feature Transforms (SIFT) [153] are used to find the position with the highest correlation. Then the two images are merged by blending the overlapping region or by just using one of the overlapping regions and discarding the other. Stitching is usually an error-prone process, where the error can usually be resolved by a subject-matter expert. There have been attempts at using more advanced approaches for improving stitching accuracy.

Nevertheless, stitching for contemporary nanoscale node technologies is even more challenging. Specifically, in such modern ICs, especially in metal layers, the features are very much similar and repetitive, causing significant corruption in the stitching process. Correlation analysis and Fourier domain analysis have been conducted in some studies to demonstrate this issue [207, 217]. An ingenious approach has been suggested utilizing leftover imperfections from the delayering process to stitch images with similar features [217]. These imperfections in deprocessing are usually very unique and unlike inherent features in the IC under study. This work also discusses the issues with stitching images in all directions on the same plane and the importance of optimizations for ensuring the best fit among neighboring images in the plane. An example of a stitching error is shown in Figure 15.

Alignment process: The images taken from layers are stacked on top of each other. The alignment is done using correlation matching, typically involving vertical interconnects (VIA). Design rule checks and manual operator intervention validate the vertical alignment of the image stack. There are several software suites that are available to ensure seamless alignment and viewing of images such as Chipwork's IC Browser [193], AIRE [23], Olyvia [105] and Hugin [46].

Emerging technologies: Although there is no exemplary work done for RE on contemporary technologies such as FinFET, some key insight can be obtained from challenges faced by the Fault Analysis community [143]. Some dielectric materials have low contrast with the silicon substrate making them harder to identify. A similar situation is shown in Figure 16 with the contrast between the contacts and the metal layers significantly reduced as compared to previous node technologies. This makes it considerably harder to visually analyze the image and hinders contrast-based image analysis techniques. It has also been suggested that samples sustain more damage under typical

radiation dose as compared to older node technologies. There are studies that combine simulation-based methods with SEM imaging for higher quality images at lower radiation dose. These hybrid methods are shown to be effective for recent node technologies. This further emphasizes the need for better noise models for noise-free image acquisition at lower dwelling times. Finally, there are challenges associated with deprocessing layers with very fine features. With a higher level of integration in ICs such as 3DVLSI, a full-scale RE workflow would be a daunting task without significant automation in imaging, deprocessing, and error resolution. The challenges related to performing RE on post-CMOS technology nodes are yet to be explored.

A note on the positive side of SEM: A limitation of data-driven approaches is the unavailability of good quality data, as stated earlier. To address this, the electron microscopy community introduced an SEM image simulator called ARTIMAGEN [39, 40]. However, in recent years, there have been attempts to generate synthetic data for evaluating data-driven approaches. This simulator can generate images with varying influences of drift, vibration, thermal expansion, and noise profiles (Gaussian/Poisson). However, the selection of materials, noise profiles, and shape contours are limited. The fault analysis community extensively uses simulated images for benchmarking Line Edge/Width Roughness (LER/LWR) algorithms [30]. A deep learning approach has been recently suggested to generate synthetic SEM images based on layout data for mask optimization and virtual meteorology [171]. Although the data used for these approaches are not publicly available, it does provide a path towards integrating data-driven approaches for RE in the imaging phase.

When it comes to applications of SEM in RE, there are some commercial solutions available. Notable devices include the Multi-SEM (mSEM) [95] from Zeiss for using multiple scanning beams for faster high quality image acquisition and Chipscanner 150 [124] from Raith for use in large-scale image acquisition with higher accuracy requirement on stitching. In contrast to the timing requirement shown in Table 2, Chipscanner 150 has a reported scan time of 4.9 hours for imaging at 4000x4000 resolution with a 40μm field-of-view on a 1mm^2 area [124]. In the same work, this scan time was brought down to 0.7 hours with a better scan generator. Although convenient, these systems are also significantly more expensive than regular SEMs [194]. The computational resource complexity is also an attention-worthy aspect of RE. For instance, the storage complexity associated with acquiring images of the entire active layer of a 45nm node technology IC has been estimated to be over 22 gigabytes on regular SEMs [44]. For high-performance imaging systems like the mSEM, this requirement is much higher [217].

4.2 Problems Associated with Handling PCB Images

As opposed to what has been explained for ICs in Section 4.1, the imaging process performed on PCBs does not require decapsulation. However, components mounted on the PCB can be removed for easier access to the PCB markings and easier imaging for multi-layered PCBs. The PCB equivalent of decapsulation in ICs is referred to as de-soldering, or the removal of componentes on the PCB. The byproduct of this de-soldering is varying levels of collateral damage to the PCB, depending on the efficacy of the decapsulation process. This will have different impacts on later stages of RE, such as image acquisition, where the damages are reflected in the form of debris, physical distortion, or noise artifacts present in the digital image. Therefore, it is recommended to avoid de-soldering when possible, but if necessary, it should be done with the utmost care as to limit the damage to other key features (trace tracks, via conductive rings, text markings on PCB surface, etc.).

The challenges and limitations associated with PCB RE overlap significantly with those presented earlier in IC RE scenarios. The main difference is that PCB RE has two focused aspects: external and internal RE. *External* PCB RE deals with the information that one can observe at both surfaces, the

top and bottom layers of a PCB. This information typically consists of the components of a design (passive elements, active elements, ICs, processors, etc.), their connections, silkscreen markings, and a variety of ports [151]. External RE would usually suffice if the PCB has only two layers, but this is often not the case. More common, however, are PCBs manufactured with multiple layers, where the majority of them are *internal* to the board and have structural and connectivity information not visible externally. In these cases, internal RE is necessary [151].

Traditionally, internal RE has been a destructive process [69] similar to that of IC RE. The process involves delayering and imaging of a PCB layer-by-layer until a working functional physical sample no longer exists. The imaging component of this process is typically done optically by using a digital camera or a high-quality optical microscope, but the destructive nature of the delayering process introduces multiple potential sources of the noise that could impact the quality of the image. Some examples include broken traces, disconnected vias, or poor quality images, making feature extraction much more difficult for analysis. These features need to be imaged to the highest degree of detail possible to facilitate optimal performance in the RE process, which is usually bound by the quality of the image under analysis. Fortunately, recent progress toward non-destructive RE via X-Ray CT has pushed the current state-of-the-art RE methods [6].

4.2.1 Imaging. The main challenges for each PCB RE modality can be broadly categorized into how to handle the noise associated with the imaging modality used for data acquisition.We expand on these issues for both the external and internal RE, as defined above.

External RE: The imaging modality used for data acquisition in external PCB RE is typically an optical microscope or a digital camera. Both are used to take images of a PCB at varying resolutions to enable the detection, classification, and analysis of the design information. Specifically, external RE uses these images to identify the components, connections, silkscreen markings, and different types of ports (high-speed serial/parallel, program/debug, display) present on the topside as well as bottomside of a PCB [69, 193]. Among all imaging modalities, the illumination variance is the most prominent noise source. In some cases, imaging an entire PCB board requires stitching, which results in multiple regions of the entire board with varying illuminance. This variation may cause differences in the appearance of even the same sample; therefore, drastically impacting the effectiveness of image analysis algorithms and the inspection results. Hence, a dedicated optical imaging station that provides consistent illumination across the entire imaged board is recommended. The dedicated imaging station should consist of a constant light source that is well distributed across an area. For example, a hanging lamp in combination with a high-resolution DSLR camera can be used to equip a larger station and an optical microscope station used for small to medium samples.

Depending on the magnification of the microscope or camera used for data acquisition, the image patches obtained vary in size and the amount of information included in them. While an increase in the magnification obtains more detailed features for extraction, the illumination noise is also amplified (see Figure 17), causing an information loss. For instance, using low magnification results in a larger image view, but we may lose small features (e.g., characters on resistor) due to the reflection. This could make the detection of Trojans, i.e., maliciously inserted/replaced components, more challenging. Although more features per image lead to more details, more image patches should be stitched together to complete the whole image, and thus, regions with the various illuminance are involved in the fully stitched sample.

On the contrary, when the image magnification increases to obtain more details, some large components on a PCB are separated into different patches. Moreover, since many of the existing

Fig. 17. Optically imaged PCB section highlighting illuminance non-uniformity

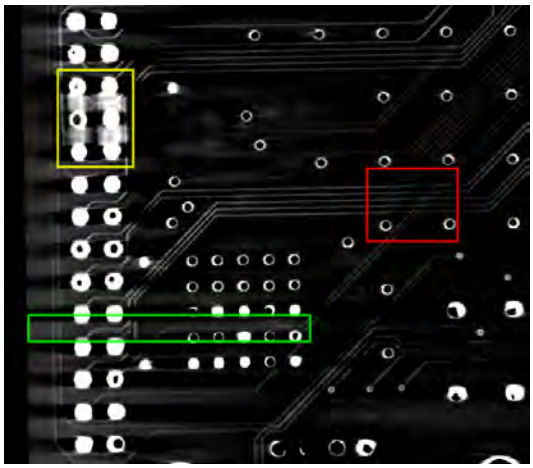


Fig. 18. Noise in X-Ray CT PCB:(red square on the right side) Neighboring Layers Aliasing (green square on the bottom left side) Blur Artifacts (yellow square on the top left side) High Impedance Material Artifacts

image analysis algorithms for segmentation, detection, and classification are heavily parameter-dependent or pixel intensity sensitive [2, 48, 91, 93, 128, 169], a holistic solution for PCB RE that is more generalizable by minimizing parameter tuning is needed.

Internal RE: If the PCB under RE has only one to two layers, the challenges encountered by the expert would be solely limited to those discussed above. However, it is more likely that modern PCBs are multilayered, where chips are connected to each other on the top, bottom, and through internal layers. Therefore, for multilayered PCBs, internal RE is required to complete the RE process. When discussing internal RE, there are two predominant methods: destructive and non-destructive RE. As explained earlier, the destructive approach is obsolete by contemporary standards and will not be considered further.

While non-destructive RE via X-Ray CT does reduce the amount of physical damage to a PCB caused by the delayering process, there are other challenges still to be faced, which impact the quality of the RE. These noise sources generated by the X-Ray process are outlined below.

- *Blur artifacts:* During the X-Ray CT process, the sample is rotated inside the X-Ray chamber by 360°at a slight tilt in the Cartesian plane to maximize the amount of information received from the X-Ray particles passing through the sample to the receiver in the chamber. This tilt, along with the rotation during the acquisition process, results in noise artifacts in the reconstructed 3D stack in the form of blurred image regions.
- *High impedance materials:* Typically, PCBs are manufactured with the majority of their parts made of silicone-based materials. However, if the PCB is populated with components, soldering is used to ensure the connectivity of the components throughout the entire board. This solder acts as a high impedance material in the presence of X-Ray particles, reducing the effectiveness of their passing-through property. Therefore, it creates noise artifacts in a populated sample or a sample with components being removed, but with remaining solder residue.
- *Aliasing between neighboring layers:* An X-Ray CT-based PCB model is a 3D stack consisting of 2D image slices. Each layer of a multi-layer PCB consists of the trace and via information that may differ from those being close to that layer. Depending on the alignment of the board in the X-ray chamber, the resolution, and the X-Ray parameters chosen, there may be slices at the fringes of neighboring layers, where the information of the layers overlaps, similar to aliasing in signal processing.
- *Beam hardening:* While an X-Ray beam passes through an object, the mean energy of the beam increases as the low energy photons are attenuated [17]. Therefore, the lower energy part of the X-ray beam is removed from its energy spectrum, and the beam is considered to become “harder". Due to this X-ray beam hardening, streaks or dark bands appear at the center of the object, compared to the edge of the object in the X-ray image. For this purpose, pre/post-filtering the X-Ray beam by using metallic materials, e.g., aluminum and copper, is applied to eliminate the low energy photons in the beam and maintain uniform average energy during the X-ray imaging.
- *Ring artifact:* In general, miscalibrated or defective detectors and elements create a bright or dark ring close to the isocenter of the scan. This can often be fixed by recalibrating the detector.

The blur caused by the X-Ray is seen as the streaks in the image (see the green square on the bottom left side of Figure 18). The bright circular regions are where the solder has impacted the X-Ray process, distorting the via features slightly, as illustrated in the yellow part on the top left side of the figure. The areas, where the trace information is intersecting each other, show aliasing that occurs between the neighboring layers (see the red square on the right side of Figure 18). While these are the main sources of the noise seen during the X-Ray process conducted on a PCB, their effects are compounded when taking the reconstruction process for X-Ray CT into account. In particular, at each slice of the reconstructed PCB, crafted by using X-Ray CT, the noise sources have a varying degree of impact since they represent the varying depths of the board and the depth of the X-Ray particles passing through the samples. Therefore, it is necessary for image analysis-related solutions to not only account for the variance seen within a single design, but also across multiple designs. Nonetheless, the impact of the noise could be reduced by adjusting parameters discussed below.

- *Tube voltage:* This parameter adjusts the peak energy of the X-Ray beam (i.e., raises the average energy of the photons). The choice of the tube voltage affects the image contrast in the scanning process. An increase in this voltage leads to a lower contrast in the images.

Table 3. Resolution limits of imaging modalities and associated processes discussed in this tutorial

Imaging Modality →	SEM	FIB	X-ray CT	Optical (DSLR)
Resolution limits →	$2nm$	$15nm$	1-2μm for ICs/ 10-50μm for PCBs/ 50-100nm for wafer-level samples	$85\mu m$

- *Tube current-exposure time product:* This refers to the number of photons produced per unit time. Random, thin, bright and dark streaks are considered as noise that may appear in the images due to the low photon counts.
- *Resolution:* The resolution of the image is defined as the pixel size selected during X-Ray image acquisition, where the pixel size can be identified as the limiting factor for spatial resolution.
- *Filtration:* Filters are used to reduce the beam hardening effects in the X-Ray beam. As the low-energy photons do not penetrate through the object, filtration improves the quality of the beam.

For the sake of comparison, Table 3 provides the resolution limits of the imaging modalities and associated processes discussed in this section.

5 ADDRESSING CHALLENGES ASSOCIATED WITH MACHINE LEARNING AND IMAGE ANALYSIS FOR RE

In the context of natural scenes, image processing plays the role of enhancing the image to the point of being discernible and pleasing to the viewer. The fine-tuning of different image parameters, such as the contrast and intensity, is considered as an art rather than an application of a set of predefined algorithms. However, with the advent of machine learning and the higher likelihood of the image being delivered to a computer than a human, the adjustment of the imaging parameters must be performed regarding the application for a particular domain and nature of the problem being addressed. For instance, a camera placed on an assembly line in a manufacturing facility might only require to examine the presence of an object rather than its color or shape. Modifying the image to be visually pleasing is neither required nor recommended in this case.

Optimizing images for a certain purpose requires in-depth knowledge of the domain and application, posing a significant challenge to the application of image processing in electronics, e.g., images taken from ICs or PCBs. It is reasonable to say that almost any data-driven approach, especially machine learning and image analysis, has its performance limited to the quality of the data provided to it. For instance, in the case of IC RE, the importance should be placed on electrical connectivity rather than visual quality. Assessing data quality using existing measures such as Signal-to-Noise (SNR) ratio does not provide insight into the true quality of the sample. Hence, invalidating the insight obtained using such samples.

Along with the extensive application of image processing in natural scene-related scenarios, the factors affecting the quality of images, such as motion blur, sensor noise, and uneven lighting, are well known and studied. This in-depth understanding enables the development of image processing algorithms that can suppress the effect of noise sources, as mentioned above, and produce high-quality images. However, this does not hold true for imaging modalities used for acquiring images of ICs and/or PCBs. Hence, the wealth of knowledge compiled over time in the field of image processing cannot be effectively utilized for RE and hardware assurance.

Moreover, in typical natural scene images, the amount of information extracted is rarely dependent on the value of a few pixels, but on the entire image or a large section of the image. On the other hand, by increasing the level of integration that puts together a higher number of transistors into a limited space, the size of the features in an IC image usually expands to only a few pixels (see Figure 19 (a, b)). An analogous task for PCB RE is detecting vias and traces in a densely populated

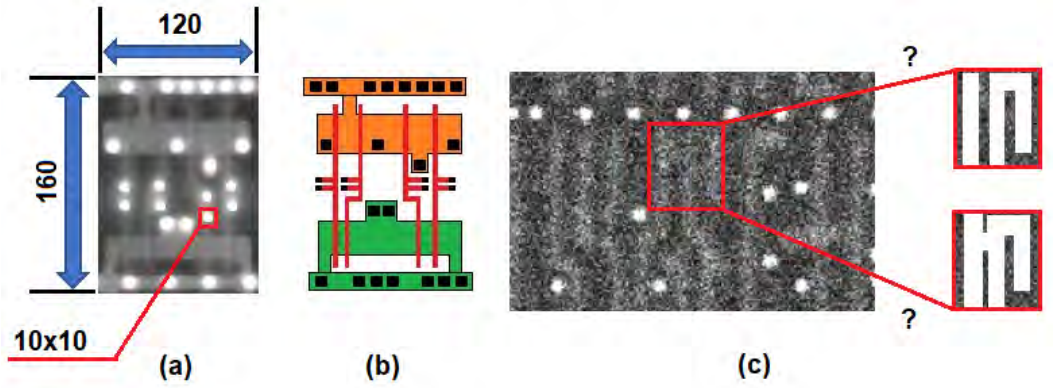


Fig. 19. Difficulties with the handling of IC images: (a) an SEM image of a logic cell showing the size of features in pixels, (b) the software-based structure of the cell shown in (a), and (c) an example illustrating the ambiguity in the feature resolution in the presence of the noise.

image where these features and structures can be only a few pixels long or wide. Hence, depending on the intensity of noise affecting such features, there are situations, where a structure containing a few pixels cannot be categorized into a feature or a noise artifact (see Figure 19 (c)). In the context of hardware assurance, this ambiguity may result in miss classification of a Trojan. Similarly, PCB images used for RE are subject to this challenge, albeit in a different way, due to the different modalities the images are taken from. For instance, optical imaging can easily fail to detect an extra component acting as a Trojan, when the color of the motherboard and the components on it are both black. Furthermore, via detection through X-Ray CT imaging may not be helpful when vias are blurred by the presence of high impedance materials that attenuate X-rays.

Challenges that can be resolved through machine learning have three factors in common: a coarse understanding of the problem, the availability of high quality labeled/unlabeled data, and understanding of the statistical features that can assist in quantifying/representing the problem. With hardware designers and manufacturers having design experiences that are specific to them, it could be hard to find features that can be generalized to all cases. Even in approaches that support automated feature discovery, such as artificial neural networks, a significant amount of labeled data is required. In many instances, obtaining such ground truth is either not possible (obsolescence) or impractical (pixel-level labeling for semantic segmentation) due to the time and resources required. With issues compounding on every basic step of the machine learning paradigm, a holistic approach that can effectively cover all RE workflow stages is extremely challenging.

The inherent complexity of using ML for RE can be demonstrated with a simple example. The steps involved in designing an IC usually start with a high-level description of all the modules. These modules are synthesized with standard cell libraries from IC manufacturers. The design is then placed, routed, and etched onto a silicon wafer die [59]. In machine learning terminology, this whole process is akin to performing a dimensionality reduction technique, such as Principal Component Analysis (PCA), on the raw data. More specifically, although the processed low dimensional data behaves in the same fashion as the raw data and can be considered equivalent, recovery of the original data from a low dimensional projected version is hard.

The goal of most RE applications is broadly classified into three types: recovery of schematics, obtain insights into the design, and to detect anomalies in the design for hardware assurance purposes. In order to satisfy these goals, the constraints on applying data-driven methods will have

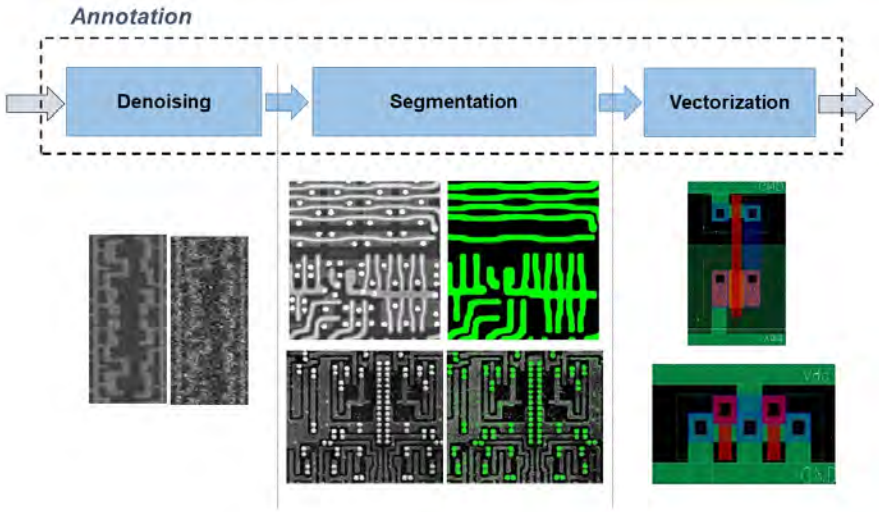


Fig. 20. Expanded workflow for the Annotation block

to be relaxed and explored within individual modules in the RE workflow, where the strengths of image processing and machine learning can be effectively utilized. In the following sections, we will explore various approaches that can get the reader as close to the original design data as possible.

5.1 Problems Associated with Applying ML for IC RE

The applications of ML algorithms in IC RE mainly include two types of methods employed to perform annotation and extract the netlist[5], described in this section.

5.1.1 Annotation. The annotation module expects image data from the previous step to be noise-free, free of deprocessing errors, well stitched, and aligned in all layers. However, in most cases, these are not fully satisfied. The annotation module can be divided into three sub-modules: denoising, segmentation, and vectorization. An overview of the annotation block can be seen in Figure 20.

Prior to denoising the image, it is necessary to ensure that the image contents are not corrupted from deprocessing and stitching errors. Currently, there are no approaches to detect corrupted images. However, some insights can be obtained by looking into the forward manufacturing workflow. For instance, stitching errors may be corrected using design rule checks. Deprocessing errors are similar to faults in the IC die. There are quality control and design validation approaches that utilize image processing and pattern recognition to detect such faults. These approaches can be re-purposed for detecting deprocessing errors in the RE workflow [137, 203].

Denoising: The denoising sub-module is responsible for ensuring that the noise component in the image is suppressed. There are several approaches currently employed in literature for processing noisy SEM images. They include spatial filtering approaches, including Gaussian, median, curvature, anisotropic diffusion, wavelet, adaptive wiener filter, and hysteresis smoothing [5, 130, 132, 195]. Simple high-frequency filtering and deep learning-based denoising approaches have also been used on SEM images [64]. These techniques are mostly naive image processing techniques and do not take the semantics of structures in the image into account. Machine learning-based denoising

[5]A netlist is a graph that shows relationships between various components.

Table 4. Denoising algorithms used on SEM images. Values in Denoised Image are improvement (in %) over original raw SEM images for that specific quality metric. Algorithms tested on IC SEM images are marked as either Yes(Y) or No (N) in the IC column. All references use different testing data.

Algorithm	Raw Image		Denoised Image		IC
	SNR	SSIM	SNR	SSIM	
Adaptive Weiner [132]	-	0.624	-	18.5	N
NLM [132]	-	0.624	-	7.2	N
Hysterisis [132]	-	0.624	-	24.2	N
Wavelet [30]	9.96	-	58.6	-	Y
BM3D [110]	10.00*	-	95.4	-	N
K-SVD [110]	10.00*	-	108.4	-	N
GOAL [194]	25.57	0.73	6.5	22.3	N
Super Resolution [194]	25.57	0.73	-0.01	12.12	N
Image Inpainting [194]	25.57	0.73	22.6	21.9	N
DLNN (SEMNet) [30]	9.96	-	164.6	-	Y

Table 5. Segmentation algorithms utilized for segmenting IC SEM images. Papers reporting multiple accuracy values is marked with a range operator (⟶)

Algorithm	Accuracy (in %)
Graph-Cuts [49]	91.00
Morphology and Semantics [51]	90.00
Watershed [113]	94⟶98
Hybrid K-Means and SVM [35]	95.83
Hierarchical Multiclassifier System [34]	91.45
Fuzzy C-means [35]	26.72
K-means [35]	26.72
Recursive Multilevel Thresholding [35]	35.25
Global Template Projection and Matching [36]	88.54
LASRE [210]	86⟶99
Deep Neural Network [82]	98.00

approaches, such as image inpainting, super-resolution and dictionary-based sparse reconstruction, have also been explored for SEM images [30, 110, 114, 194]. An extended list of all denoising approaches is presented in Table 4. Simple measures like SNR and Structural Similarity Index Measure (SSIM) or noise variance can be used to evaluate SEM image quality [92, 175, 176, 190].

Segmentation: This step involves the separation of structures in the IC image based on some qualifying fact. In SEM images, this would be the material represented by grayscale pixel intensity. Segmentation algorithms can be supervised, unsupervised or interactive. Supervised segmentation approaches, such as the Convolutional Neural Network (CNN) based deep learning approaches require massive amounts of manually ground-truthed image data [35, 82]. This massive undertaking requires considerable time and resources. It is hard to replicate with the dataset being private and may not generalize to other ICs. The unsupervised approaches are based on generalizable features that can be found in the same IC or across ICs. For instance, the technique developed by [34–36] relies on the fact that polysilicon structures and metal layer traces can be generated by simple Manhattan geometry contours. Interactive approaches require the operator to guide the segmentation [49]. Another technique relies on using frequency-based texture signatures for different materials to segment out IC structure across multiple layers [210]. Simple image processing techniques have also been explored for segmenting SEM images [51, 108, 113, 209]. Segmentation accuracy is measured in pixel accuracy, F-measure, and Intersection-over-Union (IoU). However, there are no metrics that specifically look for accuracy in electrical connectivity. A list of segmentation approaches and their reported accuracy is summarized in Table 5.

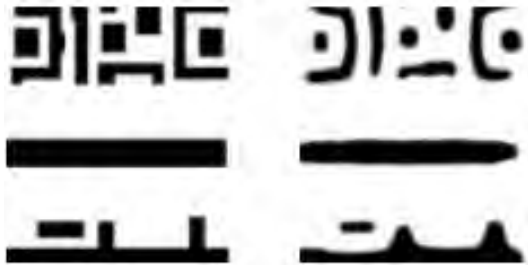


Fig. 21. Edge distortion caused by limitations in the mask generation process in transition from the GDSII layout (left) to the silicon wafer (right) [171]

Vectorization: Finally, the vectorization stage converts the image into a bunch of polygons. The idea behind this module is to recover design files as close to the original die layout as possible. This specific step enables the use of commercial off-the-shelf tools allowing smoother transition between the annotation and the netlist extraction modules. This step further serves in suppressing edge noise between materials (discussed in detail with EWR/LWR for FA [43, 134, 146]) and compressing the amount of data in the image. Vectorization has been achieved through simple edge following algorithms, supervised learning via XGBoost, and even deep learning [16, 152]. It should be noted that edges in the original layout are converted to simple curves in the SEM images (see Figure 21). This is due to the mask generation process done for etching the IC onto the wafer during manufacturing and not an artifact introduced by the imaging modality or any sample preparation step [123].

The annotation block is critical to several hardware assurance measures. Being in the middle of the RE workflow, the amount of errors accumulated at this stage is far lower than further down the line. Several approaches use segmented images of the IC layers for detecting Trojans. [10, 11] and [139] detect metal layer Trojans using classifiers trained on synthesized images. The former two works hand-craft shape features, while the latter one extract histogram of oriented gradients (HOG) features to represent discriminatory characteristics of gates. [196] and [172] apply the Fourier shape descriptor to detect modifications on cells' appearance from SEM images of the IC's active layer. The classifier training in [196] is conducted on a pre-collected IC SEM image dataset, and the training in [172] is on SEM images of on-chip electrically authenticated gates.

Other approaches utilize SEM images of the golden IC or layout and simple correlation analysis or template matching to make sure that the sample is Trojan free [45, 197]. Additionally, some approaches for avoiding Trojan insertion watermark the active layer with highly reflective filler cells. Their combined reflectance signature can be used to make sure that the IC is Trojan-free [221]. A similar approach uses thermal maps and deep learning to detect Trojans [206]. Being segmented, hardware assurance measures performed at this stage can also be free of the influence of localized variation in pixel intensity and noise, which has been demonstrated in the above works. It should also be noted that variants in Trojans, such as the parametric Trojans, can only be detected at this stage in RE. The only disadvantage at this stage is the overhead in storing and processing full-scale images.

5.1.2 Netlist Extraction. This stage involves the transition from the recovered layout into a netlist. As illustrated in Figure 22, this representation can be obtained at various levels of abstraction: transistor, gate and behavior-levels. This stage has the likelihood of having the most errors in the entire RE workflow. In contrast to popular belief, netlist extraction and debugging take more time and manual operator interaction than imaging and annotation modules. With present node

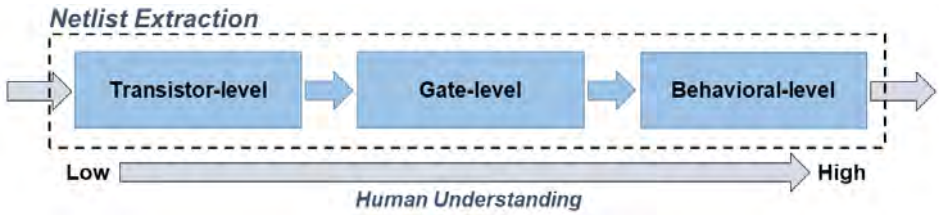


Fig. 22. Expanded workflow for the netlist block. Operator understandability and intrepretability of the RE netlist increases from transistor-level towards behavioural-level netlist

technologies integrating several billion transistors in an IC die, it is reasonable to assume that there a billion opportunities to make mistakes. This is the underlying reason behind the existence of several hardware assurance approaches at the annotation module. However, in order to ensure that the hardware is completely Trojan free (like small scale Trojans with highly unique activation sequences) and to pave a path towards re-engineering obsolescent ICs, this stage is essential. In addition, there are several counter-RE approaches implemented at this stage, making error-free RE a daunting task. On a side note, it should be understood that RE is almost always performed on digital elements in the circuit. Large analog elements are extracted manually by the operator and decoded by an SME.

Transistor-level netlist can be generated for both digital and analog circuits. But it is predominantly done in analog circuits. The majority of the exemplary work in digital IC RE skips straight to the gate-level netlist. The transistor-level netlist is obtained either by simple image processing techniques like template matching and manual operation interaction. A transistor is detected at the overlap of diffusion and polysilicon layers in the CMOS technology [22]. The width for the n-type CMOS gate is assumed to be smaller than the p-type CMOS gate [123].

Gate-level netlists operate by combining several transistors into logic gates. In most cases, the standard cell library that defines the gates are not available. Hence, with the help of Subject Matter Experts (SME), the operator has to manually identify each cell and use image-based correlation to generate a standard cell library [100, 141, 153]. Custom feature descriptors are also explored for improving cell template localization in large scale images [52]. This is a time-consuming process. Recently, an approach has been introduced that uses information from the contact layer to identify the standard cell library automatically [207]. However, this approach assumes that no obfuscation has been performed on the cells. The amount of prior information at this stage significantly help speed up the RE process. For instance, if the standard cell library is known beforehand, the process of netlist recovery would be easier. For entities that have access to the golden netlist, a simple comparison can assure that the device under test is Trojan free. The validation of both the extracted transistor and gate-level netlist is done through simulations and design rules checks. Electronic Design Automation (EDA) tool suites, such as those provided by Cadence, are used to perform these checks [152]. A sample time frame for netlist extraction reported in a case study is shown in Table 6.

A *behavioral-level* netlist is generated to understand the functionality of the circuit itself. This facilitates obtaining insights on the design, especially for competitive intelligence and IP protection. Module functionality and boundaries are recovered at this step. Another one of the core reasons for RE, the recovery of schematics, is performed at this stage. For obsolescent ICs, the RTL description can be extracted from the gate-level netlist and synthesized into contemporary node technology, which can be manufactured in a fab with or without changes to the existing design. An exemplary work has been performed for this specific purpose [100]. However, an in-house tool has been used

Table 6. Breakdown of logic gate placement and debugging netlist time frame (in minutes) for a 130nm node technology IC (Die Area: 558,000 μm^2) [100]. Debug time takes a significant portion of the time frame for the netlist extraction process. Netlist verification and validation processing times vary from 30-206 minutes in these cases

Mode	Manual	Automatic	Comment
Placement	168	0.8	Design Data Available
Debug	106	0	Design Data Available
Placement	59	-	Design Data Not Available
Debug	39	-	Design Data Not Available

for extracting RTL description from the gate-level netlist. Bao et al. list three different entities interested in RE: circuit designers, foundries, and IP vendors [13]. Another entity that may have an interest in RE is an external party. Design files, being privileged information, are not available to all entities. The spectrum of information goes on a monotonically decreasing scale from the circuit designers having access to the most information to the external party having at most access to the datasheet of the IC.

As a reflection of this fact, there is a sea of methods for handling information at the behavioral netlist-level. In situations where the netlist needs to be verified, simple and scalable graph isomorphism based approaches identify sub-circuits in the flattened gate-level netlist to generate higher-level functional/behavioral modules [29, 37, 38, 118, 120, 161, 182, 188, 212]. Stochastic algorithms assume that structural similarity implies functional similarity and exploit this principle for extracting sub-circuit when the exact definition of the sub-circuit is not available [8, 9, 59, 173, 219, 220]. Probabilistic and fuzzy approaches are essential for error-tolerant matching/analysis in corrupted or obfuscated netlists. Machine learning approaches such as genetic algorithm and embedding space-based approaches have also been investigated [26, 199]. There are some outlier detection methods that work on providing further insight into the functionality of the IC. Recovering state machine from the Input/Output pins by brute-forcing is one such approach [179]. Recently, pioneering work has been done for the adoption of deep learning methods like graph convolution neural networks, for behavioral analysis on transistor-level netlists [106].

Countermeasures against netlist extraction: There are several obfuscation methods available for securing netlist-level information. Some techniques rely on layout-level camouflage, making the layout hard to decipher visually. Some approaches rely on gate-level camouflage, making functionally distinct logic gates look very similar under visual observation [41, 157]. Since a lot of optimizations are employed in the stages between IC design and manufacturing, some approaches rely on overriding these optimization to generate functionally identical logic gates with very different physical/layout realizations [67, 68]. It should be noted that deobfuscation approaches have also been proposed against these measures [53]. However, they do hinder the RE workflow in a significant way. For instance, with SME manually evaluating and extracting logic gates for generating standard cell libraries, a camouflaged gate may be accidentally missed or miss-classified. Arguments related to such human factor errors have been discussed in earlier works [60].

Some other approaches for hardware assurance are also performed at this level. These include logic locking and split manufacturing [70]. Since they do not directly influence the RE process, these approaches are considered to be out of scope for this tutorial. Various studies that look into these approaches in detail, see, e.g., [103, 184]. Trojan detection methods utilize the gate-level netlist to look for anomalies. As indicated in Figure 2, Trojan detection can be performed with or without the golden data. Direct comparison of netlists, both transistor and gate-level, is resource-hungry. This motivated the development of Trojan net features. These features can be extracted from the golden netlist, and Trojan detection performed using several classifiers. Random forests, artificial neural

Table 7. Performance of Trojan Detection Works

Detection	Work	Golden data	Performance[1]				
			Accuracy	FPR	FNR	TPR	TNR
Image-based	[10, 11]	Golden layout	99.9%	-	-	-	-
	[139]	Golden layout	89.0%	7.7%	-	-	-
	[221]	Golden layout	-	0.5%	1.2%	-	-
	[206]	Golden layout	98.2%	-	-	-	-
	[172]	Golden layout	100%	-	-	-	-
	[196]	Golden IC	98.0%	2.0%	-	-	-
	[45, 197]	Golden IC	100% visually	-	-	-	-
Netlist-based	[75]	Golden netlist	-	-	-	96.8%	66.3%
	[76]	Golden netlist	-	-	-	85.0%	70.0%
	[77]	Golden netlist	-	-	-	70.3%	99.7%
	[33]	Golden netlist	99.8%	-	-	89.8%	99.9%
	[25]	Not required	97.5%	-	70.3%	-	-
	[163]	Not required	-	0%	0%	-	-

[1] Table presents the averaged reported performance or the best averaged performance if multiple averaged performance are available. FPR: False Positive Rate, FNR: False Negative Rate, TPR: True Positive Rate, TNR: True Negative Rate.

Table 8. Commercial and open-source tools available for RE related tasks

Name	Purpose
ARES [189]	Segmented image to GDSII layout
PIX2net[6]	Annotation
Degate [198]	Gate recognition and annotation
GDS-X [152]	Segmentation-to-polygon conversion
CircuitFinder [98]	Annotation
ICWorks [202]	Gate netlist extraction
HAL [201]	Gate netlist manipulation

networks, and SVMs have been explored in this context [33, 75–77]. When direct access to golden netlists is not available, unsupervised cluster analyses detect Trojan infected circuits as outliers [25, 163]. Another approach using test patterns generated by Automated Test Pattern Generation (ATPG) tools has also been suggested [166]. Since non-invasive Trojan detection methods is out of scope of this tutorial, interested readers are directed to other detailed surveys on the topic [54, 117, 121]. Table 7 lists hardware assurance approaches on both the annotation and netlist extraction modules.

Available tools: Unlike the imaging and annotation modules, the netlist extraction module is well-studied in the literature. There are several benchmark datasets available such as ISCAS [73], TrustHub [164], Synopsis Academic Datasets [65, 66], OpenCores [142], IWLS [4], OSU35 [144] and FreePDK [56] that help generate sample data for hardware assurance applications such as Trojan detection.

In recent years, several tools have been introduced that can significantly reduce the workload associated with RE. A list of these tools can be found in Table 8. One of the three main reasons for performing RE is achieved at this level of abstraction: detection of anomalies in the design for hardware assurance purposes. Hardware assurance approaches for post-CMOS technologies are out of scope of this tutorial. Interested readers are directed to recent work by Knechtel for more details [102].

5.2 Problems Associated with Applying ML for PCB RE

Here, similar to our discussion on how ML can be useful for IC RE, annotation, and netlist extraction techniques carried out in the context of PCB RE are explained.

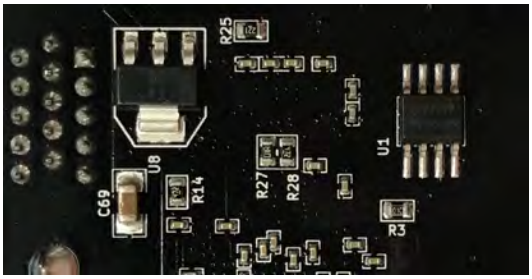


Fig. 23. An example of extracting the same color PCB component from the PCB board.

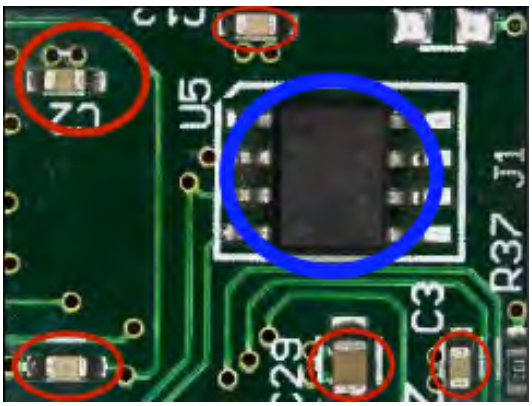


Fig. 24. Optically imaged PCB segment highlighting components: Capacitors (Red) and IC (Blue)

5.2.1 Annotation. Machine learning combined with image analysis has proven invaluable for quality control and hardware assurance in the PCB manufacturing industry, enabling automated defect detection and visual inspection to a certain degree [15, 31, 32, 32, 61, 78, 83, 84, 94, 99, 107, 115, 135, 159, 167, 191, 204, 214, 222]. Several studies have applied image subtraction to compare a golden, reference image of a PCB design or schematic to PCBs under quality check [31, 32, 94, 115, 191]. Other more complex approaches for defect detection in PCBs involve modeling-based methods, such as evaluating the roundness of drilled vias [204] or using multi-marked point processes for solder paste defect detection [15].

The first phase of the annotation for PCB deals with identifying whether the PCB is imaged optically or via X-Ray CT and whether external RE or internal RE should be considered, respectively. Clearly, the denoising required for each of these modalities is different as the noise sources vary from one to another. For external RE, this step includes generating the design's BoM by extracting the components, vias, traces, silkscreen annotations, etc. Internal PCB RE mainly concerns extracting the internal routings and connections of traces and vias, with the main difference being the noise involved. The final step for both external and internal RE infers the purpose and functionality of the circuit, sub-circuit, or system.

External RE: When applying external RE, the desired features to be annotated are the components, text, logo markings, vias, traces, etc. From an image analysis perspective, the extraction of such features falls within the scope of object detection, classification, and identification. Existing

algorithms for achieving these goals are well-developed for natural scene images [158, 200]. Nevertheless, adapting these algorithms for external PCB RE-related applications remains challenging. The components on the surface of a PCB vary in size and color depending on their functionality and packaging. This could challenge the annotation process. First, the lighting conditions and color of PCB surfaces may impact the extraction performance. Traditional image analysis methods convert an RGB image to another color map to address the lighting variance [112, 183]; however, this cannot prevent shadowing on PCB surface due to the existence of tall components, which may result in an error of using color-based segmentation methods. Moreover, the complications when the color of a PCB's surface is similar to the color of components has not been addressed completely (see Figure 23 where the colors of the surface of the PCB and components are all black). Besides, in an optically imaged PCB, text markings, traces, and vias are packed tightly compared to the objects in a natural scene image. This increased image complexity challenges feature localization, especially in a densely populated design. In addition, with the advances in technology, the size and shape of components become smaller, and their placements/orientations in the design are decided by the designer. Therefore, neither specific rules nor the encoding that hold from one design to another across even one generation can be defined.

While the above challenges should be addressed, there is a plethora of side information on the board itself that can be leveraged to make the annotation task easier. The on-board text marking near a component represents the type of components (see Figure 24 where C2/C3/C29 are capacitors and U5 is an IC). Those markings can be used as ground truth, which provide machine learning classifiers with either the labels or additional features during classification. Although there are substantial applications for these markings, extracting them is particularly challenging. The Optical Character Recognition (OCR) is the most widely used tool for text recognition [180], but its performance is not stable in the case of PCB inspection. The markings are etched or printed on PCB boards using a variety of materials and colors, and they vary in orientation, which degrades the performance of the OCR engine [62, 119]. This stresses the importance of having a robust text recognition system for external PCB RE applications. [62] looked further into these data collection issues by investigating which features of components or board text-markings can form a coreset (small weighted summaries of a larger set of data) to more efficiently and effectively train deep learning text-extraction models. Using data gathered from real-world PCB production sites, they developed a series of coresets with varying combinations of illumination variance or shape orientation and evaluated their effectiveness on training the standard ResNet [80] deep neural network model. With a top reported accuracy of 94.67% from experiments, they then determined that the most important features for accurate text-extraction were the shape and orientation of the characters.

In addition to the above-mentioned markings, information can be derived from the traces and vias on the board. The extraction and localization of traces and vias are critical because they determine the functionality and the performance of the board, which allow the validation of the system's integrity. Existing research on the detection of traces and vias has mainly focused on finding defects and usually uses the bare board to illustrate the problem [50, 185]; however, the proposed approaches are not robust in practice when traces and vias are overlapping with components.

Internal RE: For internal PCB RE, the important design information is the vias and traces on a board and the layers throughout the board. The vias establish connectivity between the layers and are consistent from one layer to another, except in a rare case of a blind/buried vias in a space-constrained design. These blind vias are unique only to their respective layers as opposed to being at the same location throughout [133]. Traces provide the main discriminatory information for each layer and determine the connectivity of the vias throughout the board. As stated previously, the noise affects the X-Ray image quality, which particularly impacts feature extraction for annotation,

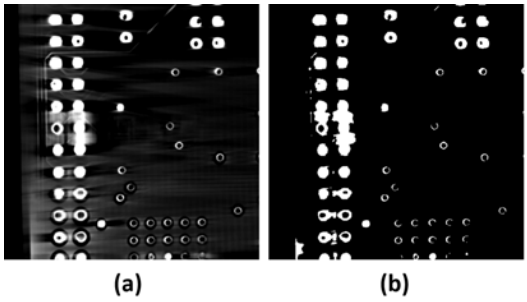


Fig. 25. X-ray CT PCB: (a) Raw Image (b) Post Segmentation

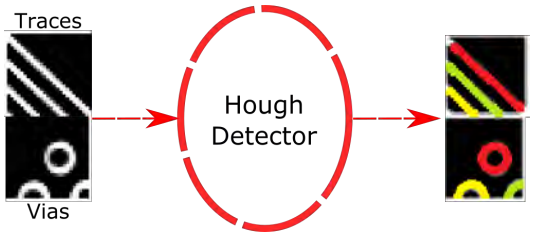


Fig. 26. X-Ray CT trace and VIA detection using Hough line/circle detectors.

when the traces and vias in internal PCB RE can be significantly altered due to the blur and high-z material noise artifacts. For example, vias in the raw image can be linked (see Figure 25 (a)) or their shape can be noticeably distorted (see Figure 25 (b)). The distortion may degrade the performance of the feature localization and identification. Vias and traces within a PCB are mainly circles and lines (see Figure 26). The predominant class of algorithms for detecting these geometries, line/circle detection using model-fitting methods, is quite sensitive to the parameters and pixel intensities. Thus, it likely would require manual tuning from one sample to another to minimize the number of missing or falsely detected objects. This is neither practical nor ideal for automated PCB RE, where it should be noise-tolerant, generalizable, and scalable for multiple technologies and designs.

The topic of automated via detection has been explored recently by [20, 125] with both leveraging the popular Hough circle transform [91] for detecting vias' circular shapes in X-ray CT images. [20] in particular combined Hough circle detection with an unsupervised iterative learning approach and PCB design domain knowledge to address the challenges seen from noise and design variance. Due to the known shortcomings of Hough circle detection, namely sensitivty to noise and propensity for false positives(See Figure 27), they utilize a series of stages to iteratively screen out false positives and learn the properties of true positive vias unique to each board at the same time. To further emphasize the need for robust approaches that can learn online in an unsupervised fashion, the authors compare their results to the current state of the art for deep learning-based object detection, Mask R-CNN [79].

Mask R-CNN(M.R-CNN) detects objects in an image while simultaneously generating a high-quality localized segmentation mask for each instance. The implementation of Mask R-CNN used in [20] has been pre-trained on the MS COCO Dataset [122], and the pre-trained weights have been used to train a variation of the network to locate and identify vias. Table 9 clearly highlights how the authors' proposed automated via detection framework vastly outperformed training and implementing Mask R-CNN for the same tasks based on commonly-used image segmentation

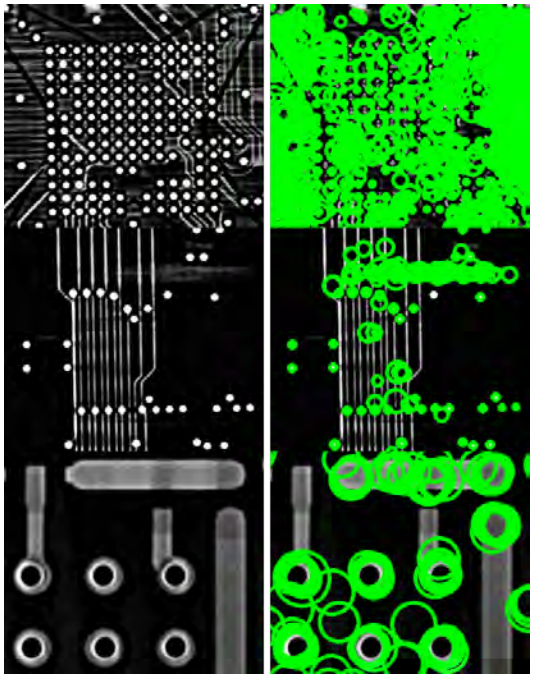


Fig. 27. Hough circle detection false positives for x-ray CT imaged board samples

Table 9. Automated Via Detection Segmentation Mask Evaluation Results: [20] Proposed Methodology Vs. Mask R-CNN (T.B. = Test Board, S3 = Spartan 3)

Automated Via Detection Segmentation Mask Evaluation						
Board	Average IoU		Average DICE		Average SSIM	
	[20]	M.R-CNN	[20]	M.R-CNN	[20]	M.R-CNN
T.B.	.877	.564	.930	.617	.973	.638
S3	.730	.511	.820	.567	.949	.847

metrics. The authors attribute this vast difference in performance to their proposed framework's ability to adapt online to novel data as opposed to being reliant upon trained data, a known hindrance to deep learning methods. Figure 28 presents the results of the automated via detection with predicted vias in green and the ground truth highlighted in red in the same image.

Trace detection in X-ray CT images has also drawn recent research interest [150]. Qiao et al. used a combination of deep convolutional neural networks (DCNN) with graph-cut models to semantically segment trace wires in a variety of X-ray CT imaging environments. The authors adopt a transfer learning approach to train their network due to traditional DCNN training requiring exorbitant and time-consuming manual pixel-level labeling of ground truth. They first trained their model for classification between the categories of trace, via, pad, and background followed by shifting the focus of the trained network from classification to semantic pixel-level segmentation after a series of architectural changes further outlined in [150]. They then use the DCNN segmented result as a probability prior for their graph cuts model that further refines the result in combination with low-level feature information from the original image. The authors compare their approach against two traditional segmentation methods (level set [213] and superpixel [90]) as well as variants of their trained network with and without graph cut refinement.

Fig. 28. Automated Via Detection Results Test Board: [20] Proposed Methodology (Top) Vs. Mask R-CNN (Bottom)

Evaluation of the method is performed based on segmentation metrics pixel accuracy(PA) and IoU, as well as classification metrics recall, precision, and F1-Score(See Table 10). The level set and superpixel-based methods both performed the worst because these methods perform segmentation based on color information or local texture and do not have the same powerful recognition ability as DCNN-based methods. However, the results of the trained DCNN methods are still coarse, with errors leaving room for improvement. These results both emphasize the need for more sophisticated segmentation methods and less training data reliant approaches due to the impracticality of requiring such extensive manual labeling, as mentioned earlier.

In addition to the challenges mentioned above, improper alignment causes another difficulty that affects the feature extraction in both external and internal PCB RE cases. Due to the trade-off

Table 10. Trace wire segmentation performance comparison [150]

Trace Detection Performance Comparison					
Method	PA	IoU	Recall	Precision	F1-Score
Levelset [213]	.8246	.5743	.4585	.3123	.3715
Superpixel [90]	.8074	.6534	.4792	.6064	.5353
DCNN-GC [150]	.9002	.8463	.8629	.8655	.8642

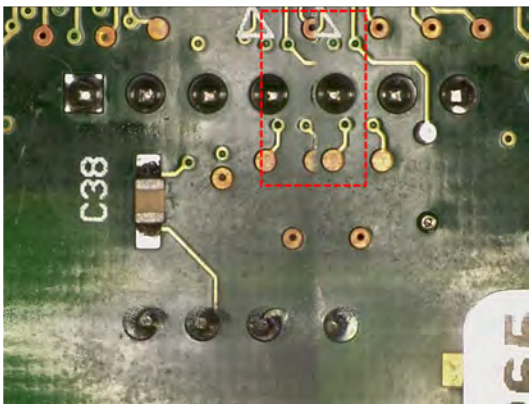


Fig. 29. Misaligned external PCB image

Fig. 30. Misaligned Xilinx Spartan board X-Ray CT slice

between details included in the features and the size of the features in external PCB imaging, some components cannot be captured completely in a single image, and thus we require aligned (stitched) images to extract the features. Although this matter has been dealt with by using the Charge-Coupled Device (CCD) camera and SEM imaging [24, 126], the lighting condition and the number of assembled components can still lead to the stitching errors (see Figure 29) in external PCB images. The same issue happens in the internal PCB RE. The aliasing effect in the slices that make up the 3D board sample (see Figure 18) is a byproduct of misalignment. This leads eventually

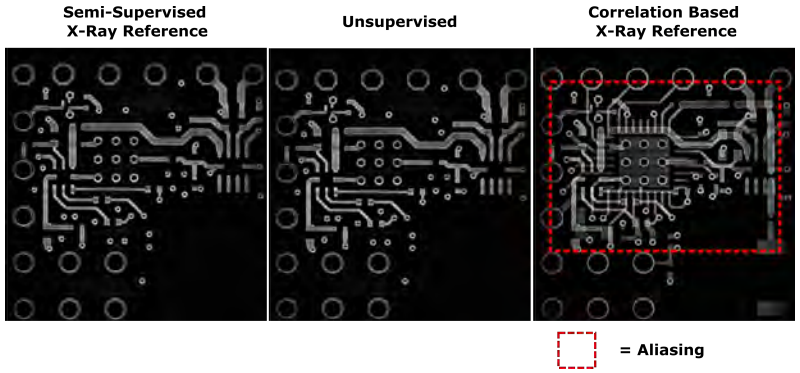


Fig. 31. Layer Identification Results [19]

to having the layers containing various amounts of feature information that may associate with a single layer or an adjacent one. Additionally, misalignment can also lead to another issue – missing information (see Figure 30 where red dashed regions show areas of missing information). Therefore, it is important to not only be able to detect these features at each slice during feature extraction, but also address misalignment beforehand in order to localize and correspond the features to their correct layer.

There has been early work to address the misalignment/aliasing challenge [18] in internal PCB RE, as well as identifying what slices belong to what layers of a volumetric PCB stack depending on varying levels of a priori information [18, 19]. First, [18] provided an algorithm that enables fully automated unsupervised 3D-stack alignment via iterative robust regression and registration based on the image gradient direction of the volumetric PCB stack. With these slices now aligned and registered, the data better facilitates slice-to-layer identification, which is key for internal PCB RE and determining which features correspond to which layers. [18] then leverages the similarity of aligned adjacent slices in an X-ray CT imaged volumetric stack by using K-means clustering, in combination with exponentially windowed cross correlation, to identify what slices belong to what layers in an automated unsupervised manner, where the reverse engineer in practice has no reference design information.

In [19] the authors then explore the effectiveness of automated slice-to-layer identification under the assumption that the RE has reference design information available either in the form of CAD software provided digital images of the layers present in the board, or their X-ray CT imaged equivalent. However, the challenge for this task is that the provided reference design knowledge may not always be of the same imaging modality as the X-ray CT data. To address this heterogeneous image comparison challenge, the authors employed a feature based approach utilizing the spatial pyramid bag of visual words model [111] in an iterative manner with various weighting schemes and then compare their results not only against the unsupervised methodology [18] but also against naive pixel intensity based approaches. Table 11 summarizes the results across the different methods from a classification perspective as well as image quality assessment due to the desired result for subsequent RE stages being a fused singular image of the slices composing a layer.

In particular, in [18], the importance of having domain knowledge of the X-Ray CT process for solving the slice-to-layer correspondence issue is highlighted. Specifically, slice location information is critical for unsupervised slice-to-layer identification due to the similarity of adjacent slices in an X-ray CT imaged volumetric stack. Unsupervised approaches tested in [18] that did not utilize exponential windowing to emphasize location did not report a single instance of an F1-Score

Table 11. Average semi-supervised classification performance and image quality assessment compared across approaches [18, 19]

Average Classification Performance & Image Quality Assessment					
Method	Precision	Recall	F1-Score	Average Correlation	Average SSIM
Semi-Supervised - Digital reference	97.2%	97.2%	97.2%	.999	.997
Semi-Supervised - X-Ray Reference	98.34%	98.34%	98.34%	.999	.998
Unsupervised	90.51%	90.51%	90.51%	.997	.974
SSIM Based Digital Reference	36.31%	36.31%	36.31%	.868	.816
Correlation Based X-Ray Reference	70.70%	70.70%	70.70%	.957	.844

above 10% for classification accuracy. Furthermore, [19] improved the peak unsupervised results through its iterative feature-focused approach as opposed to naïve intensity-based approaches that performed particularly poorly in comparison (See Figure 31).

Deep learning for PCB RE is equally challenging. Although for external PCB RE, it may seem apt to apply deep learning for object detection/classification, it can easily fail. This is due to the fact that deep learning models are data-driven. More precisely, they can be confused when encountering unseen data from custom ICs developed in-house or by a third-party foundry, as opposed to those seen before (e.g., commercial, available ICs). Besides, the passive components have a variety of footprints that often overlap, and consequently, a correct classification cannot be achieved in a straightforward manner. [107] explored the component detection/extraction topic with a deep learning (region proposal networks) and graph theory-driven approach. They reported a mean Average Precision (mAP) of 0.653 for their top model, leaving much room for improvement. They also highlighted that the main difficulties are the ambiguity/subjectivity of labeling data, necessary for training deep learning models.

Furthermore, deep learning has been adopted in studies on internal PCB RE as well. Qiao et al. has suggested using a Deep Convolutional Neural Network (DCNN) with the graph cuts to achieve segmentation in PCB CT images [150]. Although the performance is improved, when compared to the performance on natural scene images, the network still presents huge improvement potential. To apply deep learning in PCB RE cases, the authors of [150] leveraged transfer learning in combination with image patches from the complete image to address overfitting and other challenges caused due to the limited size of the training database.

Nonetheless, it is not clear how well this technique can generalize to the vast variety of board samples and whether training is required for every new sample. Even if this issue can be resolved by adding other board samples, this intensifies the labeling problem. Lastly, Botero et al. highlighted the challenges to quickly adapt existing deep learning solutions to these problems when utilizing the Mask R-CNN object detection network for via detection [20]. When the authors have utilized a pre-trained network, whose weights were further trained for vias, the performance is not only sub-par for the training dataset but has poor translation to a novel dataset not seen during training.

5.2.2 Netlist Extraction. The extracted and localized PCB features from the annotation stage are analyzed to generate a netlist that can be further manufactured. This requires the translation of the image features from the pixel domain to the geometrical domain (see Figure 32). Once the BoM has been obtained from the PCB board, a software tool is applied to interpret the information by comparing that to a standard BoM for inspection, see, e.g., [58, 87]. Moreover, the systems, such as the work proposed in [140], can generate a schematic from a netlist, enabling applications such as schematic verification, anomaly detection, replacement/upgrades, etc. However, these applications assume that the extracted features from PCB are correct, which may lead to inspection failure if the error is accumulated from earlier steps. Accordingly, it is crucial to do in-depth research in PCB feature extraction and analysis to obtain a more robust PCB RE scheme.

Anti-PCB RE approaches are focused on making RE at the PCB-level prohibitively more expensive and time-consuming than it is worth. This is done in a variety of ways, with varying complexities. The work presented in [133] focuses on the design and implementation of a few passive components, more unmarked ICs, using custom silicon, and/or having cases of missing silkscreens. These methods have low to moderate overhead with regards to design cost and manufacturing impact. However, they only increase RE costs by a small margin. Instead, by utilizing a multi-layer board, blind and buried vias, and/or routing signals for the inner layers, the RE costs can be significantly raised [151]. Additionally, obfuscation can also be utilized for anti-RE of PCBs [72], similar to its application for anti-RE at the IC level. Components referred to as permutation blocks can be used to hide the interconnects among the circuit components on PCBs.

Existing research on how to counter X-Ray-enabled RE focuses on inserting X-Ray detecting sensors and using specific materials. X-Ray detecting sensors are devices embedded in a PCB design, being sensitive to X-Rays and react once a predetermined length of exposure to X-Rays has occurred. Afterward, the sensors signal a destructive measure to take place on the board to delay the RE process or simply act as an indicator that RE has taken place. Furthermore, high-density materials with high X-Ray attenuation factors, such as Zirconia powder, could be used throughout a board to reduce the quality of the X-Ray images. Using this material in a specific pattern throughout several layers can drastically affect the X-Ray transmission through a PCB, resulting in a much lower signal-to-noise ratio and low-quality 3D reconstruction of the PCB sample [6]. The combination of the anti-RE techniques for external RE with these techniques for internal RE could provide a holistic solution to protect the system from RE.

6 FUTURE RESEARCH DIRECTIONS

Up until this point, we have described the main building blocks of a typical RE framework (see Figure 1(a)), put together to meet the main requirements of an automated approach. Moreover, numerous studies introducing and employing various ML and image analysis techniques are reviewed, where the most prominent ones used at various stages of the RE workflow are summarized in Table 12. In this respect, the advantages and disadvantages of those algorithms are highlighted and assessed with regard to their applications and performance. In fact, the end goal of the entire RE process is to leverage the advantages offered by image analysis and machine learning and eventually perform RE in an automated manner. In addition to obvious benefits, namely the reduction in manpower and costs, automated RE enables a variety of applications, which can further exploit the information provided by the RE. In this context, the following topics and possible future research directions are suggested.

(1) Enhanced Hardware Assurance: With automated RE achieved at both of the IC and PCB-levels, it can allow for enhanced levels of assurance, when validating or verifying a design. The detection of defects, design alterations, or IP infringement can be improved to a pixel-level accuracy and performed more efficiently. However, it is not known whether a substantial improvement over the state-of-the-art techniques can be achieved through these advancements. This needs to be explored in future work in this area.

(2) Qualitative Evaluation of Reverse Engineering: While each block in the RE framework is necessary to achieve a high level of automation, no method has been yet developed in the literature that can evaluate the performance of the RE process at each stage of the framework, let alone the whole process. Defining metrics and criteria for the quality assessment of RE can also provide the ability to explore not only the trade-offs between the quality at various stages, but also their impact on the entire RE process. This can, of course, facilitate

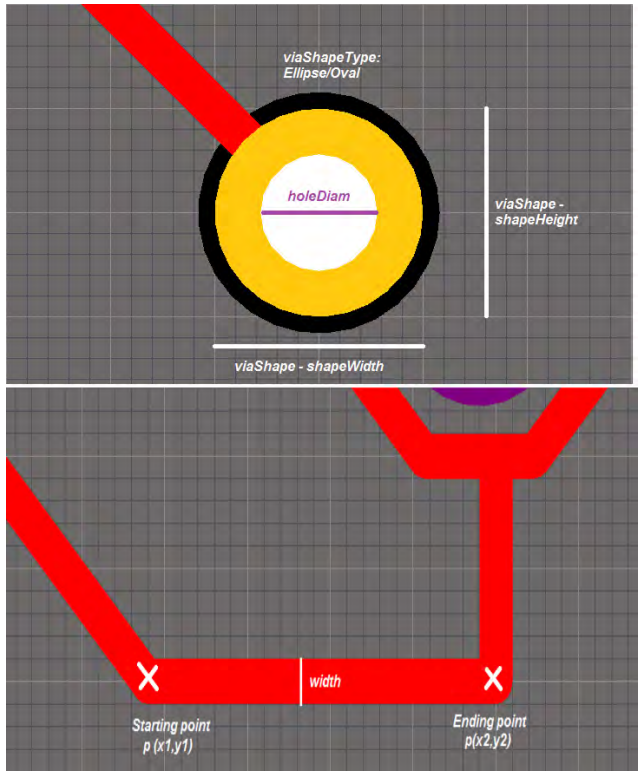


Fig. 32. Via and trace vectorized features

possible improvements in efficiency in terms of time, complexity, and required computational resources.

(3) Benchmarking: Besides the above point regarding the performance analysis of the algorithms, providing a quantitative comparison between their performance is further challenging. This is a direct consequence of the lack of a comprehensive benchmark dataset that can be used to compare the algorithms. Such a database cannot be built easily due to the complex undertaking involved in preparing instances. This problem can be even more severe for deep learning algorithms, as discussed below.

(4) Reverse Engineering Optimization via Deep Learning: Due to the lack of a sufficiently large amount of data as well as the variations in data collected across designs, the requirements of effective deep learning models cannot be fulfilled. However, after conducting an RE process, certain stages, e.g., de-noising, via/trace feature extraction, etc., can be optimized via deep learning. In this regard, we can employ synthetic data generation and augmentation, along with using previously extracted RE data as ground truth. This can indeed help to make those stages more time-efficient, when conventional deep neural networks or convolutional neural networks are applied. As this has not been thoroughly explored, the actual extent of such improvement is not known.

(5) Functional vs. Design Equivalence: Our earlier discussion of image analysis- and machine learning-enabled RE has focused on developing a method to reproduce an IC or, similarly, a PCB as close to the original one as possible. However, there are often scenarios, where only a functionally-equivalent reproduction is necessary rather than a precise design reproduction. As an example, we can refer to an automated generation of a new design built upon some arbitrary standard cells, but with the same functionally as the original one with the foundry-specific standard cells. For PCBs, this can be even more straightforward: producing a PCB, whose connectivity is maintained, but not its specifications, e.g., the trace/via width or distances. Future research should not only focus on such cases, but also go beyond those by considering a broader range of equivalence options, instead of solely functional and design equivalence.

(6) Missing Data Reconstruction: Regardless of the modality, one has to deal with the noise in the collected data. The impact of the noise can range from missing regions of the information in a de-processed IC to missing artifacts on a PCB after performing the X-Ray CT. If RE can be automated, it is reasonable to acquire a large amount of data to model particular noise characteristics observed during image acquisition. These models could then be employed to correct noisy data and even reconstruct missing data. While this is well studied in machine learning- and image analysis-related literature, the feasibility and extent to which this can be achieved for IC and PCB RE have yet to be explored.

(7) Compression Algorithms for RE: Another interesting aspect of RE to be taken into account in future work is that the minimum amount of information or data required for a successful reconstruction of images should be collected and stored on a computer system. In addition to speeding up the process of image acquisition, this has the added benefit in terms of space complexity. Unlike common image compression algorithms that attempt to attain the highest possible level of visual quality, new algorithms can be designed or adapted to accurately reconstruct the required features, which leads to a saving of the storage and processing resources.

(8) Cross-Modality Comparison and Evaluation: One of the biggest challenges facing us, when evaluating the performance of an RE process, is to compare results across different modalities. Irrespective of the modality (i.e., SEM, Optical, X-Ray CT), the final output of the RE framework should be compared to either a software-provided golden design in a digital format or a PCB schematic. This also requires the exploration of new techniques that can incorporate various factors including different characteristics of the data, the impact of the noise, and variations across the modalities.

(9) Countermeasures against Advanced RE-based Attacks: While the techniques mentioned in earlier sections are useful to stop an attacker enjoying the advantages of the current, commonly applied RE framework, this cannot be guaranteed in the future. In particular, to deal with adversaries that can conduct RE, enhanced through the adoption of machine learning and image analysis algorithms, the designer has to predict the risk of such emerging attacks. To this end, it is crucial to *estimate* the amount of effort that the attacker has to put and design measures to make the RE process significantly less effective and inefficient. Unfortunately, such estimations cannot be carried out in a straightforward manner. Therefore, new research directions regarding counter automated-RE development can be of great interest for researchers from government, industry, and academia.

Table 12. Summary of the methods applied in the context of RE

Article	Main Contribution	Scope	Algorithms	Features Used	Metrics	Evaluation Method	Shortcomings for RE
[108]	Segmentation	IC	Edge detection	Metal layers	NA	Visual	Optical microscope images
[35]	Segmentation	IC	K-means and SVM	Contact and Metal layers	F-score	Ground truth	Only applicable to vias and metal connections
[34, 36]	Segmentation	IC	K-means, Fuzzy C-Means, SVM	Polysilicon and Contact layers	Intersection over Union (IoU), pixel accuracy	Ground truth	Requires population of shape library
[51, 130, 195]	Segmentation	IC	Spatial and frequency domain filtering	Contact and Metal layers	NA	Visual	Naive applications of image processing
[82]	Segmentation	IC	DCNN	Contact and Metal layers	False Positive, Negative and semantic errors	Ground truth	Needs 500,000 labelled samples to train
[44]	Extraction of Standard Cell Library	IC	Normalized cross-correlation	Doping layer	NA	Ground truth	Designed for partial RE
[207]	Extraction of Standard Cell Library	IC	Rule based	Contact layer	NA	AES designs with ground truth	Over/Under-segmented cells
[215, 216]	Localizing standard cells	IC	Template Matching	Conductive layers	NA	NA	Uses approximation to speed up cell localization
[3, 96]	Netlist generation	IC	Template Matching	All layers	NA	NA	Requires standard cell library
[152]	Netlist generation	IC	XGBoost	All layers with pixel intensity, gradient and Hu moments	NA	Ground truth	Needs to be fine tuned for different ICs
[8, 118, 120, 182]	High-level description of sub-circuits	IC	Topological analyses, fuzzy structural similarity	Netlist	NA	Ground truth	Uses similarity between known libraries of functional blocks to generate description
[168, 189, 193]	Development of tools for RE	IC	NA	All layers	NA	NA	Assumes availability of some information, e.g., the standard cell library
[172, 196]	IC Trojan detection on active layer	IC	Rule based	Shape of logic cells	NA	Designed on-chip training data	Semi-destructive, need manual polishing

Continued on next page

Article	Main Contribution	Scope	Algorithms	Features Used	Metrics	Evaluation Method	Shortcomings for RE
[7]	Non-Destructive Imaging and Netlist Extraction	PCB	X-Ray CT Imaging and Image Segmentation	X-Ray CT Slices	NA	Dataset with De-Populated Board	Very manual and parameter dependent image processing
[31, 32, 50, 94, 115, 185, 191]	PCB Defect Detection and Quality Control	PCB	Image Subtraction[31, 32, 50, 94, 115, 191] and Deep Learning[185]	PCB Layer Images	Precision and F-Score	Golden PCB Layer Image	Requires bare board golden layer images
[119]	Text Recognition on PCB Surface	PCB	Optical Character Recognition, Binarization, and Background Estimation	Board surface image	F-Score, Precision, and Recall	Compared against freely available OCR engines OCRAD, Tesseract-OCR, Cuneiform-linux, and GOCR on ground truth	Sub-optimal accuracy
[150]	Trace segmentation	PCB	DCNN and Graph Cuts-based Semantic Segmentation	PCB CT Images	Pixel accuracy, IoU, F1-Score, Precision, Recall	50 PCB CT test images	Dealing with the noise, reliance on training data, and variance across designs/imaging.

7 CONCLUSION

In this tutorial, we have comprehensively discussed the challenges associated with RE of ICs and PCBs. It has been observed that for hardware trust and assurance, even though existing, well-known methods (e.g., functional analysis) can be considered useful, the challenges of such methods rise in proportion to the complexity of the IC. The aim of the design in the semiconductor industry is to move towards a higher performance and efficiency and the upward trend of complexity can remain intact for the years to come. Hence, the need for effective RE becomes greater than ever before.

From the imaging perspective, it has been noted that the primary challenge to be faced by an effective RE-based method is the lack of understanding of the nature of the noise in imaging modalities used for RE, e.g., SEM and CEM. This can be augmented by the techniques used to pre-process the IC for imaging, such as decapsulation and delayering. Furthermore, the time spent to acquire high-quality images with a reduced noise level makes RE infeasible for ICs employing today's technology nodes.

Our overview of machine learning going hand in hand with RE has demonstrated the need for quantifying the amount of useful information in each layer. In addition, the effect of counter-RE on machine learning-enabled techniques has been further investigated. Finally, the high variability of features between the layers of different ICs and the lack of high-quality datasets addressing this issue have been observed and regarded as an obstacle to the employment of deep learning for RE.

While relevant literature regarding PCB RE is not rich, there has been a clear interest in taking advantage of image analysis and machine learning algorithms for quality assurance in PCB manufacturing processes. These approaches typically involve image subtraction or (to some extent) building models for detecting defect/anomaly during the manufacturing process. Nevertheless, algorithms implemented for these purposes are not sufficient as they cannot resolve challenges with the external or internal PCB RE. As a prime example, external PCB RE requires robust, illumination-invariant algorithms to be developed, which ensures effective, high-quality component extraction and analysis. In addition to the intensity inhomogeneity, algorithms designed to deal with internal PCB RE must also be robust to blurring artifacts caused by the X-ray, high-z materials, and aliasing from neighboring layers. Furthermore, due to the wide variety of designs across technologies and the lack of representative datasets, a generalization of the results can pose a serious problem to RE.

Finally, we believe that this tutorial paves the way for the necessary broad discussion on the above issues and how hardware trust and assurance can benefit greatly from RE.

ACKNOWLEDGMENTS

This paper is based upon work supported by Cisco, AFOSR under award No. FA9550-14-1-0351, National Science Foundation under grant No.1821780, and National Science Foundation Graduate Research Fellowship under Grant Nos. 1315138 and 1842473.

REFERENCES

[1] Jason Abt and Chris Pawlowicz. 2012. Circuit Analysis Techniques: Delayering and Circuit Vision. http://www.techinsights.com/[Accessed: Feb. 27, 2021].

[2] Nitin Aggarwal and W Clem Karl. 2006. Line detection in images through regularized Hough transform. *IEEE transactions on image processing* 15, 3 (2006), 582–591.

[3] Haroon Ahmed, Simon Blythe, and Beatrice Fraboni. 1993. Integrated circuit structure analysis. US Patent 5,191,213.

[4] C. Albrecht. 2005. Iwls 2005 benchmarks. http://www.iwls.org [Accessed Feb. 27, 2021].

[5] N. Arazm, A. Sahab, and M. F. Kazemi. 2017. Noise reduction of SEM images using adaptive Wiener filter. In *2017 IEEE International Conference on Cybernetics and Computational Intelligence (CyberneticsCom)*. 50–55.

[6] Navid Asadizanjani, Sina Shahbazmohamadi, Mark Tehranipoor, and Domenic Forte. 2015. Non-destructive pcb reverse engineering using x-ray micro computed tomography. In *41st International symposium for testing and failure analysis, ASM*. 1–5.

[7] Navid Asadizanjani, Mark Tehranipoor, and Domenic Forte. 2017. PCB reverse engineering using nondestructive X-ray tomography and advanced image processing. *IEEE Transactions on Components, Packaging and Manufacturing Technology* 7, 2 (2017), 292–299.

[8] Johanna Baehr, Alessandro Bernardini, Georg Sigl, and Ulf Schlichtmann. 2019. Machine learning and structural characteristics for reverse engineering. In *Proceedings of the 24th Asia and South Pacific Design Automation Conference*. ACM, 96–103.

[9] Johanna Baehr, Alessandro Bernardini, Georg Sigl, and Ulf Schlichtmann. 2020. Machine learning and structural characteristics for reverse engineering. *Integration* 72 (2020), 1–12.

[10] Chongxi Bao, Domenic Forte, and Ankur Srivastava. 2014. On application of one-class SVM to reverse engineering-based hardware Trojan detection. In *Fifteenth International Symposium on Quality Electronic Design*. IEEE, 47–54.

[11] Chongxi Bao, Domenic Forte, and Ankur Srivastava. 2015. On reverse engineering-based hardware Trojan detection. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 35, 1 (2015), 49–57.

[12] Chongxi Bao, Domenic Forte, and Ankur Srivastava. 2016. On reverse engineering-based hardware Trojan detection. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 35, 1 (2016), 49–57.

[13] Chongxi Bao, Yang Xie, Yuntao Liu, and Ankur Srivastava. 2018. Reverse engineering-based hardware trojan detection. In *The Hardware Trojan War*. Springer, 269–288.

[14] Christopher F Batten. 2000. Autofocusing and astigmatism correction in the scanning electron microscope. *Mphill thesis, University of Cambridge* (2000).

[15] Csaba Benedek, Olivér Krammer, Mihály Janóczki, and László Jakab. 2012. Solder paste scooping detection by multilevel visual inspection of printed circuit boards. *IEEE Transactions on Industrial Electronics* 60, 6 (2012), 2318–2331.

[16] Simon Blythe, Beatrice Fraboni, Sanjay Lall, Haroon Ahmed, and Ugo de Riu. 1993. Layout reconstruction of complex silicon chips. *IEEE journal of solid-state circuits* 28, 2 (1993), 138–145.

[17] F Edward Boas and Dominik Fleischmann. 2012. CT artifacts: causes and reduction techniques. *Imaging in Medicine* 4, 2 (2012), 229–240.

[18] Ulbert J. Botero, Navid Asadizanjani, Damon L. Woodard, and Domenic Forte. 2020. A Framework for Automated Alignment and Layer Identification of X-Ray Tomography Imaged PCBs. In *GOMACTech*. San Francisco.

[19] Ulbert J. Botero, Fatemeh Ganji, Navid Asadizanjani, Damon Woodard, and Domenic Forte. 2020. Semi-Supervised Automated Layer Identification of X-ray Tomography Imaged PCBs. In *accepted for presentation at International Conference on PHYSICAL ASSURANCE and INSPECTION of ELECTRONICS (PAINE), 2020*. IEEE.

[20] Ulbert J. Botero, David Koblah, Daniel Capecci, Fatemeh Ganji, Navid Asadizanjani, Damon Woodard, and Domenic Forte. 2020. Automated Via Detection for PCB Reverse Engineering. In *accepted for presentation at International Symposium for Testing and Failure Analysis, 2020*. ASM.

[21] Ulbert J Botero, Mark M Tehranipoor, and Domenic Forte. 2019. Upgrade/Downgrade: Efficient and Secure Legacy Electronic System Replacement. *IEEE Design & Test* 36, 1 (2019), 14–22.

[22] Nikolaos G Bourbakis, A Mogzadeh, S Mertoguno, and Cris Koutsougeras. 2002. A knowledge-based expert system for automatic visual VLSI reverse-engineering: VLSI layout version. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans* 32, 3 (2002), 428–436.

[23] David C Bowman. 2018. Image Stitching and Matching Tool in the Automated Iterative Reverse Engineer (AIRE) Integrated Circuit Analysis Suite. (2018).

[24] Matthew Brown and David G Lowe. 2007. Automatic panoramic image stitching using invariant features. *International journal of computer vision* 74, 1 (2007), 59–73.

[25] Burçin Cakır and Sharad Malik. 2015. Hardware Trojan detection for gate-level ICs using signal correlation based clustering. In *2015 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 471–476.

[26] Burcin Cakir and Sharad Malik. 2018. Reverse engineering digital ICs through geometric embedding of circuit graphs. *ACM Transactions on Design Automation of Electronic Systems (TODAES)* 23, 4 (2018), 1–19.

[27] Stephan De Castro, Jean-Max Dutertre, Bruno Rouzeyre, Giorgio Di Natale, and Marie-Lise Flottes. 2016. Frontside versus backside laser injection: a comparative study. *ACM Journal on Emerging Technologies in Computing Systems (JETC)* 13, 1 (2016), 1–15.

[28] Rajat Subhra Chakraborty, Francis Wolff, Somnath Paul, Christos Papachristou, and Swarup Bhunia. 2009. MERO: A statistical approach for hardware Trojan detection. In *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 396–410.

[29] Wei-Hsin Chang, Shuenn-Der Tzeng, and Chen-Yi Lee. 2001. A novel subcircuit extraction algorithm by recursive identification scheme. In *ISCAS 2001. The 2001 IEEE International Symposium on Circuits and Systems (Cat. No. 01CH37196)*, Vol. 5. IEEE, 491–494.

[30] Narendra Chaudhary, Serap A Savari, and Sai S Yeddulapalli. 2019. Line roughness estimation and Poisson denoising in scanning electron microscope images using deep learning. *Journal of Micro/Nanolithography, MEMS, and MOEMS* 18, 2 (2019), 024001.

[31] Vikas Chaudhary, Ishan R Dave, and Kishor P Upla. 2017. Automatic visual inspection of printed circuit board for defect detection and classification. In *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*. IEEE, 732–737.

[32] Rasika R Chavan, Swati A Chavan, Gautami D Dokhe, Mayuri B Wagh, and Archana S Vaidya. 2016. Quality Control of PCB using Image Processing. *International Journal of Computer Applications* 975 (2016), 8887.

[33] Jinghui Chen, Chen Dong, Fan Zhang, and Guorong He. 2019. A Hardware-Trojans Detection Approach Based on eXtreme Gradient Boosting. In *2019 IEEE 2nd International Conference on Computer and Communication Engineering Technology (CCET)*. IEEE, 69–73.

[34] Deruo Cheng, Yiqiong Shi, Bah-Hwee Gwee, Kar-Ann Toh, and Tong Lin. 2018. A Hierarchical Multiclassifier System for Automated Analysis of Delayered IC Images. *IEEE Intelligent Systems* 34, 2 (2018), 36–43.

[35] Deruo Cheng, Yiqiong Shi, Tong Lin, Bah-Hwee Gwee, and Kar-Ann Toh. 2018. Hybrid K-Means Clustering and Support Vector Machine Method for via and Metal Line Detections in Delayered IC Images. *IEEE Transactions on Circuits and Systems II: Express Briefs* 65, 12 (2018), 1849–1853.

[36] Deruo Cheng, Yiqiong Shi, Tong Lin, Bah-Hwee Gwee, and Kar-Ann Toh. 2019. Global Template Projection and Matching Method for Training-Free Analysis of Delayered IC Images. In *2019 IEEE International Symposium on Circuits and Systems (ISCAS)*. IEEE, 1–5.

[37] D Cheremisinov and L Cheremisinova. 2020. Subcircuit Pattern Recognition in Transistor Level Circuits. *Pattern Recognition and Image Analysis* 30, 2 (2020), 160–169.

[38] Gregory H Chisholm, Steven T Eckmann, Christopher M Lain, and Robert L Veroff. 1999. Understanding integrated circuits. *IEEE Design & Test of Computers* 16, 2 (1999), 26–37.

[39] Petr Cizmar, András E Vladár, Bin Ming, Michael T Postek, National Institute of Standards, and Technology. 2008. Simulated SEM images for resolution measurement. *Scanning* 30, 5 (2008), 381–391.

[40] Petr Cizmar, András E Vladár, and Michael T Postek. 2009. Optimization of accurate SEM imaging by use of artificial images. In *Scanning Microscopy 2009*, Vol. 7378. International Society for Optics and Photonics, 737815.

[41] Ronald P Cocchi, James P Baukus, Lap Wai Chow, and Bryan J Wang. 2014. Circuit camouflage integration for hardware IP protection. In *Proceedings of the 51st Annual Design Automation Conference*. ACM, 1–5.

[42] Senate Armed Services Committee et al. 2012. Inquiry into counterfeit electronic parts in the department of defense supply chain. *Washington, DC: Author* (2012).

[43] Vassilios Constantoudis, Vijaya-Kumar Murugesan Kuppuswamy, and Evangelos Gogolides. 2013. Effects of image noise on contact edge roughness and critical dimension uniformity measurement in synthesized scanning electron microscope images. *Journal of Micro/Nanolithography, MEMS, and MOEMS* 12, 1 (2013), 013005.

[44] Franck Courbon. 2019. Practical Partial Hardware Reverse Engineering Analysis. *Journal of Hardware and Systems Security* (2019), 1–10.

[45] Franck Courbon, Philippe Loubet-Moundi, Jacques JA Fournier, and Assia Tria. 2015. A high efficiency hardware trojan detection technique based on fast SEM imaging. In *Proceedings of the 2015 Design, Automation & Test in Europe Conference & Exhibition*. EDA Consortium, 788–793.

[46] Franck Courbon, Philippe Loubet-Moundi, Jacques JA Fournier, and Assia Tria. 2015. SEMBA: A SEM based acquisition technique for fast invasive Hardware Trojan detection. In *2015 European Conference on Circuit Theory and Design (ECCTD)*. IEEE, 1–4.

[47] Franck Courbon, Sergei Skorobogatov, and Christopher Woods. 2016. Reverse engineering flash EEPROM memories using scanning electron microscopy. In *International Conference on Smart Card Research and Advanced Applications*. Springer, 57–72.

[48] Navneet Dalal and Bill Triggs. 2005. Histograms of oriented gradients for human detection. In *2005 IEEE computer society conference on computer vision and pattern recognition (CVPR'05)*, Vol. 1. IEEE, 886–893.

[49] Piali Das, Olga Veksler, Vyacheslav Zavadsky, and Yuri Boykov. 2009. Semiautomatic segmentation with compact shape prior. *Image and Vision Computing* 27, 1-2 (2009), 206–219.

[50] Neelum Dave, Vikas Tambade, Balaji Pandhare, and Suman Saurav. 2016. PCB Defect Detection Using Image Processing And Embedded System. *International Research Journal of Engineering and Technology (IRJET)* 3, 5 (2016), 1897–1901.

[51] Alexander Doudkin, Alexander Inyutin, and Maksim Vatkin. 2005. Objects identification on the color layout images of the integrated circuit layers. In *2005 IEEE Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications*. IEEE, 610–614.

[52] Roger Durà, Jofre Pallarès, Raúl Quijada, Xavier Formatjé, Salvador Hidalgo, and Francisco Serra-Graells. 2017. fast and robust Topology-Based logic gate identification for automated IC reverse engineering. In *ISTFA 2017: the 43rd International Symposium for Testing and Failure Analysis*. ASM International, 299.

[53] Mohamed El Massad, Siddharth Garg, and Mahesh V Tripunitara. 2015. Integrated Circuit (IC) Decamouflaging: Reverse Engineering Camouflaged ICs within Minutes.. In *NDSS*. 1–14.

[54] Rana Elnaggar and Krishnendu Chakrabarty. 2018. Machine Learning for Hardware Security: Opportunities and Risks. *Journal of Electronic Testing* 34, 2 (2018), 183–201.

[55] Luděk Frank. 2005. Noise in secondary electron emission: the low yield case. *Journal of electron microscopy* 54, 4 (2005), 361–365.

[56] PDK Free. [n.d.]. 45nm open-access based PDK for the 45nm technology node.

[57] Sean P Frigo, Zachary H Levine, and Nestor J Zaluzec. 2002. Submicron imaging of buried integrated circuit structures using scanning confocal electron microscopy. *Applied Physics Letters* 81, 11 (2002), 2112–2114.

[58] Chang-Wen Fu, Ge-Xin Zeng, De-Sheng Qiu, and Hui-Zhang Wang. 2007. System and method for generating a bill of material file. US Patent App. 11/309,173.

[59] Marc Fyrbiak. 2019. *Constructive and destructive reverse engineering aspects of digital systems.* Ph.D. Dissertation. Ruhr University Bochum, Germany.

[60] Marc Fyrbiak, Sebastian Strauß, Christian Kison, Sebastian Wallat, Malte Elson, Nikol Rummel, and Christof Paar. 2017. Hardware reverse engineering: Overview and open challenges. In *2017 IEEE 2nd International Verification and Security Workshop (IVSW)*. IEEE, 88–94.

[61] Vilas H Gaidhane, Yogesh V Hote, and Vijander Singh. 2018. An efficient similarity measure approach for PCB surface defect detection. *Pattern Analysis and Applications* 21, 1 (2018), 277–289.

[62] Sumyung Gang, Ndayishimiye Fabrice, and JoonJae Lee. 2020. Coresets for PCB Character Recognition based on Deep Learning. In *2020 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*. IEEE, 637–642.

[63] Swaroop Ghosh, Abhishek Basak, and Swarup Bhunia. 2014. How secure are printed circuit boards against trojan attacks? *IEEE Design & Test* 32, 2 (2014), 7–16.

[64] E Giannatou, G Papavieros, V Constantoudis, H Papageorgiou, and E Gogolides. 2019. Deep learning denoising of SEM images towards noise-reduced LER measurements. *Microelectronic Engineering* 216 (2019), 111051.

[65] Richard Goldman, Karen Bartleson, Troy Wood, Kevin Kranen, C Cao, Vazgen Melikyan, and Gayane Markosyan. 2009. Synopsys' open educational design kit: capabilities, deployment and future. In *2009 IEEE International Conference on Microelectronic Systems Education*. IEEE, 20–24.

[66] R Goldman, K Bartleson, T Wood, K Kranen, V Melikyan, and E Babayan. 2013. 32/28nm educational design kit: Capabilities, deployment and future. In *2013 IEEE Asia Pacific Conference on Postgraduate Research in Microelectronics and Electronics (PrimeAsia)*. IEEE, 284–288.

[67] Hector Gomez, Ckristian Duran, and Elkim Roa. 2018. Standard cell camouflage method to counter silicon reverse engineering. In *2018 IEEE International Conference on Consumer Electronics (ICCE)*. IEEE, 1–4.

[68] Hector Gomez, Ckristian Duran, and Elkim Roa. 2019. Defeating Silicon Reverse Engineering Using a Layout-Level Standard Cell Camouflage. *IEEE Transactions on Consumer Electronics* 65, 1 (2019), 109–118.

[69] Joe Grand. 2014. Printed circuit board deconstruction techniques. In *8th {USENIX} Workshop on Offensive Technologies ({WOOT} 14)*.

[70] Peng Gu, Dylan Stow, Prashansa Mukim, Shuangchen Li, and Yuan Xie. 2018. Cost-efficient 3D integration to hinder reverse engineering during and after manufacturing. In *2018 Asian Hardware Oriented Security and Trust Symposium (AsianHOST)*. IEEE, 74–79.

[71] Ujjwal Guin, Daniel DiMase, and Mohammad Tehranipoor. 2014. Counterfeit integrated circuits: detection, avoidance, and the challenges ahead. *Journal of Electronic Testing* 30, 1 (2014), 9–23.

[72] Zimu Guo, Mark Tehranipoor, Domenic Forte, and Jia Di. 2015. Investigation of obfuscation-based anti-reverse engineering for printed circuit boards. In *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*. IEEE, 1–6.

[73] Mark C Hansen, Hakan Yalcin, and John P Hayes. 1999. Unveiling the ISCAS-85 benchmarks: A case study in reverse engineering. *IEEE Design & Test of Computers* 16, 3 (1999), 72–80.

[74] LR Harriott, A Wagner, and F Fritz. 1986. Integrated circuit repair using focused ion beam milling. *Journal of Vacuum Science & Technology B: Microelectronics Processing and Phenomena* 4, 1 (1986), 181–184.

[75] Kento Hasegawa, Masaru Oya, Masao Yanagisawa, and Nozomu Togawa. 2016. Hardware Trojans classification for gate-level netlists based on machine learning. In *2016 IEEE 22nd International Symposium on On-Line Testing and Robust System Design (IOLTS)*. IEEE, 203–206.

[76] Kento Hasegawa, Masao Yanagisawa, and Nozomu Togawa. 2017. Hardware Trojans classification for gate-level netlists using multi-layer neural networks. In *2017 IEEE 23rd International Symposium on On-Line Testing and Robust System Design (IOLTS)*. IEEE, 227–232.

[77] Kento Hasegawa, Masao Yanagisawa, and Nozomu Togawa. 2017. Trojan-feature extraction at gate-level netlists and its application to hardware-Trojan detection using random forest classifier. In *2017 IEEE International Symposium on Circuits and Systems (ISCAS)*. IEEE, 1–4.

[78] Abdel-Aziz IM Hassanin, Fathi E Abd El-Samie, and Ghada M El Banby. 2019. A real-time approach for automatic defect detection from PCBs based on SURF features and morphological operations. *Multimedia Tools and Applications*

78, 24 (2019), 34437–34457.
[79] Kaiming He, Georgia Gkioxari, Piotr Dollár, and Ross Girshick. 2017. Mask r-cnn. In *Proceedings of the IEEE international conference on computer vision*. 2961–2969.
[80] Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun. 2016. Identity mappings in deep residual networks. In *European conference on computer vision*. Springer, 630–645.
[81] Mirko Holler, Manuel Guizar-Sicairos, Esther HR Tsai, Roberto Dinapoli, Elisabeth Müller, Oliver Bunk, Jörg Raabe, and Gabriel Aeppli. 2017. High-resolution non-destructive three-dimensional imaging of integrated circuits. *Nature* 543, 7645 (2017), 402.
[82] Xuenong Hong, Deruo Cheng, Yiqiong Shi, Tong Lin, and Bah Hwee Gwee. 2018. Deep Learning for Automatic IC Image Analysis. In *2018 IEEE 23rd International Conference on Digital Signal Processing (DSP)*. IEEE, 1–5.
[83] Szu-Hao Huang and Ying-Cheng Pan. 2015. Automated visual inspection in the semiconductor industry: A survey. *Computers in industry* 66 (2015), 1–10.
[84] Xingjia Huang, Shengcong Zhu, Xuanyu Huang, Bing Su, Changping Ou, and Weili Zhou. 2015. Detection of plated through hole defects in printed circuit board with X-ray. In *2015 16th International Conference on Electronic Packaging Technology (ICEPT)*. IEEE, 1296–1301.
[85] Taswar Iqbal and Kai-Dietrich Wolf. 2017. PCB Surface Fingerprints Based Counterfeit Detection of Electronic Devices. *Electronic Imaging* 2017, 7 (2017), 144–149.
[86] Girishma Jain, Sandeep Raghuwanshi, and Gagan Vishwakarma. 2017. Hardware Trojan: Malware Detection Using Reverse Engineering and SVM. In *International Conference on Intelligent Systems Design and Applications*. Springer, 530–539.
[87] Sang-Hun Jin. 2000. Method for transforming original bill-of-material for printed circuit board into standard bill-of-material. US Patent 6,041,268.
[88] Yier Jin, Nathan Kupp, and Yiorgos Makris. 2009. Experiences in hardware Trojan design and implementation. In *2009 IEEE International Workshop on Hardware-Oriented Security and Trust*. IEEE, 50–57.
[89] Yier Jin and Yiorgos Makris. 2008. Hardware Trojan detection using path delay fingerprint. In *2008 IEEE International workshop on hardware-oriented security and trust*. IEEE, 51–57.
[90] Q Kai, C Jian, L Zhongguo, et al. 2016. Automatic printed circuit board wire detecting method of cone beam CT image. *Opt. Precis. Eng.* 24, 2 (2016), 413–421.
[91] Heikki Kälviäinen, Petri Hirvonen, Lei Xu, and Erkki Oja. 1995. Probabilistic and non-probabilistic Hough transforms: overview and comparisons. *Image and Vision Computing* (1995). https://doi.org/10.1016/0262-8856(95)99713-B
[92] Nidal S Kamel and KS Sim. 2004. Image signal-to-noise ratio and noise variance estimation using autoregressive model. *Scanning: The Journal of Scanning Microscopies* 26, 6 (2004), 277–281.
[93] Michael Kass, Andrew Witkin, and Demetri Terzopoulos. 1988. Snakes: Active contour models. *International journal of computer vision* 1, 4 (1988), 321–331.
[94] Beant Kaur, Gurmeet Kaur, and Amandeep Kaur. 2014. Detection and classification of printed circuit board defects using image subtraction method. In *2014 Recent Advances in Engineering and Computational Sciences (RAECS)*. IEEE, 1–5.
[95] Anna Lena Keller, Dirk Zeidler, and Thomas Kemen. 2014. High throughput data acquisition with a multi-beam SEM. In *Scanning Microscopies 2014*, Vol. 9236. International Society for Optics and Photonics, 92360B.
[96] K Yu Kenneth and C Neil Berglund. 1992. Automated system for extracting design and layout information from an integrated circuit. US Patent 5,086,477.
[97] Shahrzad Keshavarz, Cunxi Yu, Samaneh Ghandali, Xiaolin Xu, and Daniel Holcomb. 2018. Survey on applications of formal methods in reverse engineering and intellectual property protection. *Journal of Hardware and Systems Security* 2, 3 (2018), 214–224.
[98] Gyungtae Kim, Ming Ma, and Inhag Park. 2018. A fast and flexible software for IC reverse engineering. In *2018 International Conference on Electronics, Information, and Communication (ICEIC)*. IEEE, 1–4.
[99] Jun-Oh Kim, Youn-Ae Lee, and Tae-Hyoung Park. 2012. Automatic extraction of component inspection regions from Printed Circuit Board. In *2012 IEEE/SICE International Symposium on System Integration (SII)*. IEEE, 871–876.
[100] Adam Kimura, Jon Scholl, James Schaffranek, Matthew Sutter, Andrew Elliott, Mike Strizich, and Glen David Via. 2020. A Decomposition Workflow for Integrated Circuit Verification and Validation. *Journal of Hardware and Systems Security* (2020), 1–10.
[101] Christian Kison. 2019. *Advanced methods for hardware reverse engineering*. Ph.D. Dissertation. Ruhr-Universität Bochum.
[102] Johann Knechtel. 2020. Hardware Security for and beyond CMOS Technology: An Overview on Fundamentals, Applications, and Challenges. *arXiv preprint arXiv:2001.08780* (2020).
[103] Johann Knechtel, Satwik Patnaik, and Ozgur Sinanoglu. 2019. Protect your chip design intellectual property: An overview. In *Proceedings of the International Conference on Omni-Layer Intelligent Systems*. 211–216.

[104] Stephen Kockentiedt, Klaus Tönnies, Erhardt Gierke, Nico Dziurowitz, Carmen Thim, and Sabine Plitzko. 2013. Poisson shot noise parameter estimation from a single scanning electron microscopy image. In *Image Processing: Algorithms and Systems XI*, Vol. 8655. International Society for Optics and Photonics, 86550N.

[105] Jin Won Koh, Gu Teak Hwang, Moon Seop Hyun, Jun-Mo Yang, and Jeoung Woo Kim. 2011. Semiconductor layer extraction techniques by SEM. In *18th IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA)*. IEEE, 1–3.

[106] Kishor Kunal, Tonmoy Dhar, Meghna Madhusudan, Jitesh Poojary, AK Sharma, Wenbin Xu, Steven M Burns, Jiang Hu, Ramesh Harjani, and Sachin S Sapatnekar. 2020. GANA: Graph Convolutional Network Based Automated Netlist Annotation for Analog Circuits. *Proc. DATE. ACM, New York, NY* (2020).

[107] Chia-Wen Kuo, Jacob Ashmore, David Huggins, and Zsolt Kira. 2019. Data-efficient graph embedding learning for PCB component detection. In *2019 IEEE Winter Conference on Applications of Computer Vision (WACV)*. IEEE, 551–560.

[108] Dmitry Lagunovsky, Sergey Ablameyko, and M Kutas. 1998. Recognition of integrated circuit images in reverse engineering. In *Proceedings. Fourteenth International Conference on Pattern Recognition (Cat. No. 98EX170)*, Vol. 2. IEEE, 1640–1642.

[109] SH Lau, Andrei Tkachuk, Michael Feser, Hongtao Cui, Fred Duewer, Wenbing Yun, and David Vallet. 2006. Non destructive failure analysis technique with a laboratory based 3D X-ray nanotomography system. In *LSI Testing Symposium*.

[110] A Lazar and Petru S Fodor. 2015. Sparsity based noise removal from low dose scanning electron microscopy images. In *Computational Imaging XIII*, Vol. 9401. International Society for Optics and Photonics, 940105.

[111] Svetlana Lazebnik, Cordelia Schmid, and Jean Ponce. 2006. Beyond bags of features: Spatial pyramid matching for recognizing natural scene categories. *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition* 2 (2006), 2169–2178. https://doi.org/10.1109/CVPR.2006.68

[112] Yann LeCun, Fu Jie Huang, Leon Bottou, et al. 2004. Learning methods for generic object recognition with invariance to pose and lighting. In *CVPR (2)*. Citeseer, 97–104.

[113] Jang Hee Lee and Suk In Yoo. 2008. An effective image segmentation technique for the SEM image. In *2008 IEEE international conference on industrial technology*. IEEE, 1–5.

[114] Myungjun Lee, Jason Cantone, Ji Xu, Lei Sun, and Ryoung-han Kim. 2014. Improving SEM image quality using pixel super resolution technique. In *Metrology, Inspection, and Process Control for Microlithography XXVIII*, Vol. 9050. International Society for Optics and Photonics, 90500U.

[115] Fabiana R Leta, Flávio F Feliciano, and Flavius PR Martins. 2008. Computer vision system for printed circuit board inspection. In *ABCM Symposium Series in Mechatronics*, Vol. 3. 623–632.

[116] Zachary H Levine, Andrew R Kalukin, Sean P Frigo, Ian McNulty, and Markus Kuhn. 1999. Tomographic reconstruction of an integrated circuit interconnect. *Applied physics letters* 74, 1 (1999), 150–152.

[117] He Li, Qiang Liu, and Jiliang Zhang. 2016. A survey of hardware Trojan threat and defense. *Integration* 55 (2016), 426–437.

[118] Wenchao Li, Adria Gascon, Pramod Subramanyan, Wei Yang Tan, Ashish Tiwari, Sharad Malik, Natarajan Shankar, and Sanjit A Seshia. 2013. Wordrev: Finding word-level structures in a sea of bit-level gates. In *2013 IEEE international symposium on hardware-oriented security and trust (HOST)*. IEEE, 67–74.

[119] Wei Li, Stefan Neullens, Matthias Breier, Marcel Bosling, Thomas Pretz, and Dorit Merhof. 2014. Text recognition for information retrieval in images of printed circuit boards. In *IECON 2014-40th Annual Conference of the IEEE Industrial Electronics Society*. IEEE, 3487–3493.

[120] Wenchao Li, Zach Wasson, and Sanjit A Seshia. 2012. Reverse engineering circuits using behavioral pattern mining. In *2012 IEEE international symposium on hardware-oriented security and trust*. IEEE, 83–88.

[121] Konstantinos G Liakos, Georgios K Georgakilas, Serafeim Moustakidis, Patrik Karlsson, and Fotis C Plessas. 2019. Machine Learning for Hardware Trojan Detection: A Review. In *2019 Panhellenic Conference on Electronics & Telecommunications (PACET)*. IEEE, 1–6.

[122] Tsung-Yi Lin, Michael Maire, Serge Belongie, James Hays, Pietro Perona, Deva Ramanan, Piotr Dollár, and C Lawrence Zitnick. 2014. Microsoft coco: Common objects in context. In *European conference on computer vision*. Springer, 740–755.

[123] Bernhard Lippmann, Niklas Unverricht, Aayush Singla, Matthias Ludwig, Michael Werner, Peter Egger, Anja Duebotzky, Helmut Graeb, Horst Gieser, Martin Rasche, et al. 2020. Verification of physical designs using an integrated reverse engineering flow for nanoscale technologies. *Integration* 71 (2020), 11–29.

[124] Bernhard Lippmann, Michael Werner, Niklas Unverricht, Aayush Singla, Peter Egger, Anja Dübotzky, Horst Gieser, Martin Rasche, Oliver Kellermann, and Helmut Graeb. 2019. Integrated flow for reverse engineering of nanoscale technologies. In *Proceedings of the 24th Asia and South Pacific Design Automation Conference*. ACM, 82–89.

[125] Xifeng Liu and Yuwei Hu. 2018. Automatic extraction of via in the CT image of PCB. In *Ninth International Conference on Graphic and Image Processing (ICGIP 2017)*, Vol. 10615. International Society for Optics and Photonics, 106154J.

[126] Bin Ma, Timo Zimmermann, Manfred Rohde, Simon Winkelbach, Feng He, Werner Lindenmaier, and Kurt EJ Dittmar. 2007. Use of autostitch for automatic stitching of microscope images. *Micron* 38, 5 (2007), 492–499.
[127] Kaleel Mahmood, Pedro Latorre Carmona, Sina Shahbazmohamadi, Filiberto Pla, and Bahram Javidi. 2015. Real-time automated counterfeit integrated circuit detection using x-ray microscopy. *Applied Optics* 54, 13 (2015), D25–D32.
[128] Raman Maini and Himanshu Aggarwal. 2009. Study and comparison of various image edge detection techniques. *International journal of image processing (IJIP)* 3, 1 (2009), 1–11.
[129] DW Malone and RE Hummel. 1997. Electromigration in integrated circuits. *Critical Reviews in Solid State and Material Sciences* 22, 3 (1997), 199–238.
[130] G Masalskis et al. 2008. Reverse engineering of CMOS integrated circuits. *Elektronika ir elektrotechnika* 88, 8 (2008), 25–28.
[131] Erik Matlin, Motilal Agrawal, and David Stoker. 2014. Non-invasive recognition of poorly resolved integrated circuit elements. *IEEE Transactions on Information Forensics and Security* 9, 3 (2014), 354–363.
[132] Mohadeseh Mazhari and Reza PR Hasanzadeh. 2016. Suppression of noise in SEM images using weighted local hysteresis smoothing filter. *Scanning* 38, 6 (2016), 634–643.
[133] Ian McLoughlin. 2008. Secure embedded systems: The threat of reverse engineering. In *2008 14th IEEE International Conference on Parallel and Distributed Systems*. IEEE, 729–736.
[134] Yoshihiro Midoh, Katsuyoshi Miura, Koji Nakamae, and Hiromu Fujioka. 2005. Statistical optimization of Canny edge detector for measurement of fine line patterns in SEM image. *Measurement Science and Technology* 16, 2 (2005), 477.
[135] Madhav Moganti and Fikret Ercal. 1998. Segmentation of printed circuit board images into basic patterns. *Computer Vision and Image Understanding* 70, 1 (1998), 74–86.
[136] Samuel K. Moore. 2018. *This Tech Would Have Spotted the Secret Chinese Chip in Seconds*. https://spectrum.ieee.org/riskfactor/computing/hardware/this-tech-would-have-spotted-the-secret-chinese-chip-in-seconds
[137] Ryo Nakagaki, Yuji Takagi, and Koji Nakamae. 2010. Automatic recognition of circuit patterns on semiconductor wafers from multiple scanning electron microscope images. *Measurement Science and Technology* 21, 8 (2010), 085501.
[138] Seetharam Narasimhan, Xinmu Wang, Dongdong Du, Rajat Subhra Chakraborty, and Swarup Bhunia. 2011. TeSR: A robust temporal self-referencing approach for hardware Trojan detection. In *2011 IEEE International Symposium on Hardware-Oriented Security and Trust*. IEEE, 71–74.
[139] Abdurrahman A Nasr and Mohamed Z Abdulmageed. 2017. An Efficient Reverse Engineering Hardware Trojan Detector Using Histogram of Oriented Gradients. *Journal of Electronic Testing* 33, 1 (2017), 93–105.
[140] B Naveen and KS Raghunathan. 1993. An automatic netlist-to-schematic generator. *IEEE Design & Test of Computers* 10, 1 (1993), 36–41.
[141] Karsten Nohl, David Evans, Starbug Starbug, and Henryk Plötz. 2008. Reverse-Engineering a Cryptographic RFID Tag.. In *USENIX security symposium*, Vol. 28.
[142] OpenCores. 2012. OpenCores Oliscience. https://opencores.org/projects [Accessed: Feb. 27, 2021].
[143] Ndubuisi G Orji, Mustafa Badaroglu, Bryan M Barnes, Carlos Beitia, Benjamin D Bunday, Umberto Celano, Regis J Kline, Mark Neisser, Y Obeng, and AE Vladar. 2018. Metrology for the next generation of semiconductor devices. *Nature electronics* 1, 10 (2018), 532–547.
[144] OSU. [n.d.]. Oklahoma state university system on chip (soc) design flows. https://vlsiarch.ecen.okstate.edu/flow/ [Accessed: Feb. 27, 2021].
[145] James Pawley and Heide Schatten. 2007. *Biological low-voltage scanning electron microscopy*. Springer.
[146] Jon R Pearce and Duane C Holmes. 1987. Noise Contributions To Feature Dimension Measurement In A Scanning Electron Microscope (Sem). In *Integrated Circuit Metrology, Inspection, & Process Control*, Vol. 775. International Society for Optics and Photonics, 153–158.
[147] Minxu Peng, John Murray-Bruce, Karl K Berggren, and Vivek K Goyal. 2020. Source shot noise mitigation in focused ion beam microscopy by time-resolved measurement. *Ultramicroscopy* (2020), 112948.
[148] Gatan Prashanth Prasad. 2010. Preparation of a cross-sectional semiconductor IC device sample for SEM observation. https://analyticalscience.wiley.com/do/10.1002/micro.139/full/ [Accessed: Feb. 27, 2021].
[149] EL Principe, Navid Asadizanjani, Domenic Forte, Mark Tehranipoor, Robert Chivas, Michael DiBattista, Scott Silverman, Mike Marsh, Nicolas Piche, and John Mastovich. 2017. Steps toward automated deprocessing of integrated circuits. In *ISTFA 2017: the 43rd International Symposium for Testing and Failure Analysis*. ASM International, 285.
[150] Kai Qiao, Lei Zeng, Jian Chen, Jinjin Hai, and Bin Yan. 2018. Wire segmentation for printed circuit board using deep convolutional neural network and graph cut model. *IET Image Processing* 12, 5 (2018), 793–800.
[151] Shahed E Quadir, Junlin Chen, Domenic Forte, Navid Asadizanjani, Sina Shahbazmohamadi, Lei Wang, John Chandy, and Mark Tehranipoor. 2016. A survey on chip to system reverse engineering. *ACM journal on emerging technologies in computing systems (JETC)* 13, 1 (2016), 6.
[152] Raul Quijada, Roger Dura, Jofre Pallares, Xavier Formatje, Salvador Hidalgo, and Francisco Serra-Graells. 2018. Large-Area Automated Layout Extraction Methodology for Full-IC Reverse Engineering. *Journal of Hardware and*

Systems Security 2, 4 (2018), 322–332.

[153] R. Quijada, A. Raventós, F. Tarrés, R. Durà, and S. Hidalgo. 2014. The use of digital image processing for IC reverse engineering. In *2014 IEEE 11th International Multi-Conference on Systems, Signals Devices (SSD14)*. 1–4.

[154] MT Rahman and MNA Dewan. 2014. Analytical Determination of Collisional Sheath Properties for Triple Frequency Capacitively Coupled Plasma. *IEEE Transactions on Plasma Science* 42, 3 (2014), 729–734.

[155] M Tanjidur Rahman, M Sazadur Rahman, Huanyu Wang, Shahin Tajik, Waleed Khalil, Farimah Farahmandi, Domenic Forte, Navid Asadizanjani, and Mark Tehranipoor. 2020. Defense-in-depth: A recipe for logic locking to prevail. *Integration* 72 (2020), 39–57.

[156] M Tanjidur Rahman, Qihang Shi, Shahin Tajik, Haoting Shen, Damon L Woodard, Mark Tehranipoor, and Navid Asadizanjani. 2018. Physical Inspection & Attacks: New Frontier in Hardware Security. In *2018 IEEE 3rd International Verification and Security Workshop (IVSW)*. IEEE, 93–102.

[157] Jeyavijayan Rajendran, Ozgur Sinanoglu, and Ramesh Karri. 2013. VLSI testing based security metric for IC camouflaging. In *2013 IEEE International Test Conference (ITC)*. IEEE, 1–4.

[158] Joseph Redmon, Santosh Divvala, Ross Girshick, and Ali Farhadi. 2016. You only look once: Unified, real-time object detection. In *Proceedings of the IEEE conference on computer vision and pattern recognition*. 779–788.

[159] Shams Ur Rehman, Ka Fei Thang, and Nai Shyan Lai. 2019. Automated PCB identification and defect-detection system (APIDS). *International Journal of Electrical & Computer Engineering (2088-8708)* 9, 1 (2019).

[160] Jordan Robertson and Michael Riley. 2018. The Big Hack: Amazon, Apple, Supermicro, and the Chinese Government. Bloomberg Businessweek. https://www.bloomberg.com/news/articles/2018-10-04/the-big-hack-amazon-apple-supermicro-and-beijing-respond [Accessed: Feb.27, 2021].

[161] Nikolay Rubanov. 2003. SubIslands: The probabilistic match assignment algorithm for subcircuit recognition. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 22, 1 (2003), 26–38.

[162] Makoto Sakakibara, Makoto Suzuki, Kenji Tanimoto, Yasunari Sohda, Daisuke Bizen, and Koji Nakamae. 2019. Impact of secondary electron emission noise in SEM. *Microscopy* 68, 4 (2019), 279–288.

[163] Hassan Salmani. 2016. COTD: Reference-free hardware trojan detection and recovery based on controllability and observability in gate-level netlist. *IEEE Transactions on Information Forensics and Security* 12, 2 (2016), 338–350.

[164] Hassan Salmani, Mohammad Tehranipoor, and Ramesh Karri. 2013. On design vulnerability analysis and trust benchmarks development. In *2013 IEEE 31st international conference on computer design (ICCD)*. IEEE, 471–474.

[165] Martin Salzer, Aaron Spettl, Ole Stenzel, Jan-Henrik Smått, Mika Lindén, Ingo Manke, and Volker Schmidt. 2012. A two-stage approach to the segmentation of FIB-SEM images of highly porous materials. *Materials Characterization* 69 (2012), 115–126.

[166] Esha Sarkar and Michail Maniatakos. 2019. On automating delayered IC analysis for hardware IP protection. In *Proceedings of the International Conference on Omni-Layer Intelligent Systems*. ACM, 205–210.

[167] Michael E Scaman and Laertis Economikos. 1995. Computer vision for automatic inspection of complex metal patterns on multichip modules (MCM-D). *IEEE Transactions on Components, Packaging, and Manufacturing Technology: Part B* 18, 4 (1995), 675–684.

[168] Martin Schobert. [n.d.]. GNU software degate. *Webpage: http://www. degate. org* ([n. d.]).

[169] Erich Schubert, Jörg Sander, Martin Ester, Hans Peter Kriegel, and Xiaowei Xu. 2017. DBSCAN revisited, revisited: why and how you should (still) use DBSCAN. *ACM Transactions on Database Systems (TODS)* 42, 3 (2017), 1–21.

[170] H Seiler. 1983. Secondary electron emission in the scanning electron microscope. *Journal of Applied Physics* 54, 11 (1983), R1–R18.

[171] Hao-Chiang Shao, Chao-Yi Peng, Jun-Rei Wu, Chia-Wen Lin, Shao-Yun Fang, Pin-Yen Tsai, and Yan-Hsiu Liu. 2020. From IC Layout to Die Photo: A CNN-Based Data-Driven Approach. *arXiv preprint arXiv:2002.04967* (2020).

[172] Qihang Shi, Nidish Vashistha, Hangwei Lu, Haoting Shen, Bahar Tehranipoor, Damon L Woodard, and Navid Asadizanjani. 2019. Golden Gates: A New Hybrid Approach for Rapid Hardware Trojan Detection using Testing and Imaging. In *2019 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. IEEE, 61–71.

[173] Yiqiong Shi, Bah-Hwee Gwee, Ye Ren, and Chan Wai Ting. 2012. Extracting functional modules from flattened gate-level netlist. In *2012 International Symposium on Communications and Information Technologies (ISCIT)*. IEEE, 538–543.

[174] Marek Sikul, Karel Novotny, Matthias Kemmler, and Andreas Rummel. 2018. SEM-Based Nanoprobing on In-Situ Delayered Advanced 10 nm Technology Node IC. In *2018 IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA)*. IEEE, 1–4.

[175] KS Sim, ME Nia, and CP Tso. 2011. Image noise cross-correlation for signal-to-noise ratio estimation in scanning electron microscope images. *Scanning* 33, 2 (2011), 82–93.

[176] KS Sim, ME Nia, and Chih Ping Tso. 2013. Noise variance estimation using image noise cross-correlation model on SEM images. *Scanning* 35, 3 (2013), 205–212.

[177] KS Sim, JTL Thong, and JCH Phang. 2004. Effect of shot noise and secondary emission noise in scanning electron microscope images. *Scanning: The Journal of Scanning Microscopies* 26, 1 (2004), 36–40.
[178] Sergei Skorobogatov. 2011. Physical attacks on tamper resistance: progress and lessons. In *Proc. of 2nd ARO Special Workshop on Hardware Assurance, Washington, DC*.
[179] Jessica Smith. 2013. Non-destructive state machine reverse engineering. In *2013 6th International Symposium on Resilient Control Systems (ISRCS)*. IEEE, 120–124.
[180] Ray Smith. 2007. An overview of the Tesseract OCR engine. In *Ninth International Conference on Document Analysis and Recognition (ICDAR 2007)*, Vol. 2. IEEE, 629–633.
[181] Ronald C Stogdill. 1999. Dealing with obsolete parts. *IEEE Design & Test of Computers* 16, 2 (1999), 17–25.
[182] Pramod Subramanyan, Nestan Tsiskaridze, Wenchao Li, Adria Gascón, Wei Yang Tan, Ashish Tiwari, Natarajan Shankar, Sanjit A Seshia, and Sharad Malik. 2013. Reverse engineering digital circuits using structural and functional analyses. *IEEE Transactions on Emerging Topics in Computing* 2, 1 (2013), 63–80.
[183] Shamik Sural, Gang Qian, and Sakti Pramanik. 2002. Segmentation and histogram generation using the HSV color space for image retrieval. In *Proceedings. International Conference on Image Processing*, Vol. 2. IEEE, II–II.
[184] Benjamin Tan, Ramesh Karri, Nimisha Limaye, Abhrajit Sengupta, Ozgur Sinanoglu, Md Moshiur Rahman, Swarup Bhunia, Danielle Duvalsaint, Amin Rezaei, Yuanqi Shen, et al. 2020. Benchmarking at the Frontier of Hardware Security: Lessons from Logic Locking. *arXiv preprint arXiv:2006.06806* (2020).
[185] Sanli Tang, Fan He, Xiaolin Huang, and Jie Yang. 2019. Online PCB Defect Detector On A New PCB Defect Dataset. *arXiv preprint arXiv:1902.06197* (2019).
[186] Mohammad Tehranipoor and Farinaz Koushanfar. 2010. A survey of hardware trojan taxonomy and detection. *IEEE design & test of computers* 27, 1 (2010), 10–25.
[187] Mark Mohammad Tehranipoor, Ujjwal Guin, and Domenic Forte. 2015. Counterfeit integrated circuits. In *Counterfeit Integrated Circuits*. Springer, 15–36.
[188] Zvi Terem, Gila Kamhi, Moshe Y Vardi, and Amitai Irron. 2004. Pattern search in hierarchical high-level designs. In *Proceedings of the 2004 11th IEEE International Conference on Electronics, Circuits and Systems, 2004. ICECS 2004.* IEEE, 519–522.
[189] Olivier THOMAS, SARL Texplained, and Dmitry Nedospasov. [n.d.]. On the Impact of Automating the IC Analysis Process. ([n. d.]).
[190] JTL Thong, KS Sim, and JCH Phang. 2001. Single-image signal-to-noise ratio estimation. *Scanning* 23, 5 (2001), 328–336.
[191] Xiaojing Tian, Liang Zhao, and Huajun Dong. 2014. Application of image processing in the detection of printed circuit board. In *2014 IEEE Workshop on Electronics, Computer and Applications*. IEEE, 157–159.
[192] F Timischl, M Date, and S Nemoto. 2012. A statistical model of signal–noise in scanning electron microscopy. *Scanning* 34, 3 (2012), 137–144.
[193] Randy Torrance and Dick James. 2009. The state-of-the-art in IC reverse engineering. In *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 363–381.
[194] Patrick Trampert, Faysal Bourghorbel, Pavel Potocek, Maurice Peemen, Christian Schlinkmann, Tim Dahmen, and Philipp Slusallek. 2018. How should a fixed budget of dwell time be spent in scanning electron microscopy to optimize image quality? *Ultramicroscopy* 191 (2018), 11–17.
[195] Bruno Machado Trindade, Eranga Ukwatta, Mike Spence, and Chris Pawlowicz. 2018. Segmentation of Integrated Circuit Layouts from Scan Electron Microscopy Images. In *2018 IEEE Canadian Conference on Electrical & Computer Engineering (CCECE)*. IEEE, 1–4.
[196] Nidish Vashistha, Hangwei Lu, Qihang Shi, M Tanjidur Rahman, Haoting Shen, Damon L Woodard, Navid Asadizanjani, and Mark Tehranipoor. 2018. Trojan scanner: Detecting hardware trojans with rapid sem imaging combined with image processing and machine learning. In *ISTFA 2018: the 44th International Symposium for Testing and Failure Analysis*. ASM International, 256.
[197] Nidish Vashistha, M Tanjidur Rahman, Haoting Shen, Damon L Woodard, Navid Asadizanjani, and Mark Tehranipoor. 2018. Detecting Hardware Trojans Inserted by Untrusted Foundry Using Physical Inspection and Advanced Image Processing. *Journal of Hardware and Systems Security* 2, 4 (2018), 333–344.
[198] Arunkumar Vijayakumar, Vinay C Patil, Daniel E Holcomb, Christof Paar, and Sandip Kundu. 2016. Physical design obfuscation of hardware: A comprehensive investigation of device and logic-level techniques. *IEEE Transactions on Information Forensics and Security* 12, 1 (2016), 64–77.
[199] Narayanan Vijaykrishnan and N Ranganathan. 1996. SUBGEN: A genetic approach for subcircuit extraction. In *Proceedings of 9th International Conference on VLSI Design*. IEEE, 343–345.
[200] Paul Viola and Michael J Jones. 2004. Robust real-time face detection. *International journal of computer vision* 57, 2 (2004), 137–154.

[201] Sebastian Wallat, Nils Albartus, Steffen Becker, Max Hoffmann, Maik Ender, Marc Fyrbiak, Adrian Drees, Sebastian Maaßen, and Christof Paar. 2019. Highway to HAL: open-sourcing the first extendable gate-level netlist reverse engineering framework. In *Proceedings of the 16th ACM International Conference on Computing Frontiers*. 392–397.

[202] Huanyu Wang, Domenic Forte, Mark M Tehranipoor, and Qihang Shi. 2017. Probing attacks on integrated circuits: Challenges and research opportunities. *IEEE Design & Test* 34, 5 (2017), 63–71.

[203] Junping Wang, Junming Zhang, and Yue Hao. 2007. IC Image Segmentation Using Eigenvalue Clustering. In *2007 International Workshop on Anti-Counterfeiting, Security and Identification (ASID)*. IEEE, 184–187.

[204] Wei-Chien Wang, Shang-Liang Chen, Liang-Bi Chen, and Wan-Jung Chang. 2016. A machine vision based automatic optical inspection system for measuring drilling quality of printed circuit boards. *IEEE Access* 5 (2016), 10817–10833.

[205] Yuxin Wang, Yu-chen Karen Chen, and Wilson K Chiu. 2011. In Situ 3D Imaging and Characterization of Nano-Structures with X-ray Nano-CT Technique. *ECS Transactions* 35, 24 (2011), 21.

[206] Yiming Wen and Weize Yu. 2020. Combining Thermal Maps with Inception Neural Networks for Hardware Trojan Detection. *IEEE Embedded Systems Letters* (2020).

[207] Ronald Wilson, Rabin Y Acharya, Domenic Forte, Navid Asadizanjani, and Damon Woodard. 2019. A novel approach to unsupervised automated extraction of standard cell library for reverse engineering and hardware assurance. In *ISTFA 2019: 45th International Symposium for Testing and Failure Analysis*. ASM International, 249.

[208] Ronald Wilson, Navid Asadizanjani, Domenic Forte, and Damon L Woodard. 2019. First Auto-Magnifier Platform for Hardware Assurance and Reverse Engineering Integrated Circuits. *Microscopy and Microanalysis* 25, S2 (2019), 226–227.

[209] Ronald Wilson, Navid Asadizanjani, Domenic Forte, and Damon L Woodard. 2020. Histogram-based Auto Segmentation: A Novel Approach to Segmenting Integrated Circuit Structures from SEM Images. *arXiv preprint arXiv:2004.13874* (2020).

[210] Ronald Wilson, Domenic Forte, Navid Asadizanjani, and Damon Woodard. 2020. LASRE: A Novel Approach to Large area Accelerated Segmentation for Reverse Engineering on SEM images. In *ISTFA 2020: 46th International Symposium for Testing and Failure Analysis*. ASM International, To be published.

[211] Xiaolin Xu, Bicky Shakya, Mark M Tehranipoor, and Domenic Forte. 2017. Novel bypass attack and BDD-based tradeoff analysis against all known logic locking attacks. In *International conference on cryptographic hardware and embedded systems*. Springer, 189–210.

[212] Lei Yang and C-JR Shi. 2003. FROSTY: A fast hierarchy extractor for industrial CMOS circuits. In *ICCAD-2003. International Conference on Computer Aided Design (IEEE Cat. No. 03CH37486)*. IEEE, 741–746.

[213] Jing Yuan, Egil Bae, and Xue-Cheng Tai. 2010. A study on continuous max-flow and min-cut approaches. In *2010 ieee computer society conference on computer vision and pattern recognition*. IEEE, 2217–2224.

[214] SS Zakaria, A Amir, N Yaakob, and S Nazemi. 2020. Automated Detection of Printed Circuit Boards (PCB) Defects by Using Machine Learning in Electronic Manufacturing: Current Approaches. *MS&E* 767, 1 (2020), 012064.

[215] Vyacheslav L Zavadsky, Val Gont, Edward Keyes, Jason Abt, and Stephen Begg. 2009. Method of design analysis of existing integrated circuits. US Patent 7,580,557.

[216] Vyacheslav L Zavadsky, Val Gont, Edward Keyes, Jason Abt, and Stephen Begg. 2010. Method of design analysis of existing integrated circuits. US Patent 7,643,665.

[217] David Zhang, Gooitzen van der Wal, Phil Miller, David Stoker, Erik Matlin, Naveen Marri, Gary Gan, Joe Zhang, Jane Asmuth, Sek Chai, et al. 2019. *Fast, Full Chip Image Stitching of Nanoscale Integrated Circuits*. Technical Report. SRI International Princeton United States.

[218] Fengchao Zhang, Andrew Hennessy, and Swarup Bhunia. 2015. Robust counterfeit PCB detection exploiting intrinsic trace impedance variations. In *2015 IEEE 33rd VLSI Test Symposium (VTS)*. IEEE, 1–6.

[219] Nian Zhang and Donald C Wunsch. 2003. A fuzzy attributed graph approach to subcircuit extraction problem. In *The 12th IEEE International Conference on Fuzzy Systems, 2003. FUZZ'03.*, Vol. 2. IEEE, 1063–1067.

[220] Nian Zhang and Donald C Wunsch II. 2006. Speeding up vlsi layout verification using fuzzy attributed graphs approach. *IEEE Transactions on Fuzzy Systems* 14, 6 (2006), 728–737.

[221] Boyou Zhou, Aydan Aksoylar, Kyle Vigil, Ronen Adato, Jian Tan, Bennett Goldberg, M Selim Ünlü, and Ajay Joshi. 2020. Hardware Trojan Detection using Backside Optical Imaging. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* (2020).

[222] Juanhua Zhu, Ang Wu, and Xinping Liu. 2018. Printed circuit board defect visual detection based on wavelet denoising. In *IOP Conference Series: Materials Science and Engineering*, Vol. 392. 062055.