ARTICLE IN PRESS

Microelectronics Reliability xxx (xxxx) xxx–xxx

Contents lists available at ScienceDirect

Microelectronics Reliability

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

Automated detection of counterfeit ICs using machine learning

Bahar Ahmadi[a,*], Bahram Javidi[b], Sina Shahbazmohamadi[a]

[a] REFINE Lab., University of Connecticut, United States of America
[b] Department of Electrical and Computer Engineering, University of Connecticut, United States of America

ARTICLE INFO

Keywords:
Automatic defect detection
IC counterfeit detection
3D image processing
Machine learning

ABSTRACT

The electronic industry has been experiencing a growing counterfeit market, resulting in electronic supply chains in other industries to be prone to counterfeit parts as well. Over the past few years, several methods have been developed for evaluating the reliability of an IC and distinguishing them as counterfeit or authentic. Trained experts offer services for evaluating an IC based on destructive or non-destructive methods. However, defect detection and recognition are mostly dependent on human decision, and therefore are vulnerable to error. In this paper, we propose a method to automatically detect and identify die-face delamination on an IC die. Die-face delamination is a predominant internal defect in recycled ICs but can be easily missed during defect detection. Here, we have acquired the 3D image of an IC non-destructively using X-ray computed tomography and applied image processing techniques and machine learning algorithms on the 3D image to detect die-face delamination in the forms of thermally induced cracks and damaged surfaces.

1. Introduction

In recent decades, the counterfeit IC market has grown rapidly leaving electronic industry with considerable loss (the report on counterfeit part growth states four times increase in two years 2009–2011 [1]). In general, any unauthorized reproduction, or re-marking, altering and reselling a used electronic part as new is considered to be an act of counterfeiting. Counterfeit electronic components damage the economy of the electronics industry, and at the same time jeopardize the performance of final products. This matter grows in severity with more sensitive applications like biomedical devices or defense products. Counterfeit parts in such applications will not only decrease the performance and reliability, but also put human life in danger. Hence, it is important to investigate counterfeiting and ensure the authenticity of the provided parts from the supply chain. For this aim, US Department of Defense provides guideline of measures needed to be taken to control the supply chain and prevent the infiltration of counterfeit devices [2,3]. However, these procedures restrict the supply chain in the process of assuring that the components are received from reliable distributors. Such a solution is not practical for many electronic components that are no longer produced by their original manufacturer. The alternative is to develop methods to detect counterfeit parts prior to their use.

Several works have been done on the classification of counterfeit ICs [4–7]. Generally, counterfeit defects are categorized into two main categories, physical and electrical [5]. While the physical properties of the sample are subject to inspection during the physical counterfeit detection methods, electrical inspection mainly focus on testing the parametric and the functional features of it. Hence, although electrical inspection methods are non-destructive, and fast comparing to physical inspection methods, there is a great possibility that this method failed to capture a counterfeit component since the electrical evidence may be concealed professionally, and vice versa. However, in terms of general applicability, the physical inspection methods are the better one-size-fits-all solution, since electrical tests do not cover all scenarios, and specific procedure should be designed and set up for each IC. Most of the counterfeit electronic components that can be found in the supply chain are recycled and remarked from e-waste (electronic waste) [7]. These processes leave some trackable artifacts on ICs, that can be used to distinguish counterfeit ICs from authentic ones.

There are some methods developed to prevent counterfeiting and protect intellectual property (IP). Some propose utilizing RFID tags to add an encrypted number in the chip for tracings [8–11]. However, advanced reverse engineering tools allow attackers to have access to the code and present designers with challenges to overcome. Another method for detecting counterfeits is physical inspection. Most of these detection methods are based on visual observation of the IC by an expert. Several instruments can be employed like optical, X-ray, THz imaging, or electron microscopy. Considering the economic and time cost of training and using an expert, they are always prone to human

* Corresponding author.
E-mail address: bahar.ahmadi@uconn.edu (B. Ahmadi).

https://doi.org/10.1016/j.microrel.2018.06.083
Received 1 June 2018; Received in revised form 22 June 2018; Accepted 27 June 2018

error, and most of the developed tests lack metrics and measurable features [6]. Recently, some work was done on automating the detection process by employing machine learning algorithms. To name a few, K. Mahmood et al. proposed a real time counterfeit detection method on an X-ray image of an IC obtained by an X-ray microscope, and applied a trained machine learning algorithm [12]. In another work, Tehranipoor et al. detected scratches employing ANN on an IC packaging image acquired by an optical microscope [13]. However, detailed information on Die surface would be available on 3D image. Hence, in cases where counterfeiting occurs at the die level, none of the previous efforts are applicable, and there is no work on the literature on automatically processing the 3D image of an IC and detecting the defects. In this paper, we propose a novel method to automatically detect cracks on the IC die. We obtain a three-dimensional image of an IC with a Zeiss Xradia X-ray microscope. Although there are some concerns regarding the impact of X-ray radiation on the reliability of microelectronics, research has shown that no permanent damage on hardware and IC functionality occurs for tomography < 2 h [14,15]. MATLAB software is employed for processing the data. We apply image processing techniques to extract features from 3D data, and a logistic regression algorithm to identify the defect in a counterfeit IC.

2. Problem description

An IC's counterfeit defects may be visible on its packaging, lead frame, wiring, or die. A thorough list of defects that may be introduced to the IC during the reproduction process has been developed in [5]. Although the packaging defects can be detected through optical microscopy, internal information is required to investigate defects on the other parts of an IC.

In this paper, we are developing a method to detect and identify the defects caused by the recycling process of ICs in the form of die face delamination. These defects usually initiate as cracks on the corners of IC die and may propagate to the entire die face. [16,17] However, to be able to detect these defects on the die, information on the internal structure is required and it is most desirable to gain such information non-destructively. Having that in mind, X-ray micro-CT is the tool of choice for image acquisition. The resolution is defined by the CT system and scan parameters (i.e. source spot size and working distances, number of projection, etc.). The obtained 3D data is then fed into MATLAB for post-processing. The data is in the form of a 3D matrix such that each element corresponds to a voxel value. For example, the sample demonstrated in this paper has 652x677x671 uniform coordinates lattices, with gray scale, 16-bit unsigned data, and a uniform voxel size of (20.76 × 20.76 × 20.76) μm^3.

During the imaging, the sample was mounted so that the surface of the IC was located on the "*xz* plane". Fig. 1 displays the data coordinates with respect to the sample. As it is shown, the surface of the IC is parallel to "*xz* plane", and perpendicular to "*y* axis".

The acquired 3D image can also be considered as a stack of 2D images located on "*xz* plane", in which only a small number of slices (677 slices) contain the relevant information (Fig. 2). Therefore, the first step, the pre-processing stage, is to reduce the number of slices automatically to the slices that contain relevant information. The next step is the processing stage, where the die will be extracted and regions with the possibility of housing a defect will be detected. The last step is the decision stage. At this stage, features will be assigned to each selected region and be fed to the developed decision-making algorithm to declare whether the IC is counterfeit or authentic.

3. Processing and detection strategy

3.1. Pre-processing stage

At this stage we benefit from the physics of the tomography (rotation around and axis) and IC geometry information in the 3D data histogram, to automatically crop 3D data. Then we study the data in the Frequency domain, and propose a method to determine the slices that contain the relevant information.

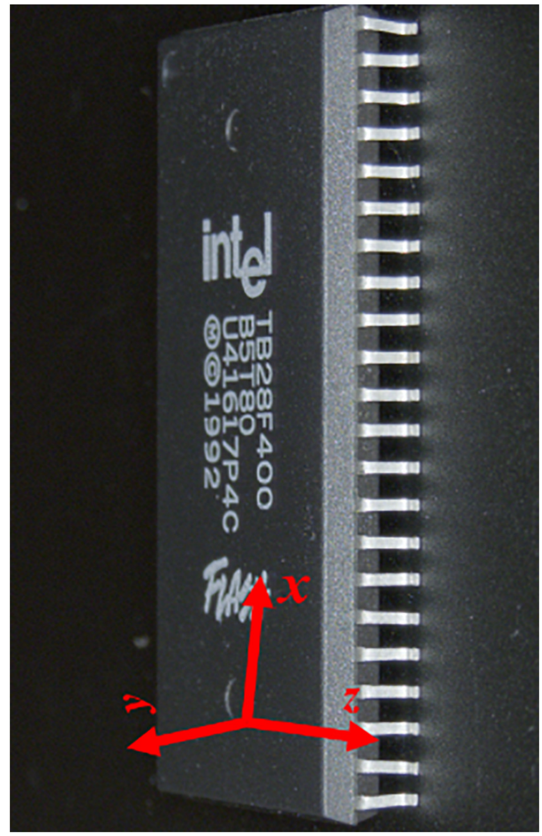

Fig. 1. Sample mounted in CT machine.

3.1.1. Automatic cropping of the 3D image

Computerized Tomography relies on reconstructing 2D images acquired while the sample is rotating around the axis perpendicular to the stage. The obtained 3D image is cylindrical. Since the IC is much thinner in one side, the *y*-direction here, compared to the *z*-direction, during the tomography, a large area of the medium around the sample is capturing as well. The value of the attenuation of air may change with a change of environment parameters. However, this tomography usually takes less than an hour, so we assume that the attenuation does not change during the tomography. Hence there is a large area on the data representing the air, and in the data histogram, this value of the air's attenuation corresponds to the highest number (Fig. 3). The images with the relevant information have pixel values higher than the air's. These facts have been employed to choose the threshold on the cropping algorithm.

The algorithm computes the median of each image on "*xy*", "*xz*", and "*yz*" plane, and compares it with the selected threshold. Applying the cropping algorithm to the 3D data leads to a new dataset of the size 480 × 480 × 629. Fig. 4 shows the histogram of the cropped data.

3.1.2. IC isolation

The number of slices of the output is reduced from 677 to 480, however, only a fraction of this number contains the die. For sifting out the desired slices, the data is studied in the Fourier domain. Fig. 5 demonstrates images in the frequency, and spatial domains for some selected slice numbers. The distributions of the image of each slice in the frequency domain (shown in Fig. 6), have two main characteristics:

1. They all are similar to the normal distribution.