WWW.IJRPR.COM

**International Journal of Research Publication and Reviews**

Journal homepage: www.ijrpr.com ISSN 2582-7421

# AI-POWERED TERAHERTZ VLSI TESTING TECHNOLOGY FOR ENSURING HARDWARE SECURITY AND RELIABILITY

***Dr. Nagendra Kumar M, Hamsa V***

*Dept of ECE, SJCIT, Chickaballapur, India*
*Email ID: mnnagendrakumar72@gmail.com, hamsav068@gmail.com*

**ABSTRACT**

The famous statement of Nano technology, the Moore's law says that "In the scaling of IC's the number of transistors in a chip doubles every two years", which headed a lot of research in Nano world.

The growing complexity of digital and mixed-signal systems makes hardware cybersecurity increasingly challenging yet vital to develop robust methods to assess and confirm the reliability and authenticity of ICs. It has become a key issue, especially for very large integrated circuits. If counterfeit, forged, or defective ICs present a significant threat to system reliability and security.

They introduced a new terahertz testing method for non-destructive and unobtrusive identification of counterfeit, damaged, forged or defective ICs by measuring their response to incident terahertz and sub-terahertz radiation at the circuit pins and analyzing the response using artificial intelligence (AI). These responses create unique signatures for ICs. We generated 2D images by measuring the response on a selected pin of a radio frequency IC (RFIC) scanned by a focused terahertz radiation.

***Keywords***— *Terahertz, hardware cyber security, reliability, authentication*

## 1. INTRODUCTION

With ever-increasing complexity, electronic devices and circuits have become more prone to various security threats. Deliberate alterations can be introduced to highly complex integrated circuits (ICs) at the design, fabrication or packaging stages. Unintended materials and device failures can happen due to the effects such as limited lifetime, premature material deterioration, unpredicted external conditions and short channel effects. Finally, legitimate components and systems can be replaced with the counterfeit ones during shipments. Specifically, the growing use of foreign off-the-shelf components makes faked integrated circuits with additional built-in secret components and/or with malicious software implemented in hardware to be an increasing and powerful hardware security threat.

Moreover, considering the fast aging of the widely deployed cyber infrastructure, it is vital to develop preventive measures and response strategies against all hardware security threats to avoid catastrophic and irreversible consequences.

Compromised or untrusted ICs can endanger all additional layers of national or international cyber systems and lead to devastating and far-reaching consequences. It is difficult, even unattainable, to ensure full fault detection using conventional AC and DC electrical testing techniques. An additional security issue comes from fake circuits designed to avoid identification by conventional testing techniques.

## 2. EXISTING TECHNOLOGIES

**TERAHERTZ SCANNING SYSTEMS:**

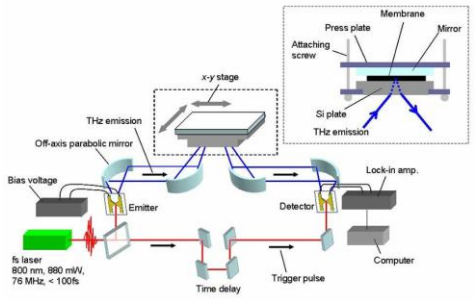

**Fig 2.1 Schematic diagram of the terahertz imaging system based on a THz-TDS.**

Figure 2.1 shows the schematic diagram of the terahertz imaging system based on a THz-TDS. The packaging materials of authentic and counterfeit ICs might differ. Based on the package materials properties, the effective refractive index and amplitude extinction coefficient vary significantly.

**IMPEDANCE BASED IC TESTING:**

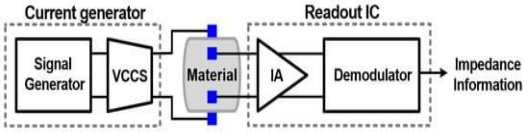


**Fig 2.2 Block Daigram of Impedence based IC Testing.**

Figure 2.2 shows the block diagram of Impedence based IC Testing. The impedance is a function of frequency and signal path within a circuit due to the complex mutual coupling effects at RF and higher frequencies.

**X-RAY IMAGING FOR IC :**

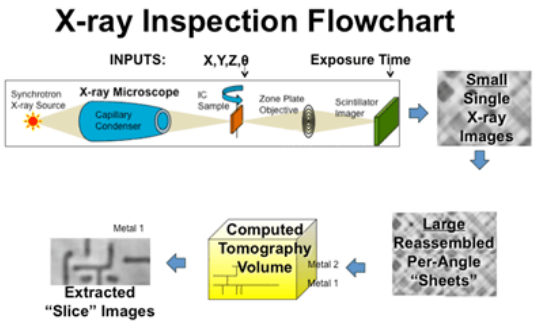


**Fig 2.3 X-ray inspection flowchart of IC**

Figure 2.3 shows the flowchart of X-ray inspection of IC. This method of non-destructive reverse engineering of electronic chips could check that chip manufacturing was done according to the original design.

## 3. RECOMMENDED SOLUTION

**BRIEF:TERAHERTZ RESPONSE BASED IC TESTING:**

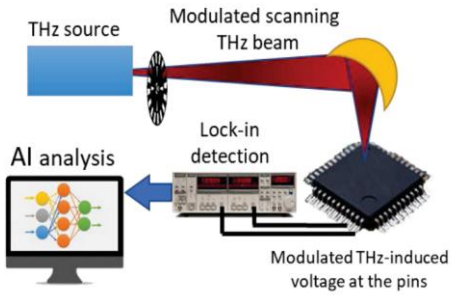


**Fig 3.1 Schematic presentation of the terahertz scanning setup for generating Spatial terahertz response map for AI based image processing.**

Figure 3.1 shows schematic presentation of the terahertz scanning setup for generating spatial terahertz response map for AI based image processing. The successful deployment of terahertz systems requires a solid understanding and accurate modeling of wireless channel conditions (propagation characteristics) between the transmitter and receiver.

Ultimately, terahertz communications will require a large and dedicated effort in system-wide channel sounding. This is the experimental technique of measuring a wireless communication channel, with all of its various complications. Results of channel sounding will be married to channel modeling for future communication systems to be predictably engineered. Summarily, the goal of channel sounding is to determine the complex channel impulse response (CIR) (or frequency response due to duality) of a wireless communication channel.

## 4. METHODOLOGY

**TERAHERTZ IC SCANNING SYSTEMS:**

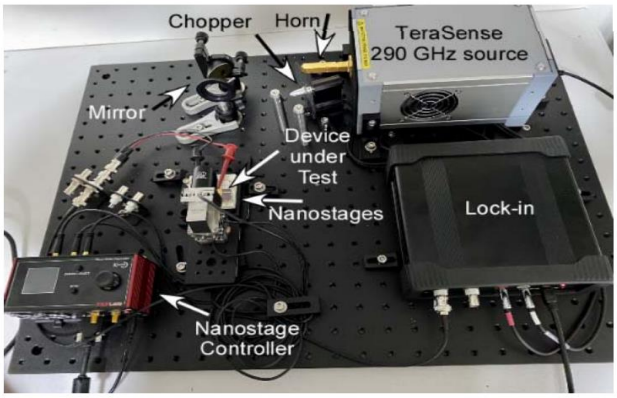


**Fig 4.1 Experimental setup for terahertz IC scanning**

Figure 4.1 shows the experimental setup of terahertz IC scanning. The samples that were wire-bonded on the chip carriers placed on three-axis nano-stages controlled with a computer connected KIM101 controller and had the steps down to 5 µm. The Stanford Research SR830 DSP lock in-amplifier measured the response with an optical chopper. Custom LabVIEW codes performed all the equipment control and data acquisition.

A recent example of the SC method was implemented at 300 GHz, offering sounding of dynamic channels with a 444 ns measurement window, with 108.5 ps (3.25 cm) resolution. It also features up to 17,590 CIR/s measurements and can distinguish Doppler shifts of up to 8.8 kHz (equivalent max speed of 31.7 km/h).

**DEEP.LEARNING–CONVOLUTION.NEURAL NETWORK (CNN):**

Many signal processing and communications system challenges still need to be addressed. The factors to be considered in signal processing in the THz realm differ significantly from those in the systems at lower frequencies; they are closely linked to the transceiver or device architectures.

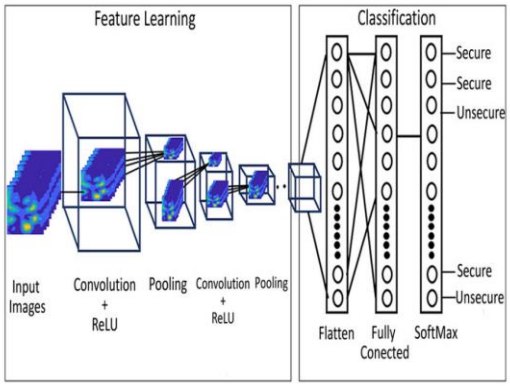


**Fig 4.2 Basic model of Convolution Neural**

**NETWORK (CNN):**

Figure 4.3 shows the basic model of Convolution Neural Network (CNN). The convolution operation is intended to extract high level features from the input image, such as edges. For CNN to capture the low-level features such as edges, color, and gradient orientation, only one convolution layer is required.

## 5. RESULTS

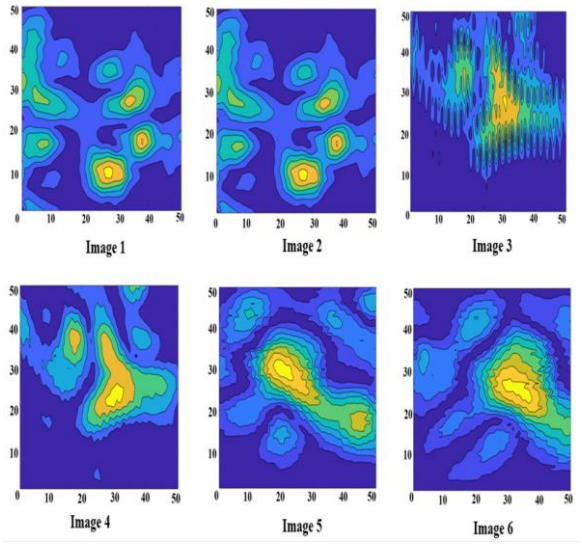


**Fig 5.1 Measured position dependent DC response at a selected pin of the tested IC while a 0.289 THz beam is scanned in 2D**

Figure 5.1 shows the Measured position dependent DC response at a selected pin of the tested IC while a 0.289 THz beam is scanned in 2D. The response measured at the selected in of the same device under the same biasing conditions. The image 1 and image 2 are results of the two subsequent scans. These two images illustrate the reproducibility of our technique. The height of the device holder was then changed for the next scans resulting in images 3 to 6. The differences in the measured scans 2 to 6 are due to the different focal point in the vertical direction.

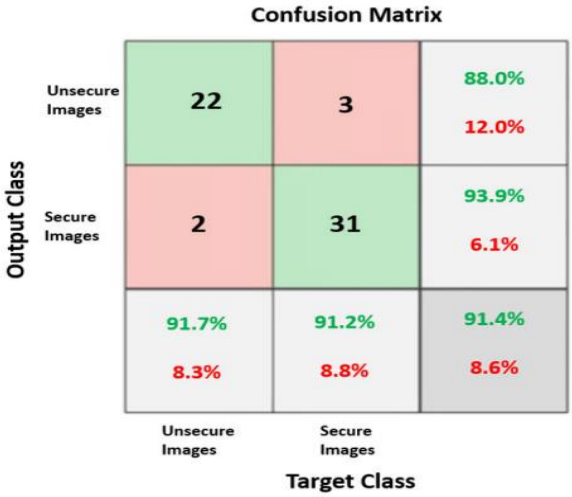


**Fig 5.2 Confusion matrix**

Figure 5.2 shows the confusion matrix A confusion matrix is a method to summarize the predicted results of a classification algorithm's performance. Using the Approach 3, they processed 288 images (168 secure images and 120 unsecure images) out of which, 80% were used for training, and 20% were used for testing. They have used the testing dataset (33 secure and 25 unsecure, totalling 58 images) to plot the confusion matrix shown in Figure 5.2.

## 6. ADVANTAGES AND APPLICATIONS

**ADVANTAGES:**

- Non destructive and unobtrusive identification of counterfeit, damaged, forged or defective ICs.
- Powerful hardware security scope.
- Proposed approach does not affect the IC specification or operation.
- Can provide detailed IC signatures and design malfunctions.

**APPLICATIONS:**

- IC foundries
- Manufacturing Industries

## REFERENCES


[1] A Gattiker, P Nigh, and R Aitken, An overview of integrated circuit testing methods, in Proc. ASM Int. Microelectron, 2019, pp. 634–642.

[2] D Hély, K Rosenfeld, and R Karri, Security challenges during VLSI test, in Proc. IEEE 9th Int. New Circuits Syst. Conf. (NEWCAS), Jun. 2011, pp. 486–489.

[3] N S Balbekin, M S Kulya, P Y Rogov, and N V Petrov, The modeling peculiarities of diffractive propagation of the broadband terahertz two dimensional field, Phys. Procedia, vol. 73, Jan. 2015, pp. 49–53.

[4] P Aryan, S Sampath, and H Sohn, An overview of non-destructive testing methods for integrated circuit packaging inspection, Sensors, vol. 18, Jun. 2018 , no. 7.

[5] S M Rooks, B Benhabib, and K C Smith, Development of an inspection process for ball-grid-array technology using scanned-beam X-ray laminography, IEEE Trans. Compon., Package., Manuf. Technol., A, vol. 18, no. 4, Dec. 1995, pp. 851–861.

[6] Y J Roh, K W Ko, H Cho, H C Kim, H Joo, and S K Kim, Inspection of ball grid array (BGA) solder joints using X-ray cross-sectional images, in Proc. 8th Mach. Vis. Syst. Inspection Metrol., vol. 3836, Aug. 1999, pp. 168–178.