

Secure and Trustworthy Cyberphysical Microfluidic Systems: NSF Award 2049335

PIs: Krishnendu Chakrabarty (Duke University), Ramesh Karri (New York University)



ABSTRACT

This project is focused on ensuring the security and trustworthiness of cyber-physical microfluidic systems (CPMS). We have thus far considered two major types of threats in CPMS: 1) Countering against biochemical threats – Molecular barcoding for digital microfluidic biochips (DMFBs) and 2) Countering result-tampering in continuous flow-based microfluidic biochips (CFMBs).

KEY PROBLEMS

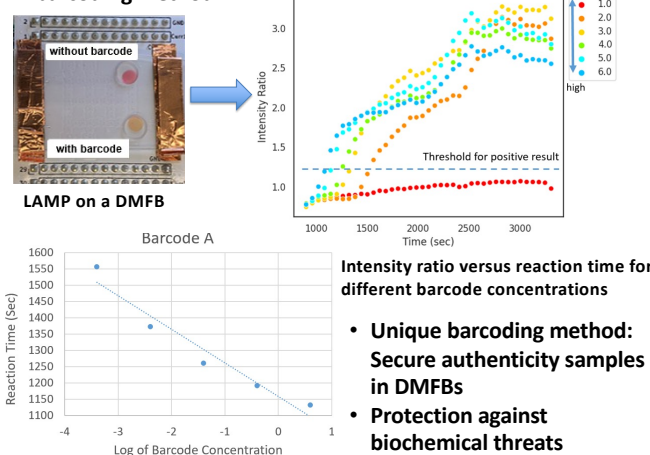
- Biochemical threats: Sample tampering in DMFBs
- Malicious threats: Structure-based (SB) and Material-based (MB) attacks on CFMBs
- IP-theft threats: Counterfeiting and overbuilding attacks on CFMBs

SCIENTIFIC IMPACT

- Ensure security and trustworthiness of biochips used for medical diagnostics and research
- The project will add knowledge and understanding toward stealthy attacks
- Help biochip designers to come up with rational countermeasures

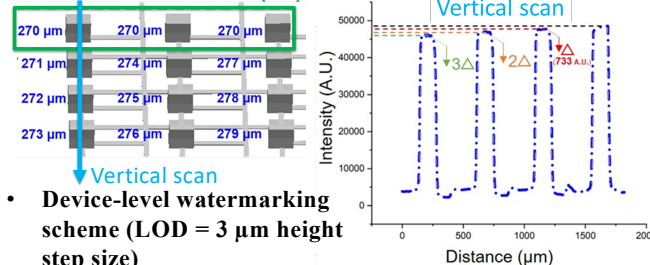
MOLECULAR BARCODING

- Loop-mediated isothermal amplification (LAMP) reactions as a barcoding method

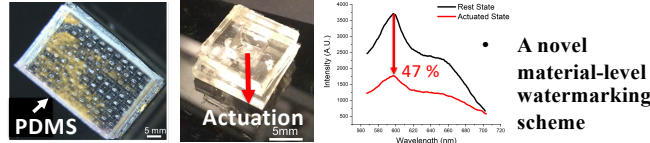


Reaction time versus barcode concentrations

STRUCTURE-BASED (SB) WATERMARKING SCHEME

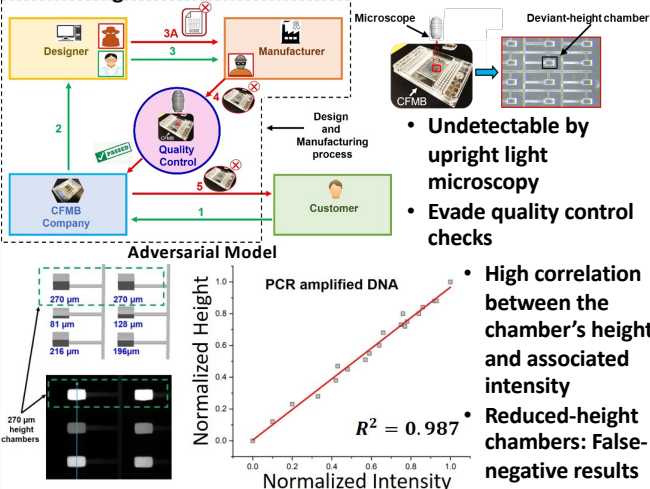


MATERIAL-BASED (MB) WATERMARKING SCHEME

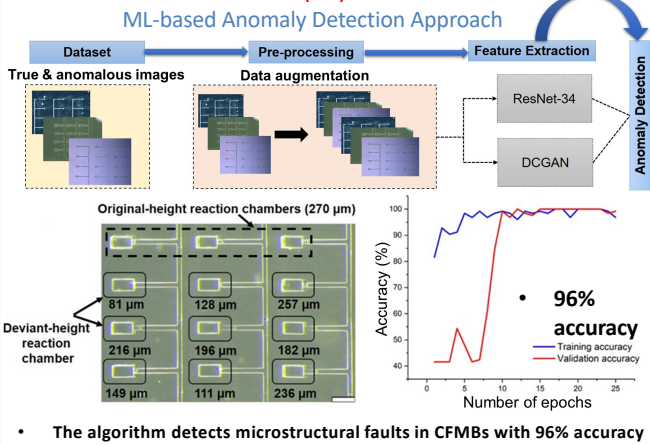


STRUCTURE-BASED (SB) ATTACK MODEL

- Deliberately decreasing reaction chamber's height to produce false-negative results



STRUCTURE-BASED (SB) DEFENSE MODEL



- Safeguard biochips in the era of global pandemics and personalized medicine

- Educate clinicians worldwide who are actively involved in clinical diagnostics

- The molecular diagnostics market is projected to be worth the 31.8 billion USD by 2026

