Detection of Unusual Thermal Activities in a Semiconductor Chip Using Backside Infrared Thermal Imaging

Swapnil S. Salvi
Mechanical and Aerospace Engineering Department,
University of Texas at Arlington,
Arlington, TX 76019

Ankur Jain[1]
Mechanical and Aerospace Engineering Department,
University of Texas at Arlington,
Arlington, TX 76019
e-mail: jaina@uta.edu

Rapid detection of hardware Trojans on a semiconductor chip that may run malicious processes on the chip is a critical and ongoing security need. Several approaches have been investigated in the past for hardware Trojan detection, mostly based on changes in circuit parameters due to Trojan activity. Chip temperature is one such parameter that is closely related to the degree of Trojan activity. This paper carries out backside infrared (IR) imaging of a two-die three-dimensional integrated circuit (3D IC) thermal test chip in order to detect unusual thermal activities on the chip. Four distinct image processing algorithms are evaluated and compared in terms of speed, accuracy, and occurrence of false positives and negatives. The impact of background thermal activity and finite duration of Trojan activity on the accuracy of detection is investigated. Within the parameter space tested in this work, the histogram method is found to be the most effective at Trojan detection in the 3D IC. Modifications in data analysis techniques are proposed that improve Trojan detection performance. This work may help develop thermal imaging as a means for real-time Trojan detection and enhancement of security of modern semiconductor chips, including 3D ICs. [DOI: 10.1115/1.4049291]

Keywords: Trojan detection, infrared thermography, three-dimensional integrated circuit, data analysis, image processing

1 Introduction

The security of modern microprocessors and other semiconductor chips is of critical importance, particularly for sensitive applications, such as defense and finance. Due to the highly distributed nature of design, manufacturing and assembly, semiconductor chips have become increasingly vulnerable to hardware and software Trojans. A hardware Trojan is any unidentified circuit that can access, distort, or disable ongoing operations anonymously [1]. The intended or unintended introduction of an undesired circuit element could occur, for example, at an external foundry or chip packaging company that simultaneously serves multiple clients across the globe. A software Trojan could be introduced in a network attack on the chip. Even though a software Trojan does not involve physical alterations in the chip, it can have similarly deleterious effect on chip operation. Rapid detection and disablement of Trojans—both hardware and software—is a critical security need for semiconductor chips [2,3].

Trojan detection is inherently challenging due to the stealthy nature of the Trojan, the behavior or characteristics of which are not known in advance and may change over time [4]. Accuracy, cost and speed of detection are key figures of merit for any Trojan detection approach. A good detection technique must minimize the likelihood of false negatives—when the detection method fails to identify a Trojan-related activity—and false positives—when an activity is detected to be Trojan-related, but is, in fact, benign.

While a hardware Trojan may, in principle, be detected using destructive testing and reverse engineering, such an approach is expensive, time-consuming, and unlikely to be practical [5]. Several nondestructive methods have been proposed for Trojan detection. These methods can be broadly categorized into side-channel analysis and full Trojan activation, also known as logic testing method [6]. Side-channel analysis methods track changes in circuit parameters such as impendence, current or power [3,7,8], path delays [9,10], and surface temperature [11], which are generally side effects of Trojan activity. The efficacy of side channel analysis depends on the magnitude of side-channel signal generated by the Trojan, which malicious players strive to keep to a minimum [2]. Logic testing methods seek to find the set of test vector patterns that, when applied to the chip, maximizes the probability of activating available hardware Trojans [12], and are often used to enhance the side-channel analysis method.

Side-channel analysis based on current or power measurements determines and compares the circuit power ratio to that of a known, trusted chip, also called as a golden integrated circuit (IC) [13]. The need for a golden IC can be eliminated by comparing IC current signatures at two different times to detect abnormal patterns and spot a hardware Trojan [7]. Path delay-based side-channel analysis methods work on generating and detecting anomalies in path delay [9,10]. The key benefit of this approach is that the Trojan does not even need to be activated for detection [14]. On-chip sensors have also been used for detecting side-channel signals [15,16], including current/power sensors [17,18] and delay counters [19,20]. Side-channel signal measurements such as localized electromagnetic emanation [21] have also been used to detect unusual patterns due to hardware Trojan activation. Synergistic combination of multiple side-channel signals has been investigated. For example, combination of current with delay [22], current with maximum frequency [4], and time with electromagnetic measurements [23] has been shown to offer improved detection than analysis based on only one signal. The logic testing approach has also been used in conjunction with side-channel analysis to improve the performance of signal measurements and improve the accuracy of Trojan detection [4,24].

Infrared (IR)-based thermography has traditionally been used in the semiconductor industry for surface temperature measurement [25,26], detecting defective chips [27], hotspot detection [28,29], etc. In principle, Trojans are intended to draw minimal current and remain undetected. Nevertheless, abnormal circuit activity

[1]Corresponding author.

Contributed by the Electronic and Photonic Packaging Division of ASME for publication in the Journal of Electronic Packaging. Manuscript received March 25, 2020; final manuscript received May 7, 2020; published online February 22, 2021. Assoc. Editor: Ronald Warzoha.

due to a Trojan is expected to cause some distortion in the temperature field of the chip due to Joule heating. Some literature is available on the use of this thermal signal for hardware Trojan detection using infrared imaging and image processing approaches. In general, the temperature field from an IR camera is represented as time-varying matrices, which are analyzed for detecting a hardware Trojan. Two-dimensional principal component analysis has been used to calculate and compare the Euclidean distance between the test chip and a benchmark chip [5]. Unsupervised clustering methods have been used for hardware Trojan detection without the need for a benchmark chip [30]. Similarly, application of Kalman filters on the difference matrices of IR thermal images at two different time periods has been used for hardware Trojan detection [31,32]. Most of this past work pertains to traditional, planar chips. In contrast, detection on a three-dimensional (3D) IC [33] —which refers to a stack of multiple die that are electrically interconnected with each other—have not been investigated much.

This paper presents measurement of temperature field of the transistor plane of a two-die 3D IC thermal test chip through infrared imaging from the backside of the top chip. Due to the infrared-transparent nature of bulk Silicon and infrared-opaque nature of insulation layers above transistors, this facilitates direct thermal imaging of the transistor plane. The occurrence of unusual thermal activities mimicked through Joule heating in embedded metal resistors is detected through image analysis. The performance of a number of image analysis algorithms is benchmarked and compared. While past work is available on temperature-based detection in traditional, planar chips, this work specifically investigates a two-die 3D IC and suggests possible mechanisms for improved Trojan detection in a 3D IC. Results from this work can be utilized to develop improvised real-time algorithms for quick and effective Trojan detection techniques.

2 Experimental Setup

Experiments are carried out to investigate the use of backside infrared thermal imaging to predict the onset of Trojan-related unusual activity on the chip. For these experiments, a two-die, 3D IC is used [34]. Figures 1(*a*) and 1(*b*) show top view and cross-sectional view schematics of the 3D IC. This 3D IC has two unequally sized die bonded face-to-face to each other. Each chip has two embedded metal resistors of around 500 Ω each on the M7 layer. The 3D IC is bonded on to a leadless chip carrier substrate such that the backside of the top die is optically accessible. I/O pads on the periphery of the larger sized, bottom die are wire-bonded to bond pads on the substrate. The substrate is, in turn, mounted on a ceramic socket. This enables electrical access to various features on both die of the 3D IC. A Keithley 2602B power source is used for passing current through the metal resistors on each die.

Figure 2(*a*) shows a picture of the experimental setup, including the two-die 3D IC packaged in a chip carrier and socket. Figure 2(*b*) shows a close-up view of the 3D IC. A FLIR A6703sc IR camera with 640×512 pixel resolution and 15 μm pixel pitch is used. Infrared emission is measured at 100 Hz frequency and converted to temperature field. The camera is mounted to focus on the bare backside of the top chip of the 3D IC. Infrared data are acquired using ResearchIR software (Flir Systems, Inc., Nashua, NH) and analyzed using MATLAB. Temperature maps obtained from emissivity field measurements are stored in the form of matrices A_n, where n depicts the time-step. The backside of the top chip is not coated with graphite because in this case, the interest is in imaging temperature distribution on the transistor plane, and not the chip backside. By not having an IR-opaque graphite layer on the backside—as is customary for surface IR thermography—the IR camera in this case is able to directly measure the temperature field on the transistor plane instead of the backside temperature. The impact of a graphite layer on the die backside is discussed in more detail in Sec. 4.4.

The thermal effect of Trojan activity is mimicked through Joule heating in independently addressable top and bottom die resistors in the thermal test chip, as shown in Fig. 1. The use of Joule heating that mimics a hardware Trojan on either the top or bottom die of the 3D IC facilitates analysis of different possible Trojan activity levels. Experiments are carried out to investigate a variety of Trojan activity scenarios, which includes variations in heating current from 0.1 mA to 25 mA for the resistors in the top and bottom die. In each case, the capability of detection, including speed, accuracy, and occurrence of false positives and negatives, is investigated.

3 Image Processing Techniques

Figure 3 shows a schematic of the data acquisition and analysis framework used in this paper. Following image acquisition as described in Sec. 2, data at various times are analyzed using four distinct image processing algorithms. Background subtraction, binary conversion, and filtering are also carried out. The performance of the image process algorithms for such detection is characterized and compared. The fundamental premise behind anomaly detection is to compare successive thermal images in time with the ultimate thermal image of the chip—also called the standard image—in response to a thermal load and determine the minimum time at which the degree of similarity between the two exceeds a certain threshold. A comparison of the performance of these algorithms is carried out in terms of minimum detection time, occurrence of false positives and false negatives, etc.

A brief summary of the four image analysis algorithms used in this work is presented below.

3.1 Binary Comparison Method. In this method, the temperature field is converted into a binary signal based on comparison with a threshold value of the temperature. The threshold is chosen to be 0.55 times the average of ten highest temperature values. Image comparison is then carried out between the binary equivalents of the image matrix under consideration and the standard image matrix. The percentage similarity between the two is defined as the percentage of pixels with a binary one entry in the term-by-term product of the two matrices.

3.2 Structural Similarity Index Method. Structural similarity index method (SSIM) quantifies the similarity between two images by using three factors for comparison—luminance, contrast, and structure [35]. The SSIM index is calculated to be [36]

$$\mathrm{SSIM}(A,B) = \frac{(2\mu_A\mu_B + C_1)(2\sigma_{AB} + C_2)}{(\mu_A^2 + \mu_B^2 + C_1)(\sigma_A^2 + \sigma_B^2 + C_2)} \tag{1}$$

where A and B are the two images to be compared, and μ_A, μ_B, σ_A^2, σ_B^2, σ_{AB} are means for A and B, covariances for A and B, and the covariance between A and B, respectively. C_1 and C_2 are constants that are included to avoid instability [37]. A high value of SSIM calculated using Eq. (1) represents a large degree of similarity between the images being compared.

3.3 Two-Dimensional Correlation Coefficient Method. The two-dimensional (2D) correlation method compares the magnitudes and locations of peaks between the test and standard images. Specifically, the zero-normalized cross correlation is calculated as follows [38]:

$$\mathrm{corr}_2 = \frac{\sum_i \sum_j (f_{i,j} - f_\mu)(g_{i,j} - g_\mu)}{\sqrt{\left(\sum_i \sum_j (f_{i,j} - f_\mu)^2\right)\left(\sum_i \sum_j (g_{i,j} - g_\mu)^2\right)}} \tag{2}$$

where $f_{i,j}$ and $g_{i,j}$ are the two datasets to be compared and f_μ and g_μ are the averages of corresponding datasets. Similar to SSIM,

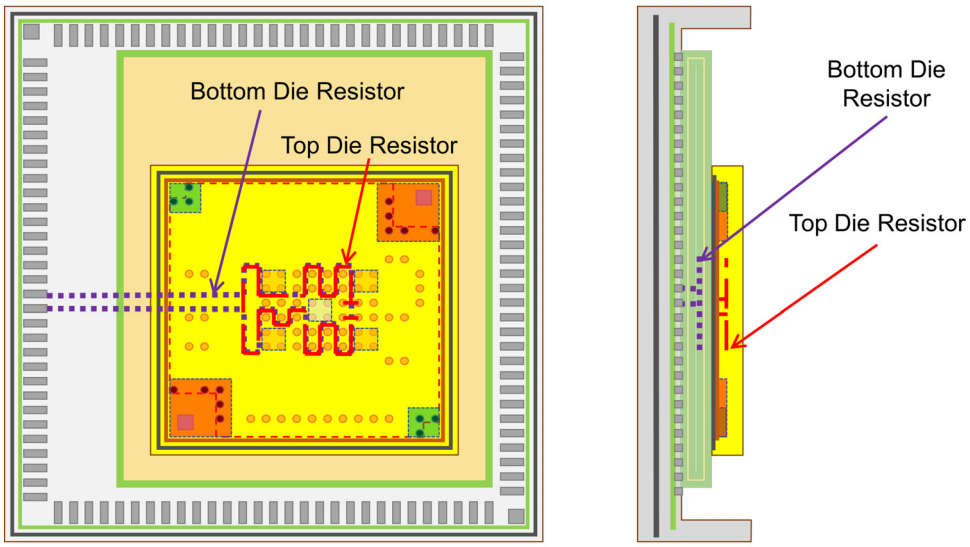

Fig. 1 Schematic picture of the two-die 3D IC used in this work. (*a*) and (*b*) show top and cross section views, respectively.

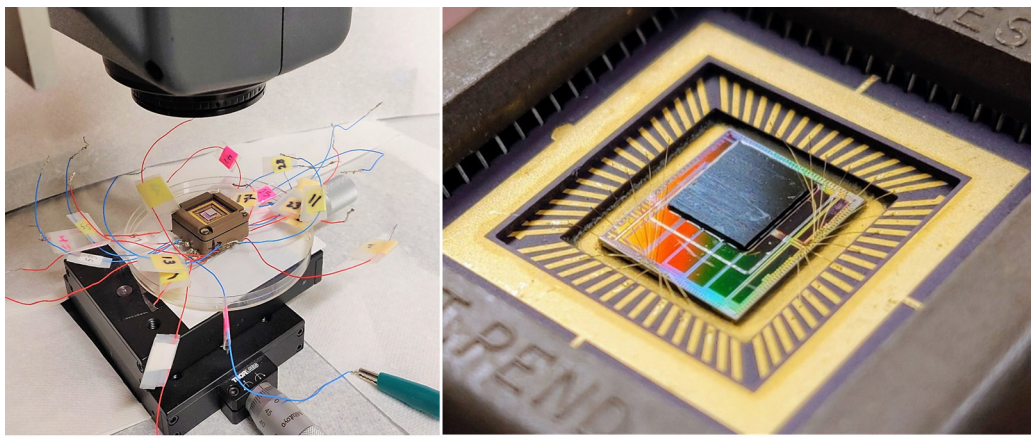

Fig. 2 Picture of the experimental setup. (*a*) shows the packaged 3D IC under the infrared camera and connected to an external power source; (*b*) shows a close-up view of the 3D IC—the two unequally sized die and wire bonds from the bottom die to the chip carrier are visible. In this configuration, the top-most surface of the 3D IC is the backside of the top die, through which, infrared thermography is carried out.

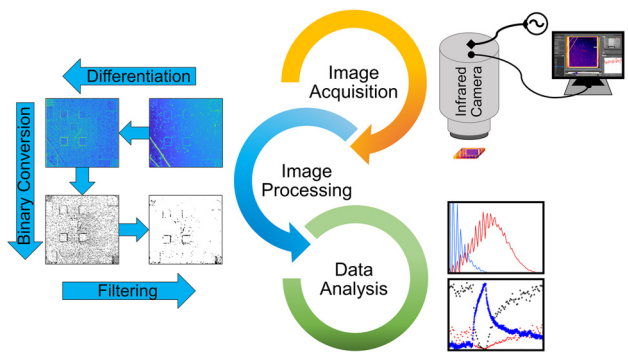

Fig. 3 Schematic of the computational framework used for data acquisition and analysis

the 2D correlation coefficient also represents a degree of similarity, although the specific values of the two parameters may differ. This correlation technique has been used in applications such as measurement of strain [38] and in-plane deformation [39].

3.4 Histogram Comparison Method. In this method, a vector, or histogram, containing the distribution of discrete pixel intensities of the differential thermal image is computed and used as the basis for comparison between a reference and test differential image [40]. The degree of similarity, defined as the average pairwise distance between the histograms of the two images, is computed. This pairwise distance is the difference between the probability density at every normalized pixel intensity for the two histograms plotted. Higher the pairwise distance, lower is the degree of similarity of test image against reference image. This approach is illustrated in Fig. 4, which plots the probability density as a function of normalized pixel intensity for a reference

image (no heating in the circuit, referred to as Dead Circuit) and a test image (10 mA current passing through the top die resistor, referred to as Active Circuit). This figure plots the number of pixels that correspond to a specific pixel intensity value. Both are plotted in normalized form. This figure shows, as expected, that the image for dead circuit has higher number of pixels with low intensity, i.e., less than 10% intensity, than the test image with active top die resistor. The histogram for test image appears to be normally distributed in the range of 0% to 35% of pixel intensity. Simulated hardware Trojan in active state produces heat due to Joule effect. The resulting change in the pixel intensity configuration of infrared image of the circuit can be easily traced by this method. Thus, sudden change in intensity of successive images will trigger the similarity index, which can be used to identify the Trojan activity.

4 Results and Discussion

4.1 Temperature Colormaps. Figures 5(*a*) and 5(*b*) present representative temperature colorplots at different times obtained from infrared imaging for experiments with 15 mA and 5 mA heating current through the top die resistor. In each case, measured temperature map at $t = 0$ s prior to passing the current is subtracted. In the 15 mA case shown in Fig. 5(*a*), a distinct signal is clearly detected even at 0.1 s, with the signal becoming more and more distinct at larger times. For the lower, 5 mA current case shown in Fig. 5(*b*), a similar detection is not visible as clearly at $t = 0.1$ s, but emerges much later due to the weaker heat generation. Figure 6 plots the average measured temperature rise as a function of time for multiple heating currents passing through the top die resistor. It is seen that the expected temperature rise for 5 mA and lower currents is quite low. While the distinction between the 15 mA and 5 mA cases can be seen visually in Fig. 5, quantitative signal processing methods are clearly desirable for systematic, real-time data analysis and Trojan detection, particularly at low activity levels.

4.2 Algorithm-Based Detection With Top Die Resistor Activated. The four image analysis algorithms discussed in Sec. 3 are applied on the differential images acquired from experiments with different currents passing through the top die resistor. Figures 7(*a*) and 7(*b*) plot the degree of similarity as a function of time for the four image analysis algorithms at 15 mA and 5 mA heating currents, respectively.

In the case of 15 mA case, each method exhibits sharp rise in the degree of similarity just after current activation. The histogram comparison approach reports the most rapid change in degree of similarity. On the other hand, the degree of similarity reported by SSIM method is relatively high even prior to current activation, due to which, the relative change in signal may be low.

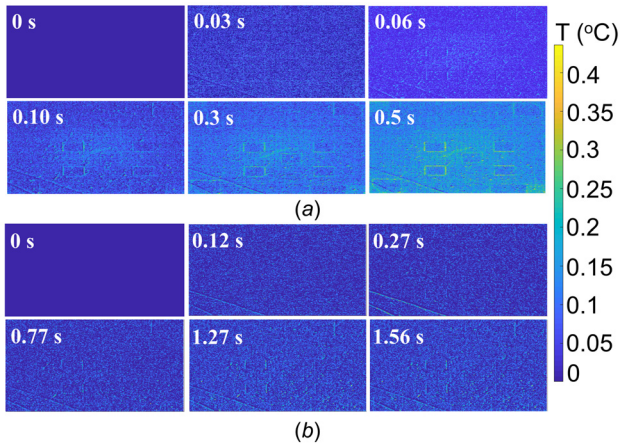

Fig. 5 Measured temperature maps on the top die, in response to (*a*) 15 mA and (*b*) 5 mA heating current in the top die resistor. Temperature maps are differential, after subtracting a baseline image prior to onset of heating.

Detection of a 5 mA signal—corresponding to only 12.5 mW power—is more challenging due to the lower heating rate. This case is shown in Fig. 7(*b*). In this case, the binary comparison and 2D correlation coefficient method fail to detect the onset of the heating activity—the predicted degree of similarity does not change appreciably following the onset of heating. On the other hand, the SSIM index and histogram comparison method work much better, and show a sharp increase in the degree of similarity. A key tradeoff between the two is that while the SSIM method jumps to 100% similarity faster, it does exhibit a high degree of similarity even prior to the onset of heating activity. This might cause SSIM to report more false negatives. On the other hand, histogram comparison method is much slower to report 100% similarity, but provides a greater contrast compared to the preheating measurement. As a result, the histogram comparison method may take longer and may report more false negatives, especially if the time window available for detection is short, but may be more immune to false positives. The final choice between the two algorithms may depend on the relative importance of fast detection and avoiding false positives/negatives in the specific application. It is possible that a hybrid evaluation that combines both methods could be employed to meet detection needs across this spectrum of requirements.

For further comparison of the four algorithms, experiments are repeated at a number of currents, up to 25 mA in the top die resistor. Figure 8 compares performance of the image analysis

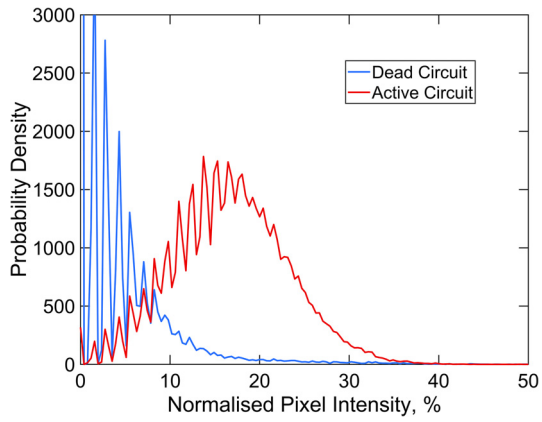

Fig. 4 Pixel probability density as a function of pixel intensity, as an illustration of the histogram comparison method

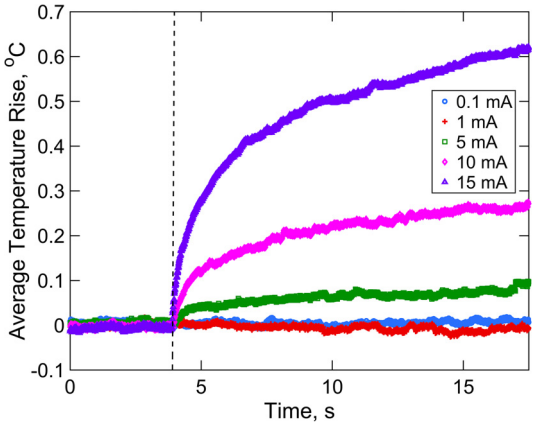

Fig. 6 Measured average temperature rise as a function of time for a number of heating currents in the top die resistor

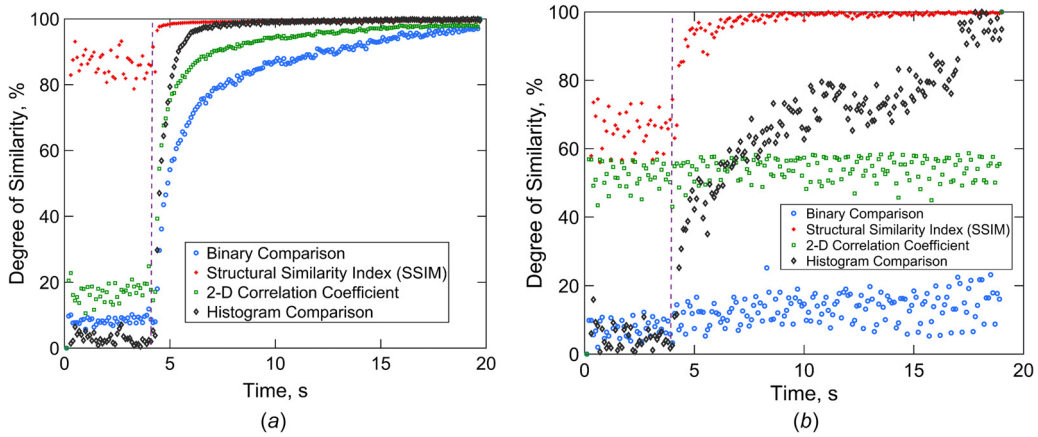

Fig. 7 Degree of similarity predicted by four different image processing algorithms as a function of time when the top die resistor is activated with (*a*) 15 mA and (*b*) 5 mA current

algorithms as a function of heating current. Figure 8 plots the mean difference in degree of similarity before and after starting the heating current in the top die. This allows comparison of the algorithms on a scale with same starting point. Higher mean difference in degree of similarity corresponds to a strong signal for identifying unusual thermal activities for a particular technique at a specific input current. Figure 8 shows that the use of binary comparison and 2D correlation coefficient method may not be effective for the detection of unusual thermal activities at lower signal. On the other hand, SSIM index and histogram comparison methods work well for small signals. The histogram comparison method exhibits a high difference in degree of similarity over the entire range of thermal signals, whereas the SSIM index method does saturate after a certain amount of current.

It is instructive to compare how the degree of similarity and average temperature rise change as functions of time. This is plotted in Fig. 9 for 5 mA heating in the top die resistor, i.e., carrying as less as 12.5 mW power. Data on degree of similarity are plotted only for SSIM and histogram comparison methods, since these appear to be more effective than the other two methods. The vertical dashed line represents the time at which the top die resistor is triggered. Figure 9 shows the even though the temperature rise may be very small (less than 0.1 °C), SSIM and histogram comparison methods are able to detect the thermal activity very quickly.

4.3 Algorithm-Based Detection of Heating Pulse With Background Thermal Activity. The set of experiments discussed is Sec. 4.2 imposed a heating current on the top die resistor representative of Trojan activity while the remaining chip is inactive. Also, the heating current stayed on throughout the experiment. In realistic conditions, Trojan activity must be detected in the presence of background thermal activity due to legitimate processes, and, in addition, the Trojan activity may last only a short time. To investigate the impact of these realistic considerations on detection accuracy, experiments are carried out where a single pulse of 10 mA current and 1 s duration is passed through the top die resistor to represent Trojan activity, while the bottom die resistor is either kept inactive, or is active with 10 mA current. Figures 10(*a*) and 10(*b*) plot the degree of similarity using SSIM index and histogram comparison methods as well as average temperature rise for these two scenarios. The location of the current pulse is shown using dashed line. Figures 10(*a*) and 10(*b*) show that the histogram comparison method accurately detects heating in the top die resistor, even in the presence of background thermal activity. The SSIM index method shows much greater noise, which may be an additional disadvantage. It is also interesting to note that the degree of similarity predicted by the SSIM index method decays very slowly following the end of the heating pulse, whereas the histogram method returns to the baseline level quite rapidly. Since there is more heat generated in active circuit case, the average

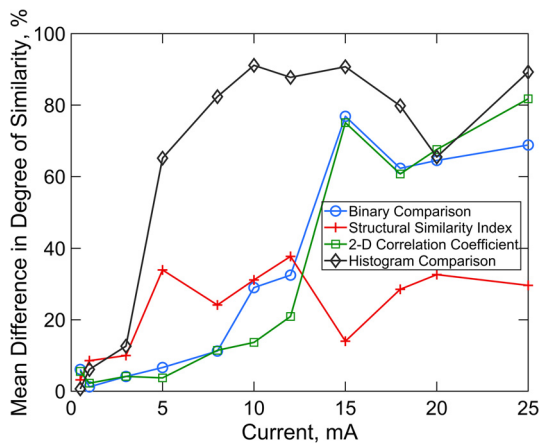

Fig. 8 Mean difference in degree of similarity before and after heating event for a number of heating current. Data are shown for four different image process algorithms.

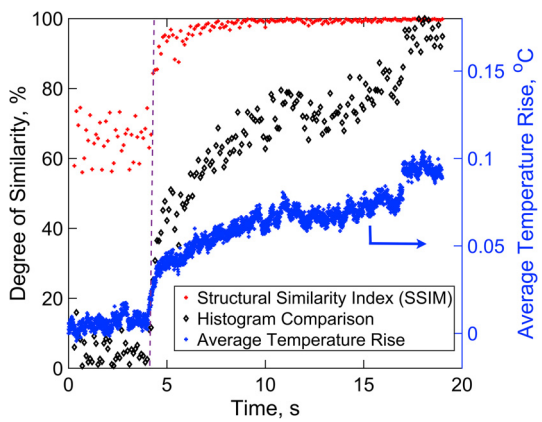

Fig. 9 Measured average temperature rise and degree of similarity plotted as functions of time for 5 mA heating current through the top die resistor. Data are shown for SSIM index and histogram comparison methods.

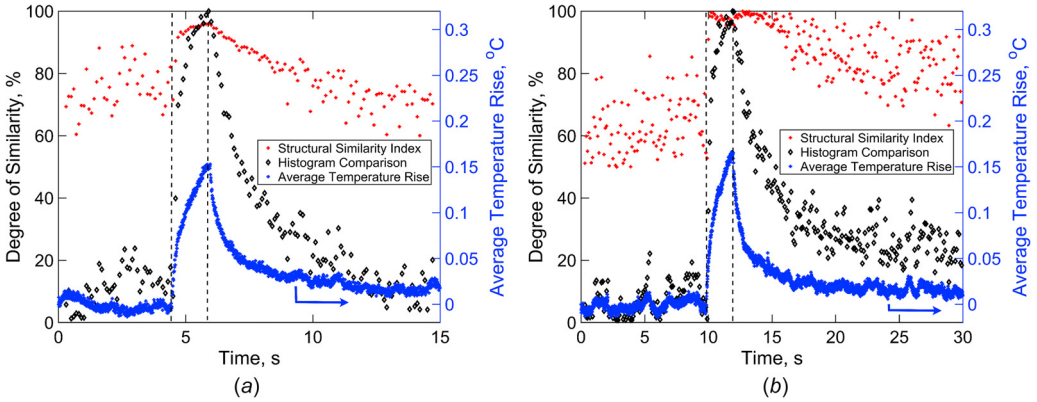

Fig. 10 Measured average temperature rise and degree of similarity plotted as functions of time for 5 mA pulsed heating current through the top die resistor. Data are shown for SSIM index and histogram comparison methods. (*a*) shows data without background heating and (*b*) shows data with background heating produced by 10 mA heating current through the bottom die resistor.

temperature rise in Fig. 10(*b*) is slightly higher than in Fig. 10(*a*). Note that Fig. 10 captures the thermal interactions between the two die in the stack, which is unique to the 3D IC architecture.

In order to demonstrate that additional data filtering can further facilitate Trojan detection, thermal noise reduction is carried out on the data shown in Fig. 10(*b*). Figure 11 presents these data in binary format, which helps understands the importance of thermal noise reduction. Figure 11(*a*) shows the thermal map before the heating current is passed, whereas Fig. 11(*b*) shows the thermal map at 2.1 s after both top die and bottom die resistors are heated with 10 mA current. The use of a median filter for noise reduction is demonstrated in Fig. 11(*c*). The median filter is a commonly used image processing tool, which reduces "salt and pepper" noise [41], such as the thermal noise observed in Fig. 11(*b*). The median filter replaces each pixel with the median value of a 3×3 matrix surrounding the pixel. As shown in Fig. 11(*c*), this significantly helps in noise reduction, thereby making it easier to detect unusual thermal activities. Specifically, with the use of median filter, the occurrence of false negatives that may be caused by thermal noise shown in Fig. 11(*b*) can be reduced significantly.

Finally, it is shown that the poor performance of binary comparison and 2D correlation coefficient methods at small current inputs can be improved by changing the emissivity value used to acquire temperature data from infrared images in RESEARCHIR software. Figures 12(*a*) and 12(*b*) plot the degree of similarity as a function of time for 5 mA heating current through the top die resistor predicted by these two methods. In each case, plots with emissivity values of 0.92 and 0.50 are both shown. Figures 12(*a*) and 12(*b*) show that lowering the emissivity significantly improves the performance of both methods. The degree of similarity remains flat despite the heating signal when the emissivity is 0.92, but there is a greater deviation when using a lower value of emissivity. Even though changing the emissivity value may result in inaccurate prediction of temperature, that may not be important since the goal here is to detect a thermal activity rather than accurately measure the temperature. It is interesting to note that there is little effect of emissivity on the accuracy of SSIM index or histogram comparison methods.

4.4 Validity of Backside Infrared Imaging. A key component of this work is the imaging of the chip from the backside in order to optically access the transistor plane. Backside imaging is more practical than frontside imaging since the frontside is usually occupied by electrical interconnection, as is the case in the chip used in this work. IR imaging of the backside of the chip still allows measurement of temperature field on the transistor plane because of the IR-transparent nature of silicon [26]. In order to independently confirm this, a separate experiment is carried out on a single-die Silicon chip comprising MOSCap circuits fabricated on the frontside. A thin graphite film is sprayed on the backside of one half of the chip while the other half is left bare. The chip is placed upside down on a hot plate maintained at 50 °C. Figure 13(*a*) shows a regular picture of the chip, whereas Fig. 13(*b*) shows an infrared image. Chip orientation is the same in both images. As shown in Fig. 13(*a*), the top half of the chip is

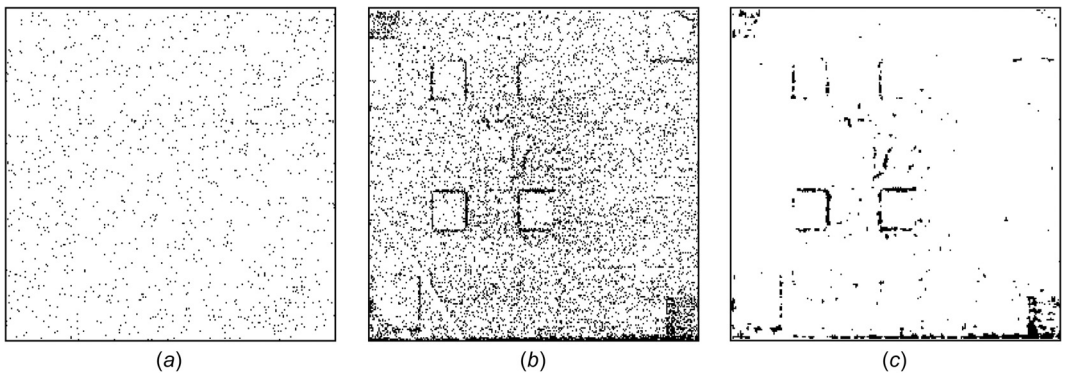

Fig. 11 Temperature maps after thermal noise reduction for the case of 5 mA heating pulse through the top die resistor, with background heating produced by 10 mA heating current through the bottom die resistor. (*a*) shows baseline state before the onset of current; (*b*) shows state 2.1 s after the onset of current; and (*c*) shows state after the onset of current, with the application of median filter.

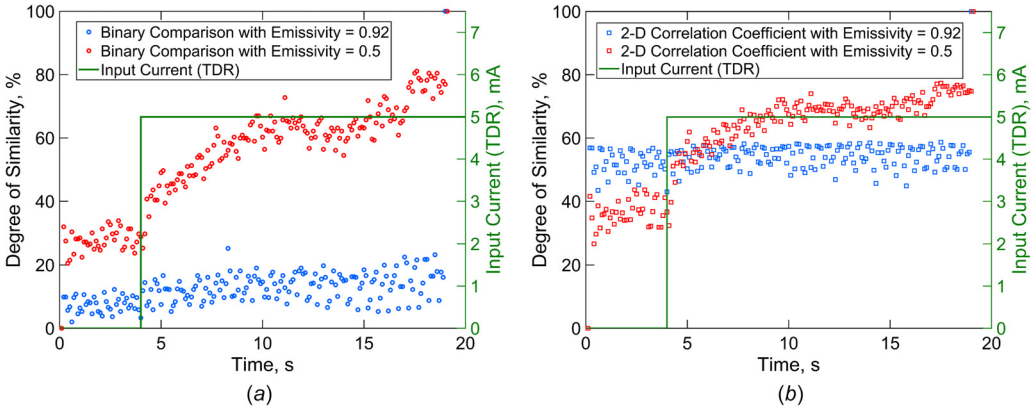

Fig. 12 Effect of change in the value of emissivity used in infrared thermography. (*a*) and (*b*) show the degree of similarity as a function of time for the case of 5 mA heating current through the top die resistor. Data are shown for (*a*) binary comparison method and (*b*) 2D correlation coefficient method.

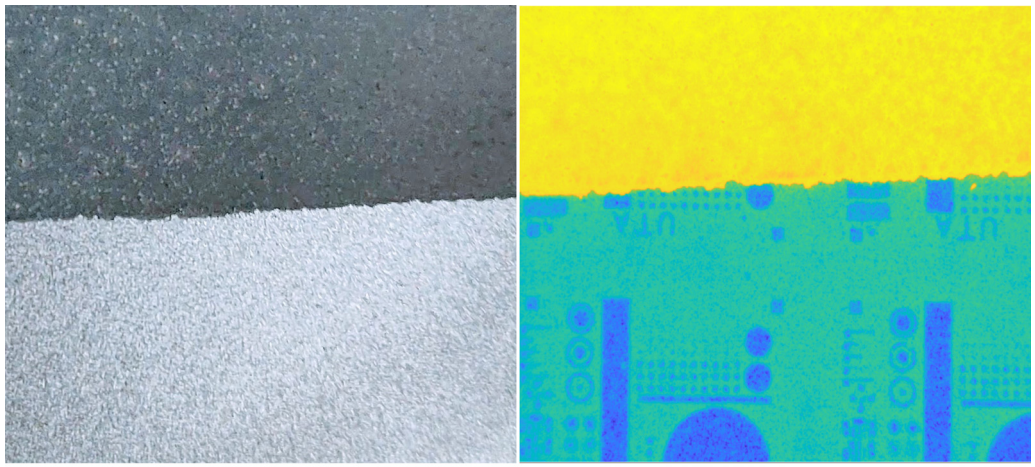

Fig. 13 Demonstration of the impact of graphite layer on the backside of a MOSCap imprinted Silicon die. Graphite is sprayed on the top half of the die. (*a*) and (*b*) show white light and infrared images of the die backside, respectively, when the chip is placed upside down on a hot plate maintained at 50 °C.

sprayed with graphite. IR imaging of the corresponding region is quite uniform, whereas IR imaging of the bottom half of the chip that is not sprayed with graphite reveals circuit features from the frontside. This shows that backside infrared imaging—without graphite coating—is able to access the transistor plane of the chip due to the infrared-transparent nature of silicon. This feature is a key enabler for IR-based Trojan detection because in most cases, only the backside of the chip is available for imaging. Note that the absolute temperature measured here is not as critical as the ability to detect frontside features, leading to detection of Trojan activity.

5 Conclusions

Chips that are fabricated and assembled globally, including by external manufacturers, are inherently prone to the insertion of malicious hardware. Detection of such hardware Trojans is an ongoing security concern. This work contributes toward this important technological need by examining the use of temperature signals to detect Trojans specifically for a 3D IC. Similar to any detection process, the time to detect and occurrence of false positives/negatives are important considerations, which are addressed in this paper. Four candidate image processing algorithms are compared, and strategies for improved performance are identified. The proposed techniques help the hardware Trojan effectively and can possibly be improved even further by a synergistic combination of multiple methods. Results presented in this work may help ensure the security of present and future semiconductor chips from hardware Trojans.

References

[1] Croteau, C. B., and Krishnankutty, D., 2017, "Cyber-Physical Security Research at UMBC's Eclipse Lab," ASME Mech. Eng., **139**(3), pp. S18–S23.
[2] Hu, N., Ye, M., and Wei, S., 2019, "Surviving Information Leakage Hardware Trojan Attacks Using Hardware Isolation," IEEE Trans. Emerg. Top. Comput., **7**(2), pp. 253–261.
[3] Nguyen, L. N., Cheng, C.-L., Prvulovic, M., and Zajic, A., 2019, "Creating a Backscattering Side Channel to Enable Detection of Dormant Hardware Trojans," IEEE Trans. Very Large Scale Integr. Syst., **27**(7), pp. 1561–1574.
[4] Narasimhan, S., Du, D., Chakraborty, R. S., Paul, S., Wolff, F. G., Papachristou, C. A., Roy, K., and Bhunia, S., 2013, "Hardware Trojan Detection by Multiple-Parameter Side-Channel Analysis," IEEE Trans. Comput., **62**(11), pp. 2183–2195.
[5] Hu, K., Nowroz, A. N., Reda, S., and Koushanfar, F., 2013, "High-Sensitivity Hardware Trojan Detection Using Multimodal Characterization," Design, Automation and Test in Europe Conference and Exhibition (DATE), Grenoble, France, Mar. 18–22, pp. 1271–1276.
[6] Tehranipoor, M., and Koushanfar, F., 2010, "A Survey of Hardware Trojan Taxonomy and Detection," IEEE Des. Test Comput., **27**(1), pp. 10–25.

[7] Narasimhan, S., Wang, X., Du, D., Chakraborty, R. S., and Bhunia, S., 2011, "TeSR: A Robust Temporal Self-Referencing Approach for Hardware Trojan Detection," IEEE International Symposium on Hardware-Oriented Security and Trust, San Diego, CA, June 5–6, pp. 71–74.
[8] Wang, Q., Chen, D., and Geiger, R. L., 2018, "Transparent Side Channel Trigger Mechanism on Analog Circuits With PAAST Hardware Trojans," IEEE International Symposium on Circuits and Systems (ISCAS), Florence, Italy, May 27–30, pp. 1–4.
[9] Amelian, A., and Borujeni, S. E., 2018, "A Side-Channel Analysis for Hardware Trojan Detection Based on Path Delay Measurement," J. Circuits, Syst. Comput., **27**(9), p. 1850138.
[10] Cha, B., and Gupta, S. K., 2013, "Trojan Detection Via Delay Measurements: A New Approach to Select Paths and Vectors to Maximize Effectiveness and Minimize Cost," Design, Automation and Test in Europe Conference and Exhibition (DATE), Grenoble, France, Mar. 18–22, pp. 1265–1270.
[11] Bao, C., Forte, D., and Srivastava, A., 2015, "Temperature Tracking: Toward Robust Run-Time Detection of Hardware Trojans," IEEE Trans. Comput. Des. Integr. Circuits Syst., **34**(10), pp. 1577–1585.
[12] Salmani, H., and Tehranipoor, M., 2012, "Layout-Aware Switching Activity Localization to Enhance Hardware Trojan Detection," IEEE Trans. Inf. Forensics Secur., **7**(1), pp. 76–87.
[13] Hou, B., He, C., Wang, L., En, Y., and Xie, S., 2014, "Hardware Trojan Detection Via Current Measurement: A Method Immune to Process Variation Effects," Tenth International Conference on Reliability, Maintainability and Safety (ICRMS), Guangzhou, China, Aug. 6–8, pp. 1039–1042.
[14] Xiao, K., Zhang, X., and Tehranipoor, M., 2013, "A Clock Sweeping Technique for Detecting Hardware Trojans Impacting Circuits Delay," IEEE Des. Test, **30**(2), pp. 26–34.
[15] Jin, Y., Maliuk, D., and Makris, Y., 2012, "Post-Deployment Trust Evaluation in Wireless Cryptographic ICs," Design, Automation and Test in Europe Conference and Exhibition, W. Rosenstiel, and L. Thiele, eds., Dresden, Germany, Mar. 12–16, pp. 965–970.
[16] Dubeuf, J., Hely, D., and Karri, R., 2013, "Run-Time Detection of Hardware Trojans: The Processor Protection Unit," 18th IEEE European Test Symposium (ETS), Avignon, France, May 27–30, pp. 1–6.
[17] Zhang, X., and Tehranipoor, M., 2013, "RON: An on-Chip Ring Oscillator Network for Hardware Trojan Detection," Design, Automation and Test in Europe, Grenoble, France, Mar. 14–18, pp. 1–6.
[18] Narasimhan, S., Yueh, W., Wang, X., Mukhopadhyay, S., and Bhunia, S., 2012, "Improving IC Security Against Trojan Attacks Through Integration of Security Monitors," IEEE Des. Test Comput., **29**(5), pp. 37–46.
[19] Davoodi, A., Li, M., and Tehranipoor, M., 2013, "A Sensor-Assisted Self-Authentication Framework for Hardware Trojan Detection," IEEE Des. Test, **30**(5), pp. 74–82.
[20] Kim, L. W., and Villasenor, J. D., 2015, "Dynamic Function Verification for System on Chip Security Against Hardware-Based Attacks," IEEE Trans. Reliab., **64**(4), pp. 1229–1242.
[21] Soll, O., Korak, T., Muehlberghuber, M., and Hutter, M., 2014, "EM-Based Detection of Hardware Trojans on FPGAs," IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), Arlington, VA, May 6–7, pp. 84–87.
[22] Cao, Y., Chang, C. H., and Chen, S., 2014, "A Cluster-Based Distributed Active Current Sensing Circuit for Hardware Trojan Detection," IEEE Trans. Inf. Forensics Secur., **9**(12), pp. 2220–2231.
[23] Ngo, X.-T., Exurville, I., Bhasin, S., Danger, J.-L., Guilley, S., Najm, Z., Rigaud, J.-B., and Robisson, B., 2015, "Hardware Trojan Detection by Delay and Electromagnetic Measurements," Design, Automation and Test in Europe Conference and Exhibition (DATE), Grenoble, France, Mar. 9–13, pp. 782–787.
[24] He, C., Hou, B., Wang, L., En, Y., and Xie, S., 2014, "A Novel Hardware Trojan Detection Method Based on Side-Channel Analysis and PCA Algorithm," Tenth International Conference on Reliability, Maintainability and Safety (ICRMS), Guangzhou, China, Aug. 6–8, pp. 1043–1046.
[25] Oh, S. K., Lundh, J. S., Shervin, S., Chatterjee, B., Lee, D. K., Choi, S., Kwak, J. S., and Ryou, J.-H., 2019, "Thermal Management and Characterization of High-Power Wide-Bandgap Semiconductor Electronic and Photonic Devices in Automotive Applications," ASME J. Electron. Packag., **141**(2), p. 020801.
[26] Pandey, P., Oxley, C., Hopper, R., Ali, Z., and Duffy, A., 2019, "Infra-Red Thermal Measurement on a Low-Power Infra-Red Emitter in CMOS Technology," IET Sci. Meas. Technol., **13**(1), pp. 25–28.
[27] Andonova, A., Angelov, G., and Chernev, P., 2014, "Diagnostics of Packaged ICs by Infrared Thermography," Proceedings of the 37th International Spring Seminar on Electronics Technology, Dresden, Germany, May 7–11, pp. 261–266.
[28] Hamann, H. F., Weger, A., Lacey, J. A., Hu, Z., Bose, P., Cohen, E., and Wakil, J., 2007, "Hotspot-Limited Microprocessors: Direct Temperature and Power Distribution Measurements," IEEE J. Solid-State Circuits, **42**(1), pp. 56–64.
[29] Cheng, H. C., Huang, T. C., Hwang, P. W., and Chen, W. H., 2016, "Heat Dissipation Assessment of Through Silicon Via (TSV)-Based 3D IC Packaging for CMOS Image Sensing," Microelectron. Reliab., **59**, pp. 84–94.
[30] Nowroz, A. N., Hu, K., Koushanfar, F., and Reda, S., 2014, "Novel Techniques for High-Sensitivity Hardware Trojan Detection Using Thermal and Power Maps," IEEE Trans. Comput. Des. Integr. Circuits Syst., **33**(12), pp. 1792–1805.
[31] Tang, Y., Li, S., Zhang, F., and Fang, L., 2018, "Thermal Maps Based HT Detection Using Spatial Projection Transformation," IET Inf. Secur., **12**(4), pp. 356–361.
[32] Zhong, J., and Wang, J., 2018, "Thermal Images Based Hardware Trojan Detection Through Differential Temperature Matrix," Optik, **158**, pp. 855–860.
[33] Banerjee, K., Souri, S. J., Kapur, P., and Saraswat, K. C., 2001, "3-D Ics: A Novel Chip Design for Improving Deep-Submicrometer Interconnect Performance and Systems-ON-Chip Integration," Proc. IEEE, **89**(5), pp. 602–633.
[34] Choobineh, L., Jones, J., and Jain, A., 2017, "Experimental and Numerical Investigation of Interdie Thermal Resistance in Three-Dimensional Integrated Circuits," ASME J. Electron. Packag., **139**(2), p. 020908.
[35] Wang, Z., Bovik, A. C., Sheikh, H. R., and Simoncelli, E. P., 2004, "Image Quality Assessment: From Error Visibility to Structural Similarity," IEEE Trans. Image Process., **13**(4), pp. 600–612.
[36] Brunet, D., Vrscay, E. R., and Wang, Z., 2012, "On the Mathematical Properties of the Structural Similarity Index," IEEE Trans. Image Process., **21**(4), pp. 1488–1499.
[37] Gao, Y., Rehman, A., and Wang, Z., 2011, "CW-SSIM Based Image Classification," 18th IEEE International Conference on Image Processing, Brussels, Belgium, Sept. 11–14, pp. 1249–1252.
[38] Pan, B., Qian, K., Xie, H., and Asundi, A., 2009, "Two-Dimensional Digital Image Correlation for in-Plane Displacement and Strain Measurement: A Review," Meas. Sci. Technol., **20**(6), p. 062001.
[39] Sadek, S., Iskander, M. G., and Liu, J., 2003, "Accuracy of Digital Image Correlation for Measuring Deformations in Transparent Media," J. Comput. Civ. Eng., **17**(2), pp. 88–96.
[40] Brunelli, R., and Mich, O., 2001, "Histograms Analysis for Image Retrieval," Pattern Recognit., **34**(8), pp. 1625–1637.
[41] Zhu, R., and Wang, Y., 2012, "Application of Improved Median Filter on Image Processing," J. Comput., **7**(4), pp. 838–841.