Structural Attacks and Defenses for Flow-Based Microfluidic Biochips

Navajit Singh Baban, Sohini Saha, Ajymurat Orozaliev, Jongmin Kim, Sukanta Bhattacharjee, Yong-Ak Song, Ramesh Karri, *Fellow, IEEE*, and Krishnendu Chakrabarty, *Fellow, IEEE*

***Abstract*—Flow-based microfluidic biochips (FMBs) have seen rapid commercialization and deployment in recent years for point-of-care and clinical diagnostics. However, the outsourcing of FMB design and manufacturing makes them susceptible to susceptible to malicious physical level and intellectual property (IP)-theft attacks. This work demonstrates the first structure-based (SB) attack on representative commercial FMBs. The SB attacks maliciously decrease the heights of the FMB reaction chambers to produce false-negative results. We validate this attack experimentally using fluorescence microscopy, which showed a high correlation ($R^2 = 0.987$) between chamber height and related fluorescence intensity of the DNA amplified by polymerase chain reaction. To detect SB attacks, we adopt two existing deep learning-based anomaly detection algorithms with ∼96% validation accuracy in recognizing such deliberately introduced microstructural anomalies. To safeguard FMBs against intellectual property (IP)-theft, we propose a novel device-level watermarking scheme for FMBs using intensity-height correlation. The countermeasures can be used to proactively safeguard FMBs against SB and IP-theft attacks in the era of global pandemics and personalized medicine.**

***Index Terms*—Deep learning, Microfluidic biochips, structural attacks, watermarking.**

I. Introduction

MICROFLUIDICS refers to the interdisciplinary study of fluid manipulation at nanoliter/microliter volumes. A microfluidics-based biochip (a.k.a lab-on-a-chip) miniaturizes and integrates different macroscopic biochemical functionalities (e.g., mixing, filtration, and detection) to a sub-millimeter scale [1]. These lab-on-a-chip microsystems offer various advantages over conventional biochemical analysis techniques. These include reduced sample volume, faster biochemical reactions, higher system throughput, and ultra-sensitive detection. They are revolutionizing biomedical applications such as point-of-care (POC) medical diagnostics [2], deoxyribonucleic acid (DNA) amplification platforms [3], and cancer research [4]. According to the 2021 Lancet commission report on diagnostics, 47 percent of the global population has little or no access to diagnostics [5]. At the end of 2019, the first reports of coronavirus disease 19 (COVID-19) appeared in China [5]. The COVID-19 pandemic spotlighted diagnostics, highlighting years of under-investment and neglect leading to gross inequity concerning access to diagnostics. However, the pandemic has accelerated the development of new technologies, solutions, and partnerships that can reduce the diagnostic gap [5]. Today, we are seeing extraordinary momentum for innovation in diagnostics technology and access. The molecular diagnostics market is projected to be worth 31.8 billion United States Dollars (USD) by 2026, up from 17.8 billion USD in 2021, a 79% increase [6]. The polymerase chain reaction (PCR) tests are forecast to experience extremely high growth in the future [6]. In May 2020, the European Investment Bank invested 6 billion Euros in health systems for COVID-19, including 1.5 billion Euros for companies that include diagnostics [5]. The Access to COVID-19 Tools (ACT) Accelerator, launched in April 2020, is a global effort to expedite the end of the COVID-19 pandemic [7]. The ACT-Accelerator strategic budget for 2021 reported a funding gap of 22.1 billion USD, out of which 8.7 billion USD is attributed to diagnostics [7]. There is a strong case for investment to improve access to diagnostics, which is likely to lead to the widespread use of microfluidic-based biochips. The products and services related to molecular diagnostics include reagents, microfluidic-based biochips, POC devices, and tabletop instruments (sensors and networked computers) [8]. Our work presents a structure-based (SB) cyber-physical vulnerability of flow-based microfluidic biochips (FMBs) that an attacker can use to tamper with the results, leading to low-quality diagnostics. The repercussions of such attacks are severe, with the potential to harm patients, cause resource waste, and generate negative economic consequences. Health practitioners can lose trust and discontinue using these products if they perceive them to be

Manuscript received 27 June 2022; revised 15 September 2022; accepted 18 October 2022. Date of publication 9 November 2022; date of current version 14 February 2023. The work of Ramesh Karri was supported by NSF under Awards 1833624 and 2049311. The work of Krishnendu Chakrabarty was supported by NSF under Grant 2049335. This paper was recommended by Associate Editor P. Georgiou. *(Corresponding author: Navajit Singh Baban.)*

Navajit Singh Baban, Ajymurat Orozaliev, and Jongmin Kim are with the Department of Engineering, New York University Abu Dhabi, Abu Dhabi 129188, UAE (e-mail: nsb359@nyu.edu; ajymurat.orozaliev@nyu.edu; jk181@nyu.edu).

Sohini Saha and Krishnendu Chakrabarty are with the Department of Electrical and Computer Engineering, Duke University, Durham, NC 27708 USA (e-mail: sohini.saha@duke.edu; krish@duke.edu).

Sukanta Bhattacharjee is with the Department of Computer Science and Engineering, Indian Institute of Technology Guwahati, Guwahati 781015, India (e-mail: sukantab@iitg.ac.in).

Yong-Ak Song is with the Department of Engineering, New York University Abu Dhabi, Abu Dhabi 129188, UAE, and also with the Department of Chemical and Biomolecular Engineering as well as Department of Biomedical Engineering, New York University, New York, NY 10012 USA (e-mail: rafael.song@nyu.edu).

Ramesh Karri is with the Department of Electrical and Computer Engineering, New York University, New York, NY 10012 USA (e-mail: rkarri@nyu.edu).

This article has supplementary material provided by the authors and color versions of one or more figures available at https://doi.org/10.1109/TBCAS.2022.3220758.

Digital Object Identifier 10.1109/TBCAS.2022.3220758

of low value in clinical care. These repercussions can motivate adversaries to maliciously target the vulnerabilities associated with FMBs for their own gains. Thus, it is essential to proactively safeguard diagnostics-related products such as FMBs against such attacks. In this work, we experimentally study potential SB attacks on FMBs and propose effective countermeasures using deep learning (DL) methods to secure FMBs against such attacks. Further, to protect FMBs against intellectual property (IP)-theft threats such as counterfeiting and overbuilding, we provide a device-level watermarking scheme by exploiting the height-dependency of the microchambers and microchannels on fluorescence intensity. The rest of the paper is organized as follows: Section II describes the background and motivation. Section III presents the adversarial model. Section IV shows the experimental results on the SB attacks. Section V presents the DL-based defense to detect the SB attacks. Section VI presents a novel device-level watermarking scheme to protect FMBs against IP-theft threats. Section VII gives a discussion on the obtained results. Finally, Section VIII concludes the paper. Materials and Methods are given in Section I of the separate Supplementary Materials file.

II. Background and Motivation

A flow-based microfluidic biochip (FMB) uses microchannels and pressure-driven elastomeric micro-valves to manipulate the continuous flow of fluid for performing various bioassays (Supplementary Materials, Section II). The rapid spread and impact of COVID-19 has placed a significant burden on public health systems, highlighting the critical need for high-throughput and innovative testing approaches to combat future pandemics. The widespread use of the SARS-CoV-2 reverse transcription (RT)–PCR test has led to a significant gap in the availability of test kits, emphasizing the need for ultra-high-throughput screening. High cost and scarcity of reagents [9] hampered the global scale-up of PCR testing, creating a void in adequately monitoring communities for COVID-19.

Significant false-negaive rates (10-30%) from PCR have been widely reported [10], [11] posing a major challenge in curbing the spread of infection. Poor sample quality (with low viral loads) that evades standard PCR methods [12] further exacerbates the situation. An additional challenge concerning COVID-19 spread is the role of asymptomatic transmission [12], [13]. Reports suggested that 40-80% of infected individuals are either pre-symptomatic, asymptomatic, or only mildly symptomatic [9]. Thus, early detection of infection in these asymptomatic individuals is critical for disease control. However, asymptomatic carriers sometimes carry low viral loads (1 to 40 viral copies/μL) [9] that a standard RT-PCR test may miss. Therefore, it is critical to have more sensitive detection methods that can detect low viral loads.

The above concerns related to throughput can be addressed by miniaturizing the testing volume to the nanoscale regime [14]. This can significantly increase the diagnostic space for independent reaction chambers [14]. In addition, such a strategy provides a cost-effective microfluidic active cyber-physical system [8] with several advantages: a nanoliter volume per reaction (lower reagent consumption per assay), a parallelized assay system (high throughput), automation compatibility (increased precision), capable of running a large number of replicates per sample (higher confidence in test results) and the ability to test for multiple pathogens (broader diagnostic capability) simultaneously. This strategy has the potential for assay multiplexing to identify additional pathogens and sample pooling to increase throughput, leading to a further reduction in per-test costs. This principle is the basis of Fluidigm's proprietary Integrated Fluidic Circuitry that has been deployed in several of their FMBs for genotyping, gene expression, and single-cell and DNA analysis [15].

Concerning low viral load detection, Xie et al. [14] demonstrated ultra-sensitive detection of low SARS-CoV-2 viral loads (1 to 40 viral copies/μL) using quantitative (q)RT-PCR via a commercial microfluidics platform with 4608 independent microscale reaction chambers containing fluids in nanoliter volumes. Their approach of using nanoscale qRT-PCR enhanced the limit of detection by 1000-fold compared to conventional RT-PCR techniques, enabling detection below one copy/μL. They used 182 swab samples, 91 positive samples, and 91 negative samples each, including samples previously diagnosed as negative by an accredited diagnostic laboratory. Out of the 91 negatively diagnosed samples, 17 were found to be positive using the nano-miniaturized biochip, indicating a 18.7% false-negative rate of the conventional RT-PCR technique.

A recent study by Sharkawy et al. [16] reported similar results where they tested paired COVID-19 samples to compare the conventional RT-PCR diagnosis versus saliva-based diagnosis, which they performed using a commercial FMB. In particular, they compared specimens (nasopharyngeal (NP) versus saliva samples) from hospitalized patients with symptomatic COVID-19 and found 15 discordant samples.

Out of the 15 discordant samples, 3 were positive in NP (conventional RT-PCR) but negative in saliva (FMB-based RT-PCR) technique. In comparison, 8 out of 15 discordant samples tested negative in NP (conventional) but were diagnosed positive with the saliva-based technique. The remaining 4 samples gave inconclusive results. The reason for discordance behind the three NP-positive (but saliva-negative) samples given was the high dilution of saliva. However, the 8 samples that were declared negative by the conventional NP technique tested positive with the saliva-based technique, and that too after 8-10 days post symptom onset. Here, the reason for discordance given was low viral loads (1 – 40 viral copies/μL), which the conventional technique was not able to detect.

Thus, samples with low viral loads (1-40 copies/μL) either due to poor sample quality resulting from wrong handling, extraction, and storage of the samples or through asymptomatic carriers with low viral loads might go undetected with conventional RT-PCR techniques. In comparison, FMBs can detect these low viral load samples.

Currently, FMBs are not widely used in clinical diagnostic of SARS-Cov-2; rather, they mainly serve biomedical research purposes. However, they have tremendous potential for diagnostics, given the limits of standard PCR techniques [10], [11], [15] and the dire need to narrow the diagnostic gap worldwide [5]. The manufacturing of integrated fluidic circuits on a biochip has many steps and requires multiple entities, some of which might be untrusted. The manufacturing steps include

the creating design files (ideally either by a trusted third-party designer or an in-house manufacturing unit) and executing the design files in a foundry to fabricate the final product (again ideally either by a trusted third-party designer or an in-house manufacturing unit). These stages of design and manufacturing highlight structure-based (SB) attacks, where an attacker can introduce structure-based positional and dimensional variation in the biochip's embedded components to critically affect the diagnostic outcomes, producing incorrect results.

With the advent of manufacturing-as-a-service [17], biochips can become more vulnerable to SB attacks. The goal of such an attacker is to produce false or misleading test results, compromising the integrity of molecular diagnostics research, jeopardizing the healthcare industry, and making health practitioners lose trust and discontinue using the biochips. The adversary's economic interests will then be satisfied as the customers would switch to other biochip companies in the marketplace.

Physical reverse-engineering [18], [19] to steal intellectual property (IP) can be a second line of attack. These attacks involve stealing the biochip architectural layout, component-level netlist, and information about the bio-protocol without incurring development costs [19]. IP theft using physical reverse-engineering provides an attacker with knowledge about the biochip's structural components and associated functionality to perform the bioassay. While fabricating the reverse-engineered biochips, the attacker can then intentionally alter the structure of components, producing discordant results to defame the original biochip manufacturer. Furthermore, using the stolen information, adversaries can carry out piracy of IP and test protocols, counterfeiting, and overbuilding of biochips for illegal monetary gain.

We categorize attacks in two main threat categories: (1) malicious physical level threats, which incorporate the SB attack, and (2) IP-theft threats, which incorporate physical reverse-engineering, counterfeiting, and overbuilding attacks. For the first threat category, we investigate SB attacks using a commercial FMB as an exemplar. We employ two existing deep learning (DL) models to catch microstructural anomalies on FMBs. For the second category of threats, we propose a novel structure-based device-level watermarking solution to validate the authenticity of the biochip. The watermarking scheme increases the height of the reaction chambers or microfluidic channels at specific locations to obtain fluorescent markers that can be detected using fluorescence microscopy. The pirated or counterfeited FMBs would most likely be identified and discarded by the authentic end-user or the entity that received the fabricated FMB from a third-party manufacturer by checking for these watermarks in the FMBs.

III. Adversarial Model

Fig. 1 illustrates the adversarial model and highlights the vulnerable points corresponding to an SB attack. The model has five parties: the customer, the FMB company, the designer, the manufacturer, and the quality control unit.

Biochip designers integrate reaction chambers, microfluidic lines, and valves to create a functional microfluidic platform in

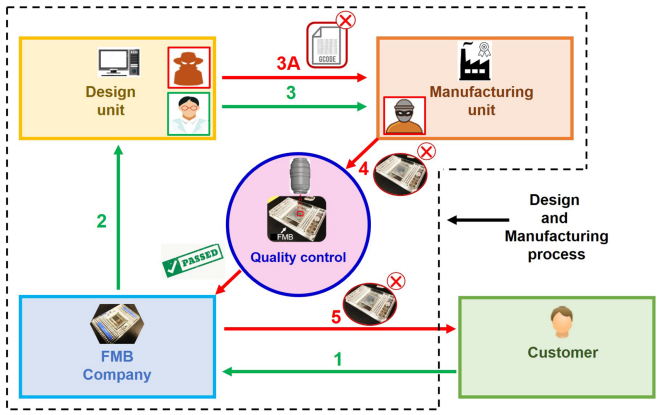

Fig. 1. Process flow of a biochip service and attack points. A customer places a biochip order received by the FMB company (route 1). The FMB company sends the order to the design unit (route 2). Now, there are two possible routes. First, an attacker in the design unit sends the altered design files to the manufacturing unit (route 3 A). Second, the authentic designer sends the design files (G-Codes) to the manufacturing unit. However, an attacker in the manufacturing unit alters the G-codes in the fabricating machine to carry out the SB attack (route 3). In either case, the attacked biochip reaches the quality control unit (route 4) and escapes detection owing to the stealthy nature of the attack. Finally, the compromised biochip is delivered to the customer (route 5).

the form of design files. After the design files are generated, they are sent to the manufacturing unit, where fabrication and assembly of the biochip take place.

We make a distinction between the technical and operational abilities of an attacker. Technical abilities refer to the knowledge an attacker has on the working of the microfluidic platform and the capabilities to extract information and resolve the ambiguities that arise from experimentations. For instance, the attacker, who is part of the design team (also known as design-level threat model), can target reaction chambers or microfluidic lines connecting the chambers and use the knowledge of the system to alter the structural design codes (geometry (G)-codes) to hamper the associated physical processes. Operational abilities refer to the mode of operation employed by an attacker in the manufacturing unit to launch the attack. For instance, the attacker in the manufacturing unit can target critical structural components and alter relevant parameters to perform an SB attack.

The process flow of a typical biochip service [20] is shown in Fig. 1. A typical service starts with a customer submitting a service request for a biochip (route 1). After the service request is generated, it is sent to the design unit (route 2). The design unit is either in-house or third-party. In either case, the designer generates design files to create structural design codes (G-codes). The design unit sends the generated codes to the manufacturing unit. There are two potential attack possibilities; in the first case (route 3 A), an attacker in the design team can target the crucial microstructures of the biochip and secretly change the design codes to alter the structures producing false outcomes after the bioassay execution. The maliciously modified design codes go to the manufacturing unit. In the second case (route 3), an authentic designer sends the right design codes to the manufacturing unit (route 3). However, an attacker in the manufacturing unit alters relevant machine parameters before

manufacturing the biochip to perform the attack. In both cases, the attacked biochip reaches the quality control team (route 4) and evades fault detection owing to the stealthy nature of the attack. Finally, the compromised biochip is delivered to the customer (route 5).

Prior methods on securing FMBs against malicious attacks presented a high-level overview of attacks and defense methods [8]. Chen et al. proposed a systematic framework for the insertion and detection of hardware Trojans in FMBs [21]. For Trojan insertion in FMBs, Shayan et al. [22] presented a microfluidic valve-based Trojan design. Here, an attacker increases the thickness of the valve membrane, requiring higher pressure to operate than the normal membrane. Such a valve response can cause a malfunctioning of biochips and can be used to launch attacks such as contamination, denial of service, and parameter tampering. So far, no work has been reported that explores malicious structural modification of FMB components to produce false-negative results.

With respect to IP-theft-attacks and associated countermeasures for FMBs, Chen et al. [19] demonstrated a layout-level reverse-engineering attack using image analysis. A recent work presents a design obfuscation technique to thwart reverse-engineering of bioprotocol by obscuring the actuation sequence by carefully inserting dummy valves in the FMB [1], [23].

Previous research has demonstrated malicious attacks such as actuation tampering; however, the attacks were shown only on digital microfluidic biochips (DMFBs) [24], [25], [26], [27]. While the previous studies showed tampering attacks on DMFBs, such attacks have not been thoroughly explored for FMBs. Similarly, regarding watermarking solutions, a previous study demonstrated a watermarking technique to protect bioprotocols (bio-protocol level watermarking) by hierarchically embedding secret signatures in DMFBs [28]. The same bioprotocol level watermarking scheme can be applied to FMBs. However, no device-level watermarking schemes have been proposed for FMBs where the watermark is inherently embedded in the physical FMB.

In this work, we present a device-level watermarking scheme for FMBs by increasing the height of the microchambers or microchannels at specific locations to obtain fluorescent markers that can be detected and quantified using fluorescence microscopy. In this work, we present security solutions against malicious cyber-physical and IP-theft threats. For the malicious threats, we study SB-based result tampering by conducting experiments on our laboratory-made FMB, whose design was adapted from a commercial biochip. For countermeasures, we present a DL-based defense to secure FMBs against malicious SB attacks. For IP-theft threats, we provide a device-level watermarking scheme for FMBs by using the dependency of the height of the microchambers and microchannels on fluorescence intensity.

IV. Results on SB Attacks

To steal IP and reverse-engineer the PCR regions of the biochip containing integrated microfluidic lines, valves, and the reaction chambers, we obtained the architectural layout and components netlist of a commercial chip using light and electron microscopy techniques (Supplementary Materials, Section III).

By delayering the biochip, crucial PCR micro-components were imaged, and the related bio-protocol information was obtained based on the information provided on the biochip's website and operation manuals. Among the microfluidic components identified during the microscopy investigations, we focused on the reaction chamber to experimentally investigate the SB attacks. A reaction chamber is a key component in which sample and reagent mix before undergoing PCR heating and (de)heating cycle for DNA amplification and fluorescence-based quantification. In the SB attack, the attacker can decrease the volume of the reaction chamber by reducing the height of the cuboidal reaction chamber while preserving the top face of the original reaction chamber. The malicious volume decrement can decrease the fluorescence response producing misleading or false-negative results. As a proof of concept, we quantified the fluorescence intensity of different microscale volumes of amplified synthetic SARS-Cov-2 DNA and found the effect of intensity reduction when the volume was decreased (Supplementary Materials, Section IV). The results show a 60% decrease in the maximum intensity when the volume decreased from 1.5 μL to 0.8 μL. When the volume was decreased to 0.1 μL, we saw a 90% reduction in the intensity compared to 1.5 μL intensity.

The commercial biochip chosen as a reference for this study uses nanoscale fluid volumes in its chambers. To evaluate the effect of nanoscale volume decrement on representative commercially available biochips, we fabricated relevant reaction chambers connected with the microfluidic lines using 3D printing techniques. The dimensions of the reaction chambers and the microfluidic lines were adapted from the commercial biochip. To mimic attacks, we decreased the reaction chambers' heights in the design files. Using the design files, we 3D printed the FMB mold. After replication using PDMS, we obtained the FMB. Bright-field images were taken to determine if the reduced height chambers are detected during quality control checking. The results showed that it is hard to detect the reduced height chambers because the light-microscopy only uses top-view two dimensional (2D) views for the identification (Supplementary Materials, Section V).

Following light-microscopy investigations, we separately pipetted a fluorescent dye (Alexa Fluor 488), and PCR amplified mice DNA into the reaction chambers. We recorded the relative intensity decrease using a fluorescent microscope. Fig. 2(a) shows the bright-field image of the fabricated reaction chambers with two of the chambers having 50% less height than the original. Fig. 2(b) shows the fluorescence image of the same reaction chambers shown in Fig. 2(a). Fig. 2(c) shows the associated intensity versus distance response along the horizontally scanned line shown in Fig. 2(b). The response indicated about 50% less intensity for the deviant (i.e., 50% reduced) height chamber. Similarly, Fig. 2(d) shows the vertical scan intensity versus distance response as we move from the bottom reaction chamber (50% less height) to the top one (regular) via the microfluidic channel. The height of the microfluidic channel

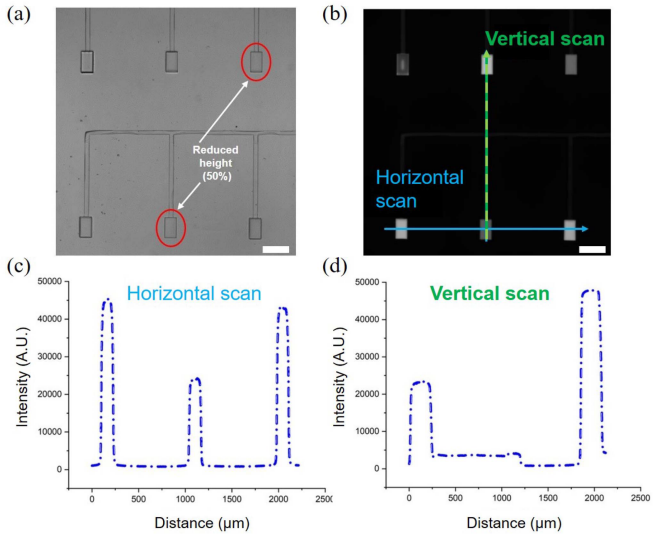

Fig. 2. Experimental demonstration of an SB attack. (a), A bright-field image of the reaction chambers where the heights of the two chambers were reduced by 50% of the original height (270 μm). The scale bar is 280 μm. (b) A fluorescence image of the reaction chambers as shown in Fig. 2(a). (c) Intensity versus distance plot along the horizontally scanned line shown in Fig. 2(b). The scale bar is 280 μm. (d) Intensity versus distance plot along the vertically scanned line as shown in Fig. 2(b).

was 90% less than the height of the original reaction chamber. The response illustrated a high degree of correlation between the intensity and the height of the microfluidic components where a continuous transition of intensity, along the order: 50%, 90%, no channel, and 100% height, was recorded, as seen in Fig. 2(d).

To quantify correlation, we developed a linear regression model to relate the normalized heights of the reaction chambers to the corresponding normalized intensities of the fluorescence measurements. Normalization with respect to the maximum height and intensity was done to make the parameters dimensionless. Fig. 3(a) shows an example of the height change carried out to obtain data points for the regression model. The first row in Fig. 3(a) contains the regular reaction chambers with 100% height, i.e., 270 μm. All the other reaction chambers are less in height than the regular ones, seen schematically in Fig. 3(a). The effect of the height difference on intensity can qualitatively be seen in the corresponding fluorescence image. A linear fit was obtained using 18 height-dependent data points with a high R-square value of 0.984, seen in Fig. 3(b). This implies that the model explained 98.4% of the change in the intensity actuated by the change in the reaction chamber's height. A similar linear regression model, having a R-square value of 0.987, was obtained with 21 data points but with PCR amplified mice DNA, as seen in Fig. 3(c)–(d).

An attacker can use linear regression models of the type presented here to perform an attack to deliberately create false-negative results. It is important to note that one chamber corresponds to one patient's sample. In the context of a disease that can cause a pandemic such as Covid-19, even one false-positive can increase the transmission rate, leading to serious consequences. The results shown in Fig. 3 considered only the intensity decrement based on the height decrement as we pipetted already amplified DNA into the reaction chambers. However DNA amplification usually takes place in the reaction chamber using heating and (de)heating cycles. The decreased height inserts a layer of PDMS (an insulator) in between the reaction chamber and heating source, hampering the process of heating and (de)heating. Using finite-element simulation, we show that the SB-attack can not only decrease final fluorescence intensity but can affect PCR heating/de(heating) (Supplementary Materials, Section VI), which can further tamper the PCR results.

In a resource-constrained system, randomized-checkpointing-based quality checks can offer better security [22]. To quantitatively evaluate the stealthy nature of the SB attack, we propose a security metric to compute the evasion probability during randomized-checkpointing-based checks. With microscale reaction chambers, the quality control checks would most likely be done by a microscope, either manually or by using a charge-coupled device (CCD) camera connected to the microscope. However, checking a large number of reaction chambers will require several rounds of checking sessions using the camera. This is because there has to be a sufficient zoom or magnification to view the reaction chambers for detecting structural faults. For example, the reference FMB used here has 2304 reaction chambers; however, based on our microscopy sessions using a 10X objective, only 12 of these could be seen clearly to identify structural irregularities in the reaction chambers, as shown in Fig. 4(a).

For comparison, Fig. 4(b) shows the microscopic view of 12 reaction chambers of the FMB microfabricated in our laboratory. Fig. 4(c) shows the randomized checkpointing schematic where the microscope scans specific regions on the FMB at an instance. Here, we divided the FMB into 192 regions (12 rows and 16 columns), where each region contained 12 reaction chambers. In general, suppose R views are needed to scan the whole FMB. For example, Fig. 4(c) shows 192 regions needed to scan the chip. Therefore, $R = 192$. Assume r of the views contain anomalous or deviant-height reaction chambers. For example, in Fig. 4(c), one view has deviant chambers. Therefore, $r = 1$. Let n be the number of random trials to detect the structural anomaly. For $n = 1$, the probability that an anomaly is detected is $\frac{r}{R}$. The probability that an anomaly is missed or evasion probability (P_e), is given by (1).

$$P_e = 1 - \frac{r}{R} \tag{1}$$

For n random trials, the probability of evasion P_e is given by (2):

$$P_e = \left(1 - \frac{r}{R}\right)\left(1 - \frac{r}{R-1}\right)\left(1 - \frac{r}{R-2}\right) \cdots \left(1 - \frac{r}{R-(n-1)}\right) \tag{2}$$

The criteria for detecting an SB attack could be some identifiable physical anomaly compared to the surrounding chambers. For example, we found less reflected light from the walls of the deviant-height chambers compared to the original chambers.

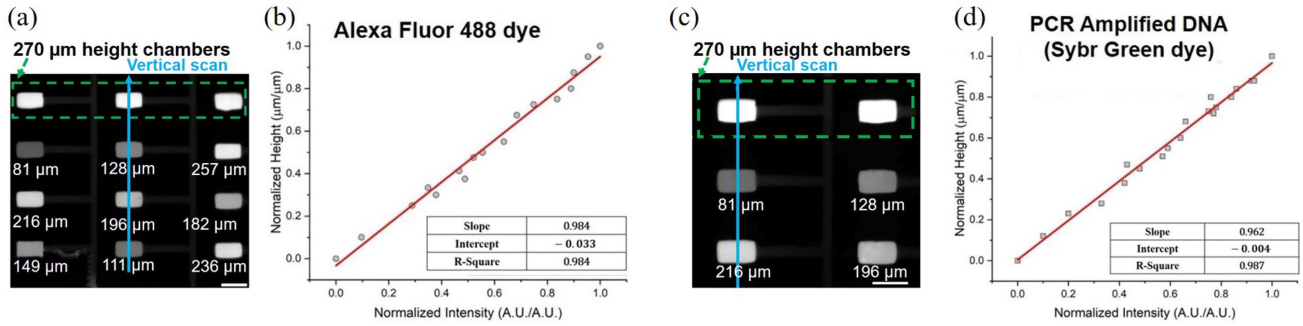

Fig. 3. Linear regression models for the SB attack. (a) Decrease in fluorescence intensity (Alexa Fluor 488 dye) with reduced-height chambers: the image shows reduced fluorescence intensity for the deviant-height chambers compared to the original height chambers (270 μm). The height of the deviant chambers are mentioned below them. The scale bar is 250 μm. (b) Linear regression model between normalized height and normalized intensity of the Alexa Fluor 488 dye. (c) Decrease in fluorescence intensity (PCR Amplified DNA, Sybr Green Dye) with reduced-height chambers: the image shows reduced fluorescence intensity compared to the original height chambers (270 μm). The height of the deviant chambers are mentioned below them. The scale bar is 250 μm.(d) Linear regression model between normalized height and normalized intensity of the PCR amplified DNA (SYBR Green dye).

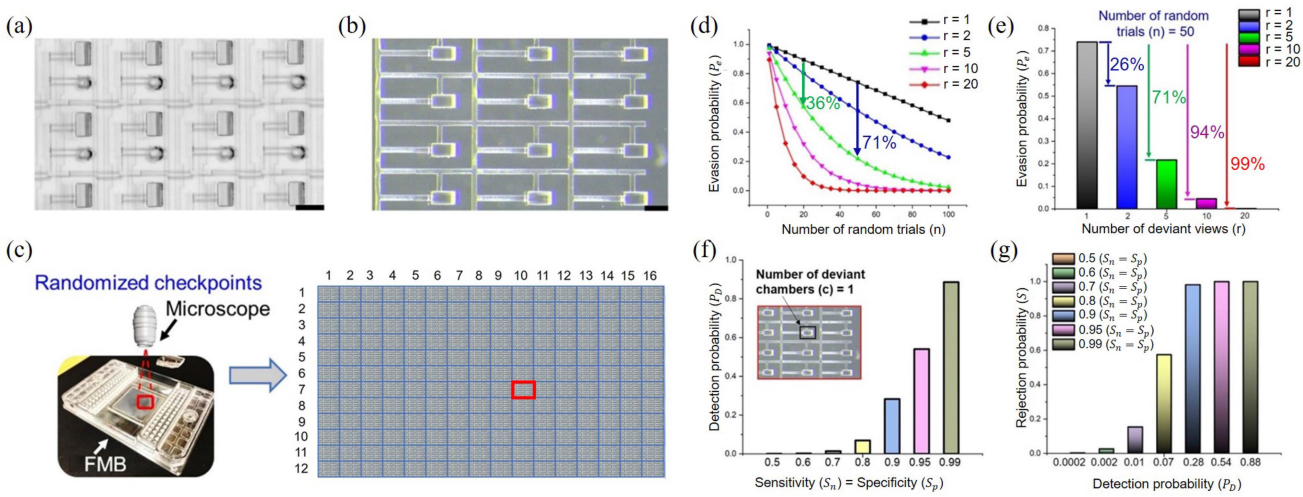

Fig. 4. Microscopic view of 12 out of 2304 reaction chambers and security metric plots. (a) A bright-field microscopic view of 12 reaction chambers in the reference FMB. The scale bar is 140 μm. (b) A bright-field microscopic view of 12 reaction chambers in our laboratory-made FMB. The scale bar is 250 μm. (c) A schematic showing the randomized checkpointing policy to detect structural anomalies on the FMB. (d) The plot of evasion probability (P_e) versus the number of random microscopy trials (n) to detect structural anomalies. (e) The plot of evasion probability (P_e) versus the number of deviant views (r) containing structural anomalies. (f) The plot of detection probability (P_D) versus sensitivity (S_n) = specificity (S_p) of the detecting microscopes. (g) The plot of detection probability (P_D) versus rejection probability (S).

For the reference FMB, $R = 192$, while r and n remain as variables. An attacker is likely to increase r as much as possible to make the attack more lethal. However, increasing r decreases the P_e. To quantify this, we plot a graph between P_e and n by varying r. Fig. 4(d) shows that P_e exponentially decreases as r increases from 1 to 20. When $n = 20$ and $r = 5$, P_e decreases by 36% compared to the $r = 1$ case. In comparison, for the same $r = 5$, when $n = 50$, P_e decreased by 71%, indicating a strong dependence of P_e on n. To record the effect of r on P_e, we fixed $n = 50$ and plotted P_e for r ranging from 1 to 20 (Fig. 4(e)). When r was increased from 1 to 2, a 26% reduction in P_e was recorded, and for $r = 5$, a 71% reduction in P_e was recorded. The P_e reduced 99% for $r = 20$ compared to the $r = 1$ case. Thus, a drastic decrease in P_e was recorded with an increase in r for the given $n = 50$. An attacker would aim to increase r as much as possible; they are aware that increasing r would be easily detected by randomized checkpointing. There is an inherent tradeoff between r and n.

An attacker can use such metrics to decide on r given an n. For example, let us consider the case of $r = 5$ and record the decrease in P_e with respect to $r = 1$. If $n = 20$, the attacker would likely choose r to be 5 that shows a 36% of decrease in P_e compared to the case where $n = 50$, which shows 71% of decrease in P_e. This selective tactic based on the proposed metric will give them a 35% higher chance of evasion, shown in Fig. 4(c). The FMB companies could use such randomized checkpointing to proactively secure their biochips.

We propose another security metric based on independent Bernoulli trials, where the quality control checks are done on all the chambers (using all 192 views) rather than the randomized checks described above; thus, $r = R$ here. After applying this relation in (3), P_e becomes zero. This ensures that a detecting

system would surely detect the anomaly if all the chambers are viewed, assuming that the detecting system is an ideal one. However, P_e would not be zero if the detecting system is not ideal. The ideality of the detection system can be quantitatively evaluated using the associated sensitivity and specificity parameters.

For structural anomaly detection in the reaction chambers via optical microscopes, we define sensitivity (S_n) to be the conditional probability of detecting the structural anomaly when the anomaly is actually present. On the other hand, specificity (S_p) is the conditional probability of not detecting the structural anomaly when the anomaly is not present. Here, we focus our attention only on the region where the structural anomaly can be seen and evaluate the detection probability (P_D) of the microscope for varying values of S_n and S_p. For example, consider the case shown in Fig. 4(f), where the red outlined inset depicts the region containing one deviant height chamber out of 12 reaction chambers. Based on the Bernoulli trial scheme, P_D can be evaluated using the following (3), where c is the number of deviant chambers in a microscopy view showing 12 chambers. Note that S_n and S_p denote sensitivity and specificity of the microscope, respectively.

$$P_D = (S_n)^c \cdot (S_p)^{12-c} \tag{3}$$

A manufactured FMB is rejected if at least one of the checking sessions identifies SB-attacked deviant-height reaction chambers. If the quality control checker is aware of the anomaly detection method, such as shadow/reflection-based anomaly detection, at least one anomalous view will lead to the lot's rejection. Otherwise, the SB attack will go undetected. Assuming that the checker or detector knows the anomaly detection policy, we define a metric that quantifies the probability (S) of rejecting a FMB if an anomaly is detected during the scanning of the whole biochip. As per the commercial reference FMB, 12 reaction chambers can be observed for anomaly detection, as shown in Fig. 4(f). Therefore, 12 independent trials are needed to detect the number of deviant-height chambers. Let c be the number of deviant-height chambers found during the 12 independent trials. The inset in Fig. 4(f) shows the situation where $c = 1$ out of the 12 chambers. Let P_D be the detection probability during the 12 independent trials. Then the probability of successfully rejecting the biochip (rejection probability, S) is the probability of detecting an anomaly for at least one trial out of 12 trials, which is equal to 1 minus probability of not detecting any anomaly at all. Equations (4)–(6) below relate S with P_D where k denotes number of anomaly detection events out of 12 trials.

$$S = P(k \geq 1) = 1 - P(k = 0) \tag{4}$$

$$P(k = 0) = \binom{12}{0} (P_D)^0 (1 - P_D)^{12-0} \tag{5}$$

$$S = 1 - (1 - P_D)^{12} \tag{6}$$

We apply (3) to evaluate P_D for different $S_n = S_p$ ranging from 0.5 to 0.99, seen in Fig. 4(f). P_D increased when S_n and S_p were increased. For example, when $S_n = S_p$ increased from 0.8 to 0.9 and 0.95, P_D increased by 2.9-fold and 7.4-fold, respectively. When S_n and S_p increased from 0.95 to 0.99, P_D increased by 64%. Using the P_D values, we evaluated the rejection probabilities (S) using (6), plotted in Fig. 4(g). The plot indicates S increases considerably with an increase in P_D. A 41% increase in S was recorded when P_D increased from 0.07 (corresponding to $S_n = S_p = 0.8$) to 0.28 (corresponding to $S_n = S_p = 0.9$). For P_D equal to 0.54 and 0.88 (corresponding to $S_n = S_p = 0.8$ and 0.99, respectively), S converged to unity. Thus, sensitivity and specificity of the detecting microscopes can affect rejection probabilities to discard SB-attacked FMBs. The Bernoulli trial-based security evaluation shows that even if the whole FMB is scanned for anomaly detection, an attacker can evade detection due to the limits of the detecting system. Using these metrics, attackers can pick an attack scheme that maximizes their chances of escaping detection. Defenders can proactively compute these metrics to safeguard FMBs against SB attacks.

V. Defense Against SB Attacks

To protect against the attack described in Section IV, we have to inspect all the reaction chambers present on the biochip. However, an inspection of all the reaction chambers, which could be in thousands, is not practical in realistic scenarios for low-cost biochips. Therefore, we have employed two DL-based anomaly detection algorithms for detecting deviant chambers. We next present these DL-based anomaly detection techniques to counter SB attacks.

Anomaly detection or outlier detection is a technique that helps to identify data instances which deviate significantly from majority of data instances. Outlier detection [29], [30], [31], [32] can be key to detecting malicious behavior, and thereby prevent compromised biochips from being sold commercially. In recent years, machine learning (ML) methods, especially DL, have been increasingly adopted for predictive analysis. Automated feature extraction in DL helps us to define the boundary between normal and anomalous behaviour in the dataset. The dataset in our application is composed of a microscopic view of reaction chambers in the biochip.

Our approach is presented in Fig. 5(a). We consider true images to be those where each of the reaction chambers has 100% height, that is, 270 μm, as shown in the top row in Fig. 5(b). If any reaction chamber has a height that is not equal to 270 μm, then the image is deemed to be an outlier. The deviant-height reaction chambers can be seen in all the other rows in Fig. 5(b). Our goal is to detect the outliers and prevent the attack from succeeding. In order to perform outlier detection, the DL model must be trained on a large dataset (Supplementary Materials, Sections VII and VIII). The image dataset is comprised of two different classes of data which indicate true and anomalous images each amounting to 400 images. We further split the dataset into a training dataset with 80% of the images and validation dataset with the remaining 20% of the images.

Many ML techniques have been considered for anomaly detection; these include fuzzy logic [33], [34], Bayesian approach [35], [36] genetic algorithm [37], [38], and neural network [39], [40]. However, DL has been shown to be more effective than traditional ML methods [41], [42], [43]. The

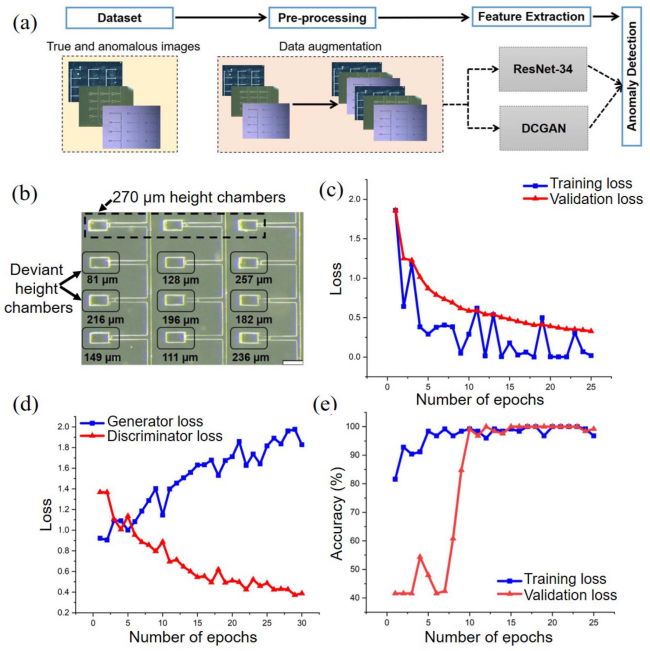

Fig. 5. DL-based anomaly detection. (a) A schematic describing the DL-based anomaly detection. (b) The image taken from a light microscope shows the original-height (270 μm) and the deviant-height ($<$ 270 μm) reaction chambers. 9 out of 12 chambers have deviant heights. These deviant height chambers are marked as red boxes. The scale bar is 270 μm. (c) Training and validation losses for the ResNet-34 model. (d) Generator and discriminator Losses for the GAN model. (e) Training and validation accuracy for ResNet-34 model.

most frequently used DL methods are based on generative adversarial networks (GANs) [33], autoencoders [44], convolutional neural networks (CNNs) [45], and Long Short-Term Memory (LSTM) [46]. Deeper convolutional neural networks can extract image representations by stacking layers in the network architecture and can classify the images with higher accuracy. However, stacking more layers gives rise to a problem of vanishing/exploding gradients, which adversely impacts convergence. This problem, however, can be solved by performing normalization of the initial and intermediate layers, but when these deeper neural networks start converging, a problem of degradation occurs whereby the accuracy saturates and then degrades rapidly.

In order to address this problem, deep residual networks have been proposed. Residual neural networks or ResNets [47] perform image recognition, image segmentation, and visual object detection, and they have been used in healthcare-related applications [48], [49], [50], [51], [52]. These networks stack residual blocks on top of each other to form a network; e.g., ResNet-50 comprises fifty layers using these blocks. There are residual connections connecting the pre-activation from one layer with the input of a previous layer in an additive fashion skipping several layers in between, and the non-linear activation is applied to the sum to compute the input for the next layer.

A generative adversarial network (GAN) is a type of deep neural network that generates new data from the training dataset. GANs consist of two key components, known as the generator (G) and the discriminator (D), which are trained against each other in an adversarial manner. The Generator model generates images that are then evaluated by the discriminator model. The GAN model maximizes the probability $pdata(x))$ that any real input image, x, is classified as belonging to the true dataset while any fake image generated by G has minimum probability $(pz(z))$ of being classified as belonging to the real dataset. If $G(z)$ represents that the generator function maps a latent space vector z to the input data-space, the loss function used by GAN maximizes the function $D(x)$ while minimizing $D(G(z))$. Thus, D and G can be considered to be two agents playing a minimax game with loss/error function given by $V(D, G)$ given by (7), where E represents expectation in terms of probability.

$$\min_G\{\max_D\{V(D,G)\}\} = \mathrm{E}_{x\sim p\,\mathrm{data(x)}}[\log D(x)] + \mathrm{E}_{z\sim pz(z)}[\log(1-D(G(z)))] \tag{7}$$

Among GAN architectures, deep convolutional generative adversarial networks (DCGAN) are especially effective for data augmentation with limited dataset size [53]. The DCGAN architecture was proposed to expand on the complexity of the generator and discriminator networks. It uses CNNs for the generator and discriminator networks.

We used two approaches to detect anomalies: a 34-layer deep residual neural network ResNet-34 and a GAN-based network DCGAN. The ResNet-34 model is preferred to the other deeper neural networks because it solves the problem of vanishing gradients by using residual networks, which enables it to skip connections backward from later layers to initial layers, thereby allowing gradients to flow. This helped ResNet-34 in convolving the images, extracting features, and finally performing quality control checks on products.

We trained the ResNet-34 model with the Adam optimization algorithm and the cross-entropy loss function for 25 epochs, with a batch-size of 32 image samples and a learning rate of 1×10^{-4}. The Adam algorithm is a one-step optimization algorithm for random objective function. The hyper-parameters for the Adam algorithm can be easily adjusted to support back propagation with faster convergence speed and effective learning. The cross-entropy loss function used for training helped in updating the weights and bias at a reasonable speed. The loss curves for the training and validation datasets can be seen in Fig. 5(c). DCGAN-based anomaly detection appeared to be useful since there is a shortage of ground-truth anomalies; it helped us to capture the real data distribution alongside the generation of simulated data. The DCGAN model was trained with a mini-batch size of 32 images for 30 epochs using the Binary Cross Entropy loss (BCE Loss) function. The BCE Loss function helped in linear back-propagation with a finite loss value. The training for the G and D networks was done using separate Adam optimizers. The optimizer for D used a learning rate of 1×10^{-4} while that for G used a learning rate of 2×10^{-4}. The loss curves for the DCGAN model are shown in Fig. 5(d). As training progresses, the loss values for D keeps on decreasing while that for G keep on increasing which clearly indicates that D has learned to discriminate between the ground truth and anomalous data while G has failed in fooling D.

Fig. 5(e) shows the classification accuracies for the ResNet-34 model for the training and validation data sets, respectively. The best recognition accuracy was found to be about 96% indicating that the model was effective in identifying the images having deviant height reaction chambers.

Further, to evaluate performance measurements of our DL models, we have used precision score, recall score, F1 score, false positive rate (FPR), and false negative rate (FNR) as evaluation metrics (see Supplementary Materials, Section VIII). Our results indicate 0.0476 FPR and 0 FNR for ResNet-34, and 0 FPR and 0.0454 FNR for DCGAN, showing that are models are able to achieve high performance.

VI. Watermarking

We propose a device-level watermarking scheme for FMBs using the reaction chamber's height-intensity correlation. We leverage this inherent dependence of fluorescence intensity on the reaction chamber height to embed fluorescent markers into FMBs. We increased the height of certain reaction chambers and of the microfluidic channels at specific locations. When a fluorescent dye was pipetted to these increased height portions, fluorescent markers were obtained that were quantifiable using fluorescence microscopy. Thus, these fluorescent markers, when seen using a fluorescence microscope, acted as a watermark. In the event of an SB attack suspicion or suspicion regarding piracy, forgery, and counterfeiting, this secret watermark from the biochip can be undeniable authorship proof, safeguarding the biochip against these attacks.

In Section IV, we showed that reducing the height of a reaction chamber can decrease fluorescence intensity. However, reducing the height of a reaction chamber compromised the PCR amplification outcomes resulting in false-negative readings. As an alternative, increasing the chamber height stealthily as an embedded signature is a viable watermarking policy and this would not compromise amplification results. Furthermore, these increased-height chambers can remain effectively hidden and can only be quantitatively extracted using the distance-intensity graph, as shown in Fig. 6.

Fig. 6(a) shows a schematic where the reaction chambers heights were increased to quantify the increase in fluorescence intensity. The height of the first-row chambers was kept the same while the others were changed with a step size of 1 μm. The corresponding bright-field image was taken from a light microscope. All chambers are qualitatively indistinguishable from each other due to the minimal height increment. However, the change becomes evident when we used fluorescence microscopy to quantitatively characterize the intensity-height relationship. Fig. 6(b) and (c) show the blue lines, which indicate the horizontally and vertically scanned paths of intensity-distance plots. Fig. 6(d) and (e) show the intensity-distance plots corresponding to Fig. 6(b) and (c), respectively.

The response in Fig. 6(d) shows a minimal change in intensity due to the same height (270 μm) across all the three top-row chambers. We attributed this change to be noise and defined a parameter named standard deviation (σ) to quantify the noise. We calculated the σ by subtracting the maximum (48488 A.U) value

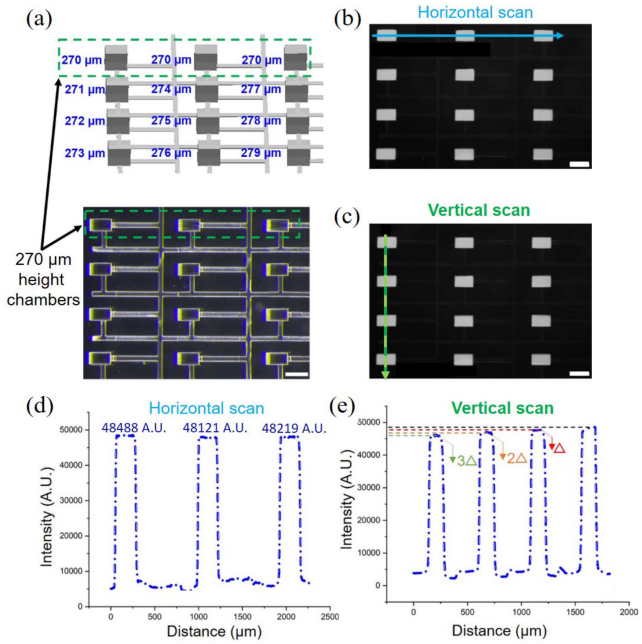

Fig. 6. Watermarking using reaction chambers' height increment. (a) A schematic showing increased height chambers to evaluate the intensity-distance relationship. The bright-field image taken from a light microscope shows the reaction chambers. The original and watermarked chambers are qualitatively indistinguishable. The scale bar is 250 μm. (b) The fluorescent image shows the Alexa Fluor 488 dye-filled chambers. A horizontal scan was done on the top row of the fabricated chambers. The scale bar is 250 μm. (c) The fluorescent image shows the Alexa Fluor 488 dye-filled chambers. A vertical scan was done on the leftmost column chambers. The scale bar is 250 μm. (d), The intensity versus distance plot corresponding to the horizontal scan in Fig. 6(b). (e) The intensity versus distance plot corresponding to the vertical scan in Fig. 6(c). Δ corresponds to the mean difference in the intensity for 1 μm height difference, which was recorded to be 733 A.U.

from the minimum (48121 A.U.), which resulted in the $\sigma = 367$ A.U. In comparison, the response in Fig. 6(f) shows increased intensities corresponding to the increased heights across the left-most first-column chambers shown in Fig. 6(d). The results demonstrated the highly sensitive nature of detection, where the response changed for even 1 μm of height increase. For the limit of detection (LOD), we defined a parameter Δ that corresponds to the difference in the intensity for 1 μm height difference, which we recorded to be 733 A.U. Using σ and Δ, we defined the limit of detection in (I_{LOD}) as in (8) [54]. By inserting the relevant values, we obtained $I_{LOD} = 1834$ A.U., which dictated the minimal step size to be followed for varying heights of the reaction chambers to insert the watermarks. Considering the obtained I_{LOD}, we propose the step size to be 3 μm, which can effectively give detection readings without getting interfered with noise signals. Thus, increasing the height of the chambers, leading to an increase in the fluorescence intensity post PCR amplification, offers an effective scheme for watermarking. By choosing certain reaction chambers (with increased heights), a watermark can be embedded that can be quantified using fluorescence intensity measurement. For a sensitive fluorescence microscope, which can quantify even 3 μm of height increment, as shown in this work, a FMB designer has several height

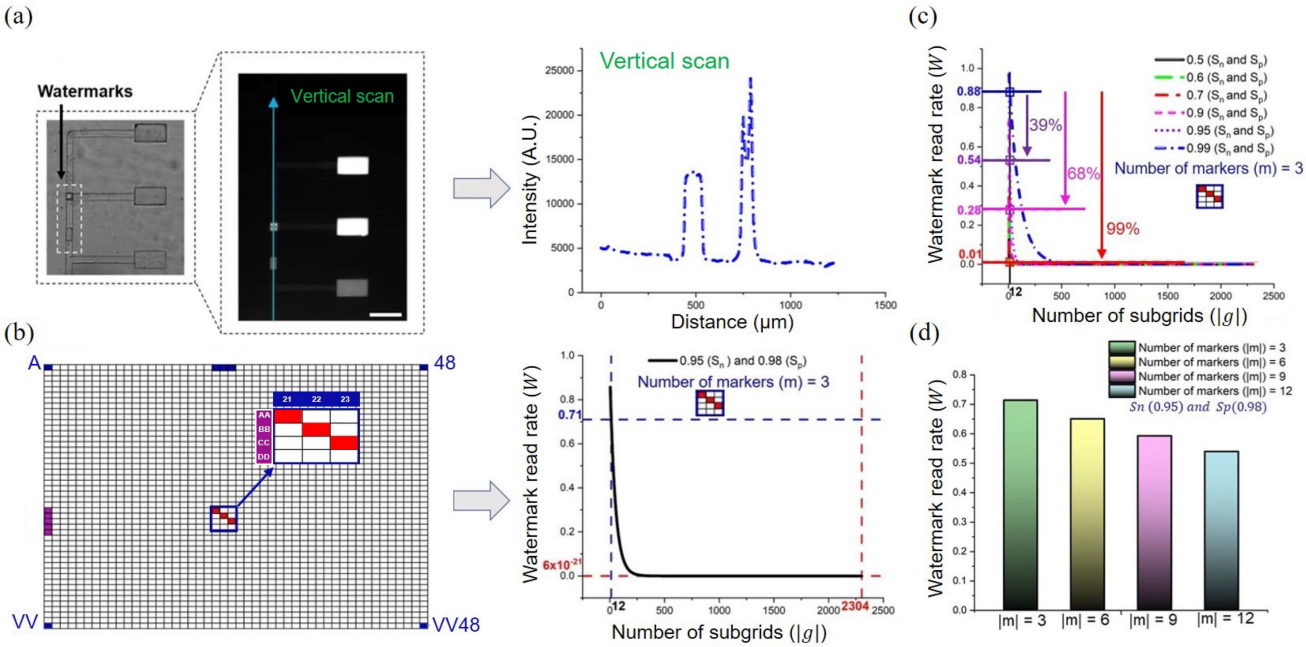

Fig. 7. Watermarking using microfluidic lines and watermark read rates. (a) Inserted structural and fluorescent watermarks and associated fluorescence intensity-distance response. The bright-field image shows the structural markers in the microfluidic lines. The zoomed image shows the fluorescent markers embedded in the microfluidic lines. The dimensions of the square marker are: height (200 μm), 50 μm $\times$ 50 μm, and the rectangular marker are: height (67.5 μm), 100 μm $\times$ 50 μm. The scale bar is 250 μm. (b) The schematic shows a labeled reference FMB to identify the location of the reaction chambers. The zoomed schematic shows the watermark where the number of markers is three, shown in red color. The sensitivity (Sn) is 0.95, and the specificity (Sp) is 0.98. The plot shows the associated watermark read rate (W) with respect to the number of sub grids ($|g|$) to detect the watermark. The number of markers is three, sensitivity (S_n) is 0.95 and specificity (Sp) is 0.98. (c) Watermark read rate versus $|g|$ for different $S_n = S_p$. (d) Watermark read rate versus number of markers (m) for $S_n = 0.95$ and $S_p = 0.98$.

options, which they can use to watermark or fingerprint the FMBs.

$$I_{LOD} = \Delta + 3\sigma \tag{8}$$

We considered signatures embedded only in the microfluidic lines, excluding the reaction chambers. By increasing the height of microfluidic channels at specific locations in the channels, structural (detected only by light microscopes) and fluorescent markers (detected only by fluorescence microscopes) can be obtained. These markers can act as a secret watermark, which can be used as a piece of evidence by the authentic party to claim ownership of the biochip. Fig. 7(a) shows light (for structural markers) and fluorescence microscopy (for fluorescent markers) images of the embedded markers in the microfluidic lines. The results (Supplemnetary Materials, Section IX) highlight the variability (location- and dimension-wise), which can be used to insert unique signatures for either watermarking or fingerprinting FMBs. This watermarking scheme provides two layers of protection where even though an attacker copies the structural watermark, copying the fluorescent markers, which involves matching the exact intensity-distance response based on the increased height of the channel portion, is difficult to achieve.

We quantitatively evaluated the efficacy of such a watermarking scheme, in terms of accuracy and stealth, by defining a metric, W, which is the probability of successful readout rate of the embedded watermarks. Although inserting watermarks was 3D in nature, the microscopy-based detection is 2D, where a set of markers needed to be detected on a set of the 2D grid for authenticity verification. The set of all grids (G) corresponded to the maximum possible number of markers that could be inserted on the grid. For the example shown in Fig. 7(b), $G = \{A1, A2, A3, \ldots, VV48\}$ contain 2304 elements. Let g be the subset of G whose elements contain sub grids to narrow down the search region for detecting the watermark markers. For the example in Fig. 7(b), the set $g = \{AA21, AA22, AA23, BB21, BB22, BB23, CC21, CC22, CC23, DD21, DD22, DD23\}$ contains 12 elements. Let m be the set of markers chosen for the watermark. For the example in Fig. 7(b), the set $m = \{AA21, BB22, CC33\}$ contains 3 elements. Let $|m|$ markers (cardinality of the set m be chosen out of $|g|$, where $|m| \leq |g|$. The set m serves as the watermark. The watermark can be codified by vectorizing the grid. For example, a 3×3 grid embedded with markers on the diagonal is coded by vectorizing the grid as $\{1, 0, 0, 0, 1, 0, 0, 0, 1\}$, where each entry is a grid location.

Let D be the event of detecting the markers when they are present (denoted by the event M). Similarly, let D' be the event of not detecting the markers when they are not present (denoted by the event M'). (9) relates W to the conditional probabilities of successfully detecting the markers ($P(D|M)$) when they are present and not detecting the markers ($P(D\prime|M\prime)$) when they are not present. These conditional probabilities are raised to

the power $|m|$ and $|g|-|m|$, respectively, to account for the probability of a successful watermark readout rate [17]. Note that $P(D|M)$ and $P(D'|M')$ can also be regarded as sensitivity (S_n) and specificity (S_p) [17], respectively, as shown in (10).

$$W = P\left(D' \mid M'\right)^{|g|-|m|} \cdot P(D \mid M)^{|m|} \tag{9}$$

Which implies that

$$W = (S_p)^{|g|-|m|} \cdot (S_n)^{|m|} \tag{10}$$

Note that S_n and S_p depend on the detection abilities of the system, such as the microscope and the CCD camera attached to it. Based on [17], we chose $S_n = 0.95$ and $S_p = 0.98$. After choosing the value of S_n and S_p, we fixed $|m|$ as to be 3 as per Fig. 7(b). We then varied $|g|$ from 3 to 2304 ($|m| \leq |g|$, therefore $|g|$ starts from 3) and recorded the variation in W. We varied $|g|$ up to 2304 ($|G|$) because the commercial biochip has a maximum of 2304 reaction chambers, schematically shown in Fig. 7(b). Using (10), we plotted W against $|g|$ for $S_n = 0.95$, $S_p = 0.98$, and $|m| = 3$, seen in Fig. 7(b). As $|g|$ denotes maximum number of sub grids in which the markers must be detected, we labeled the X-axis of Fig. 7(b) to be "Number of sub grids to detect the watermark ($|g|$)." The response in Fig. 7(b) suggests an exponential decrease in W with an increase in $|g|$. To interpret the results, we considered the following conditions.

Let us assume that an authentic end-user knows the watermarking scheme and the value $|g|$. After accessing the biochip, the user can simply zoom on to the pre-known $|g|$ under a microscope, to check the watermarks. We consider that a view from the microscope can successfully fit 12 reaction chambers at the given magnification. The user can detect three embedded markers out of 12 chambers using the microscopic view. Thus, for the authentic end-user, $|g| = 12$ and $|m| = 3$, and as per (10), $W = 0.7$, seen in Fig. 7(b). In contrast, an attacker who is willing to search and steal any watermarks has to search all the chambers using the microscopes (light or fluorescence). Therefore, for an attacker, $|g| = 2304$ and $|m| = 3$. As shown in Fig. 7(b) plot, the signature read rate W is 6×10^{-21}, which is close to zero given $S_n = 0.95$, and $S_p = 0.98$ for the microscope. Note that W approaches zero near $|g| = 250$. Thus, the attacker is most likely to miss the watermark.

We evaluated the effect of different $S_n = S_p$ values (ranging from 0.5 to 0.99) on W given $|g| = 12$ and $|m| = 3$. The results, plotted in Fig. 7(c), show a 39% and 68% decrease in W when $S_n = S_p$ decreased from 0.99 to 0.95 and 0.9, respectively. When $S_n = S_p$ was decreased from 0.99 to 0.7, W decreased to 99%. Further, when $S_n = S_p$ was decreased below 0.7, that is 0.6 and 0.5, the decrement in W showed 99% saturation. Thus, the evaluation highlighted a notable effect of S_n and S_p on W. Next, we increased the number of markers and evaluated W versus $|m|$ given $S_n = 0.95$ and $S_p = 0.98$. When the number of markers was increased from 3 to 6, we recorded a 8.8% decrease in W, as seen in Fig. 7(d). For 9 and 12 markers, we recorded a 17% and 24% decrease in W, respectively, with respect to the $|m| = 3$ case. For more specific detecting systems, increasing the number of markers decreases W owing to the $|m|$ variable that is present in the exponent of S_p, as seen in (10). Similar findings were reported by Tiwari et al. [17], where increasing the number of markers decreased the watermark read rate. Using such watermarking metrics, a quality control team can gain insights into the counterintuitive events, where even increasing the number of markers can decrease the read rate. Including such metrics in quality-control checks will help in the design of effective watermarks.

To tackle the reduction in W in Fig. 7(d), redundancy of grids can be useful [17]. (11) or (12) gives the signature read rate with redundancy (W_R), where R denotes replication of the grids used for the watermark. For $R = 1$, (12) reduces to (10). For $|g| = 12$, $|m| = 6$ and $R = 1$, $W_R = W = 0.65$, presented in Fig. 7(d). However, for $|g| = 12$, $|m| = 6$, and $R = 2$, $W_R = 0.78$, thereby increasing the read rate by 20% (Supplementary Materials, Section X). Thus, redundancy improves the read rate of the embedded watermarks if the detecting system is more specific than sensitive. However, the benefits do not always increase with increasing redundancy. This is because, while the sensitivity of the markers increases with redundancy, their specificity also increases with redundancy. Thus, the designer must select redundancy such that $\log W_R > \log W$ [17]. Solving this inequality, yields a cutoff factor, α_{cuttoff} (see (13)) to compute $|g|$ and $|m|$ so that W increases when using redundancy. α_{cuttoff} can be obtained using (14).

For example, for $R = 2$, $S_n = 0.95$, and $S_p = 0.98$, $\alpha_{\text{cuttoff}} = 0.33$. After inserting $\alpha_{\text{cuttoff}} = 0.33$ in (13) with $|g| = 12$, we get $|m| = 4$, which serves as a cutoff value for the number of markers. We evaluated two cases where $|m| = 3$ and 4, and we evaluated W with and without redundancy. For $|g| = 12$, $|m| = 3$ and $R = 1$, $W_R = W = 0.71$. However, when $|g| = 12$, $|m| = 3$ and $R = 2$, $W_R = 0.68$, a 4.2% decrease in the read rate. However, for $|g| = 12$, $|m| = 4$ and $R = 1$, $W_R = W = 0.69$. Moreover, when $|g| = 12$, $|m| = 3$ and $R = 2$, $W_R = 0.72$, indicating a 3.3% increase in the read rate, validating the cutoff effect (Supplementary Materials, Section X).

$$W_R = \left(P\left(D' \mid M'\right)^{R(|g|-|m|)}\right) \cdot \left(1 - \left(1 - P(D \mid M)^R\right)\right)^{|m|} \tag{11}$$

$$W_R = \left(S_p^{R(|g|-|m|)}\right) \cdot \left(1 - (1 - S_n)^R\right)^{|m|} \tag{12}$$

$$|g| \leq \frac{|m|}{\alpha_{\text{cuttoff}}} \tag{13}$$

$$\alpha_{\text{cuttoff}} = \frac{(R-1)\log_e S_p}{\log_e\left(\frac{S_n \cdot S_p^{R-1}}{1-(1-S_n)^R}\right)} \tag{14}$$

VII. Discussion

Flow-based microfluidic technologies are being commercialized for point-of-care, clinical, and molecular diagnostics. The complex manufacturing steps involved in fabricating FMBs result in a horizontal supply chain, making them vulnerable to cyber-physical threats. Considering the biomedical uses of FMBs, it is important to secure them against such threats.

We have focused on the security and trustworthiness of FMBs against two major threats: first, malicious cyber-physical threats,

which include the SB attack, and second, IP-theft threats, which include counterfeiting and overbuilding.

The SB attack deliberately decreases the heights of the FMB reaction chambers to produce false-negative results. These attacks can be deployed during the design and manufacturing of a FMB. An attacker in the design unit alters design codes to introduce structural faults and the compromised FMB is manufactured. In another scenario, an attacker in the manufacturing unit modifies the machine parameters to launch an SB attack. In either case, the compromised FMB evades detection by the quality control team and a faulty FMB is delivered to the customer. Microscope-based quality checks typically use 2D top views of FMBs to detect structural faults introduced during manufacturing. Since the reduced height of the reaction chambers cannot be easily detected from the 2D view using light microscopes, the SB attack is stealthy.

We experimentally demonstrated an SB attack on a FMB fabricated in our laboratory, whose fluidic lines and reaction chambers were adapted from a commercial biochip. Using a fluorescence microscope, we recorded the relative intensity decrease to quantify the effect of an SB attack. The attack reduced the fluorescence intensities with reduced-height reaction chambers with a high degree of correlation. To quantify the correlation, we developed regression models between the chambers' normalized height and intensity using a fluorescent dye (Alexa Fluor 488) and PCR-amplified DNA. The linear regression models showed 98.4% and 98.7% R-square values for the Alexa dye and amplified DNA, respectively. Using such a model, an attacker can decrease the chamber height to match fluorescence intensity of negative controls, generating false-negatives.

To circumvent such attacks, randomized checkpointing is a viable option in a resource-constrained system. We evaluated the stealth of SB attacks using a security metric based on randomized checkpoints. Assuming that the anomaly detection strategy, such as shadow-based or reflection-based anomaly detection on the chambers, is known a priori, a quality control checker can perform random trials (n) to detect the structural anomalies on the FMB. If the structural anomalies are not detected, the SB-attacked FMBs will evade the quality checks. We found an exponential decrease in the probability of evasion (P_e) with the number of views containing anomalous chambers (r). For example, a 71% decrease in P_e was recorded when r was increased from 1 to 5 given $n = 50$. A 36% decrease in P_e was recorded when r was increased from 1 to 5 for $n = 20$. Hence, by knowing n, an attacker can pick an optimum value of r to maximize P_e. On the other hand, FMB companies could proactively use randomized checkpointing metrics to secure their biochips.

Another security metric that we proposed uses independent Bernoulli trials, where the quality control checks are done on all the chambers rather than on a random subset described above. When checking all the chambers in a FMB using microscopes with different sensitivity (S_n) and specificity (S_p), we note a considerable increase in P_e for microscopes with low S_n and S_p values. We evaluated this using the Bernoulli trial-based metric by recording detection probabilities (P_D) for different S_n and S_p values. A manufactured FMB is rejected if at least one check identifies an SB-attack chamber. If the checker knows the anomaly detection policy, we defined the probability (S) of successfully rejecting a FMB for different P_D values. We evaluated P_D for different $S_n = S_p$ ranging from 0.5 to 0.99 and found that P_D increases when $S_n = S_p$ increases.

For example, when $S_n = S_p$ increased from 0.8 to 0.9 and 0.95, the P_D increased 2.9-fold and 7.4-fold, respectively. Using these P_D values, we evaluated the rejection probabilities (S). There is a considerable increase in S with the increase in P_D. For instance, a 41% increase in S was recorded when P_D increased from 0.07 (corresponding to $S_n = S_p = 0.8$) to 0.28 (corresponding to $S_n = S_p = 0.9$). In comparison, for P_D values equal to 0.54 and 0.88, corresponding to $S_n = S_p = 0.8$ and 0.99, respectively, S converged to unity. Thus, sensitivity and specificity of the microscopes can affect rejection probabilities to discard the SB-attacked FMBs. The Bernoulli trial-based security metric shows that even when the whole FMB is scanned for anomaly detection, there are opportunities for evasion depending on the capabilities of the detecting system. These two security metrics (randomized checkpoints and Bernoulli trials) can thus be used to safeguard FMBs against SB attacks.

To perform anomaly detection, we focused on DL algorithms to detect the structural anomalies in the image dataset. The image dataset was composed of microscopic images of the reaction chambers on the biochip. We consolidated our captured images and manually labeled them to represent ground truth and anomalies. The ground truth images were the ones where all reaction chambers are at 100% height. The presence of at least one reaction chamber with a different height was considered anomalous data. Our goal was to detect these anomalies and thwart the attack. We implemented two DL algorithms for anomaly detection: a 34-layer deep residual neural network ResNet-34 and a GAN (generative adversarial network)-based network-DCGAN. ResNet-34 was preferred compared to other deep neural networks since it solved the vanishing gradient problem by using residual network blocks. GAN-based anomaly detection, on the other hand, solved the problem of limited dataset size by generating synthetic data. The two approaches are promising in detecting the structural changes (with a recognition accuracy of 96%) in the FMB and hence, could be used for automatic quality control checks.

We proposed a device-level watermarking scheme for FMBs to secure them against IP-theft-based threats, such as physical reverse-engineering, counterfeiting, piracy, and overbuilding. The watermarking scheme increases the heights of specific reaction chambers and microfluidic channels at specific locations on the biochip. We showed that the height increments yield secret fluorescent watermarks, which could not be detected by light microscopes but would only be detected by fluorescence microscopes. We experimentally demonstrated this watermarking approach where even a 1 μm height change was detected by fluorescence microscopy. However, based on the standard deviation (noise) and mean value of the recorded measurements, we propose a minimum step size of 3 μm for height increment. We utilized this scheme of height increments at specific locations on the microfluidic channels that yielded structural markers (detected by light microscopes only) and fluorescent markers

(detected by fluorescence microscopes only) that jointly act as a watermark. These watermarks provide two layers of protection. Even if an attacker manages to find and copy the structural watermark, finding and copying the fluorescence-distance responses based on the channel height is exceedingly difficult.

To evaluate the efficacy of the watermarking schemes, we developed a watermark read rate (W) metric. We placed three markers ($|m| = 3$) on the reference biochip and calculated W for varying number of sub grids ($|g|$). These sub grids were the ones meant to detect the watermarking markers given $S_n = 0.95$ and $S_p = 0.98$. The $|g|$ varies based on the watermark location. For instance, an authentic end-user who knows the watermark location would directly go to the location for identification using a microscope. However, an attacker who does not know about the watermark location has to scan the whole biochip to steal the watermark details. We showed that W exponentially decreases with the increase in $|g|$, which is good for an authentic user but bad for the attackers, as they must search many more grids to identify the watermark. We compared W, given $|g| = 12$ for microscopes having S_n and S_p values ranging from 0.5 to 0.99. The read rate drastically reduced by reducing S_n and S_p values.

For example, we recorded a 99% decrease in W when $S_n = S_p$ values were decreased from 0.99 to 0.7. For detecting microscopes, which are more specific than sensitive, like in the case where $S_n = 0.95$ and $S_p = 0.98$, we observed that W decreased when a greater number of markers were used for a given watermarking region. To tackle this decrement, we proposed adding redundancy (R) by replicating the markers, which can subsequently increase W. However, the benefits are not indefinite with increasing redundancy, and there is a cutoff factor (α_{cuttoff}) that needs to be accounted for, ensuring the increase in W with redundancy. This is because, while the S_n of the markers increases with redundancy, the associated S_p also increases. Thus, the designer must carefully select redundancy by deciding on the α_{cuttoff} to satisfy $\log W_R > \log W$. A statistical metric like the ones proposed in this work can help designers embed watermarks in FMBs, which can be identified by an authentic user but not by an attacker, thus safeguarding FMBs against IP-theft-based attacks.

The device-level watermarking scheme increases the height of microfluidic components and channels. This can influence the manufacturing of biochips depending on the watermarking designs chosen by the biochip company. On the watermarking of designs, we present two scenarios here: watermarking and fingerprinting. On the other hand, in watermarking, the same watermark design is repeated in every biochip. In fingerprinting, a unique watermark design is embedded in each biochip, which is different from the others.

Watermarking: Since the mass manufacturing of FMBs is generally based on molding-based methods such as injection molding or hot embossing, there will be no significant influence of watermarking on the manufacturing of biochips. This is because the master molds need to be fabricated once, which can either be made by 3D printing or lithography techniques. Once the master molds are ready, the biochips can be mass manufactured using them along with the watermarks. For mass manufacturing, injection molding and hot embossing are the techniques largely employed in industries for easy and cost-effective manufacturing.

For 3D printing, the increased-height components will be directly incorporated into the associated design files for manufacturing. For lithography, however, the manufacturing process would include an extra fabrication step to take care of the increased height components. Once the master molds are ready, the biochips can be mass manufactured using them along with the watermarks.

Fingerprinting: Since fingerprinting here implies that each watermark is unique from sample to sample, design codes or process parameters must be changed every time the master mold is made. This is because the watermark design needs to be altered either location-wise on the biochip or height-wise (as the change in height induces a change in fluorescence intensity) to induce design variability with regard to the fingerprinted watermarks.

Fabricating a new master mold for each biochip to ensure the fingerprints would be extensive, instead, opting for batch-wise alteration of watermarks (where each batch contains a certain number of biochips) could be a feasible option.

This paper focused on device-level watermarking for FMBs, not fingerprinting.

VIII. Conclusion

This work focused on ensuring the security and trustworthiness of FMBs against two major threats: malicious physical level threats (including SB attacks) and IP-theft-based threats, which include counterfeiting and overbuilding.

SB attacks deal with deliberately decreasing the heights of the reaction chambers of FMBs to produce false-negative results. We experimentally demonstrated an SB attack on an FMB and showed that the attack can effectively reduce fluorescence intensity by lowering the height of the reaction chambers.

We quantified the correlation between the parameters using linear regression models, which showed 98.4% and 98.7% R-square values for the Alexa Fluor dye and PCR amplified DNA samples, respectively. To circumvent SB attacks, we adopted two existing DL models, which showed up to 96% validation accuracy in detecting microstructural faults.

To safeguard FMBs against IP-theft threats, we propose a device-level watermarking scheme by increasing the height of the microfluidic components and channels. We recorded sensitive stimulus-response pairs and demonstrated that even changes in height as small as 3 μm could be detected by fluorescence microscopy.

Acknowledgment

The authors thank New York University Abu Dhabi's Core Technology Platform (CTP), Dr. Mame Massar Dieng, and Dr. Priyam Narain for their help and support in this research.

References

[1] M. Shayan, S. Bhattacharjee, A. Orozaliev, Y.-A. Song, K. Chakrabarty, and R. Karri, "Thwarting bio-IP theft through dummy-valve-based obfuscation," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 2076–2089, 2020.

[2] C. Wang, M. Liu, Z. Wang, S. Li, Y. Deng, and N. He, "Point-of-care diagnostics for infectious diseases: From methods to devices," *Nano Today*, vol. 37, 2021, Art. no. 101092.

[3] M. B. Kulkarni and S. Goel, "Advances in continuous-flow based microfluidic PCR devices–a review," *Eng. Res. Exp.*, vol. 2, no. 4, 2020, Art. no. 042001.

[4] N. Mahhengam, A. F. G. Khazaali, S. Aravindhan, A. O. Zekiy, L. Melnikova, and H. Siahmansouri, "Applications of microfluidic devices in the diagnosis and treatment of cancer: A review study," *Crit. Rev. Anal. Chem.*, vol. 52, pp. 1863–1877, 2021.

[5] K. A. Fleming et al., "The lancet commission on diagnostics: Transforming access to diagnostics," *Lancet*, vol. 398, no. 10315, pp. 1997–2050, 2021.

[6] A. Mehra, "Molecular diagnostics industry worth $30.2 billion by 2027 – Report by Markets and markets," *marketsandmarkets.com*, 2022. Accessed: Nov. 16, 2022. [Onlin]. Available: https://www.marketsandmarkets.com/PressReleases/molecular-diagnostic.asp

[7] T. Lancet, "The act accelerator: Heading in the right direction?," *Lancet (London, England)*, vol. 397, no. 10283, 2021, Art. no. 1419.

[8] J. Tang, M. Ibrahim, K. Chakrabarty, and R. Karri, "Security implications of cyberphysical flow-based microfluidic biochips," in *Proc. IEEE 26th Asian Test Symp.*, 2017, pp. 115–120.

[9] D. P. Oran and E. J. Topol, "Prevalence of asymptomatic SARS-CoV-2 infection: A narrative review," *Ann. Intern. Med.*, vol. 173, no. 5, pp. 362–367, 2020.

[10] J.-F. Zhang, K. Yan, H.-H. Ye, J. Lin, J.-J. Zheng, and T. Cai, "SARS-CoV-2 turned positive in a discharged patient with COVID-19 arouses concern regarding the present standards for discharge," *Int. J. Infect. Dis.*, vol. 97, pp. 212–214, 2020.

[11] M. Dramé et al., "Should RT-PCR be considered a gold standard in the diagnosis of COVID-19?," *J. Med. Virol.*, vol. 92, pp. 2312–2313, 2020.

[12] F. Yu et al., "Quantitative detection and viral load analysis of SARS-CoV-2 in infected patients," *Clin. Infect. Dis.*, vol. 71, no. 15, pp. 793–798, 2020.

[13] R. Zhou et al., "Viral dynamics in asymptomatic patients with COVID-19," *Int. J. Infect. Dis.*, vol. 96, pp. 288–290, 2020.

[14] X. Xie et al., "Microfluidic nano-scale QPCR enables ultra-sensitive and quantitative detection of SARS-CoV-2," *Processes*, vol. 8, no. 11, 2020, Art. no. 1425.

[15] M. Teymouri et al., "Recent advances and challenges of RT-PCR tests for the diagnosis of COVID-19," *Pathol.- Res. Pract.*, vol. 221, 2021, Art. no. 153443.

[16] F. El-Sharkawy et al., "Saliva versus upper respiratory swabs: Equivalent for severe acute respiratory syndrome coronavirus 2 university screening while saliva positivity is prolonged after symptom onset in coronavirus disease 2019 hospitalized patients," *J. Mol. Diagnostics*, vol. 24, pp. 727–737, 2022.

[17] A. Tiwari, E. J. Villasenor, N. Gupta, N. Reddy, R. Karri, and S. T. Bukkapatnam, "Protection against counterfeiting attacks in 3D printing by streaming signature-embedded manufacturing process instructions," in *Proc. Workshop Additive Manuf. (3D Printing) Secur.*, 2021, pp. 11–21.

[18] S. S. Ali, M. Ibrahim, J. Rajendran, O. Sinanoglu, and K. Chakrabarty, "Supply-chain security of digital microfluidic biochips," *Computer*, vol. 49, no. 8, pp. 36–43, 2016.

[19] H. Chen, S. Potluri, and F. Koushanfar, "Biochipwork: Reverse engineering of microfluidic biochips," in *Proc. IEEE Int. Conf. Comput. Des.*, 2017, pp. 9–16.

[20] S. Bhattacharjee, J. Tang, M. Ibrahim, K. Chakrabarty, and R. Karri, "Locking of biochemical assays for digital microfluidic biochips," in *Proc. IEEE 23rd Eur. Test Symp.*, 2018, pp. 1–6.

[21] H. Chen, S. Potluri, and F. Koushanfar, "Flowtrojan: Insertion and detection of hardware trojans on flow-based microfluidic biochips," in *Proc. 18th IEEE Int. New Circuits Syst. Conf.*, 2020, pp. 158–161.

[22] M. Shayan, S. Bhattacharjee, Y.-A. Song, K. Chakrabarty, and R. Karri, "Microfluidic trojan design in flow-based biochips," in *Proc. Des., Automat. Test Europe Conf. Exhib.*, 2020, pp. 1037–1042.

[23] M. Shayan, S. Bhattacharjee, Y.-A. Song, K. Chakrabarty, and R. Karri, "Desieve the attacker: Thwarting IP theft in sieve-valve-based biochips," in *Proc. Des., Automat. Test Europe Conf. Exhib.*, 2019, pp. 210–215.

[24] T.-C. Liang, M. Shayan, K. Chakrabarty, and R. Karri, "Secure assay execution on meda biochips to thwart attacks using real-time sensing," *ACM Trans. Des. Automat. Electron. Syst.*, vol. 25, no. 2, pp. 1–25, 2020.

[25] M. Shayan, J. Tang, K. Chakrabarty, and R. Karri, "Security assessment of micro-electrode-dot-array biochips," *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, vol. 38, no. 10, pp. 1831–1843, Oct. 2019.

[26] S. S. Ali, M. Ibrahim, O. Sinanoglu, K. Chakrabarty, and R. Karri, "Security assessment of cyberphysical digital microfluidic biochips," *IEEE/ACM Trans. Comput. Biol. Bioinf.*, vol. 13, no. 3, pp. 445–458, May/Jun. 2016.

[27] J. Tang, M. Ibrahim, K. Chakrabarty, and R. Karri, "Secure randomized checkpointing for digital microfluidic biochips," *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, vol. 37, no. 6, pp. 1119–1132, Jun. 2018.

[28] M. Shayan, S. Bhattacharjee, J. Tang, K. Chakrabarty, and R. Karri, "Bioprotocol watermarking on digital microfluidic biochips," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 11, pp. 2901–2915, Nov. 2019.

[29] Y. Cong, J. Yuan, and J. Liu, "Sparse reconstruction cost for abnormal event detection," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, 2011, pp. 3449–3456.

[30] W. Li, V. Mahadevan, and N. Vasconcelos, "Anomaly detection and localization in crowded scenes," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 36, no. 1, pp. 18–32, Jan. 2014.

[31] M. Sabokrou, M. Khalooei, M. Fathy, and E. Adeli, "Adversarially learned one-class classifier for novelty detection," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, 2018, pp. 3379–3388.

[32] M. Sabokrou, M. Fayyaz, M. Fathy, and R. Klette, "Deep-cascade: Cascading 3D deep neural networks for fast anomaly detection and localization in crowded scenes," *IEEE Trans. Image Process.*, vol. 26, no. 4, pp. 1992–2004, Apr. 2017.

[33] I. Goodfellow et al., "Generative adversarial nets," in *Proc. 27th Int. Conf. Neural Inf. Process. Syst.*, 2014, pp. 2672–2680.

[34] M. Nakano, A. Takahashi, and S. Takahashi, "Fuzzy logic-based portfolio selection with particle filtering and anomaly detection," *Knowl.-Based Syst.*, vol. 131, pp. 113–124, 2017.

[35] H. N. Akouemo and R. J. Povinelli, "Probabilistic anomaly detection in natural gas time series data," *Int. J. Forecasting*, vol. 32, no. 3, pp. 948–956, 2016.

[36] S. Mascaro, A. E. Nicholso, and K. B. Korb, "Anomaly detection in vessel tracks using Bayesian networks," *Int. J. Approx. Reasoning*, vol. 55, no. 1, pp. 84–98, 2014.

[37] A. H. Hamamoto, L. F. Carvalho, L. D. H. Sampaio, T. Abrão, and M. L. Proença Jr., "Network anomaly detection system using genetic algorithm and fuzzy logic," *Expert Syst. Appl.*, vol. 92, pp. 390–402, 2018.

[38] Y. Li, L. Guo, Z.-H. Tian, and T.-B. Lu, "A lightweight web server anomaly detection method based on transductive scheme and genetic algorithms," *Comput. Commun.*, vol. 31, no. 17, pp. 4018–4025, 2008.

[39] Z. Chiba, N. Abghour, K. Moussaid, A. El Omri, and M. Rida, "A novel architecture combined with optimal parameters for back propagation neural networks applied to anomaly network intrusion detection," *Comput. Secur.*, vol. 75, pp. 36–58, 2018.

[40] T. Kubota and W. Yamamoto, "Anomaly detection from online monitoring of system operations using recurrent neural network," *Procedia Manuf.*, vol. 30, pp. 83–89, 2019.

[41] V. Hodge and J. Austin, "A survey of outlier detection methodologies," *Artif. Intell. Rev.*, vol. 22, no. 2, pp. 85–126, 2004.

[42] M. Agyemang, K. Barker, and R. Alhajj, "A comprehensive survey of numeric and symbolic outlier mining techniques," *Intell. Data Anal.*, vol. 10, no. 6, pp. 521–538, 2006.

[43] M. Injadat, F. Salo, A. B. Nassif, A. Essex, and A. Shami, "Bayesian optimization with machine learning algorithms towards anomaly detection," in *Proc. IEEE Glob. Commun. Conf.*, 2018, pp. 1–6.

[44] W. Xie, J. Lei, B. Liu, Y. Li, and X. Jia, "Spectral constraint adversarial autoencoders approach to feature representation in hyperspectral anomaly detection," *Neural Netw.*, vol. 119, pp. 222–234, 2019.

[45] N. Chouhan et al., "Network anomaly detection using channel boosted and residual learning based deep convolutional neural network," *Appl. Soft Comput.*, vol. 83, 2019, Art. no. 105612.

[46] T.-Y. Kim and S.-B. Cho, "Web traffic anomaly detection using C-LSTM neural networks," *Expert Syst. Appl.*, vol. 106, pp. 66–76, 2018.

[47] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, 2016, pp. 770–778.

[48] Q. Wu, Y. Chen, and J. Meng, "DCGAN-based data augmentation for tomato leaf disease identification," *IEEE Access*, vol. 8, pp. 98716–98728, 2020.

[49] D. Jha et al., "A comprehensive study on colorectal polyp segmentation with resUNet, conditional random field and test-time augmentation," *IEEE J. Biomed. Health Inform.*, vol. 25, no. 6, pp. 2029–2040, Jun. 2021.

[50] J. Dai, Y. Li, K. He, and J. Sun, "R-FCN: Object detection via region-based fully convolutional networks," in *Proc. 30th Int. Conf. Neural Inf. Process. Syst.*, 2016, 379–387.

[51] C.-Y. Fu, W. Liu, A. Ranga, A. Tyagi, and A. C. Berg, "DSSD: Deconvolutional single shot detector," Jan. 2017, doi: 10.48550/arxiv.1701.06659.
[52] Z. Wu, C. Shen, and A. Van Den Hengel, "Wider or deeper: Revisiting the resnet model for visual recognition," *Pattern Recognit.*, vol. 90, pp. 119–133, 2019.
[53] A. Radford, L. Metz, and S. Chintala, "Unsupervised representation learning with deep convolutional generative adversarial networks," in *Proc. 4th Int. Conf. Learn. Representations*, Y. Bengio and Y. LeCun, Eds., San Juan, Puerto Rico, May 2-4, 2016.
[54] F.-G. Banica, *Chemical Sensors and Biosensors: Fundamentals and Applications*. Hoboken, NJ, USA: Wiley, 2012.

Navajit Singh Baban received the B.Tech. degree in mechanical engineering from VIT University, Vellore, India, during 2008–2012, and the M.Tech. degree in materials science from the Indian Institute of Technology, Kanpur, India, during 2012–2014, and the Ph.D. degree from NYU Mechanical and Aerospace Engineering, New York, NY, USA, as a Global Ph.D. Fellow, during 2016–2021. From 2014 to 2016, he was an Assistant Professor of mechanical engineering with Lovely Professional University, Punjab, India. He is currently with the Center for Cyber Security, New York University Abu Dhabi, United Arab Emirates, as a Postdoctoral Associate. His research interests include cyberphyiscal security of microfluidic biochips, mechanobiology and bioinspired adhesion, and fracture Mechanics.

Sohini Saha received the B.Tech. degree from the Indian Institute of Engineering Science and Technology, Shibpur, India, in 2019. She is currently working toward the Ph.D. degree with Duke University, Durham, NC, USA. She was a Software Developer with PwC, New Delhi, India, creating and delivering Web applications in an agile environment till 2021. Her research interests include building secure and resilient hardware while using machine learning techniques and microfluidic biochips.

Ajymurat Orozaliev received the Diploma in engineering from International Alatoo University, Bishkek, Kyrgyzstan, in 2011, and the Master of Science degree in microsystems engineering from the Masdar Institute of Science and Technology, Abu Dhabi, UAE, in 2013. He is currently a Research Engineer with New York University Abu Dhabi, United Arab Emirates. His research interests include microfluidics, microfabrication, and biosensors.

Jongmin Kim received the B.S., M.S. and Ph.D. degrees in chemical engineering from Chungnam National University, Daejeon, Korea, in 2011, 2013, and 2017, respectively. He is currently a Research Associate with Engineering division, New York University Abu Dhabi, Abu Dhabi, UAE. His research interests include microfluidics, nucleic acid sensors based on electrokinetic, CRISPR-Cas technologies, and Organoids on a chip.

Sukanta Bhattacharjee received the B.Sc. (with Hons.) degree in computer science and the B.Tech. degree in computer science and engineering from the University of Calcutta, Kolkata, India, in 2006 and 2009, respectively, and the M.Tech. and Ph.D. degrees in computer science from the Indian Statistical Institute, Kolkata, India, in 2012 and 2017, respectively. He is currently an Assistant Professor with the Department of Computer Science and Engineering, Indian Institute of Technology, Guwahati, India. He was a Postdoctoral Fellow with the Center for Cyber Security, New York University Abu Dhabi, Abu Dhabi, UAE. He was also a Visiting Scientist with the Advanced Computing and Microelectronics Unit, Indian Statistical Institute. His research interests include design automation algorithms, microfluidics, and security.

Yong-Ak Song received the B.S., M.S., and Ph.D. degrees in mechanical engineering from RWTH Aachen University, Aachen, Germany. He is currently an Associate Professor of mechanical and biomedical engineering and Head of the Bioengineering Program with NYU Abu Dhabi, UAE. He is also the Director of the Micro- and Nanoscale Bioengineering Group with the New York University, Abu Dhabi. He was with Micro/Nanofluidic BioMEMS Group, Department of Electrical Engineering and Computer Science, MIT, Cambridge, MA, USA, before joining the Division of Engineering with NYU Abu Dhabi in August 2012. His research and teaching interests include interdisciplinary in both engineering disciplines such as multiscale fluid mechanics, micro/nanofabrication, and in biological engineering areas such as Biosensors, Biomimetics, and Biomechanics.

Ramesh Karri (Fellow, IEEE) received the B.E. degree in ECE from Andhra University, Visakhapatnam, India, and the Ph.D. degree in computer science and engineering from the University of California at San Diego, La Jolla, CA, USA. He is currently a Professor of electrical and computer engineering with New York University (NYU), New York, NY, USA. He also co-directs the NYU Center for Cyber Security. He also leads the Cyber Security thrust of the NY State Center for Advanced Telecommunications Technologies, NYU. He Co-founded the Trust-Hub. His research and education interests include hardware cybersecurity include trustworthy ICs, processors and cyber-physical systems, security-aware computer-aided design, test, verification, validation, and reliability, nano meets security, hardware security competitions, benchmarks, and metrics, biochip security, and additive manufacturing security.

Krishnendu Chakrabarty (Fellow, IEEE) received the B. Tech. degree from the Indian Institute of Technology, Kharagpur, India, in 1990, and the M.S.E. and Ph.D. degrees from the University of Michigan, Ann Arbor, MI, USA, in 1992 and 1995, respectively. He is currently the John Cocke Distinguished Professor of electrical and computer engineering, Duke University, Durham, NC, USA. His research interests include design-for-testability of 3D integrated circuits, AI accelerators, microfluidic biochips, hardware security, AI for healthcare, and neuromorphic computing systems. Prof. Chakrabarty was the Editor-in-Chief of *IEEE Design & Test of Computers* during 2010–2012, *ACM Journal on Emerging Technologies in Computing Systems* during 2010–2015, and IEEE TRANSACTIONS ON VLSI SYSTEMS during 2015–2018. He is a Fellow of ACM and AAAS, and a Golden Core Member of the IEEE Computer Society.