SECURITY THROUGH PHYSICAL DYNAMICS IN MEDICAL AND MANUFACTURING PLATFORMS

By

TUAN LE

A dissertation submitted to the

School of Graduate Studies

Rutgers, The State University of New Jersey

in partial fulfillment of the requirements

for the degree of

Doctor of Philosophy

Graduate Program in Electrical and Computer Engineering

Written under the direction of

Saman Zonouz & Mehdi Javanmard

and approved by

____

____

____

____

New Brunswick, New Jersey

May, 2019

ABSTRACT OF THE DISSERTATION

Security through Physical Dynamics in Medical and Manufacturing Platforms

by Tuan Le

Dissertation Directors:
Saman Zonouz & Mehdi Javanmard

Portable medical diagnostic or point-of-care (POC) devices enable the transition from reactive, clinical-based healthcare to preventive, patient-centered management. POC devices have been shown to have accuracy and performance equivalent of laboratory equipment. However, this does not remove medical practitioner's involvement in result analysis. The diagnostic results would be exchanged between the patients and medical practitioners. In this framework, a trustworthy and usable healthcare requires not only effective diagnostics but also lightweight user privacy-preserving capabilities.

On the other hand, Additive Manufacturing (AM) or 3D printing has been found applicable in manufacturing safety-critical parts and medical implants. AM is projected to reach 50% market potential by 2038. Due to its potential expansion, AM has become an attractive target to the attackers. Initiatives have been undertaken to study the impact of malicious attacks to critical components. Correspondingly, we develop an end-to-end malicious attack detection in AM in this study.

This thesis focuses on the developing of solutions for diagnostic information and user privacy protection leveraging the physical system designs of biomedical device and the malicious detection in manufacturing platform. The thesis will focus on three major tasks: information protection, user privacy protection, and malicious attacks detection.

In information protection, we introduce a diagnostic information protection for impedance flow cytometry. The encryption scheme is developed leveraging the design of the microfluidic device. The sensor of a microfluidic device is designed to be mechanically re-configurable to enable the encryption of information.

In user privacy protection, we present a protection scheme leveraging functionality of impedance flow cytometry. In this scheme, we perform a domain specific user authentication by embedding the synthetic microbeads in the test device as authentication strings. This alternative method removes the authentication burden from users and protects their privacy by preventing them from linking personal information to the test results.

Applying the similar physical design concept, we present the solution for malicious attack detection in additive manufacturing or 3D printing. The scheme incorporates real-time tracking of instrument and post production material analysis to reconstruct the physical design model for verification and detection of malicious modification. This allows the end user to accurately verify and manage the 3D printed models in real-time.

Furthermore, we present a design of portable malicious material detection device in additive manufacturing. The design utilizes the lock-in amplifier architecture to detect the change of material during printing. The portable device can be used in real-time malicious detection of material modification in traditional 3D printing.

Acknowledgements

I would like first to thank my doctoral committee: Dr. Raheem Beyah, Dr. Janne Lindqvist, Dr. Saman Zonouz, and Dr. Mehdi Javanmard for their valuable feedback.

I woud like to thank the researchers that I had the pleasure of collaborating with including Gabriel Salles-Loustau, Luis Garcia, Sriharshar Etigowni, Christian Bayens, Pengfei Xie, Zhongtian Lin, Niloy Talukde, Abbas Furniturewalla, Xueyuan Zhao, Vidyasagar Sadhu, Naixin Song, Wen Shen, Dario Pompil, Laleh Najafizadeh, Raheem Beyah, and Mark Allen; as well as my labmates: Jianye Sui, Azam Gholizadeh and Sakshi Sardar.

I would like to give special thank and appreciation to my advisers Dr. Saman Zonouz and Dr. Mehdi Javanmard for their unwavering patience and guidance in my study.

To my friends, Edyn Pineda, Eric Wengrowski, Gradeigh Clark, Kliti Kodra, Maja Skataric, Tim Phan, and Sanket Wagle, I'd like to express my gratitude for their friendship throughout the duration of my study.

Finally, I would like to express my great appreciation to my parents for their boundless love and support they have given. To my brother Duy-Anh Le and my sister Van-Anh Le, thank you for all the laughter and memories. I could not have finished my study without them.

Dedication

For my parents who inspired my curiosity.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

Healthcare management and delivery costs in developed countries are skyrocketing. In response to this trend, federal agencies have supported diverse lines of applied research in the use of technology for health monitoring and intervention [75, 103]. In the market report of 2013, the portable medical devices is expected to be worth $20 Billion by 2018 [32]. The intention is to take advantage of the state-of-the-art technologies to compile information about medical health, securely, and in real-time, and thereby, transition from reactive and hospital-centered to preventive, patient-centered and cost-effective health care and management with greater focus on well-being.

Mobile-based Point-of-Care (POC) diagnostics by taking advantage of miniaturized devices and mobile technology can dramatically increase the role patients take in their own health care, and consequently reduce health care costs. POC diagnostics refer to in-vitro diagnostic tests that do not require the involvement of laboratory staff and facilities to make results available both to the medical professional and the patient [49, 63, 31]. The possibility of integrating POC systems with mobile platforms has been recently demonstrated through the diagnosis of a series of conditions including vitamin-D deficiency and Kaposi's Sarcoma disease [81, 72, 79]. At the same time, the recently increasing popularity of using information technologies for health care has attracted cyber criminals to this area as well, giving birth to various types of malware and adversarial intrusions against medical critical infrastructures. The number of data breaches across health care sectors have increased by 30% during 2013 [59]. As a result, while the availability of mobile-based POC diagnostics systems to the public creates great opportunities in the health care domain, it will be associated with serious privacy and security concerns, due to vulnerabilities on the cyber end.

As an example of specific use case, a mobile-based biomedical diagnostic device design consists of a portable diagnostic tool and mobile device for transferring information to remote server for computation and storage. In this diagnostic device, the attacker can leverage the compromised mobile device to access medical records and user's private information associating with the records. Furthermore, in current practice, medical records and associating user's information are protected via IT infrastructure at the remote server. In this setting, a single point of failure would lead to exposing users' information. Therefore, in this thread model, the attacker can use multiple attack vectors such as compromising the link between the diagnostics device and the remote server, or the IT infrastructure to gain access to medical records and user's private information.

While the development of POC device helps enabling patient-centered, preventive healthcare, it does not remove the role of medical practitioners. The users would have to communicate the diagnostic results and user's information with healthcare providers. In this scenario, an ideal protection scheme is to obfuscate the medical and user's information prior to sending data to remote server. Within this framework, we develop the encryption using small trusted computing base and authentication scheme embedded within the physical design of POC device. More specifically, the deployment of an ideal medical diagnostics solution necessitates meeting three core requirements:

i) portability and low-cost. Ease-of-use and user convenience requires a portable solution so that the users, e.g., elderly patients with regular diagnostic/testing prescriptions, can get themselves tested without having to make hospital visits. Additionally, replacing legacy inexpensive (though sometimes tedious) clinical testing calls for a low-cost solution that can be purchased and used by ordinary civilians;

ii) accuracy and performance. Due to their importance and potential life-changing impact, the correctness of the outcome of medical tests, e.g., HIV tests, is crucial. Furthermore, because of the same reasons, patients are often willing to pay higher cost for more accelerated testing procedures. Consequently, the proposed solution must satisfy both needs.

iii) usable security and privacy guarantees. Encryption and user authentication apply per medical record at the POC device while performing diagnosis. Medical and user's information are protected prior to sending to remote server. The POC device increases granularity of information and privacy protection per medical record as addition to the database-wise encryption at remote server in the event of IT infrastructure failure. Furthermore, the development of information and user's privacy protection scheme should not impair the usability of the POC device.

Similarly, the rapid expansion in Additive Manufacturing (AM) or 3D printing has become an attractive target to the attackers. With the estimation of reaching 50% market potential in 2038 [124], AM has been found more applicable in industries for both prototyping and production-quality manufacturing of safety-critical parts in engines for automotive and aerospace [23, 37, 88]. 3D printing has also been employed to produce components in defense projects [52, 56]. Apart from aerospace and automotive, AM also has wide application in medical field. Researchers have studied the use of 3D printing in tissues and organs fabrication, creating prosthetic, medical implants, and anatomical models [89, 12, 121].

Works have been undertaken to understand the impact of malicious attacks to safety-critical and medical components in 3D printing. Yampolskiy, *et al.* outline a taxonomy for the potential of misusing 3D printer as a weapon [129]. The attacker can compromise a 3D printer to alter mechanical properties in safety-critical components in the jet engines. In some cases, the 3D printer itself can be turned into a weapon which can endanger human life. For instance, a Massachusetts 3D printing company Powderpart had their printer exploded and inflicted third-degree burns on a company employee [109]; concurrently, the FBI has acquired 3D printers to study the feasibility of manufacturing homemade explosive devices [108]. Yampolskiy, *et al.* further analyzes the security challenges with metal and alloys where the attackers seek to change physical properties of 3D printed components by manipulating the manufacturing equipment [130].

Major industries have also investigated mitigation techniques to detect the malicious attacks. Boeing investigated several imaging techniques to detect voids, cracks, or foreign materials in 3D structure [43]. Others used ultrasound, X-ray, and computed tomography (CT) scan to detect cracks and bonding defects in non-destructive inspections [104, 47]. However, these post-production mitigation techniques do not prevent the malicious attacks from happening. While these quality control inspections can detect the malicious attacks, the manufactured parts already compromised. The manufacturer would have to shut down the assembly line for repair; and the product would have to be recalled and replaced.

In detection of malicious attacks in AM, the second part of this thesis focuses on the development of an end-to-end solution on the entire manufacturing process to detect the attack as it happens. Leveraging the inherent acoustic signal and physical movement of 3D printer, we devise a 2-parts solution to monitor the 3D printing process in real-time and verify the 3D printed models after printing. We further expand the thread model in 3D printing attacks to include the attack vector where the 3D printing materials are used in embedding malicious attacks. While the current studies do not focus on the attack leveraging the materials in 3D printing, embedded active materials can alter the structure of 3D printed objects when stimulated [21, 71, 86].

To address the cybersecurity of portable devices, in this thesis, we develop the solution consisted of three major design aspects of an ideal POC diagnostic device: security, flexibility, and portability. We first propose an information and users privacy protection scheme in medical diagnostic device using impedance flow cytometry.

We then propose the solutions for verification and malicious detection in additive manufacturing with biomedical applications. Lastly, we present a complete design of the portable, real-time malicious material detection in additive manufacturing.

Trusted Sensing for Signal Protection in Point-of-Care Device. Trustworthy and usable healthcare requires not only effective disease diagnostic procedures to ensure delivery of rapid and accurate outcomes, but also maintaining the confidentiality of patient's medical test results.

Chapter 2 presents diagnostic data protection scheme for cytometry-based point-of-care (POC) systems. Our solution consists in a biomarker detection sensor integrated with a smartphone to provide users with easy-to-use real-time diagnostic capabilities, thereby, reducing the need for in-person clinical visits. The proposed hardware-level trusted sensing framework obfuscates the measured analog signals that relate to patient's blood cell counts. The diagnostic outcome, based on the cell counts, is protected through an encryption scheme, before sending out the data through the smartphone to the cloud for analysis. The outcome of the analysis is then sent back to the device for decryption and user notifications. The proposed data protection scheme is realized for a prototype consisting of a biosensor connected to a smartphone. A smartphone app and cloud-based service that perform the analysis have also been implemented. This design guarantees the data protection by considering the smartphone and the cloud server possibly untrusted: the proposed setup assumes a honest-but-curious security model.

Transparent User Authentication through Biophysical Channels. Information exchange between the patient and medical practitioner requires the patient and the test results to be respectively authenticated and identified on the storage service to ensure that the medical diagnostic results are properly stored and their access is protected. Ideally, the information exchange between the patient and practitioner is an automated and transparent process for the patient.

Chapter 3 presents the domain specific solution for user authentication. Portable medical devices reduce the dependency on healthcare infrastructure. While these devices provide convenient heath monitoring features, they still require a medical practitioner involvement to analyze the results. The secure authentication phase is particularly critical for medical diagnostics: patient data exposure could lead to negative social effects. This work focuses on providing a transparent authentication mechanism for patient blood tests performed using impedance flow cytometry. The goal is two-fold: first, to alleviate the user from security procedures, precisely an authentication step, while using the medical device; second, to provide a unique identifier for the test results when stored in a remote server. This chapter describes a domain specific authentication method for impedance flow cytometry devices. We combine micro synthetic beads of different sizes, at determined concentrations, to generate the unique authentication strings which identify specific test results on the remote storage service. These authentication strings embed in the test devices and can be used as a convenient alternative to generic authentication method, such as logins and passwords. This alternative method removes the authentication burden from the user and protects the patients privacy further by preventing them from linking their personal information to their test results.

Malicious Fill Pattern Detection in Additive Manufacturing. Additive Manufacturing is an increasingly integral part of industrial manufacturing. Safety-critical products, such as medical prostheses and parts for aerospace and automotive industries are being printed by additive manufacturing methods with no standard means of verification.

Chapter 4 develop the schemes of verification and intrusion detection that is independent of the printer firmware and controller PC. The scheme incorporates analyses of the acoustic signature of a manufacturing process, real-time tracking of machine components, and post production materials analysis. Not only will these methods allow the end user to verify the accuracy of printed models, but they will also save material costs by verifying the prints in real time and stopping the process in the event of a discrepancy. In this investigation, we present a use case in which an erroneous print of a tibial knee prosthesis is identified.

Malicious Materials Detection in Additive Manufacturing. Materials in 3D printing has yet to be scrutinized [131]. The detection of material changes is crutial in preventing the embedding of unknown material within 3D printed object.

Chapter 5 presents the preliminary design and evaluation of a portable malicious material detection in additive manufacturing. The design utilizes the lock-in amplifier architecture to detect the changes of materials during 3D printing. The portable device can effectively verify the materials being used in the 3D printer and help cutting production cost by early detection of malicous materials.

Chapter 6 concludes this thesis and opens discussion for potential future works.

Chapter 2

Trusted Sensing for Signal Protection in Point-of-Care Device

1 Introduction

Based on the Gallup Poll for the Institute for Health Freedom [36], 70% of the respondents were concerned about the confidentiality of their medical records [29]. Due to increase of vulnerabilities exploited on the information technology (IT) infrastructures, concerns about the privacy of medical records have increased among patients, as sensitive information disclosure may result in undesired consequences such as insurance premium raises and negative social affects. Medical institutions often fail to properly protect patient information and data leaks are common. For example, in 2015, 269 unsecured health information breaches, affecting more than 113M user records, were reported to the breach portal of the U.S Department of Health and Human Services [94]. Such information leaks would have a lesser impact if the data was protected using encryption. Unfortunately, at least 47% of the medical institutions do not use encryption on medical records [106]. Even if encryption is used, the safety of the data relies on the safety of institutions' IT infrastructure. In existing models, patients have no choice but to trust medical institutions to properly handle and store their records.

Point-of-care (POC) medical devices enable a shift from clinic-based medical tests by enabling patients to perform medical diagnostics on their own. Even though such solutions attempt to minimize the necessity to be physically present in a clinic, they do not necessary eliminate the dependence on IT infrastructures. Two examples of such dependency are:

- The test (e.g. cytometry measurements) might require computational tools and resources to determine a diagnosis from a set of measurements.

- The patient may eventually want to share the diagnostic outcome with a health care professional, requiring the use of an IT infrastructure.

As a result, it is critical to develop new solutions for POC devices that can guarantee confidentiality of patients' medical information.

This study introduces an innovative obfuscation scheme, with a small trusted computing base (TCB), that is designed to protect the diagnosis obtained through impedance cytometry. Cytometry and particle quantification have been successfully used for the diagnosis of a wide range of pathological conditions such as cancer and infectious (both viral and bacterial) diseases [48, 11, 83, 82, 16, 17, 80, 28, 122, 61, 62, 125, 119, 68].

Impedance cytometry relies on identifying special characteristics of the signal, measured by the sensor, which corresponds to the impedance of the cells passing through the channel. These characteristics includes the width and the amplitude of the peaks observed in the signal that can be used to identify and count the number of different types of cells that exist in the sample (e.g. the blood sample) under the test. Detecting the peaks and identifying their characteristics from the measured signal typically require computing resources. Previous work [81, 33, 72] have utilized smartphones or remote systems to perform these computations, where raw patient data is disclosed to the computing resource. However, general purpose operating systems and smartphone operating system are known to be vulnerable to failures and compromises. As such, protection mechanisms that do not assume that local (e.g. user's smartphone) or remote (e.g. cloud service) computing resource is trusted are needed to protect the confidentiality of the measurements or the diagnostic outcome against cyber-attacks.

The scheme proposed in this work relies on a novel sensor design that allows the user to dynamically change the sensor configuration while performing measurements on a blood sample. The obfuscation relies on the premise that each configuration will generate a different output for a given input (i.e. a type of blood cell). The resulting signal cannot be interpreted by an observer unaware of the user-imposed configuration of the sensor.

The configuration parameters correspond to the encryption key. This key is similar to a One-Time Pad, i.e. a set of parameters correspond to a specific sensor configuration, and thus, a specific signal obfuscation. Therefore, only an observer who knows these parameters can correctly interpret the results by reverting the changes that are due to the sensor configuration.

Since the obfuscation takes place while measuring the signal at the sensor level, the trusted computing base of this system consists only of the sensor itself. The threat model assumes that the external computing resource (in charge of analyzing the signal) follows an *honest but curious* security model, i.e. the computing resource might collect, share or analyze the data it receives and try to recover the information, but it will correctly perform the operations requested. While this domain specific encryption resembles to the One-Time Pad digital data encryption mechanism, it differs from already existing encryption and scrambling techniques by operating in the analog domain, during the signal acquisition phase, rather than relying on a post-acquisition sequence of transformations.

This chapter is organized as follows. Section 2 reviews the previous studies related to this work and presents an overview of the components of the POC system. Section 3 describes the design of the microfluidic device for the proposed encryption scheme. Section 4 details the signal protection mechanism. Section 6 concludes the chapter.

2 Related Work and Overview

This section reviews signal encryption, medical device security, and microfluidic biomarker detection related work.

General-purpose and traditional digital symmetric data encryption [25] would require to decipher the samples on the server side for analysis and would reveal the clear dataset. Existing homomorphic encryption algorithms [42] currently do not provide the calculus flexibility and performance required to deal with biomarker sensor measurements. Additionally, conventional cryptography work on digital data points that would require addition of fairly complex analog-to-digital circuitry.

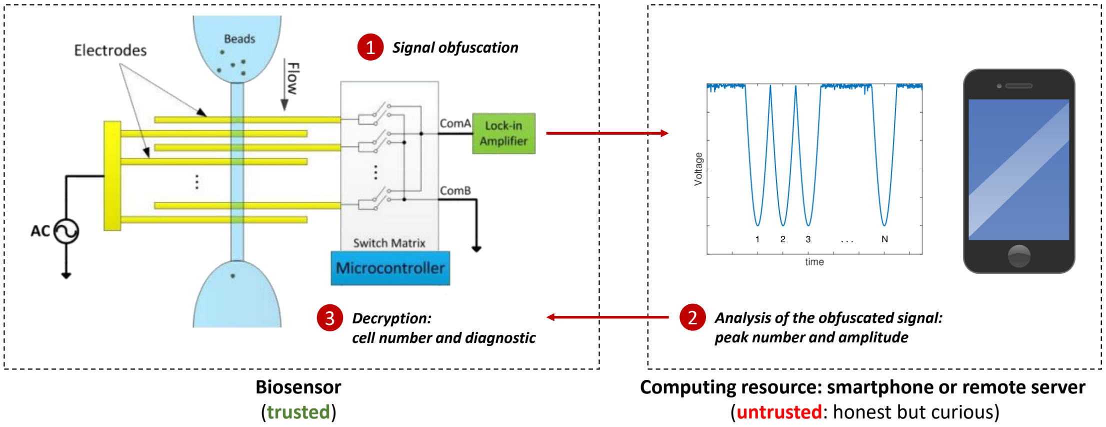

Electrodes
Beads
Flow
1 Signal obfuscation
ComA
Lock-in Amplifier
ComB
Switch Matrix
Microcontroller
AC
3 Decryption: cell number and diagnostic
Voltage
1
2
3
...
N
time
2 Analysis of the obfuscated signal: peak number and amplitude
Biosensor
(trusted)
Computing resource: smartphone or remote server
(untrusted: honest but curious)

Figure 2.1: A conceptual representation of the biosensor configuration and operation. (1) Multi-electrode excitation: Input electrodes commonly are connected to an AC voltage source. Output electrodes are connected to a matrix switch that is controlled by a microcontroller. The microcontroller randomly activates different subsets of electrodes, resulting in the creation of multiple peaks for each cell that is passed through the channel. (2) The obfuscated signal is sent to the untrusted computing resource for analysis. (3) The analysis results are sent back to the sensor microcontroller that recover the actual cell count and emits the diagnostic.

For analog signal protection, the past work has proposed signal scrambling techniques [132] that implement a limited set of transformations using a key. Those techniques do not consider adversarial settings, and hence, are reversible by potential attackers on the server. In the medical field, INTRAS proposes a key exchange and data encryption method based on interpolation and random sampling as an alternative symmetric encryption technique for electrocardiogram physiological signals [14]. These techniques are implemented in software, and require powerful processors to encrypt fine-grained analog signals once original measurements are acquired by the sensor hardware.

The solution presented in this work reconfigures the sensor hardware such that the acquired measurements are already encrypted. This eliminates the need for powerful computational and memory resources as large trusted computing bases. Hence it brings down the size, complexity and cost of the device, while improving the overall security. To the best of our knowledge, this work is the first physical based encryption scheme for cytometry that do not rely on any software-based analog or digital signal manipulation.

Flow cytometry has been studied extensively as an alternative to impedance cytometry for diagnosing and monitoring diseases such as HIV, malaria, and tuberculosis [11, 83, 44, 82, 117]. For instance, [11] has shown the high correlation of CD4+T-lymphocytes counts by flow cytometry and the standard of Coulter cytosphere assay. White blood cell counts have also been studied to characterize Plasmodium falciparum-infected patients, Plasmodium vivax-infected patients, and the uninfected patients [83]. However, the technique is expensive and requires highly trained technicians adhering to the strict protocols. These challenges call for the design and development of cost-effective disposable testing solutions without sacrificing the sensitivity[30]. Microfluidic protein quantification also has been conducted using a mobile platform [33, 81, 72]. The protein is aggregated with gold nanoparticles and detected with LED light. The results from the experiment are stored in text file and distributed over the network via Google Drive. However, for sensitive medical information, such as HIV diagnosis, the confidential results should be kept secured for patient's privacy. Our proposed method allows for higher diagnostic accuracy through single-cell and single particle detection, but also for improved domain-specific embedding security at the physical sensor level.

Impedance cytometry consists in measuring the impedance of different types of cells to estimate the count for each type of cell in the sample under the test (e.g. patient's blood sample). In combination with a capture chamber, impedance cytometry can be utilized to estimate the number of cells of interest that are captured in the chamber, by measuring the difference in cell count before and after chamber. Accordingly, two main information need to be protected in the measured data: *the type of the cell* passing through the channel, which can be characterized by the amplitude and the width of peaks observed in the measured signal, and the *cell count* or difference in cell count when using a chamber, in the sample under the test. Therefore, to protect a patient diagnostic, a cipher would have to protect three main sensitive features in the acquired signal: the number of peaks, the amplitudes of the peaks, and the width of the peak in every measurement.

Figure 2.1 presents the general principle for the proposed obfuscation scheme. The sensor is composed of a channel along which the sample is passing through, and a set of interleaved electrodes (multi-electrode) placed on top of the channel. Depending on the number of electrodes that are interleaved, the sensor generates different peaks patterns associated with each cell that goes through the channel. A microcontroller controls the electrodes and can either activate or deactivate them. Therefore, multiple peak patterns can be generated for each cell going through the channel.

In addition to the number of electrodes, other design parameters of the sensor can also be used to further protect the information related to impedance measurements and obfuscate the characteristics for each generated peak. For example, an amplification factor, i.e. a gain from the lock-in amplifier, applied to each activated electrode can be used to alter the amplitude of the peaks. Additionally, the flow rate of the fluid passing through the channel can be modified to generate peaks with varying width for each cell. While all or a combination of these sensor parameters can be used to implement the obfuscation scheme, this work mainly focus on the peak count protection by changing the number of electrodes activated in the sensor. The goal is to obfuscate the true number of cells that pass through the channel. This number of cells is a crucial parameter for disease diagnosis. For instance, the white blood CD-4 cell count is currently the strongest indicator of human immunodeficiency virus (HIV) progression in lab tests [92, 93, 84]. To evaluate the encryption of the signal characteristics related to the peak, we rely on simulation, where we investigate numerous configuration for sensor setup.

The close coupling between the signal acquisition and the encryption process allows our setup to have a very small TCB. The TCB includes the sensor, which physically manipulates the sample under the test (e.g. patient's blood sample), and the combination of a microcontroller and a multiplexer responsible for the encryption of the impedance cytometery measurements. No other component has access to the cytometry information. The proposed solution does not trust the smartphone or the remote server that perform the peak analysis, since they only manipulate obfuscated measurements. This model does assume that the computing resource (smartphone or server) correctly perform the peak analysis procedure and do not alter the results, hence the *honest but curious* security model.

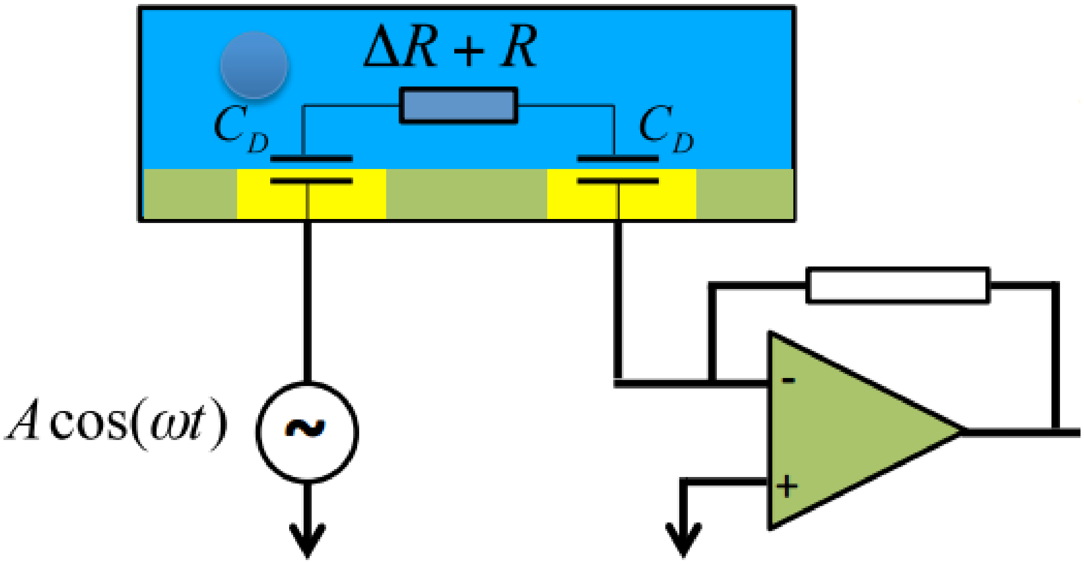


Figure 2.2: Model of operation of planar electrode pair. The electrode-electrolyte interface is modeled by the double layer capacitance. The electrical impedance in the channel fluctuates as the cell/bead passing between the measurement electrodes.

3 Cytometry Sensor Design

In this Section, we present the design and the fabrication process of the core components of the impedance cytometer.

3.1 Biosensor

The biosensor is integrated in the microfluidic system and acquires data by monitoring the electrical impedance across the channel. The sensor measures changes in complex impedance between the electrode pair. Figure 2.2 shows the electrical model of the sensing electrode pair in the microfluidic channel. The input electrode is excited with a continuous AC signal at a fixed frequency. The output electrode is connected to a lock-in-amplifier that converts the current to voltage, and locks into the AC excitation frequency. As the cell passes over a given electrode pair, a partial occlusion of ions passing between the two electrodes causes an increase in the electrical impedance. These voltage variations in the output of the lock-in-amplifier correspond to the cell passing through the microfluidic channel.

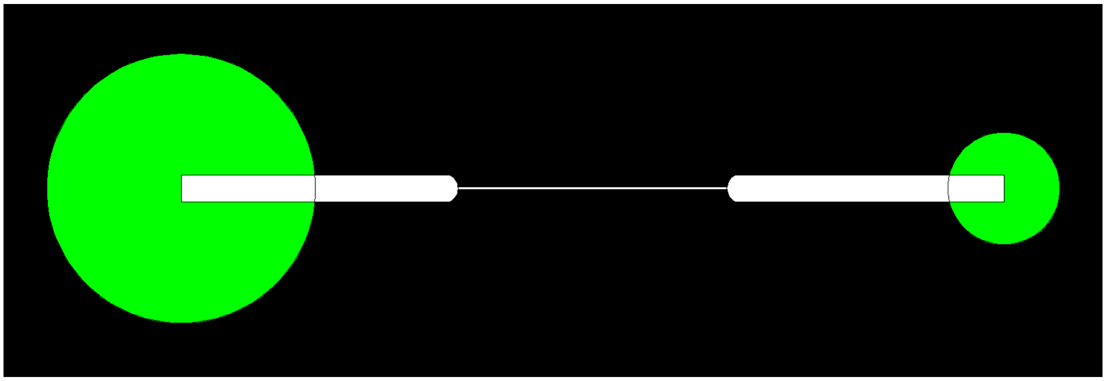


Figure 2.3: Microfluidic channel design. The measurement pore (narrow channel at the center) has a width of 30 µm and a length of 500 µm. The two circles depict the inlet and outlet of the microfluidic channel.

The system shown in Figure 2.2 corresponds to a series of capacitors and a resistor [30]. The resistor represents the resistance of the fluid and the ionic current passing across the sensing electrodes. The parasitic capacitance (C_D in Figure 2.2) results from a double layer of ions forming at the electrode, i.e., the electrolyte interface. When a voltage is applied to the input electrode, a layer of ions accumulates at the surface of electrode. The electric field from the electrodes is screened by the free ions in the double layer, similar to a parallel plate capacitor. This system of capacitors and resistors in series will have a distinct capacitive-dominant region and resistive-dominant region in response to a range of applied frequencies. At low frequencies (<10 kHz), the system response is dominated by the electrical characteristic of the capacitors, and thus the measured impedance is relatively high (MΩ range). At higher frequencies (>100 kHz), the capacitors are short circuited, resulting in resistive-dominate impedance. The optimal frequency regime to operate is where the resistance is dominant, since we are interested in measuring changes in ionic resistance that results from the presence of cells between the electrodes. Each cell passing through a pair of electrodes results in a single peak in the output voltage.

3.2 Microfluidic Channel

Figure 2.3 illustrates the design of the microfluidic channel. The microfluidic channel directs the cells in the sample through the electrode pairs. The measurement pore, which is a narrow channel at the center, helps to single out and deliver cells in the sample, in succession, to facilitates the counting and the modulation of the number of peaks generated for each cell. The wide regions at both ends of the measurement pore allow the cells to disperse before entering the measurement pore of the microfluidic channel. The two circles depict the inlet and outlet of the channel after the polydimethylsiloxane (PDMS) is removed using biopsy punchers.

3.3 Multi-Electrode Signal Acquisition

As shown in Figure 2.1, the sensor uses multiple electrodes with inputs shorted together, and outputs independent of one another. This setup generates multiple consecutive peaks as each cell passes by. The individual electrode outputs are the core components of this analog signal encryption. Output electrode signals can be selected or discarded through the multiplexer. The selection of the electrodes (selected or discarded) follows a (pseudo-)random selection process similar to a cryptographic one-time pad. Independent output electrodes can be randomly switched on or off via the multiplexer chip. As a result, for each cell passing through the channel, this setup can generate multiple peaks up to the total number of electrodes, resulting in the possibility of creating random patterns of peaks for each cell passing by. Therefore, a potential eavesdropper without access to the encryption key will not be able to discern the true number of cells that have passed by.

4 Sensor-Based Analog Signal Encryption

This section describes the signal encryption scheme. This design provides a symmetric encryption scheme that solely relies on the choice and secrecy of a key to protect the encrypted measurements. The ciphertext is an analog signal. Since the encryption is only based on the biosensor setup, this solution does not require software-based encryption of the digitalized measurement. As discussed in Section 2, in addition to multi-electrode signal acquisition, two extra design parameters can also be considered to protect the signal confidentiality: a per electrode gain, that permits the generation of peaks of different amplitude for a same cell passing through the channel, and the sample flow rate, that distorts the peak width.

4.1 Cipher Design and Security Analysis

The strength of this signal encryption scheme relies on the biosensor's reconfigurability to generate various signal measurements, possibly with different amplitudes and shapes for a single cell passing through the channel. The sensor configuration is determined dynamically by the randomly generated key on the biosensor microcontroller. The biosensor design hides the information carried by a signal from the external untrusted entities by generating multiple signal peaks of different shapes.

A cell passing through the electrodes consistently creates voltage variations (peaks) between the electrodes. As an example, Figure 2.4 shows such a variation obtained from our experiments. The counting of the observed peaks carries important information and can be used to infer a medical diagnosis. This cipher leverages a specific sensor design and a custom protocol to multiply and transform a signal acquired from a single cell into a random sequence of signals unrelated to the cell properties. Only the random sequence issued by the microcontroller, which defines the sensor configuration at the time of data acquisition, can decrypt the values behind the sensor measurements. To randomly clone a single peak signal into multiple peaks signal, the sensor activates and uses multiple electrodes that are selectively powered on or off in such a way that the biosensor generates a random succession of electrode order. The response of such an electrode configuration causes the number of peak counts at the output to be larger than the actual number of cells passing through the micro channel as in Figure 2.5. Therefore, the resulting multi-peak signal conceals the actual number of cells passing through the channel.

The resulting encrypted signal hides the true number of cells, but still carries information about the cells. Specifically, the amplitude or the width of a voltage drop can reveal information about the composition or shape of the cell. To protect both information, the cipher design can leverage two more parameters. First, randomly chosen voltage gains can be applied to individual electrodes such that none of the peaks

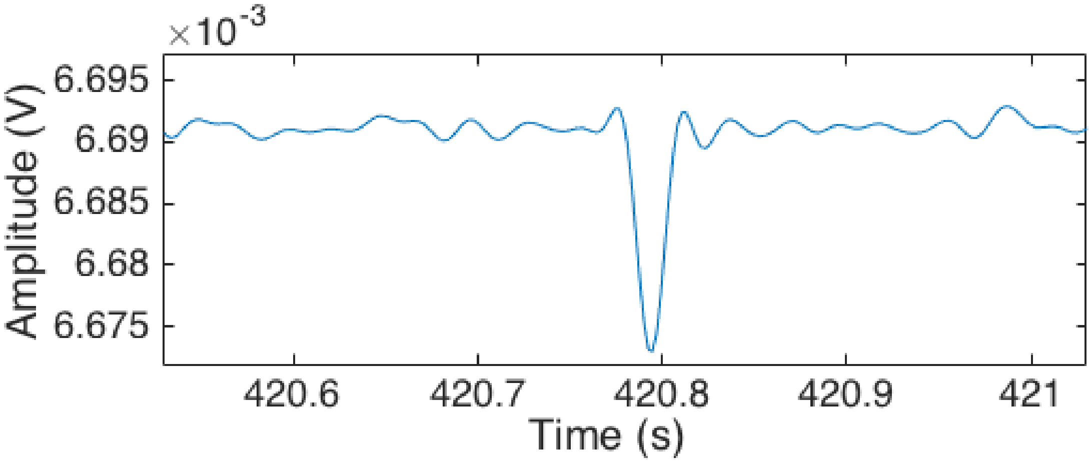


Figure 2.4: Normalized signal measurement of single synthetic micro bead in the microfluidic channel. As the micro bead passing the microelectrode pair embedded in the channel, it changes the impedance between electrode pair. The change in impedance creates the voltage drop measurement in microfluidic channel.

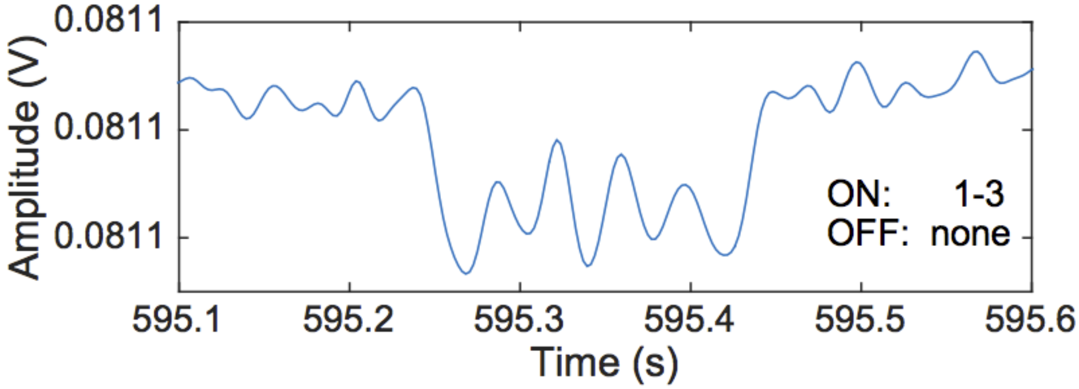


Figure 2.5: Representative normalized encrypted cytometry data for the measurement of a red blood cell. Multiple output electrodes are activated by microcontroller to generate multiple peaks for for single cell measurement.

carries the amplitude of the original signal. This gain information can be incorporated as part of the encryption key. Similarly, a modification of the flow rate in the channel results in peaks of arbitrary widths for cells of identical type. By leveraging these three parameters (the number of active electrodes, the electrode amplification factor and the fluid flow rate in the channel), the microcontroller can generate any number of peaks of any shape. These transformations allow the sensor to conceal the sensitive information and to later recover them thanks to the parameters embedded in the key.

The specific sequence of electrodes turned on or off, the set of output gains applied to electrodes and the fluid flow rate in the micro channel constitute the encryption key. To preserve the initial signal's confidentiality, every peak p associated with a cell would have a different set of chosen parameters, or key K_p, such that:

$$K_p = (E_p, G_p, S_p) \tag{2.1}$$

where E_p is the binary vector representing the sequence of on/off electrodes, G_p is the sequence of electrodes gains, and S_p represents the immediate flow speed in the channel. Such a design choice would lead to a key size of length $L = cK_p$ for c number of cells passing through the channel. Such a setup is comparable to the perfectly secret one-time pad encryption scheme [101]; every signal peak is encrypted with its own randomly generated key. The key length varies linearly as function of the number of cells. Such an encryption algorithm would ensure a perfectly secret encryption since it can produce any resulting shape for a given original signal.Figure 2.6 illustrate this point: the origin signal is acquired with a sensor using a single pair of electrodes. The curves Key #1 and Key #2 represent the encrypted signal obtained by using two different encryption keys that control the number of electrodes on (4 for Key #1 and 3 for Key #2), their respective gain and the flow speed on the channel.

In practice, applying a different set of parameters per cell measurement is challenging as it increases the key size, and would require the biosensor to be aware of every cell entering and leaving the channel. We observed that multiple cells can pass through the channel with a distance interval inferior to the distance between the first and the last electrode. Thus, two or more cells may appear among the electrodes simultaneously; this complicates the signal encryption and decryption procedures. Consequently, the final encryption mechanism implements an alternative scheme that periodically changes the encryption parameters every time unit:

$$K(t) = (E(t), G(t), S(t)) \tag{2.2}$$

This cipher has the key characteristic that the encrypted signal can still be processed to detect peaks in the measured signal. A peak detection algorithm can be applied on the encrypted signal to return the encoded peak count, with associated time-stamps, amplitudes and widths. Given a ciphertext, it is impossible for a domain knowledgeable attacker to correctly estimate the true number of cells and infer patient's test result. Only the microcontroller, which knows the input secret values applied to each control parameter, is able to recover the real signal amplitude, and true number of cell counts associated to the ciphertext signal peaks. It is noteworthy that the presented encryption scheme does not infer any noticeable encryption computation overhead or delay since it is only based on the hardware configuration that is built into the sensor. The decryption requires light computation (multiplications and divisions) and can be performed on the resource-constrained microcontroller. The decryption operation consists in matching the time periods to the configuration, and can be performed in linear time by going through the detected peak list.

The multiple peaks per cell hides the true number of cells with the multiple electrodes sensor deployment such that it is not possible recover the true number of cells captured in the chamber. A potential attack on this obfuscation scheme requires recovering the number of electrodes turned on and off in order to recover the peak multiplication factor generated by the multiple electrodes. By dividing the number of peaks observed in a data set by the multiplication factor, an attacker would recover the initial number of cell passing through the channel. Considering that each cell has a specific signature in terms of voltage drop when passing through a set of electrodes, the attacker would try to detect consecutive peaks of the exact same amplitude and

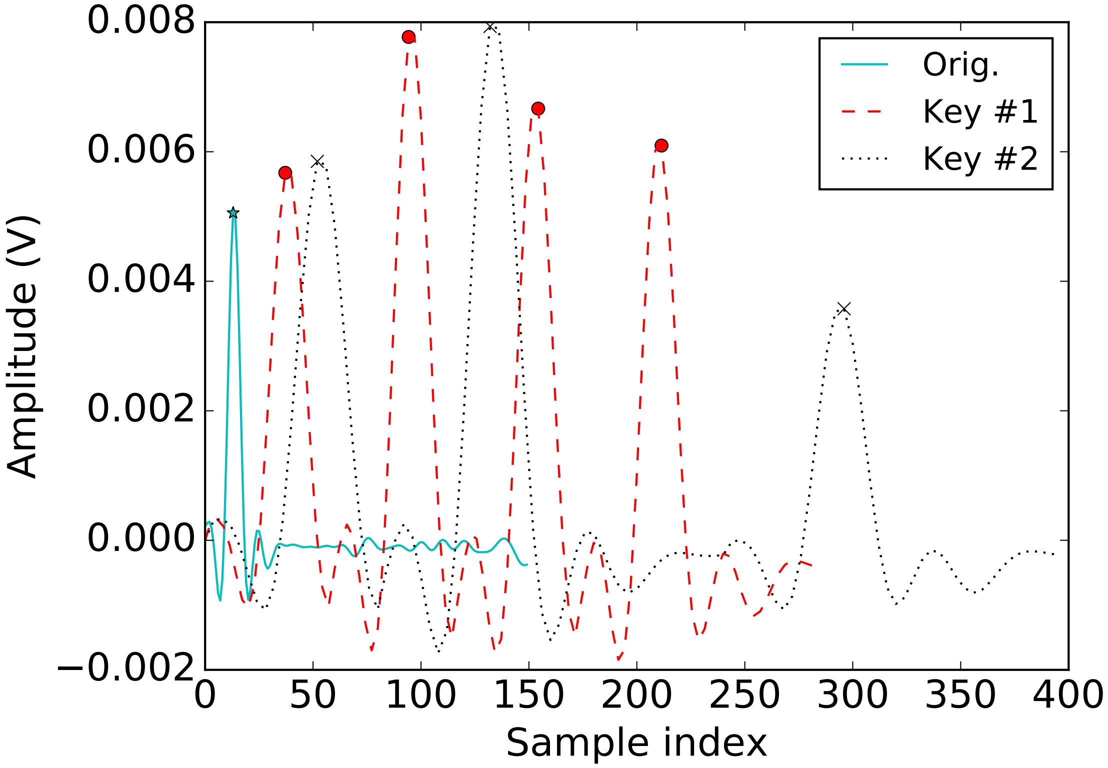


Figure 2.6: Encryption simulation for two sensor setup. Each key leads to a different obfuscated signal in terms of number of peaks, peak amplitude and peak width.

then infer the number of electrodes on. The cipher design protects this information by applying random gains on each electrode output. This changes the signal amplitude and thus conceals the initial signal characteristic. Similarly, an attacker could try to recognize peaks that correspond to a single cell by observing the width of the curve that would remain unchanged by modifying the amplitude. By modifying the fluid flow rate through the channel, the resulting signal width is altered to protect this information as well. The slow fluid speed results in peaks with larger widths.

4.2 Key Space Size Analysis

The encryption key chosen to encrypt the original signal corresponds to different design parameters. All combined, these parameters define possible combinations to obfuscate the signal. These parameters must be chosen carefully so that the resulting signal remains detectable and measurable without introducing an attack surface for bruteforce password attacks because of a limited key space size.

Minimum and maximum measurable signal amplitude The key space and the entropy of the cipher is closely related to the *signal to noise ratio* that the sensor can achieve. Intuitively, if an electrode gain is so large that it "buries" another electrode signal in its noise, the peak recognition as well as the decryption would fail. In practice, this is not always true, since multiple measurements allow some redundancy and permit to decrypt the signal even with high noise. We here provide a conservative analysis (ignoring extra information due to multiple measurements) of the entropy of this cipher.

Condition C1: *The minimum gain applied to an electrode during one period multiplied by the minimum peak size must be superior to the maximum gain applied multiplied by the noise amplitude for the same period.*

Practically, the decryption phase considers signal peaks that exceed a predefined threshold above the average. The electrode encryption gains must be chosen such that no encrypted signal has a cumulative gain on the electrodes too low in comparison to other periods. This results in a constraint on having uniform cumulative gains across various periods, which makes the encrypted signal indistinguishable to the adversaries. Consequently, it becomes harder to detect a change based on the average noise over time periods.

Condition C2: *The sum of the gains of the electrodes over various signal periods must add up to a single value throughout the experiment.*

The feasible amplitude range is dictated by the circuit's physical constraints, i.e., *minimun_signal* vs *maximum_noise*. The signal to noise ratio impacts the amount of entropy attainable per encrypted peak.

Encryption time period duration in addition to the experiment parameters that obfuscate the signal (multiple electrodes, gains, flow speed), the encryption key can be changed periodically in order to add entropy to the obfuscated signal. This rekeying allows a better protection by obfuscating the original signal following different parameters over time. The duration of the key period must be chosen carefully. In an ideal scenario, the time period would correspond to the time for a cell to transit across all of the electrodes assuming that cells are passing through the channel at a constant interval rate. In practice, the period depends on the concentration of cells and the time length of the measurement corresponding to one cell passing. the encryption period must be defined such that it is not too long, because otherwise, an extrapolation of the result over the cell transit period would lead to the diagnostic false positive. The period should not be too short either, since a period switch might happen during a single measurement and generate a distorted signal caused by the same single cell.

Formulation of the key length in function of the experiment parameters we provide below a calculation of the number of possible key combinations that can be used for encryption by combining the different experiment parameters. The number of key combination possible by simply turning electrodes on or off for a n electrode pair sensor is 2^{n-1}, assuming that zero electrode on is not a valid combination and that shifted combinations are equivalent (e.g.: on a four electrode sensor, 1 denoting a pair of active electrode and 0 denoting a pair of electrode off, 0101 is the same as 1010, 1100 is the same as 0110 and 0011, etc). Moreover, assuming that m different levels of gains can be applied per electrode pair and that the same gain is not used twice on two electrodes pairs in a same combination, we obtain a number of possible key combination equal to:

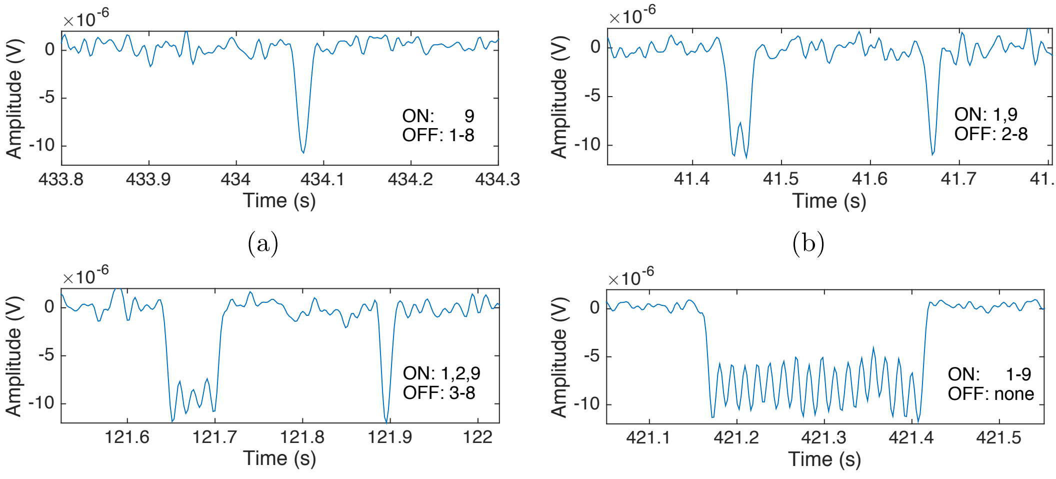
$$\sum_{k=0}^{n-1} \frac{(n-1)!}{k!(n-1-k)!} \frac{m!}{(m-k-1)!}$$

where $\frac{(n-1)!}{k!(n-1-k)!}$ corresponds to the number of different combination possible with $k+1$ electrode(s) on for n electrodes sensor and $\frac{m!}{(m-k-1)!}$ corresponds to the number of ways of choosing $k+1$ different gains levels for these pair of electrodes on.

In addition to the electrode pattern and gains applied per electrode a rekeying happens periodically and a different flow speed is used at each one of this phase.

5 Evaluations

This section provides an evaluation of the biosensor. We evaluated its performance using micron-sized synthetic beads (7.8 µm and 3.58 µm - MicroChem) and real blood



(a)

(b)

(c)

(d)

Figure 2.7: Representative normalized encrypted cytometry data of a sensor with 9 input electrodes and 9 output electrodes detecting a single bead. Pseudo-random sequence selection of output electrodes. Output activated electrode numbers are specified. True number of peaks can only be decrypted using the secret key.

cells suspended in Phosphate-buffered saline (PBS). These specific bead diameters were chosen as they are comparable to various particles found in blood, in terms of size. The solution is pumped through the microfluidic channel at a rate of 0.08 µL.

The implementation below considers a multiple electrode setup with no per-electrode gain. Results for the full setup are provided through a simulation. This simulation generates encrypted data points from data acquired with a single pair of electrode on with a constant flow speed. The simulation generates signal repetitions that correspond to the multielectrode effect and applies coefficients to the time and voltage measurements in order to respectively emulate flow speed changes and per-electrode gains.

5.1 Sensor-Based Data Encryption

Figure 2.7 illustrates how the sensor replicates the data generated for one electrode such that the multi-peak signature prevents the disclosure of number of beads passing through the channel. The figure shows the response of the biosensor to the 7.8 µm synthetic bead solution at 2 MHz. When selecting the random sequence for output electrodes, the remaining unselected electrodes need to be grounded to prevent interference. The multiplexer chip (Maxim Integrated MAX14661 16 : 2) provides a dual output channel that can be utilized for this purpose. The encrypting algorithm will select a random sequence of output electrodes and route it to the first output channel of the multiplexer. The remaining unselected electrodes will be routed to the second output channel, which is connected to the ground port. Figure 2.7a shows the measured response of the biosensor when one output electrode is selected and the remaining output electrodes are routed to the ground port. Figure 2.7b shows the response where the lead electrode (or electrode 9) is selected along with the last electrode (or electrode 1). Figure 2.7c shows the response of the biosensor when lead electrode 9 and electrode 1, 2 are selected. Figure 2.7d shows the outcomes when all the electrodes are activated. These measurements are then send for cloud-based peak detection analyses.

In Figure 2.7, the response time for each peak is approximately 20 ms. The distance each bead travels through a pair of electrodes, so a peak can be measured, is 45 µm (25 µm pitch, and 20 µm of two halves of electrode). The microfluidic channel dimension is 30 µm width, and 20 µm height. By dividing the volume of the solution passing through a pair of electrodes in the channel at the approximated time, the actual flow rate in the channel can be calculated to be 0.081 µL/min.

The current solution deployment presents two limitations. First, the ninth electrode, for all signals (Figure 2.7), only generates one peak while all other electrodes generate double peaks. This is a minor fabrication flaw of the sensor that can be solved by adding another input electrode after the ninth electrode. Second, successive electrodes do not generate distinct non-differentiable peaks. Instead, a passing bead has an influence on multiple adjacent electrodes. Figure 2.7b illustrate this effect where the double peak at time 41.42s is not a double clone of the signal at time 41.65s. Similarly, if we consider multiple beads passing through the channel, we can notice that, due to the small distance interval between electrodes by comparison to the longer distance separating beads passing through the channel, there is a long delay between groups of peaks corresponding to a specific bead. This effect is illustrated in Figure 2.7d where all the electrodes are selected; the resulting signature is a relatively flat periodic train of 17 peaks, which is dissimilar from randomly passing beads. This information could be leveraged by a domain knowledgeable attacker to recover the true number of beads in the sample and thus the final diagnostic outcome. Both limitations can be solved by either putting more space between the electrodes or by selecting an electrode key pattern that does not use successive electrodes. Both of these changes are minor design modifications that increase the ciphertext strength against adversarial information disclosure attempts.

5.2 Signal Analysis and Decryption

To validate the accuracy of this platform, we performed runtime diagnosis analysis multiple times over several blood samples. A typical diagnostic procedure using this sensor takes a 0.01 mL of blood sample and complete all the steps, including sensor-side encryption, cloud processing, decoding and diagnostics, within 1 minute. However, to exercise and evaluate the peak analysis framework ability to handle large data sets, we ran each sample through our biosensor for 3 h which generated approximately 600MB of encrypted biosensor measurements, captured in csv files. To improve the network transfer efficiency, the smartphone uses zip data compression when a transfer to the cloud is required. This reduced the sample size to 240MB. This provides a more adaptable solution to smartphone data plans when interacting with our cloud service. The encryption key size for this sample was 0.12 MB. This key stays on the microcontroller through the whole experiment. Such a small key size facilitates a cloud-backed key sharing (not implemented) between the patient and the practitioners so that practitioners can decrypt the cloud-hosted test results.

We compare the accuracy of this sensor by comparing the cell detection rates with and without encryption (i.e. one pair of active electrode, no gain, fixed flow speed). The accuracy of the base biosensor is evaluated by comparing the empirically detected peaks and the estimated elements passing through the microfluidic channel. We diluted the 7.8 µm and 3.58 µm beads with PBS, which is a commonly used biological buffer that mimicks physiological samples like blood. We diluted at different concentrations to evaluate the empirical peak detection. The estimated number of elements in the solution is calculated according to the concentration information provided by the manufacturer, where we purchase the sample from. Four samples of each concentration

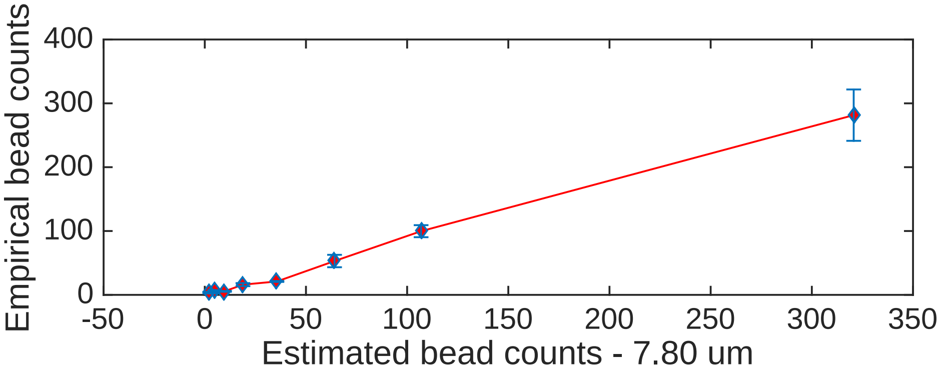


Figure 2.8: Bead count verification of 7.8 µm synthetic beads. Measured bead counts vs expected number of beads for different concentrations of 7.8 µm synthetic beads. The blue bars represent the mean counting error margins of the empirical counts against the calculated counts.

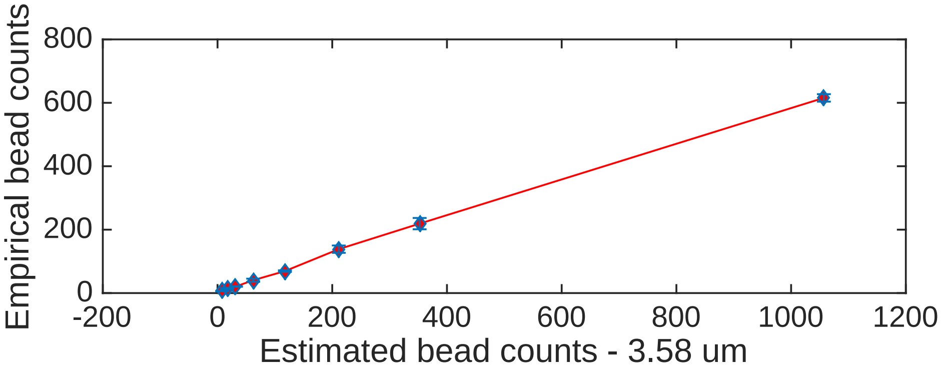


Figure 2.9: Measured bead count vs expected number of beads for different concentrations of 3.58 µm synthetic beads. The blue bars represent the mean counting error margins of the empirical counts against the calculated counts.

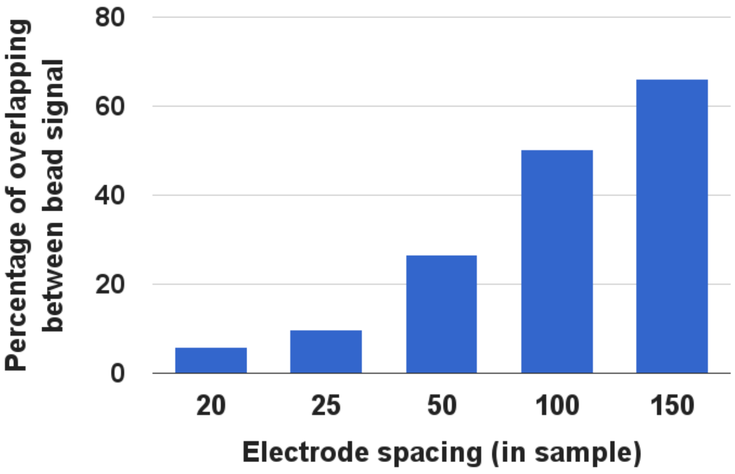


Figure 2.10: Bead encrypted peaks overlapping rate, for a fixed concentration, as a function of the electrode spacing (in sampling intervals).

are collected. The bead count data is taken from the first 5 min from each sample. Figure 3.9 and Figure 2.9 show the correlation of the empirical peak detection to the estimated peak counts in the microfluidic channel for 7.8 µm and 3.58 µm synthetic beads. As expected, the empirical peak detection varies linearly to the estimated peaks at different concentrations. The difference in bead counts is due to several reasons. For synthetic beads, the longer the experiments run, the more error would be expected on the empirical bead counts as many beads sink to the bottom of the inlet well and never make it to the sensor downstream in the micro-channel. The other reason for the bead count loss is due to the beads being adsorbed to microfluidic channel walls. These are issues that can be ultimately resolved with optimization of channel material and surface chemistry, which was beyond the scope of the current work. When adding encryption, Figure 2.10 shows the percentage of success for matching a sequence of peaks to a single bead when varying the space between electrodes in the setup. We observe that long sensors create numerous overlaps between different bead peaks and might lead to decoding errors. Practically, this constraint is usually addressed by reducing the concentration of the initial sample. This is a precaution that needs to be taken into account for other reasons as well: the sample must be diluted enough not to avoid bead

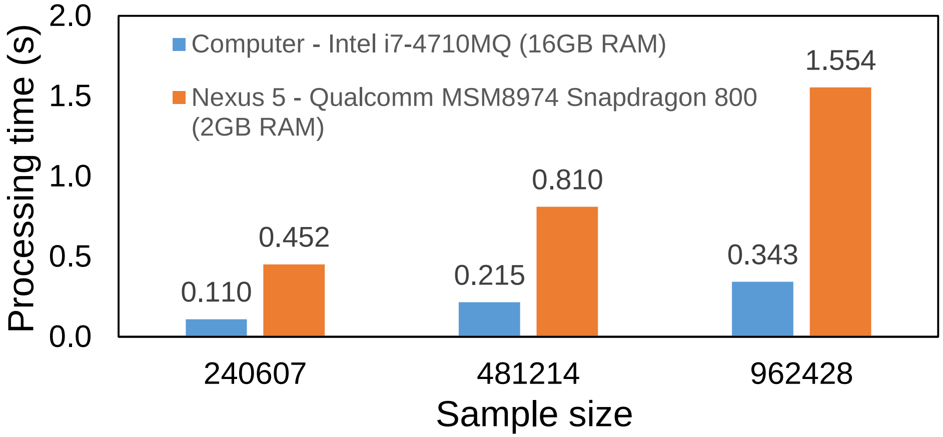


Figure 2.11: Peak analysis performance on a computer and smartphone.

aggregations in the channel that cause clogging.

Figure 2.11 shows a performance comparison of the peak detection algorithm, when it runs on a standard computer system (possibly a cloud virtual machine) and on an Android smartphone device. It is noteworthy that a standard system provides much better performance than a mobile device, as the sample size grows larger. Aside from the storage capabilities, the enhanced computing power motivates the use of a cloud based service for handling peak detection and post-processing rather than using the smartphone. For smaller samples, however, this solution could be configured to perform the peak counting signal processing on the smartphone locally.

6 Conclusions

We presented a portable point-of-care disease diagnostics solution that ensures low-cost and accurate outcomes through use of the smartphone computational resources. This solution provides in-sensor hardware-based analog signal encryption. The specific encryption design enables cloud-based analysis of encrypted analog signals without disclosing the users' privacy and confidential medical information. Our real-world implementation of the biosensor circuitry and software stack proves its accurate and secure diagnostics capabilities empirically.

Chapter 3

Transparent User Authentication through Biophysical Channels

1 Introduction

Portable medical diagnostic or point-of-care (PoC) devices enable a healthcare management transition from hospital-centered to a preventive, patient-centered, and cost-effective alternative. PoC device users can monitor and detect early medical anomalies. Early detection contributes to reducing individual healthcare costs [38]. However, this would create the security concerns for the sensitive medical information such as HIV diagnosis

Portable medical diagnostic devices do not replace medical practitioners: patients need to consult and share their medical results with medical practitioners. This information exchange requires careful consideration when designing PoC devices. Current solutions provide an access to medical records to both parties using online services: previous works [81, 72, 79] demonstrate the integration of medical diagnostic devices with a mobile platform that stores the experiment results in text file and distributes them through Google Drive cloud services. This dependency on online services comes at a cost of extra security mechanisms, such as the necessity for a strong user identification and authentication to ensure the protection of the patient data. Unfortunately, authentication mechanism are often a burden on the user and impair the usability of the device [13].

Security researchers are constantly trying to improve authentication mechanisms [13]. As of today, login and password credentials are the reference solution to identify or authenticate users. However, users dislike passwords [5] and user generated passwords provide a poor security protection. Users reuse their passwords across accounts, forget

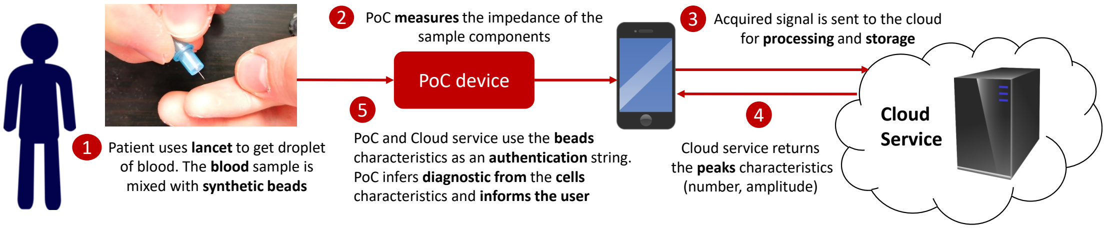

2 PoC measures the impedance of the sample components
3 Acquired signal is sent to the cloud for processing and storage
PoC device
Cloud Service
5
4
1 Patient uses lancet to get droplet of blood. The blood sample is mixed with synthetic beads
PoC and Cloud service use the beads characteristics as an authentication string. PoC infers diagnostic from the cells characteristics and informs the user
Cloud service returns the peaks characteristics (number, amplitude)

Figure 3.1: High level operation of the point-of-care (PoC) medical diagnostic device with transparent authentication mechanism. (1) Users utilize the dedicated pipettes with embedded unique authentication strings to collect the blood samples. The authentication strings, constructed from the mixture of micro-size synthetic beads, will mix with the blood samples. (2) The PoC device measures the impedance of the contents of the beads and blood solution using impedance flow cytometry. (3) The device sends the acquired signal to the remote server for analysis and/or storage leveraging the connection of the mobile device. (4) The cloud service analyzes the impedance signal to count the peaks corresponding to beads and blood contents. (5) Users or medical practitioners can request the specific test result using the unique authentication string by matching the known mixture of beads to the measured impedance signal of the beads in the solution. The method provides the transparent authentication mechanism as the convenient alternative to the traditional on-screen authentication.

their passwords, or create passwords that are too easily brute forced [35, 87, 46, 5]. Also, user credentials or biometric authentication [57] respectively leverage what the user *knows* or *is* and thus create a link between patient identities and their medical data. For example, current healthcare institutions leverage patients private information, such as their name, date of birth, social security number, to index the medical records.

This work introduces a transparent authentication mechanism for impedance flow cytometry PoC devices by embedding the passwords in the test protocol. The proposed authentication mechanism differentiates either individual tests, or individual users, by leveraging unique authentication strings respectively per test or user. The proposed design does not require any interface for the user to authenticate and thus reduces the overall system complexity. This domain specific authentication method does not require any patient information, which protects further the patient privacy.

The proposed solution leverages different combinations of synthetic beads to generate authentication strings. Recent development of microfluidic device allow the high throughput and accurate particles counting [114]. This can be used to differentiate bead counting in authentication strings. These authentication strings are unique and identifiable by the amplitude of the peak signal response in the impedance flow cytometry measurements. By carefully choosing the synthetic beads, the peak signal response of the synthetic beads differs to the peak signal response of the predominant elements in the test solution, such as the blood cells or the cells of interest. Both the user and the remote server know the authentication string. Users can request the test result using the known combination and concentrations of the synthetic beads from the test. This proposed scheme provides a domain specific authentication and an alternative to users credentials.

This chapter is organized as follow. Section 2 describes the use of synthetic micro-beads in the authentication strings as the alternative to traditional on-screen entering of identifications. Section 3 describes system design. This including the fabrication of the microfluidic device and the process of the acquired signal from impedance flow cytometry measurement. Furthermore, this section analyzes the information entropy of using the synthetic micro-size beads in the cytocoded passwords. Section 5 concludes the work on the chapter.

2 Overview

In this section, we present the design and evaluation procedure of a domain specific and transparent authentication scheme for the PoC diagnostic device. Figure 3.1 describes the test procedure for a user performing a blood test with the device. The transparent authentication operates as follow: the user collects a blood sample with a dedicated lancet embedded with a unique authentication string. This authentication string corresponds to a set of synthetic beads of different sizes and concentrations. The PoC device measures the impedance of the synthetic beads and blood cells in the mixed sample using impedance flow cytometry. The PoC device then transmits the signal acquired to the remote server for analysis and storage using the network connection of the mobile device. The cloud service analyzes the impedance signal and extracts the count of peaks corresponding to the synthetic beads and blood contents. The peaks count of the combination of synthetic beads corresponds to the authentication string

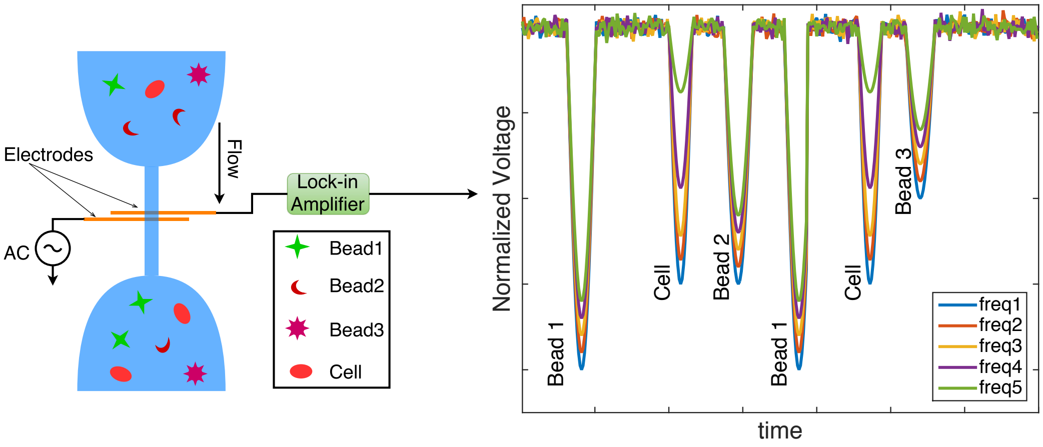


Figure 3.2: Operation model of the integrated system. The biosensor electrodes are excited with multiple frequencies. The lock-in amplifier recovers the measurement signal. The distinct combination of synthetic beads generates the authentication string associated with a test. Synthetic beads and cells have different impedance responses due to their dielectric property difference. Furthermore, the biosensor can distinguish further between the measurement of the embedded authentication strings and the measurement of cells in the test samples using signal responses at multiple frequencies.

for the blood test. Both the user and the cloud know this information at this stage of the test. Upon request, the user can share the authentication string with the medical practitioner who, in turn, requests the specific test result stored on the remote server. This authentication scheme does not require any patient information such as in a login and password credential authentication.

The biosensor is embedded in the microfluidic channel. This sensor enables impedance cytometry measurements. Figure 3.2 describes the particle detection operation in the biosensor. The input electrode of the biosensor embedded in the microfluidic channel is excited with multiple signals at different frequencies while the output electrode measures the impedance change in the channel between the electrode pair. The lock-in amplifier recovers the measured signals. Impedance responses varies between synthetic beads and blood cells due to the dielectric properties differences of these particles. The biosensor acquires the signal responses for these particle and differentiates the embedded authentication strings from the measurement of the cells in the test sample.

The *characters* of the proposed authentication string correspond to composition and concentration of synthetic beads in the blood sample. An optimal sensor accuracy and thus a good resolution of the different sizes and concentration of beads and cells is the fundamental objective. It enables the detection of the different types and sizes of cells in the blood sample and provides an accurate analysis of the sample. It also enables the detection of subtle variations of bead sizes and concentrations, or *character*, used as authentication string. A good resolution multiplies the number of characters usable in an authentication string and enhances the protection provided by this mechanism. In this work, we evaluate the authentication strings strength by the granularity of the impedance detections and concentrations of the micro synthetic bead compositions as the *characters* in the authentication strings.

3 Microfluidic System Design

In this section, we describe the biosensor, microfluidic device, and the design of authentication strings.

3.1 Biosensor

The impedance flow-cytometry biosensor is integrated in its microfluidic system. The sensor acquires data by monitoring the electrical impedance change across the electrode pairs in the channel. Micro-electrodes are fabricated on the glass substrate using standard photolithography procedures [127]. The biosensor fabrication procedure follows the following steps. A thin layer of photoresist AZ5214 (MicroChem, MA, USA) is spin-coated on the glass substrate and cured at 80 °C on the hot plate. The spin-coated photoresist is then exposed to UV light under the photomask with the micro-pattern of the micro-electrodes in the biosensor. The pattern of the biosensor is imposed on the thin layer of photoresist. After the exposure, the pattern of the biosensor is developed in photoresist developer. Photoresist exposed to UV light will be washed away; thus uncovering the glass substrate underneath. Whereas, the unexposed regions of the photoresist will be retained on the glass wafer.

Biosensor is fabricated by deposit the thin layer of chromium and gold on the glass wafer using electron beam (e-beam) evaporation. The chromium and gold deposit on the exposed micro-region of the glass substrate will form the biosensor with the micro-electrodes. The regions which are covered in photoresist will prevent the Chromium and Gold to adhere to the glass substrate. In this fabrication, a thin layer of 5 nm Chromium and 200 nm of Gold are deposited on the glass wafer to form the biosensor. After the e-beam evaporation, the glass wafer is put through the lift-off process to remove excess regions covered with Chromium and Gold. The excess regions are the regions which has a layer of photoresist underneath the Chromium and Gold layer. By submerging the glass wafer in the Acetone bath, the photoresist will be lifted off from the glass wafer. Hence, the Chromium and Gold from the excess regions also removed from the glass wafer.

3.2 Microfluidic Channel

The microfluidic channel is designed to accommodate the transport of blood cells and beads across the electrode pair for signal measurement. In this work, we evaluate the authentication strings composed of micro-size synthetic beads. The beads are mixed with blood samples and used to identify the test result at the remote servers. An authentication string consists of different bead sizes at specific concentrations. The sensor is designed to count individual particles (beads or cells) in a small volume of the test solution. The microfluidic channel is design with a thin pore to deliver a single particle at a time through the electrode pair at the measurement region as described in previous chapter. The pore is the narrow channel at the center, which can single out and deliver cell or synthetic bead in succession. The larger well in which we deposit the test solution, allows the beads or blood cells to dispersed before entering the measurement pore of the microfluidic channel.

Microfluidic channel is fabricated using polydimethylsiloxane (PDMS). To fabricate the microfluidic channel, first a mold need to be constructed. The procedure to fabricate the mold is similar to the procedure of fabricating the biosensor. The standard photolithography procedure is used to fabricating microfluidic mold with SU-8 photoresist. First, SU-8 is spin-coated on Silicon (Si) wafer. The photoresist is cure at 95 °C on the hot plate. The photoresist is exposed to UV light under the photomask designed for microfluidic channel. The SU-8 coated wafer is then developed in the SU-8 developer after the exposure. The SU-8 exposed to UV light will retain on the wafer while the unexposed SU-8 will be washed off the wafer. Now we would have the mold for fabricating the microfluidic channel.

In fabricating the microfluidic channel, Sylgard® 184 silicone elastomer base and curing agent (Dow Corning) are mixed uniformly at 10:1 in weight ratio to produce PDMS solution. The solution mixed and is degassed in the vacuum desiccator and poured on the mold. The PDMS is then cured at 80 °C for one hour. The cured PDMS is peel off from the mold which form the microfluidic channel. Biopsy punch is used to cut out the wells at the ends of the microfluidic channel. The larger well is used as the inlet well; whereas the smaller well is used as the outlet well. The fluid is withdrawn through the microfluidic channel at the outlet well using an external pump.

3.3 Microfluidic System

To fabricate the microfluidic device for testing, the microfluidic channel is attach to the biosensor on glass wafer. PDMS can be covalently bonded to the glass substrate by oxidizing the contact surfaces. PDMS is exposed to oxygen plasma to generate a thin layer of silanol terminated PDMS. When brought in contact with the oxidized glass surface, the silanol terminated layers condensed and formed the irreversible, conformal covalent bond. Figure 3.3 shows the microfluidic device under the microscope. In this work, only the counting of beads and cells via the peak signal response of a single micro-electrode pair is of interest. The test solution is driven through the microfluidic channel using an external pump (Harvard Apparatus 11 Pico Plus Elite). The biosensor is excited and the signal is measured using lock-in amplifier Zurich Instruments HF2IS impedance spectroscope coupling with HF2TA trans-impedance amplifier.

3.4 Signal Analysis

Several environment factors such as the changes in temperature, the buffer concentration, etc. can influence the measurements read at the electrodes. Due to the changes in the measurement environment overtime, the measured signal has to be processed before

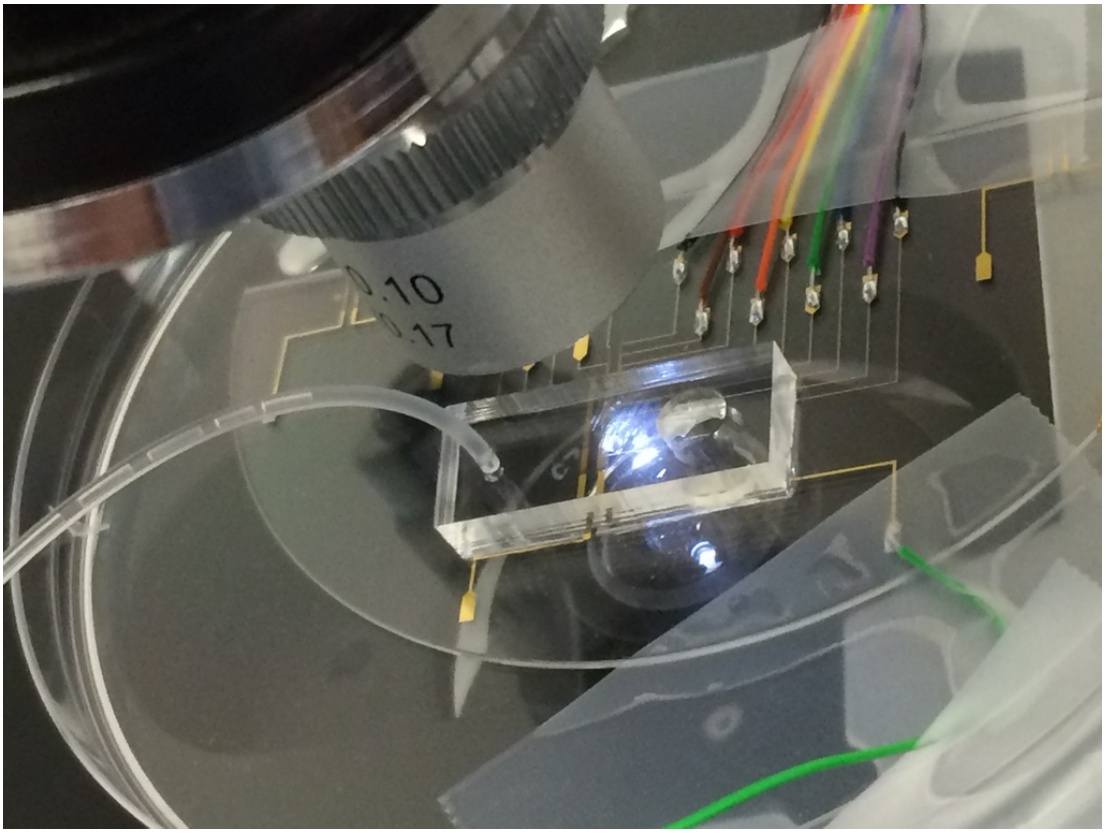


Figure 3.3: Microfluidic device under test. PDMS channel is bonded to the biosensor to create microfluidic device. The electrode pair is embedded in the microfluidic channel to detect the impedance changes as synthetic beads and cells passing through the channel. The fluid is driven through the channel via an external peristaltic pump.

the peak count procedure. The two main tasks before peak count analysis are signal denoising and detrending. The main sources of noise in the measured signal are the white noise and flicker noise. By modulating the signal to the higher frequency using the lock-in amplifier, the flicker noise is effective canceled at measurement. A simple low-pass filter can be used for the denoising process.

Another source of noise is the change in temperature and/or buffer concentration over time during measurement. This would cause the baseline of the measured signal to drift arbitrarily. We perform the peaks counting using the simple thresholding method. However, due to the arbitrary drift of the baseline during measurement, we need to remove the baseline drift in the data set. One method can be used for signal detrending is polynomial fitting and detrending according to the polynomial line. Strategically, higher order of polynomial fitting is preferable to match the signal drifting of the baseline. However, this method could cause over fitting or heavy computation issues. Moreover, over fitting deforms the peak signal response after signal detrending which could cause a miss in peak detection. For lower order of polynomial fitting on the long sequence of measured signal, the fitting line might not be conformal to the baseline drifting. This problem would be under-fitting.

4 Evaluations

In this section, we evaluate the micro-device and the authentication strings. The synthetic micro beads are also evaluated against the blood cells to show the ability to differentiate the synthetic particles and blood cells in a test. However, for different cell types or protein, different synthetic micro beads can be used to make up the authentication strings. This domain specific authentication method use a variation of the bead sizes and concentrations as an authentication strings. This section evaluates how robust these authentication strings are. To read different authentication strings, the sensor must be able to recognize the size difference of the synthetic beads and correctly count the number of beads in each size in the specific composition. As part of the evaluation, we determine the sensibility of the sensor to assess the ability to differentiate the *characters* in the authentication string. Furthermore, we evaluate the method for data analysis to count the peaks in the data set under the influence of baseline drifting.

To evaluate the sensibility of the sensor, we use two groups of micro synthetic beads of 3.1 µm, 3.23 µm, 3.58 µm diameter, and 7.1 µm, 7.26 µm, and 7.8 µm diameter. In this experiments, we determine the ability of the sensor to contrast the small variations of peak signal responses within the group. The compositions of synthetic beads of different sizes, at different concentrations create the unique authentication strings. In this examination, the authentication strings consist of one variation in each of 3 µm, 4 µm, 5 µm, 6 µm, and 7 µm diameter synthetic beads at different concentrations.

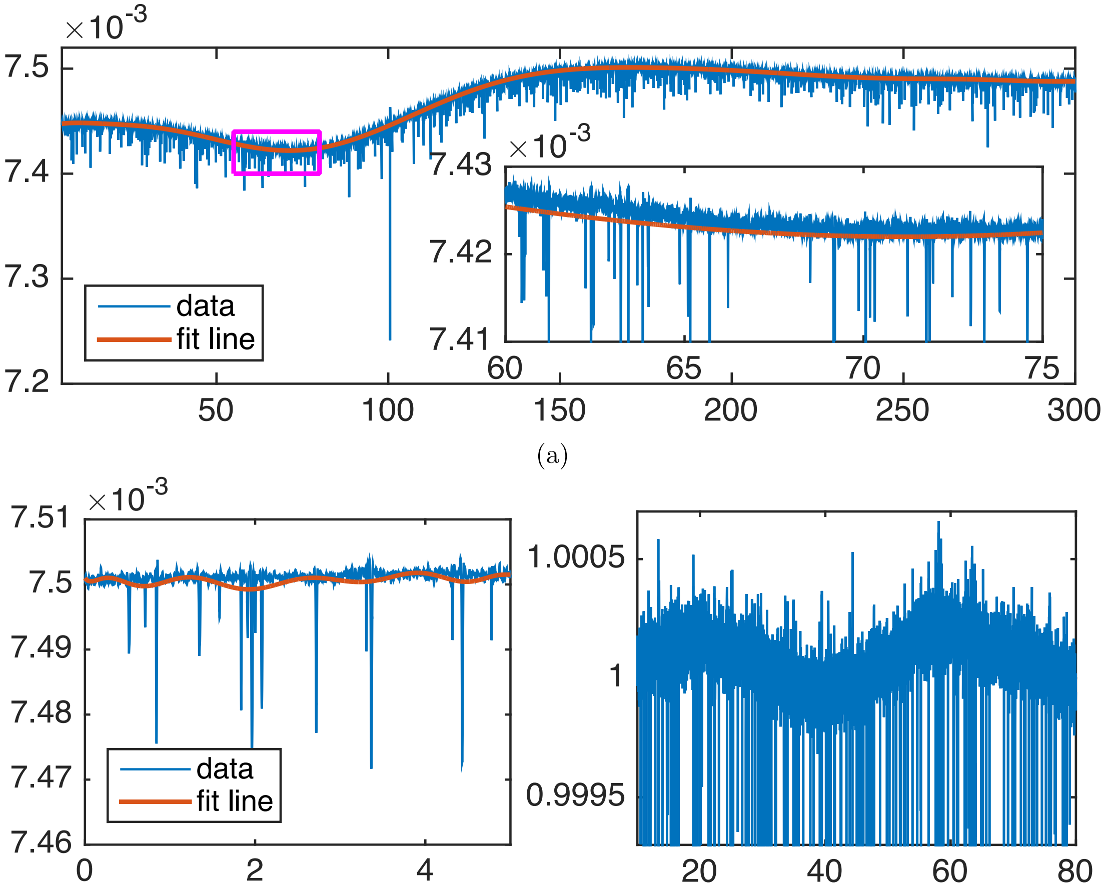
To obtain several concentrations of each bead size, we derive the concentrations from the single stock solution of each bead size. We calculate the diluted concentrations to have the specific bead counts. We confirm the synthetic bead counts from each concentration using the Multisizer$^{\text{TM}}$3 Coulter Counter. We measure the empirical bead counts of the diluted concentrations using the biosensor described in Section 3, and compare the empirical mean counts of the diluted concentrations with the theoretical calculations.

Additionally, we compare the signal response of synthetic beads and the blood cells in the biosensor to show the difference in peak signal responses. Finally, we show that the combinations of synthetic beads sizes and concentrations are suitable to be used as the authentication strings for this domain specific authentication method.

4.1 Signal Analysis

The analysis of the acquired data consists in the following steps. A first preprocessing step removes the arbitrary baseline drifting in the raw data set due to the change of temperature and concentration. We use a polynomial fitting to isolate the contour of the baseline. We then normalize the data set by dividing the polynomial fit line. We use simple threshold to detect the peak signals corresponding to the synthetic bead counts.

The polynomial order must be high enough to conform to the baseline, but should not be too high to avoid an over-fitting problem. To verify this problem, we empirically increased the order of polynomial line until it fits the baseline. At the lower order, the

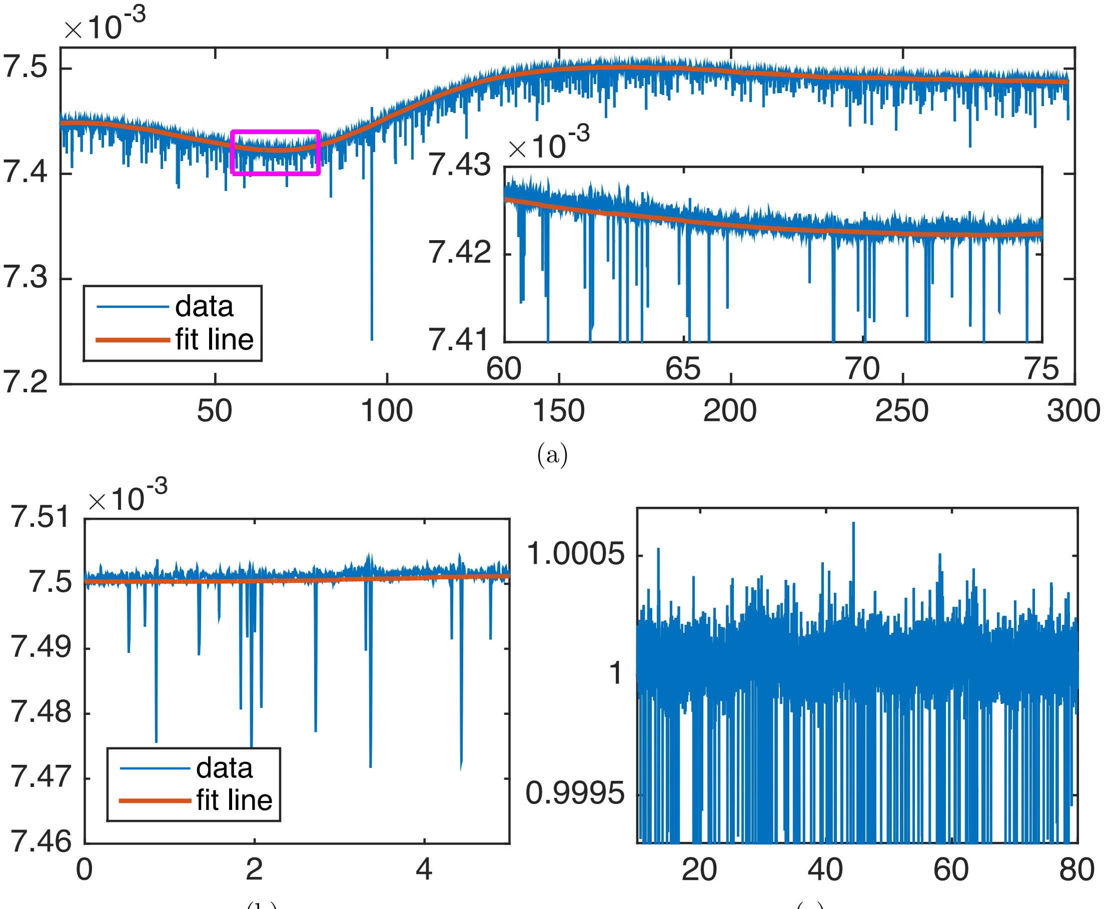


(a)

(b)

(c)

Figure 3.4: Baseline detrending using high order polynomial fitting. The polynomial line is fitted along the baseline of dataset. The baseline is normalized against the polynomial fitted line. (a) Polynomial fitting of the large data set. The inset figure show the fitting error for data set with large number of data points. (b) Over fitting of high order polynomial line in smaller data set. (c) Baseline after the detrending. The wavy appearance of the baseline is due to the error fitting in the large data set or. This also applies to the smaller data set. The over fitting would result in the further distortion of the baseline and peak signal.



(a)

(b)

(c)

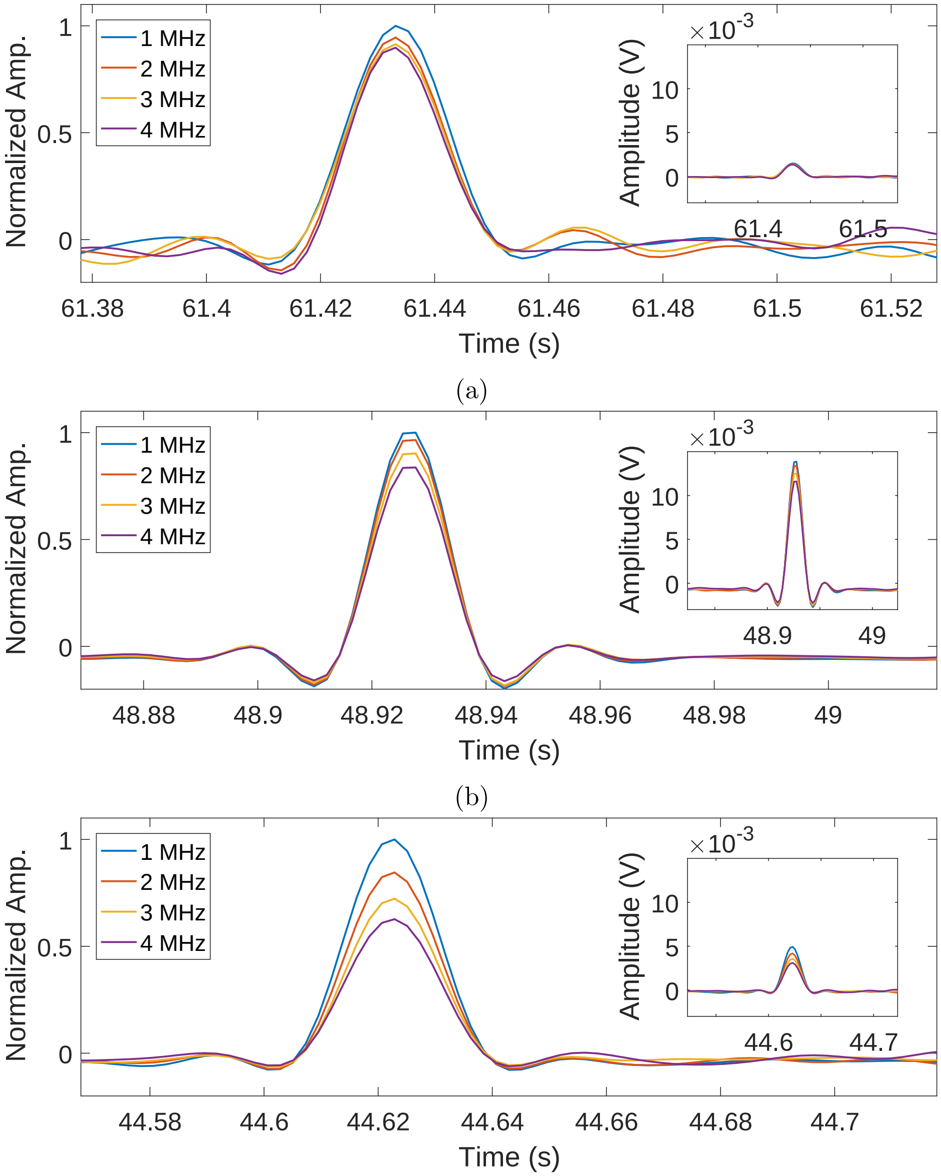
Figure 3.5: Baseline detrending using second order polynomial fitting. The data set is partitioned into smaller sub-sequences. The polynomial is fitted to each sub-sequence and concatenated to create the polynomial line fitted along the baseline of dataset. The baseline is normalized against the polynomial fitted line. (a) Polynomial fitting of the large data set. The inset figure show the close fitting for data set with large number of data points. (b) Second order polynomial remove the over fitting in smaller data set. (c) Baseline after the detrending.

polynomial fit line cannot follow the arbitrary drift of the entire baseline. However, at the higher order, the local fitting would be influenced by the peak signals in the data set. Figure 3.4 shows the baseline fitting using 12th-order polynomial fit line. The higher order is required for the polynomial line to follow the arbitrary movement of the baseline. The inset figure in Figure 3.4a shows that the higher fitting order would result in a good baseline tracking. However, this would only work ideally when the peak signal responses distribute in the near uniform manner. When the peak signal responses concentrate at one region and sparse at the other regions, we can see the over-fitting issue at the local group of signal response as seen in Figure 3.4b. This result in the fluctuation in the baseline after normalizing the data set as seen in Figure 3.4c.

By partitioning the data set into smaller sequences, we normalize the data set using lower order polynomial fitting. The arbitrary drift of the baseline is the result of changes in the testing environment over time. By dividing the data set into smaller sequence, we can have sequences of measurement with very little change in the baseline. This also brings the advantage of using the fix polynomial order in the analysis algorithm to speed up the process. In our analysis, we use 2nd-order polynomial fit line to detrend the small sequences of the data set. The 2nd-order allow the flexibility to fit the small curve of the baseline in small sequences of the data set. The sequences of data are overlapped to remove the fitting error at both end of the smaller data sequence. Figure 3.5 shows the result of signal detrending using 2nd-order polynomial fit line. The inset figure in Figure 3.5a shows the conformal fit of the concatenated polynomial lines to the baseline of the entire data set. Figure 3.5b shows the close fit to the baseline where the peak signal response distributed heavily at one region and sparsely at the others. The result in Figure 3.5c shows the normalized signal response without the fluctuating effect as seen previously. For the sufficiently small sequence of data, the second order fitting has proved more than adequate for signal detrending.

4.2 Bead Size Differentiability

In order to read the authentication strings in the microfluidic channel, the sensor examines the peak signal responses of the beads and the blood cells. Therefore, the peak



(a)

(b)

(c)

Figure 3.6: Normalized impedance measurement of (a) 3.58 µm synthetic beads, (b) 7.8 µm synthetic beads, and (c) blood cells at different frequencies. At higher frequencies, the impedance of blood cell attenuate greatly comparing to the impedance of synthetic beads. Using this signal response, the biosensor can differentiate the cell and beads that have similar impedance responses at the lower excitation frequencies. The inset figures show the difference in amplitude response of 3.58 µm synthetic bead, 7.8 µm synthetic bead, and blood cell.

signal response of synthetic micro-beads used in the authentication string must not have the same amplitude response as the blood cells. According to [18], different bead sizes would have different peak amplitude responses. [18] demonstrates the peak amplitude difference of 4 µm, 5 µm, and 6 µm synthetic beads. Similarly, we evaluate the unique *characters* in authentication string by using different beads sizes. Different bead sizes are identified based on the amplitude of the peak response of the bead in the microfluidic channel. In our previous work [69], we evaluate the amplitude of peak signal response of 3.58 µm and 7.8 µm diameter synthetic beads and blood cells. The blood cells have typical diameter of 6 µm-8 µm. Figure 3.6 shows the impedance measurement of bead 3.58 µm, 7.8 µm, and blood cell. At the measurement of the lower frequency, the amplitude response of the beads and blood cells do not vary significantly. At the higher frequencies, the amplitude of the blood cells attenuate faster than the amplitude response of the beads. Using this attribute, we can differentiate the peak signal response of the bead that similar to the blood cells in the test solutions. Figure 3.7 shows the peak signal responses of 7.8 µm and 3.58 µm bead. The amplitude of the signal response of 7.8 µm and 3.58 µm bead indicated that the biosensor can identify these beads as the unique characters in the authentication string.

Additionally, we evaluate the biosensor ability to identify the small variations of beads diameter and the blood cells in the microfluidic channel. As mentioned, we use the small variation of the 3 µm, and 7 µm synthetic bead groups.

Figure 3.8 shows the cluster of peak signal response of the beads and blood cells. There are three distinctive group of peak signal response of the 3 um synthetic bead group, 7 um synthetic bead group, and blood cells. The signal response of 3.1 µm, 3.23 µm, and 3.58 µm are similar to each other. However, the inset figure in Figure 3.8 shows that the lowest measurable amplitude from each bead size increases as the diameter of the beads increasing. Although the sensor cannot complete distinguishes the group of 3 µm beads, it indicates the sensitivity of the sensor nevertheless. Similarly for the 7 µm bead group, the sensor can detect the slight difference in sizes based on the lowest detectable amplitude whilst not completely separates the bead sizes. However, the sensor can clearly distinguish the peak signal response of 3 µm beads, 7 µm beads,

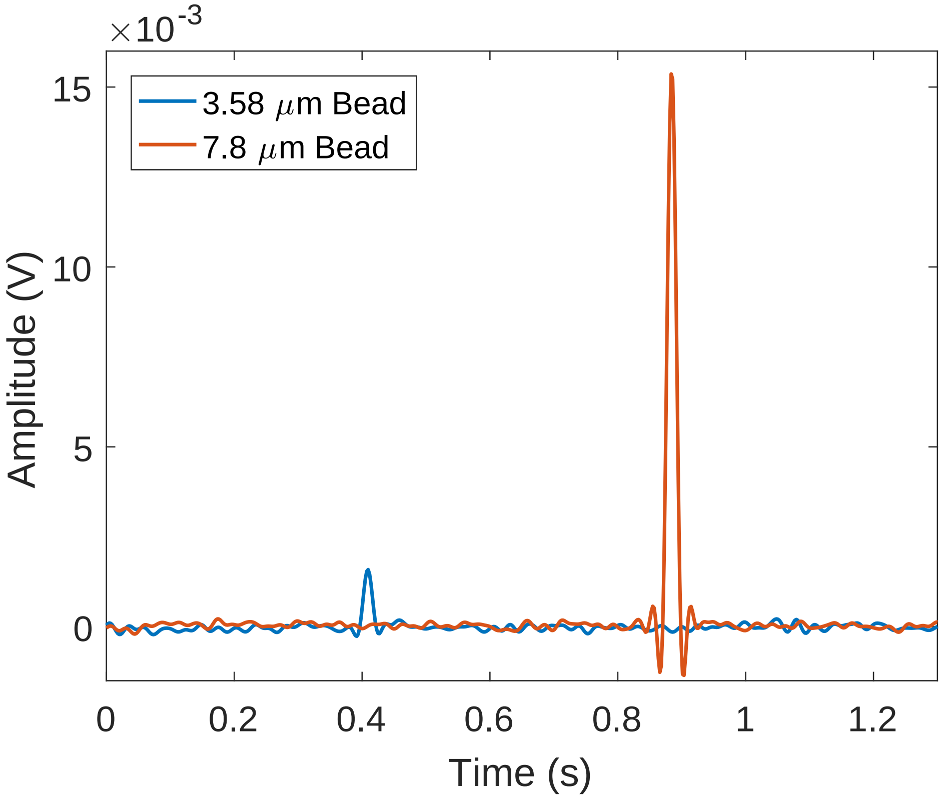


Figure 3.7: Peak signal response of 7.8 µm and 3.58 µm beads. Synthetic beads with different diameter can be differentiated in the microfluidic channel due to the difference in impedance response.

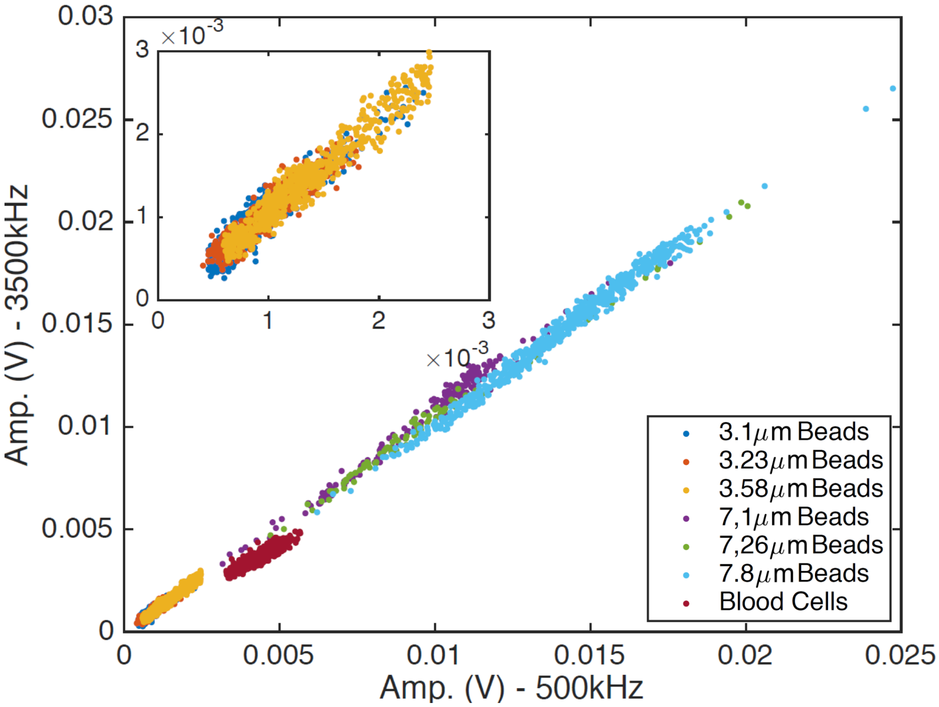


Figure 3.8: Cluster of impedance response of synthetic beads and blood cells. There is distinct impedance response between the 3 µm group, 7 µm group, and the blood cells. Within the group of 3 µm and 7 µm, there is a slight variation in impedance response. The inset figure shows s slight higher impedance response for the larger beads of the 3 µm beads. Likewise in the 7 µm group, the beads with larger diameter have slightly higher impedance response. The slight variation of signal responses in the 3 µm and 7 µm groups demonstrates the sensitivity limit of the sensor.

and the blood cells.

Therefore, using the peak signals response across a range of excitation frequencies, beads at suitable sizes can be distinguished in the mixture of beads and blood cells. An authentication string consist of synthetic beads of suitable sizes can be use as an unique identifier to a specific test result.

4.3 Bead Concentration Differentiability

The authentication strings consist of different bead sizes can be used to identify a specific test result. However, due to the limit of bead sizes that can pass through the microfluidic channel, there is a limit on the number of authentication strings created by the combination of bead sizes. Recall that our biosensor is designed to perform the cell counting. To broaden the size of characters in authentication strings, we can

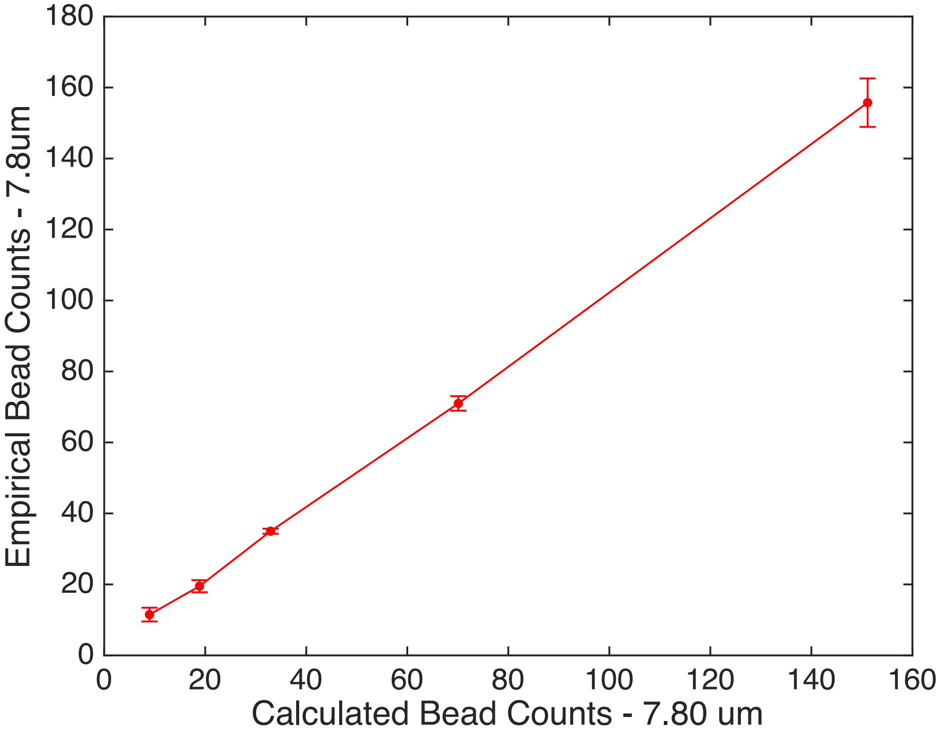


Figure 3.9: Verification of bead concentrations of 7.8 µm beads using Multisizer$^{\text{TM}}$3 Coulter Counter. The predetermined beads concentration is measured using the biosensor in microfluidic channel. The concentration is verified again using the Multisizer$^{\text{TM}}$3 Coulter Counter. The bar at each data point shows the standard error of the microfluidic channel to the measurement of Coulter Counter.

specify the concentrations of each beads size in the strings. The challenge is to correctly distinguish the authentication strings based on the different concentration of beads in the strings.

In this test, we use the 7.8 µm beads to evaluate the empirical measurement of beads at different concentrations. To demonstrate that we can control the concentrations of the beads as the characters in the authentication strings, we first measure the preliminary bead count at the arbitrary stock concentration using the Coulter counter. The measured number of beads in the stock concentration is used to calculated the desired concentrations for the beads in the authentication strings. In the empirical experiment, beads count is measured in the total of 0.4 µL solution of beads suspended in Phosphate-buffered saline. In the preliminary measurements, the results suggested that the shorter measurement time of the samples would give more accurate results. This is due to the beads settling to the bottom of the well at the longer period of time during measurement.

In the empirical measurement, we aim to measure the total count of 10, 20, 40, 80, and 160 in the different concentrations. The concentration of each sample is calculated from the preliminary result. After the empirical measurement using the biosensor, the solution of each concentration is verified again using the Coulter counter. Figure 3.9 shows the verification of empirical measurements of different bead concentrations against the confirmation of the Coulter counter. Each data point in Figure 3.9 shows the mean of the empirical measurement, the standard error, and its verification against the Coulter counter. The plot indicates the accuracy of the sensor as the empirical measurement varies linearly with the ground truth measurement using the Coulter counter.

By carefully selecting the concentrations of different beads, we can create the unique authentication strings to determine the specific test result. The sensor can identify beads of different sizes, coupling with the ability to differentiate the beads concentration, the sensor can distinguish the unique authentication strings.

4.4 Authentication String Alphabet Size

As shown in the previous subsections, different bead sizes and concentrations can be evaluated based on the sensor's counting ability and differentiating the dielectric characteristics of synthetic micro-breads. The distinct signal responses of different bead sizes and counts in concentration can be used to make up the *characters* in the authentication strings. The unique authentication strings composed of different bead sizes at different concentrations can be used to identify the specific test results from the users. The authentication strings alphabet size corresponds to the different bead sizes and concentrations this solution can differentiate. The alphabet size determines the strength and therefore, the effectiveness of the passwords. Here we assess the strength of the authentication strings according to the current acquired results. In this study, we show that the sensor can identify m different bead sizes in the microfluidic channel. Furthermore, for each bead size, the sensor can differentiate N concentrations. Therefore, the number of total possible S combination of the authentication strings using synthetic micro-size beads is

$$S = \overbrace{N * N * N \cdots * N}^{\text{m times}}$$

therefore the number of entropy bits E_{bit} in the authentication string is

$$E_{bit} = log_2(S)$$

In this work, we evaluate the bit entropy of the authentication string using the evaluation of the data measurement of 3 µm and 7 µm synthetic beads, and the conjecture of the measurement of the 4 µm, 5 µm, and 6 µm synthetic beads [18]. In our experiment, we successfully identified 3 µm and 7 µm beads. Furthermore, the result from Figure 3.8 shows that the response of the sensor can recognize the small change in beads diameters. Despite the large overlap of signal response, the result shows the sensitivity of the sensor nonetheless. The results from [18] shows that the sensor in impedance flow cytometry can distinctively separate the response of 4 µm, 5 µm, 6 µm, and blood cells. These data suggest that we can at the minimum, use the bead sizes of 3 µm, 4 µm, 5 µm, 6 µm, and 7 µm beads to create the authentication strings.

Additionally, Figure 3.9 shows that we can differentiate multiple concentrations of a single bead size. The lowest bead counts have the means of 11 beads for 0.4 µL test solution. The standard errors indicate the granularity of the concentrations of the beads in the concentration stings. The standard error of the measurement is 2.64 beads. The next distinguishable bead count has the mean of 20 beads. By conjecture, we can create the authentication strings with 3 µm, 4 µm, 5 µm, 6 µm, and 7 µm with the concentrations varying from 10 bead count to 160 bead count for 0.4 µL with increment of 10 counts per concentration.

To create the authentication strings with 5 different bead sizes and 16 different concentrations, we can select arbitrary the concentration in the range for each bead size in the string. The authentication strings can be consisted between one to five different bead sizes. Therefore, the concentration of one or more bead in the string can be zero. In this case, there are 17 concentration of 5 bead sizes to select for the authentication strings. To simplify the case, we count the range of concentration from zero to 150 bead counts for 0.4 µL of sample. The total number of all possible combination of the authentication string would be $16^5 - 1$, where the subtraction of one accounts for the case where all the concentration of beads in the string is zero. In term of password strength, the authentication string would have 20 bits of information entropy for the authentication strings.

5 Conclusions

In this work, we presented a domain specific authentication scheme for PoC medical diagnostic devices. This authentication scheme is embedded in the diagnostic procedure and can serve as a convenient alternative to on-screen input credentials from the users. We have evaluated the biosensor's ability to identify and differentiate unique authentication strings formed from known concentrations of synthetic micro-size beads. We evaluated a small sample of bead sizes and concentrations. The combination of beads sizes and concentrations can create a large number of unique authentication strings which can be used to identify the associated medical diagnostic results at the remote storage servers. By expanding the number of bead sizes and the concentrations in the sample, we can increase the scale of the usage and the strength of the authentication strings.

Chapter 4

Malicious Fill Pattern Detection in Additive Manufacturing

1 Introduction

Additive Manufacturing (AM), also known as 3D printing, is an emerging field that shows promise in reducing waste, time, and infrastructure needed in a manufacturing process. Many major companies including Ford, GE, Airbus, SpaceX, Koenigsegg, and NASA are currently utilizing AM for both prototyping and production-quality manufacturing [100, 2, 1, 60, 26, 58]. Additionally, AM has been employed as a useful tool for printing medical implants [12], and cutting edge research is underway on producing food, drugs, and living tissue using AM techniques [4, 53]. Across industries, AM is expected to reach a market potential of 50% by 2038 [124].

Because of this potential for wide-spread use of AM in the coming decades, work has begun on understanding the security challenges that are unique compared to traditional manufacturing and cyber-physical security. Mark Yampolskiy, *et al.* [129] outlined a taxonomy for the potential of the misuse of a 3D printer as a weapon (3D-PaaW). In their work, they identify the elements which may compromise or manipulate an AM environment, the targets of attack (printed object, printers, or environment), and the parameters for understanding the potential effectiveness of a given attack.

In this work, we focus on the use of a 3D-PaaW to manipulate the physical properties of a printed object through manipulation of the object specifications, manufacturing parameters, and/or source material. According to the taxonomy described by Yampolskiy, *et al.* each of these are classified as attacks which would be achievable by an adversary through the manipulation of printer firmware or the controller PC. It has been shown that structural integrity can easily be compromised by introducing slight modifications in the model, e.g., a minuscule void injected into a manufactured dog bone can reduce the yield load by 14 percent [112]. In order to combat these forms of attack, we propose three methods of verification of design parameters that utilize analysis of the acoustic signal, embedded materials, and spatial position of machine components. These are chosen because they provide information about the manufactured design *without* access to the STL file or the G-code instructions[1] read by the printer. We do not consider our techniques to be a panacea for all verification needs. They are meant to be complementary to domain-specific verification methods. In some cases, this may be means of saving costs, e.g., by detecting malicious prints in real-time and ending them at the onset of a detection. In other cases, this may be a means of ensuring safety, e.g., by detecting malicious materials or designs before the print is used. Throughout the course of this work, we will consider the use case of printing the tibial portion of a knee prosthesis.

Our contributions are as follows:

- A multi-layered approach to the verification of design specifications, manufacturing parameters, and materials used in an AM.
- Proposed implementations of aforementioned approach for in-house and third-party AM producers.
- A case study of a scenario in which a malicious print of a medical prosthetic is identified.

The chapter is organized as follows. We first provide a background in AM verification along with a system overview and threat model in Section 2. We then provide details for the different types of verification methods that we proposed in Section 3. We conclude in Section 6 and discuss future work.

[1] An STL file is a STereoLithography file for CAD software used in 3D printing. G-code is the set of actual instructions for 3D printers that are generated for particular models given an STL file and the print configuration, e.g., print speed and infill density.

2 Background and System Model

In this section we discuss the previous efforts related to side-channel analysis of AM and verification of the physical models. We then provide a system overview of our approach as well as the threat model that will be used for the rest of this chapter.

2.1 Side-Channel Analysis

In this work we provide a means of verification by utilizing the various side-channels of the printing process. We also use materials science based verification to verify that the intended physical model is printed. As such, we first review previous efforts that have been made for the analysis of the side-channels involved in the AM process. We then provide a brief review on materials-based verification techniques like Raman spectroscopy and computed tomography (CT).

Acoustic, Magnetic, and Motion Sensing. KCAD [19] provided the first method of using the analog emissions of AM processes for the purpose of detecting so-called zero-day kinetic cyber-attacks. However, the work utilizes only one 3D printer and only investigates attacks in which simple variations in the exterior design. The paper also lacks any means of verifying the printed materials post-manufacturing. The focus of the majority of previous work on the analysis of side-channels from 3D printers used in AM has been its usefulness in obtaining intellectual property. Chen Song, *et al.* [105] and Avesta Hojjati, *et al.* [54] each showed that the array of sensors available on a modern smart phone can be leveraged to re-create designs produced from 3D printers or CNC machines. The sensors used in each study to collect side-channel data included the microphone, magnetometer, and accelerometer. Each group was able to reconstruct simple printed designs using supervised machine learning and manual analysis of sensor signals respectively. However, each group was only able to reconstruct very simple shapes such as two-dimensional outlines of airplanes or keys with no fill structure.

Beyond 3D printing and manufacturing, acoustic signals have also been shown to be useful in a growing number of security applications. As an example, Guri Mordechai, *et al.* [50] showed that information can be transmitted from a speakerless PC using

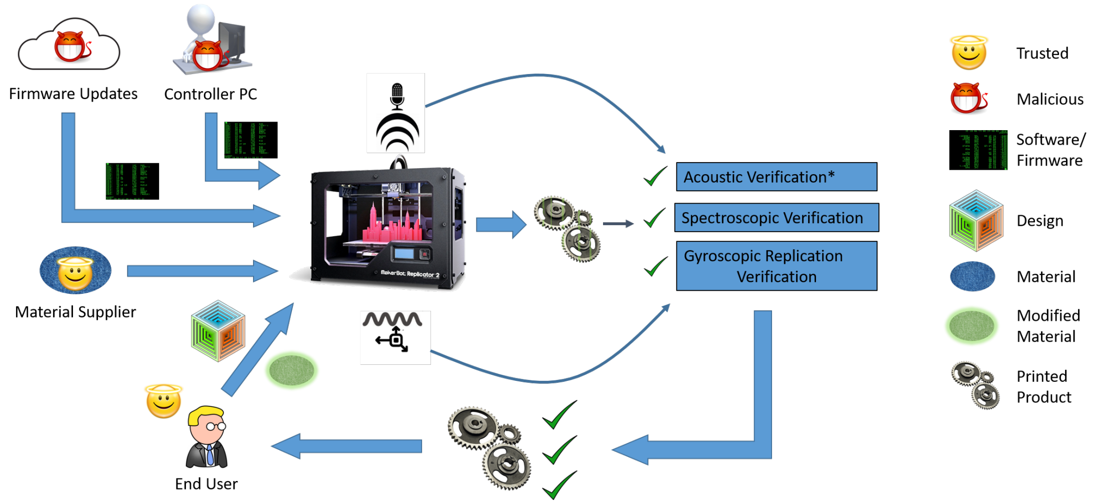


Figure 4.1: System Model.

information embedded in the sound of a cooling fan. Likewise, accelerometers have been used across industries as quality control sensors in CNC machines [73].

2.2 Physical Model Verification

The physical model that is printed from the AM machines are typically verified in a manner specific to the domain, such as mechanical strength testing [112]. Chien, *et al.* [20] use several techniques such as surface morphology characterization to verify 3D-printed tissue scaffolds. Furthermore, several solutions have been presented as preventative measures to future physical failures, such as the solution presented by Stava, *et al.* [107] for detecting and correcting models prior to being printed. However, these only correct the models that are being sent to the printer and do not verify the actual physical model in the event that the printer itself is compromised.

Imaging Analysis. We will now discuss the background for two modalities used for observing the composition of materials that will be explored in this work for the verification of 3D printed models. It is important to note that we do not consider these modalities to be the most effective imaging techniques nor the most cost-effective solutions. We chose these two modalities as they were readily available and are generalizable. Both solutions will act as a template for imaging techniques that are used to identify embedded materials. The choices for both the imaging technique and the associated embedded materials will be specific to the context in which they are applied.

Raman Spectroscopy. Surface-enhanced Raman spectroscopy (SERS) has been shown to be sensitive to single-molecule detection [90, 66, 85, 70]. Nie, *et al.* [90] have shown that silver colloidal nanoparticles can be used to amplify the spectroscopic signature of adsorbed Rhodamine 6G (R6G) and enable the single R6G molecule detection at room temperature. Furthermore, the sizes and shapes of the colloids enhance the spectral responses at different plasmon bands [91, 95]. We find that this technique can be utilized for post-production verification of 3D printed objects. By embedding a series of detectable markers of contrast agents in SERS at specific location within the 3D printed object, the SERS process would be able to reconstruct the model and verify the integrity of the internal structure of an object.

Computed Tomography. CT is typically used in medical applications to enable doctors to view precise images of their patients' internal organs [64]. Additionally, CT scanning also has been used in a wide variety of applications for verifying structural integrity. Cnudde, *et al.* [22] discuss the application of CT scanning in the context of geomaterials. Akin, *et al.* [6] also discuss the use of CT as a non-destructive method for imaging multiphase flow in porous media in the context of petroleum engineering research. Similarly, Alymore [8] discusses how CT scanning was used as a non-destructive method for studying soil behavior and soil/plant/water relations in space and time. In this study, we utilize CT in a similar fashion to construct models and verify the integrity of completed objects.

2.3 System Model

Figure 4.1 provides an overview of the system model that includes all verification techniques presented in this study. Our system assumes that there is an end user with a 3D model design. The design will be printed on a 3D printer that is controlled by a controller PC. The 3D printer may or may not be controlled by a third party entity. The end user will send her design to be printed. Throughout the printing process, the object will be verified using three verification layers. The first two layers are achieved through acoustic side-channel analysis and spatial sensing which analyze the sound and physical position of printing components respectively. The third layer is that of materials verification in which imaging techniques are used to verify that the print is made from the proper material and printed correctly.

The end user may supply her own modified set of materials to the printer so that physical model verification may be performed upon completion. The goal is to embed special materials into the filament that is used in 3D printing. The modified filament can be used for materials verification purposes.

For the remainder of the chapter, acoustic side-channel verification, spatial side-channel verification and materials verification are referred to as the acoustic layer, spatial layer, and material layer respectively.

2.4 Threat Model

The threat model assumes that the attacker has full knowledge of both the printer and its control software. If a third party manufacturer or affiliate of the user is involved, they are trusted as an organization. Therefore, they are willing to provide information about the print for verification. However, malicious entities may include network intruders, disgruntled employees, or other insider threats. The attack is carried out such that the printer behaves maliciously despite being sent G-code [2] for a non-malicious print. Meanwhile, the controller PC indicates that the print is being carried out correctly. This attack is feasable using a a cyber-physical rootkit such as Harvey described by Garcia, *et al.* [41].

It is also assumed that training prints may be performed under supervised circumstances in which it may be reasonably assumed that no attack is taking place. This may be achieved by a direct connection between the controlling machine and the printer via USB. The materials supplier shown in Figure 4.1 is assumed to be trusted. Untrusted materials suppliers are beyond the scope of this study. For the materials-based verification, the modified filaments with the embedded materials are to be supplied directly by the end user. Furthermore, all communication channels among trusted entities are

[2] G-code is the set of instructions interpreted by a 3D-Printer, CNC, or other machine that includes information about motion direction, speed, and other operations.

assumed to be secure.

2.5 Use Case: Prosthetic Tibial Implant

For a specific use case example, the tibial implant portion of a prosthetic knee was chosen. Unlike the titanium alloy component of the prosthetic knee that attaches to the femur, the tibial portion of the implant is made from polyethylene and has been identified as a component that could easily be manufactured through AM [12, 3]. Furthermore, the knee undergoes more mechanical stress than any joint [102]. Thus much research has been conducted which describes the medical implications of its wear and tear [118, 65]. Therefore, an attack is considered in which alterations are made to the internal structure of tibial knee implant that would dramatically increase the rate of wear.

3 Verification Layers and Implementation

The main focus of this work is to verify the unseen internal fill structure present in all 3D printed objects. When a print is converted from a design on a computer to G-code instructions for a 3D printer or CNC, an internal structure for the physical product must be generated. These can range from low density for prototyping or non-load bearing prints to high density for load bearing or industrial use. The fill itself may take on a honeycomb pattern, rectilinear pattern, or other various patterns as specified by the user. Failure to produce the proper internal fill will render a final product that may externally look like the design intends, but fails to provide other required physical characteristics.

In order to develop a robust verification scheme, methods were needed that would allow for real-time identification and visualization of potentially malicious prints as well as visualization of a completed print to ensure its usability. Analysis of the acoustic side-channel can be used as a non-destructive method of identification. For real-time visualization, a method of tracking the moving components of printer or CNC machine can be a useful way of understanding the process without relying on control software.

Finally, the imaging method from materials science may be used to observe the internal structure of the printed object in non-destructive way.

3.1 Side-Channel Verification

The side-channel analysis verification layers provide a means of verifying printed models in real-time. The goal is to infer as much information as possible from the given side-channels, but we do not expect each modality to be able to verify the entire print in itself. We will first discuss the experimental setup for each side-channel modality.

Acoustic Layer. As a physical byproduct of nearly any mechanical process, acoustic signals have been explored as a method of understanding information being processed by both traditional printers [9] and 3D Printers used in AM [105, 54, 19]. Because traditional printing methods now rely on lasers or ink jets, the information obtained from these is minimal. However, 3D printers will continue to rely on various actuators and fans for the foreseeable future which produce useful acoustic data. This is especially true for large-scale implementations of the technology.

In this verification layer, we assume that a particular design with a given infill structure will be printed multiple times. We use an open source audio classifier similar to the Shazaam [7] or SoundHound Applications. Using a training audio file, it locates noise-resistant peak frequencies and their temporal location within the file. It then locates frequency peaks in the test data that match the location, frequency, and spacing from other peaks. When a test file is identified, it is accompanied by a confidence score among other information. The confidence score indicates the number of peaks that the test has in common with the training data.

For AM verification, we use a single print as a training set by recording it with a microphone to obtain an audio file. Because even a simple print can take many minutes, the resulting file is separated into a number of segments of a given length (some number of seconds) and indexed in ascending order. Each indexed segment of the print is then trained as a different "song" and stored in a database. In many machine learning schema, common practice is to train multiple sets of data. However, because acoustic classification involves one-to-one comparison of audio files, a single-file training set is

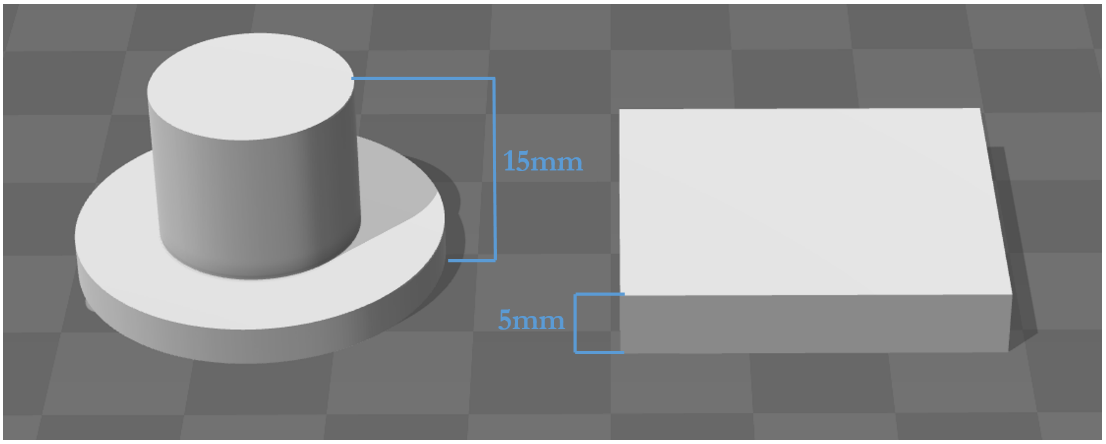


Figure 4.2: 3D Printed models described as (left) Top Hat and (right) Rectangular Prism.

appropriate.

Test data is collected using the same method as training data and split into segments of the same length. Each indexed segment is then classified independently and a confidence score is returned. The confidence score represents the number of frequency peaks that a given file has in common with the training file. Verification that a repeated print is unaltered from the training set is determined in two ways:

1. The classification results are such that the index values appear in ascending order. If they are out of order, it is likely that a change has been made.

2. The confidence score of one or more indexed classification results falls below a given threshold value. The threshold value is referred to as the confidence threshold (CTh) for the remainder of the chapter. Its value is optimized manually for each printer to maximize the true positive rate and minimize the false positive rate.

With this, a print will be considered verified if each indexed audio file is classified correctly, in the correct order, and with confidence values greater than the CTh. A non-verified print conversely will be classified but out of order or with one or more confidence values less than CTh.

To test this method, two designs, shown in Figure 4.2 are used throughout this study. They are described as a Rectangular Prism (right) and a Top Hat (left). Each was printed several times with “Honeycomb” and “Rectilinear” fill patterns of 20%, 40%, and 60% density. For each print style, a single set of audio data was split and stored in a unique database as described above.

In order to derive quantitative results to the test classifications, we assign a “score” to each segment of the audio data which are defined as follows:

- If a segment is in proper sequence and the confidence value is greater than CTh, its score is equal to that of the confidence value.
- If a segment is out of sequence, its score is equal to $-1 *$ confidence value.
- If a segment is in sequence, but the confidence value is less than CTh, its score is set equal to $-1 *$ confidence value.

If a negative score is calculated for any segment of the sliced audio file, a positive error classification may be determined. If no negative values are calculated, a negative error classification is determined.

Sample results are shown in Figure 4.3. The print is a Rectangular Prism with a 20% density Honeycomb fill pattern. The top chart shows the averaged results of three known negative error classifications (true negatives). Each bar represents a 90 second slice of the printing data, and CTh is set to 35. Likewise, the bottom chart represents various positive error classifications (true positives) caused by incorrect fill densities or patterns. Each type of error is printed four times and the results are averaged. For errors involving the Honeycomb fill pattern with erroneous densities, a positive error classification is achieved within 270s or the first 60% of the print. For the erroneous Rectilinear fill pattern, positive error classification is achieved within 180s or 40% of the print. In each case, the first 90s slice is always receives high scores due to the fact that the design always starts with a 100% density fill of the first three layers. This is standard in 3D printing to ensure that the exterior is solid.

Spatial Sensing Layer. When performing 3D prints, it was found that the software used to monitor print progress simply displayed the progress of the G-code instructions being sent to the printer. This is regardless of the actual actions of the printer. The

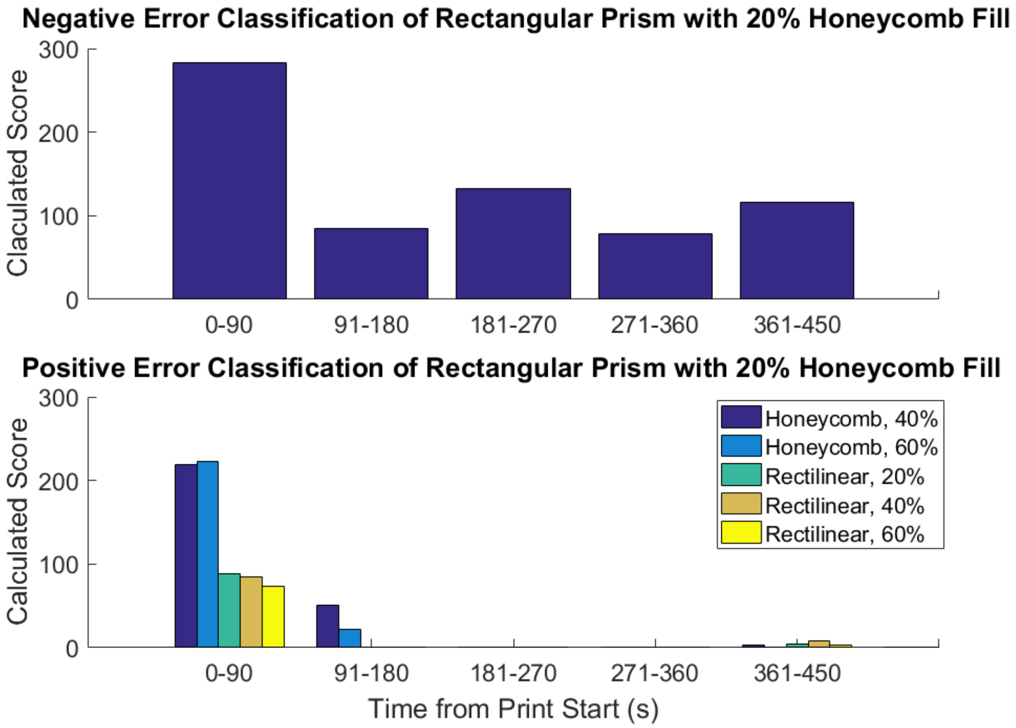


Figure 4.3: Classification example.

goal in setting up a spatial sensing verification scheme was to physically monitor the position of the printing nozzle with respect to the printing base, in order to observe their actual positions throughout the printing process.

The first consideration was to use a ride-along accelerometer such as those described in Section 2. However, due to the double integration from acceleration to position and the noisiness of the accelerometer data, visual representations of the printer's path became prohibitively difficult to obtain.

With this in mind, a scheme was developed in which the a gyroscopic sensor was paired with a linear potentiometer in order to construct a set of spherical coordinates to describe the printer's motion. This proved more effective because no integration was needed for the data, and only simple moving average filtering was necessary to reduce noise.

To obtain these measurements, the following devices were used: a Unimeasure linear potentiometer model number LA-PA-10-N1N-NPC, a SparkFun Triple Axis Accelerometer and Gyro Breakout – MPU-6050, and a Teensy 3.2 board. The experiments were

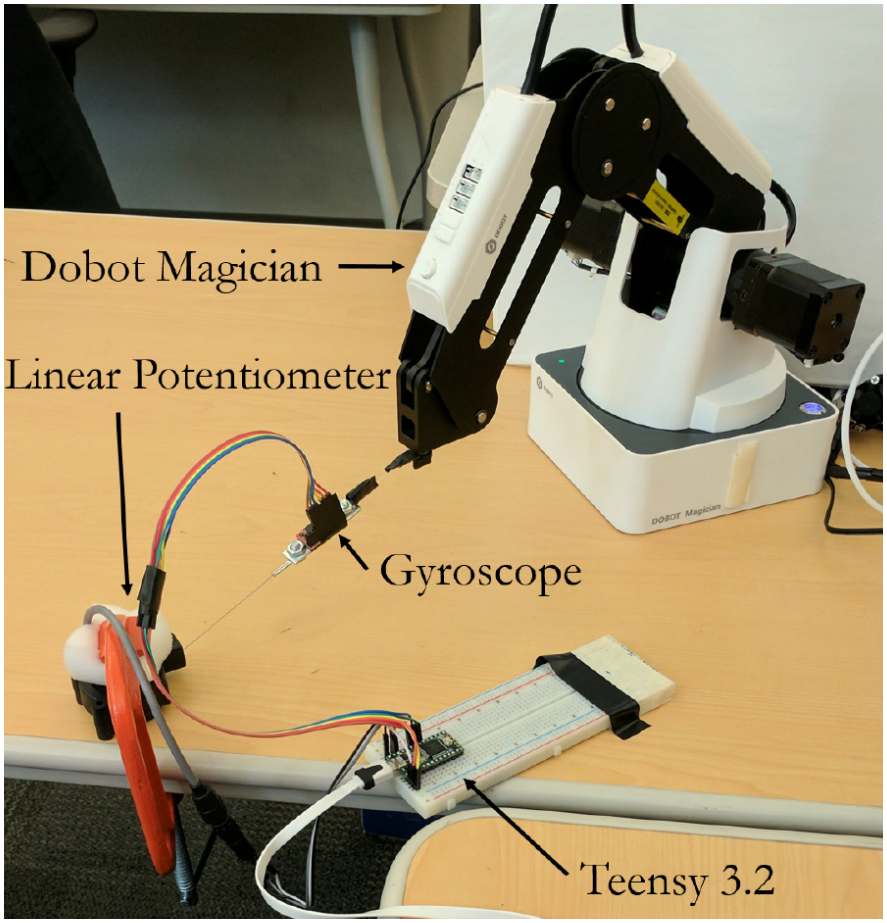


Figure 4.4: Spatial sensing setup with Unimeasure linear potentiometer model number LA-PA-10-N1N-NPC, SparkFun Triple Axis Accelerometer and Gyro Breakout, and Teensy 3.2 board.

conducted in a setup as shown in Figure 4.4 with a Dobot Magician desktop CNC and 3D Printer. For experimental purposes, the actual 3D printing extruder was removed and "dummy" prints were performed. The test prints were a single layer of a circular disk printed with Honeycomb and Rectangular fills each with a 20% and 40% density. Data is collected at a rate of 100Hz. In Figure 4.5, each print is shown as the G-code representation next to the reconstructed path of the printer. The data shown is smoothed using a moving average filter with a window of five.

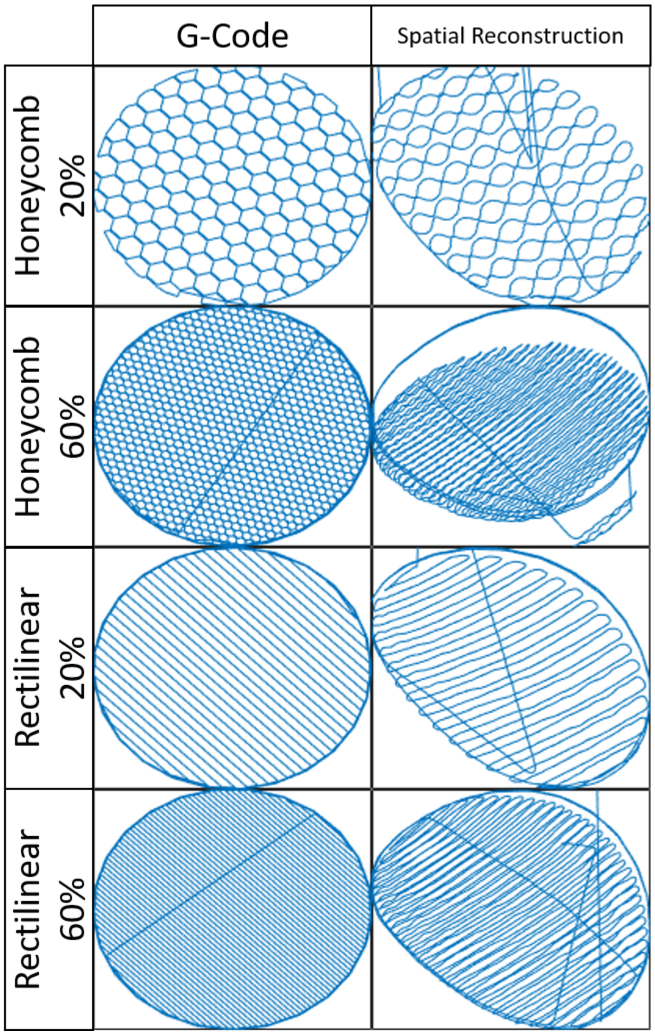


Figure 4.5: Comparison of G-code reconstruction to gyroscopic sensing reconstruction of single layers of various fill types and densities.

3.2 Materials Verification

The objective of our materials-based verification is to embed contrast agents that will act as signature markers for particular prints without compromising the structural integrity of the original model. The contrast agents are chosen based on the materials as well as the scanning modalities. This approach is similar to the approach presented in Chapter 3 for privacy-preserving techniques for secure point-of-care medical diagnostics in which the synthetic beads with different dielectric properties are used for user identification. In this case, we embed a single type of nanoparticle at different points in the printed model to generate a pattern specific to the model. This will allow us to ensure that the model was not modified by either an attacker who compromised the firmware and is duping the manufacturer, or a malicious insider who has physical access to the printing process. While it is arguable that embedded markers would change the integrity of the material itself, numerous studies have shown that the use of nanoparticles actually *improves* the materials' mechanical strength [126, 24, 39, 78].

Here, we explore two types of scanning modalities: Raman spectroscopy and computed tomography (CT). Although both modalities are not necessarily cost-effective, our goal is to explore their effectiveness in our verification techniques. In both cases, we assume that the end user will provide the necessary materials to the manufacturer, who will be responsible for printing the model. The design sent to the manufacturer will not include any information about the embedded materials. We will now briefly discuss the different scanning modalities in detail.

Raman Spectroscopy. The first of the aforementioned modalities is Raman spectroscopy, which has been shown to be applicable for specific target identification and quantification [90, 66, 85, 70, 97, 111, 133]. The target sample is irradiated with a monochromatic light source such as laser. The majority of the scattering light has the same frequency of the incident light. This elastic scattering is called Rayleigh scattering. A small fraction of the scattering is inelastic. It has a small shift in photon frequency due to the energy transfer with the target molecules. When excited at a specific frequency, the target molecules can either increase or decrease in vibrational energy. Thus, the small fraction of the scattering light reduces (Stokes shift) or gains (anti-Stokes shift) equally the energy of the molecule vibration.

Due to to the unique covalent bonds and atomic mass of the each molecule, different molecules require specific excitation energy to change the molecule vibration [77]. The combination of multiple energy shifts creates the unique spectrum for each target molecule. The distinct spectra can be use to identify the target molecule in Raman spectroscopy.

Contrast agents in Surface enhanced Raman spectroscopy (SERS) can be used to amplify the Raman spectra of the target samples. As the electromagnetic wave (laser) irradiates the contrast agent molecules, it excites the localized surface plasmons on

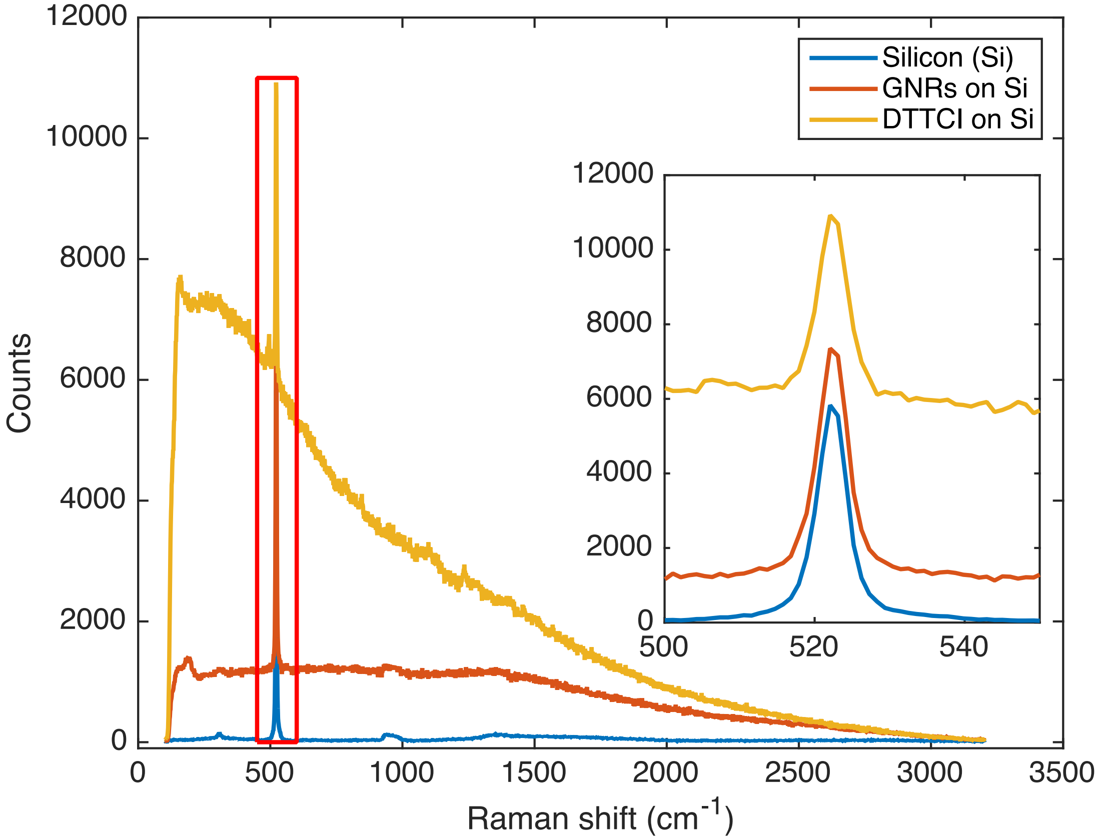


Figure 4.6: Raman scattering measurement of Silicon wafer with gold nanorods (GNRs) and 3,3'-Diethylthiatricarbocyanine iodide (DTTCI). The Raman spectrum of Si is amplified when using the enhancers.

the rough surface. This results in the enhancement of electromagnetic fields near the surface [34, 15, 110]. The increase in intensity of the electromagnetic fields would also increase the intensity of Raman scattering. Thus, the Raman spectra is amplified. As a result, by coupling the contrast agents with the target molecules, SERS technique can be applied for identification of target molecules. Furthermore, SERS is also shown to be applicable for *in vivo* studying [98, 55]. Qian, *et al.* has shown that pegylated gold nanoparticles can be used to target tumor cells in live animals in an *in vivo* study.

In this study, we utilize gold nanorods particles (GNRs - *Sigma Aldrich*) and 3,3'-Diethylthiatricarbocyanine iodide (DTTCI - *Sigma Aldrich*) as the two different contrast agents in SERS detections to verify the material of the 3D printed object. The contrast agent can be embedded in the filament at specific locations for material identification. The internal structure of the 3D printed object can be verified using the embedded materials. Figure 4.6 shows the result of the standard Raman scattering measurement of the Silicon (Si) wafer and the Raman scattering of GNRs and DTTCI drop coat on top of the wafer. The Si wafer is used to calibrate the Raman instrument prior to the experiments. The Si Raman spectra has been studied thoroughly [96, 115, 99]. In Figure 4.6, the GNRs and the DTTCI amplified the signal response of the Si Raman scattering intensity.

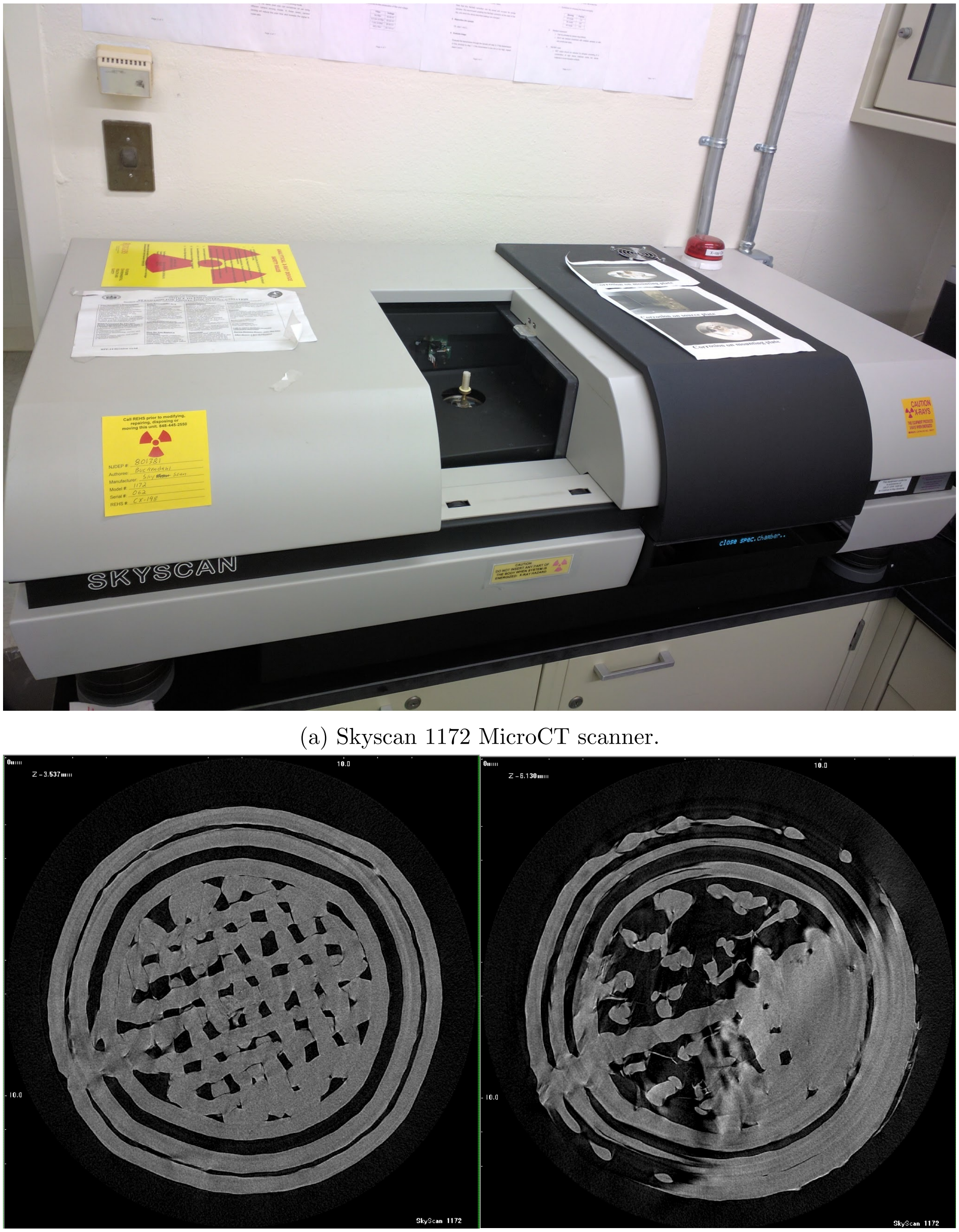
Computed Tomography. The second scanning modality is a computed tomography (CT) scan. Just as in the SERS experiment, we needed to find an effective contrast agent that would allow us to view the embedded materials within the 3D printed model. Because it has been shown that gold works as an excellent contrast agent due to its X-ray density [51] and because we already had the materials at our disposal, we decided to reuse the GNRs as our contrast agent. Furthermore, the GNRs' biocompatability will allow us to apply our verification procedures to the tibial prosthesis.

We initially experimented with the use of GNRs as a contrast agent for CT scanning by embedding them in a simple 3D printed model. We developed and printed a cylindrical 3D model using a standard acrylonitrile butadiene styrene (ABS) filament as the control material of the model. Multiple layers of ABS filament with embedded GNRs were deposited in between the bulk material.

Figure 4.7 shows the initial results of the 3D printed model with a layer of injected GNR filament. We performed a CT scan using a Skyscan 1172 MicroCT scanner. As the figure shows, the GNRs did indeed contrast with the ABS filament. This was sufficient to prove that GNRs could be used as a contrast agent for our printing use case.

4 Evaluation

In this section we evaluate the three-layered verification method. We describe the identification of a malicious print, the observation of the detected error, and the post-production materials verification. Then, we evaluate the effectiveness of the acoustic and spatial verification on the use case of a 3D printed tibial knee implant.



(a) Skyscan 1172 MicroCT scanner.

(b) ABS control print.

(c) GNR layer print.

Figure 4.7: CT scan of ABS cylindrical tube with embedded GNRs.

To quantify the accuracy of the results of the various tests, the data is fit into a logistic regression model with the binary dependent variable of "malicious print detected" or “no malicious print detected”. From the model, we extract the probabilistic classification outcomes and create a receiver operating characteristic (ROC) curve. The area under the ROC curve (AUROC) is the metric used to predict classification accuracy.

Also, it is important to note that due to the fact that these machines are used to produce real 3D prints, large amounts of data were not practical to obtain. Furthermore, the imaging analysis techniques used for the materials verification were also time-consuming with limited availability. Therefore, sample sizes in this section will be significantly smaller than papers dealing with computer simulations.

4.1 Identification of Malicious Prints

In this section, we evaluate the usefulness of the proposed verification method in simply identifying an error in a potentially malicious print. This initial identification will be carried out primarily by the acoustic layer with redundancy in the spatial layer to reduce false classifications.

Classification Accuracy. In order to gain initial understanding of the parameters that affect the accuracy of the acoustic layer, several experiments were carried out with a small number of trials. The printers used in the tests were a Lulzbot Taz6, Lulzbot TazMini, and an Orion Delta. The AKG P170 condenser microphone was placed on a stand as close to the moving extruder head without being knocked over by the moving components of the printer. The audio classifier is called dejavu [123] and is an open-source project written in python.

In order to generate data useful for logistic regression, a vector of scores, $\mathbf{S}$, is generated using the exact method as is described in Section 3.1. For example, the components of $\mathbf{S}$ are what are shown in Figure 4.3. The vector $\mathbf{S}$ is of length n where $n = \lfloor \frac{\text{audio length}}{\text{audio slice length}} \rfloor$. We then calculate a print score, p, where

$$p = \sum_{n} S_n \ . \tag{4.1}$$

The value p associated with a given print now determines how likely the print is to be the same as the training print with higher values meaning more likely and lower values meaning less likely.

In Figure 4.8, the ROC curves are shown for the classification results of the Rectangular Prism design with Honeycomb and Rectilinear fills. The audio is segmented to 90 second and 120 second segments, each CTh = 35. The same original audio files are used whether the audio files are segmented to 90 seconds or 120 seconds. The Honeycomb and Rectilinear tests each consist of nine target prints and sixty malicious prints. The reason for the large number of known positive error classifications was that each print is considered an erroneous version of each other print.

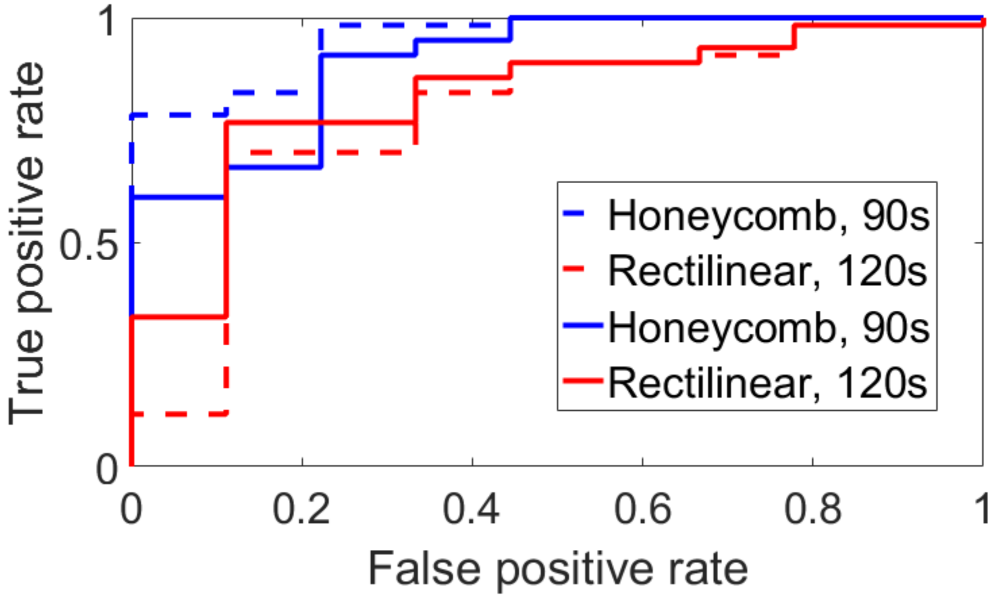


Figure 4.8: ROC Curve for Rectangular Prism, CTh = 35.

The poorest performance was an AUROC of 0.7815 for the rectilinear fill with the audio segmented at 90 seconds. That was determined to be unacceptable especially considering the high likelihood of false positives. To find an explanation for the poor classification, the G-code was inspected. Upon investigation of the G-code which was generated by Slic3r, it was found 9 lines which specified x and y coordinates along with the extrusion rate were repeated 12 times each out of 15 layers needed to complete the print in both the Rectilinear and Honeycomb fill patterns. Also, upon investigating sequentially repeated blocks of code, it was found that blocks of G-code describing three entire layers were repeated twice during the course of the print. This symmetry was hypothesized to be the cause of the classification confusion.

To test this hypothesis, a second set of tests were conducted with the Top Hat design, which is asymmetrical along the z axis. The same number of prints was performed with Honeycomb and Rectilinear fill being sliced to 90s and 120s each and CTh set to 35. The ROC curve of these experiments are shown in Figure 4.9. Each sample consists of nine target prints and sixty malicious prints, and the same data is used for the 90 second audio slice length as the 120 second slice.

Upon investigation of the G-code, the only repeated lines were those that define the nozzle speed at the beginning and do not include extrusion. Furthermore, there are no blocks of G-code or layers that are entirely repeated verbatim. This is suspected to contribute greatly to the increased performance seen in Figure 4.9. Here, least AUROC is 0.9852 which is suitable for verification purposes. Between the 120 second and 90 second slice lengths, we see little change in performance. Although audio classification is shown here to be effective in identifying malicious prints, it is still susceptible to both false positives. By introducing data from the spatial layer, these may be reduced. For instance, Figure 4.10 compares the data from the x, y, and z axes of the 40% Honeycomb

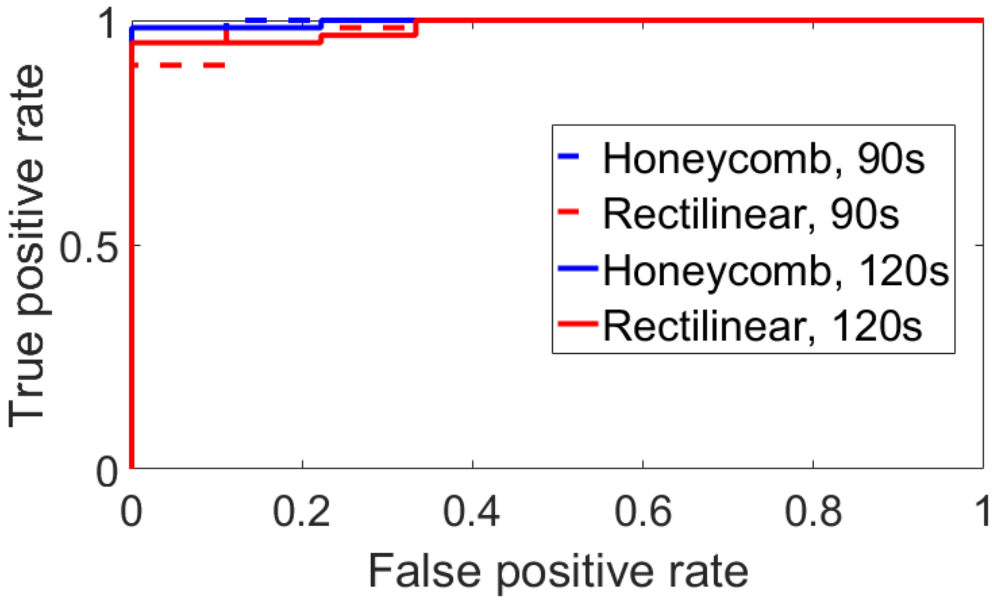


Figure 4.9: ROC Curves for Top Hat.

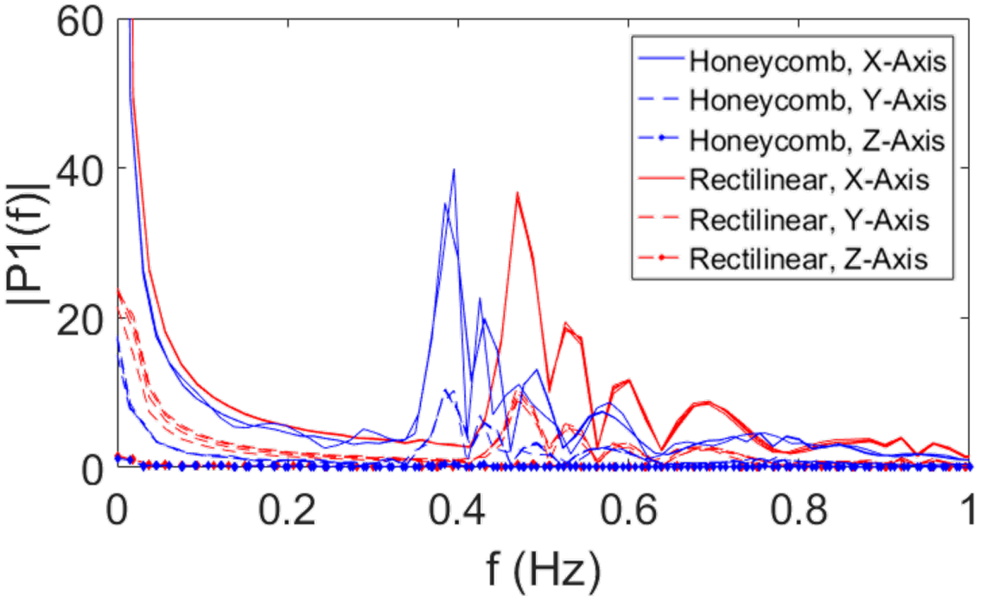


Figure 4.10: Comparison of the frequency response between a single layer of Honeycomb 40% fill and Rectilinear 40% fill. Four samples of each fill are compared.

and 40% Rectilinear fills from Figure 4.5. Here, we see a significant difference between the two prints. Each frequency response has a similar shape, but the major features of the 40% Rectilinear fill are shifted to the right because the back-and-forth motion is not impeded by the creation of small Honeycomb structures.

For classification, the four most prominent peaks are used as features along with their locations. We conducted a test in which the target print was chosen to be the disk with 20% density Rectilinear fill shown above. All other prints were considered malicious. With this, we had 10 target prints and 12 malicious prints. Training using the linear regression model, an AUROC of 1.0 was achieved in differentiating between malicious and target prints.

While the spatial sensing layer is primarily for the purpose of print visualization, its role in conjunction with the acoustic layer allows for 100% accuracy in detecting malicious prints.

Varied Printer Models. In order to understand the effectiveness of audio classification for print verification on different printer models, several prints were performed on a Lulzbot TazMini and Orion Delta. Acoustic data recordings are obtained using the same microphone. In each print, a Top Hat design identical to the one described above was printed and the audio was sliced to 120s. The optimized CTh for the TazMini, Orion Delta, and Taz6 are 150, 20, and 35 respectively. The ROC curve results are shown in Figure 4.11. Because the Honeycomb and Rectilinear fill patterns are considered together, each data set consists of 18 target prints and 120 malicious prints. Consequently, the acoustic verification method is generalizable to printers of different sizes and configurations. The AUROC does not fall below 0.9542 in these tests.

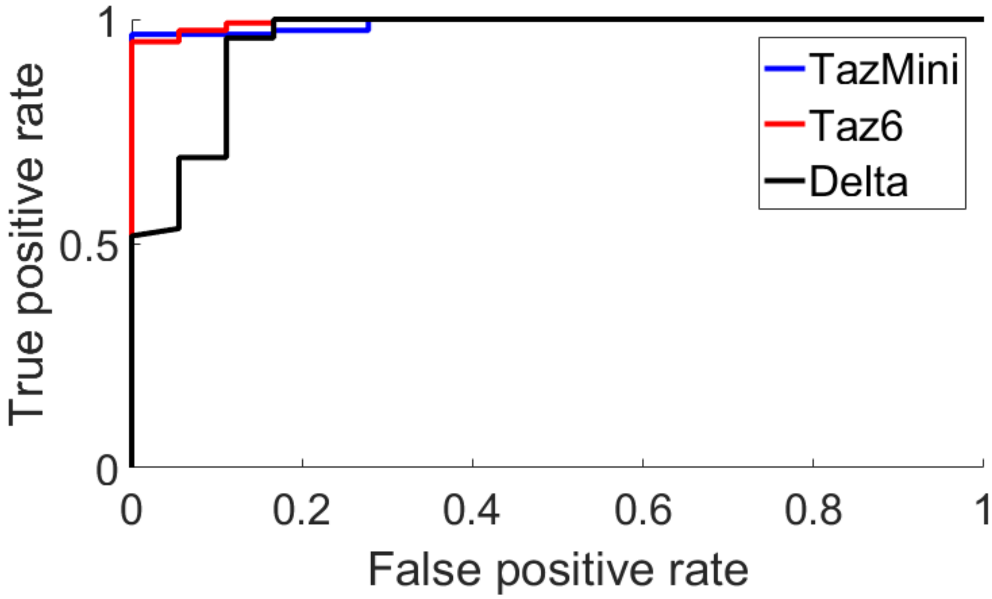


Figure 4.11: ROC curves for top hat design printed using a TazMini, Orion Delta, and Taz6 perint. Prints audio was sliced to 120 seconds and the confidence threshold is 150, 20, and 35 respectively.

Classification in Noisy Environments. Other experiments were conducted using an Afina H40 3D Printer with an eBoTrade Digital Voice Recorder wide-range microphone. This setup was in a noisy university makerspace with people talking near the printer. In this experiment, the classification accuracy suffered greatly (AUROC ≈ 0.5). Because it is shown that acoustic verification is useful on different types of printers above, we assume that the loss of classification accuracy is due to the noise in the environment. Also, because the microphone was wide range and not directional, the talking near the printer can be clearly heard. Therefore, in the implementation of this verification scheme it is important to use a directional microphone and noise isolation as much as possible.

4.2 Visualization of Malicious Prints

When a potentially malicious print is identified as described above, it is important to have the capability to visualize the potential threat. This visualization must be independent of the intended G-code which may be interpreted differently by malicious firmware. This is achieved in real time through use of the spatial sensing layer and in post-production by the materials inspection layer.

Real-Time Visualization. In the event that a potential malicious print is identified, a user has the capability of viewing the real-time print in progress through the spatial sensing as seen in Figure 4.5. By viewing the layer in progress, significant fill pattern changes such as those between the 20% Honeycomb and 20% Rectilinear fill are obvious. However, less obvious changes made to the print such as those between the 40% Honeycomb and Rectilinear fills are identifiable through FFT Analysis as in Figure 4.10. This is particularly true, as will be shown in Section 4.3, if the user has access to the frequency response of a reference print.

While the spatial sensing layer is useful for identifying the type of fill pattern that is being maliciously generated, it is less useful for identifying if the design itself has been altered due to the warping that occurs in the data. This, however, is an easy issue to solve through the use of a webcam which can easily identify the shape of the design. In this sense, it may seem that spatial sensing may be replaced altogether by a webcam, but it is important that the latter uses far more data and does not readily provide information about the frequency response.

Post Production Visualization. The aforementioned materials-based verification methods are meant to be generalized for any scanning method that can detect the embedded contrast material within a 3D model. In our case, we chose Raman spectroscopy and computed tomography because those modalities were readily available to us at the time of evaluation.

Given the results shown in Figure 4.6, we concluded that the GNRs and DTTCI can be combined for use as a contrast agent in Raman spectroscopy. The contrast agents amplify the photon count across the Silicon spectrum in Raman spectroscopy. To echo the results shown in Figure 4.6 for the 3D printed disk, we use 10 nm diameter GNRs 780 nm absorption, and DTTCI 765 nm absorption *(Sigma Aldrich)* diluted in ethanol as the two distinct contrast agents. Each contrast agent is drop coated on the surface of the 3D printed disk. The Raman spectra of the blank 3D printed disk is also taken as the control data.

To emulate the filament with the embedded contrast agent, we produced the filament from ABS pellets using the filament maker *(Filabot)*. For the GNRs embedded filament, the ABS pellets are submerged in a GNR solution and left to dry. In this test, a 4 mL GNR solution was mixed with 12 g of pellets. Based on the information from the manufacturer, we naively calculated the number of GNRs per mL of solution to be approximately 7.284e11. Per 12 g of pellets, we can produce approximately 2 m of filament with a 2.5 mm diameter. The 3D printed disk has 50 µm in layer thickness. Therefore, for the area of 1 μm^2 on each layer of the 3D printed disk, there are approximately 4 GNRs particles. This approximation only serves as the estimation of the GNRs within the measurement area. Due to the non-uniform mixing of the the GNRs in the pellets, the distribution of GNRs within the 3D printed disk varies considerably. For the DTTCI embedded filament, while the quantity of DTTCI in the filament is not estimated, larger quantities of the DTTCI enhancer were available to produce the modified filament. The blank ABS filament is extruded using only ABS pellets.

Precise Embedding of Contrast Agents. In an ideal case, we would have the ability to embed the contrast agents or markers at precise Cartesian coordinates within the 3D printed models. However, for our proof of concept, we chose to simply create an ABS filament that was saturated in the GNRs or DTTCI throughout the entire spool of filament. The precise embedding of markers location is beyond the scope of current work. It can be explored in the near future. We then used a Lulzbot Taz dual extruder tool head to provide the capability of localize the embedded filament at precise locations.

In the following subsection, we evaluate the Raman spectra of the blank 3D printed disk, the 3D disk with GNRs or DTTCI drop coat on the surface, and the 3D printed disk with GNRs or DTTCI embedded filament. We wrote a simple C++ program that allowed the user to embed filament at desired locations by modifying the G-code where necessary, i.e., switching between the extruder nozzle containing the normal filament and the nozzle containing the GNR filament. The user can specify the beginning and end points of embedded material within the normal print path. This method was used for both the initial CT scan results as well as the final evaluation.

Imaging Analysis. In the evaluation using Raman spectroscopy, the 3D printed disk is excited with with 785 nm infrared light for 20 s per accumulation of data at 100 % power setting in Renishaw InVia micro-Raman system. Figure 4.12 shows the mean measurement results all data spectra of the 3D printed disks. Similar to the results from Figure 4.6, the spectrum of the 3D printed disk with DTTCI coated surface has significant improvement of photons counts across the spectrum comparing to the control data of the blank 3D printed disk. The spectra of the 3D printed disk from DTTCI embedded filament also shows the elevation of photons counts comparing to the control data. These spectra fall in between the spectra of the control data and the surface coated 3D printed disk. This conforms with the fact that the surface coated would accumulate more contrast agent at the measurement site comparing to the embedded filament. While the Raman spectroscopy can be used to quantify the concentration of the target particles, the elevation of the photons count in Figure 4.12 does not reflect the approximate distribution of contrast agent embedded in the filament. The measurement site in Raman spectroscopy might be a cluster or spare of contrast agent or markers. As mentioned above, the markers might not be uniformly distributed in the filament. This is confirmed in Figure 4.7c as a result of the MicroCT scanner. The high reflection in the CT scan shows the large cluster of the GNRs in the embedded filament. Due to the low resolution of the MicroCT scanner, the scan would not highlight the areas where the GNRs are sparsely distributed. While the Raman spectroscopy results of the GNRs embedded filament are not shown, the similar response can be discerned.

In classification of 3D printed blank ABS, GNRs embedded, and DTTCI embedded disk, mean and standard deviation of the spectra are used to distinguish the cluster of data set. Figure 4.12 shows the mean of the typical response of Raman spectra of 3D printed disk with blank ABS, DTTCI coated disk, and DTTCI embedded ABS filament. By observation, the greatest change of Raman shift is in the range of $100cm^{-1}$ and $800cm^{-1}$. The details of the Raman scattering separation can be seen in Figure 4.20 in Section 7.1. This is in the range of $791.21nm$ and $837.60nm$ scattering; whereas the sample is irradiated at $785nm$. Therefore, this is the reasonable range of interest for Raman scattering for all data selection. By training the logistic regression model, the classification using mean and standard deviation shows 100 % accuracy against the blank ABS (226 samples) filament for both GNRs (179 samples) and DTTCI (71 samples) embedded filaments.

In Raman spectroscopy, the maximum setting depth penetration for the Renishaw InVia micro-Raman system is approximately 300 µm, we cannot verify the 3D printed object where the GNRs or DTTCI embedded filament is implanted further inside the object. Therefor, the Raman spectroscopy would not be sufficient for the verification that require depth. In further analysis, we use the MicroCT scanner to evaluate the internal structure of 3D printed objects.

The initial results for the CT scan approach presented in Figure 4.7 showed that although the GNRs embedded filament contrasted well in the CT scan, we could not rely on the custom filament due to the sparse distribution of the GNRs. We did not have the equipment nor the expertise to manufacture a heavily saturated filament.

For a more precise proof of concept, we used commercially available stainless steel filaments where the filament is heavily saturated with stainless steel particles. Under the CT scanning, the steel particles would produce similar response to the GNRs due to high X-ray density. Although stainless steel is not biocompatible, it will serve as a substitute for the GNRs in order to provide precise visibility in the CT scan. Furthermore, we changed the control filament from ABS to polylactic acid (PLA) after comparing the densities in the CT scan. The X-ray properties of PLA versus ABS have been studied [120], but we confirmed our assumption after simple trial and error. Figure 4.14 highlights the contrast in X-ray densities between the PLA filament and the stainless steel filament. We will discuss in the subsequent section how we evaluated this approach on a tibial prosthesis.

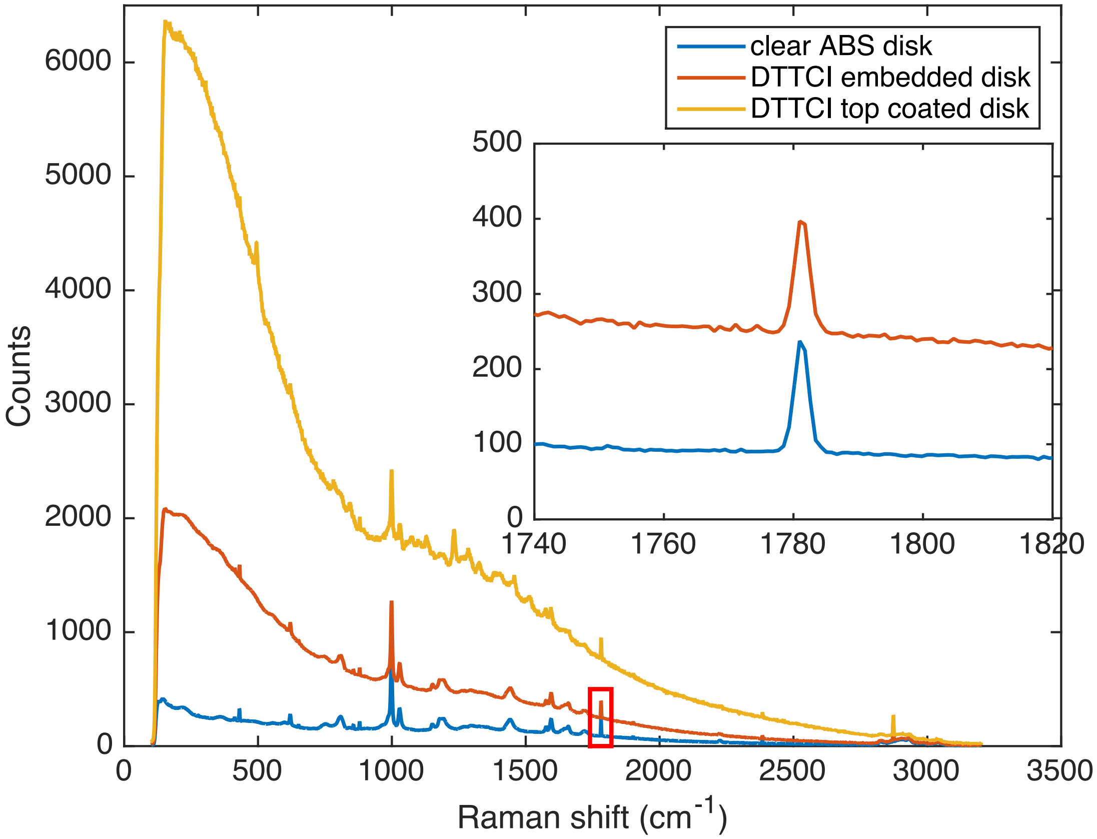


Figure 4.12: Mean measurement of Raman scattering of 3D printed disks using acrylonitrile butadiene styrene (ABS) filament and ABS with gold naonorods (GNRs) and 3,3'-Diethylthiatricarbocyanine iodide (DTTCI) embedded.

4.3 Case Study: Prosthetic Knee

As described in Section 2.5, a model of the tibial component of a prosthetic knee implant was used as a design for a use case test. Prosthetics differ slightly between patients, so we assume that malicious print identification is performed periodically with a known standard prosthetic design. Real-Time and post-production visualization are still performed on each print.

Error Identification. The acoustic verification results are shown in Figure 4.15 which shows the confidence values of both the target print and the malicious print. These results are gathered using the same technique as those described in Section 3 with audio slices of length 120s and CTh = 0. By setting CTh = 0, we see that a positive error classification can be made within the first 360s of the print or the first 4% of the total known print time by only observing out-of-sequence index classifications. The CTh

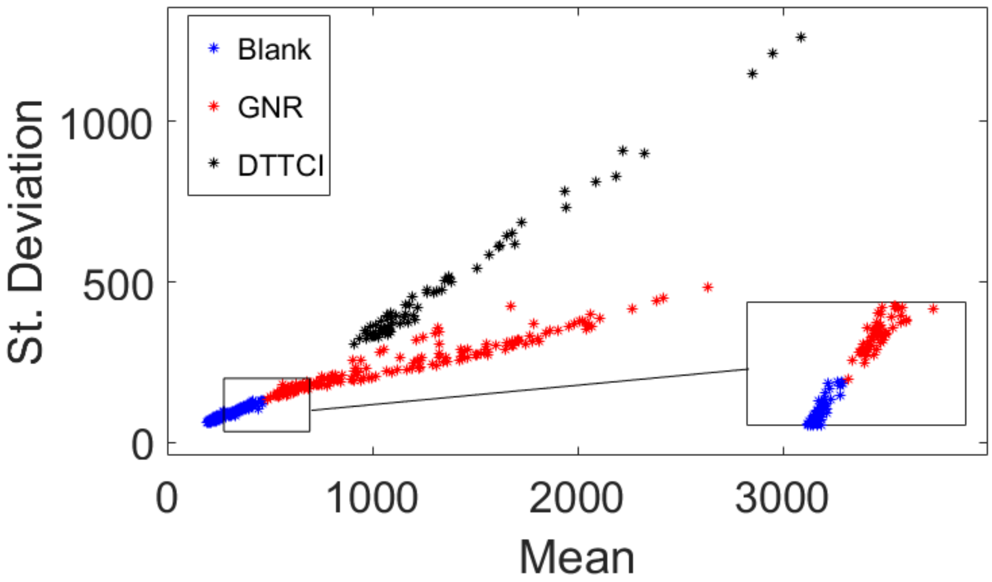
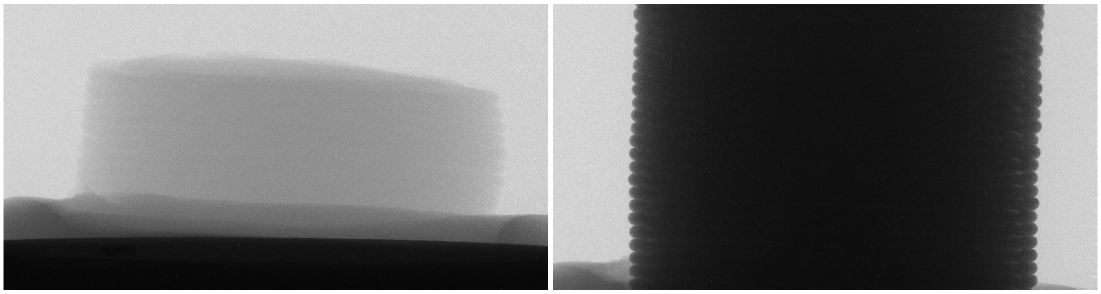


Figure 4.13: Classification of blank acrylonitrile butadiene styrene (ABS), gold nanorods (GNRs), and 3,3'-Diethylthiatricarbocyanine iodide (DTTCI) dye embedded filament in 3D printed disks.



(a) PLA filament.

(b) Stainless steel filament.

Figure 4.14: Comparison of X-ray densities of PLA and stainless steel filaments.

may be set to anything less than 18 without causing a false positive. Overall, acoustic error detection itself saves over 2 hours of print time and prevents a potentially harmful print from being completed. A detailed table of the results shown here can be found in Section 7.2.

In Figure 4.16, the FFT of a target print and a malicious print are compared to a training print. Similar to Figure 4.10, the malicious print shows a different frequency response near 0.2Hz as highlighted by the lower box. The upper box highlights the closeness of the peaks between the training and target prints and the difference between those and the malicious print. The full print of the object requires 111 layers, so it

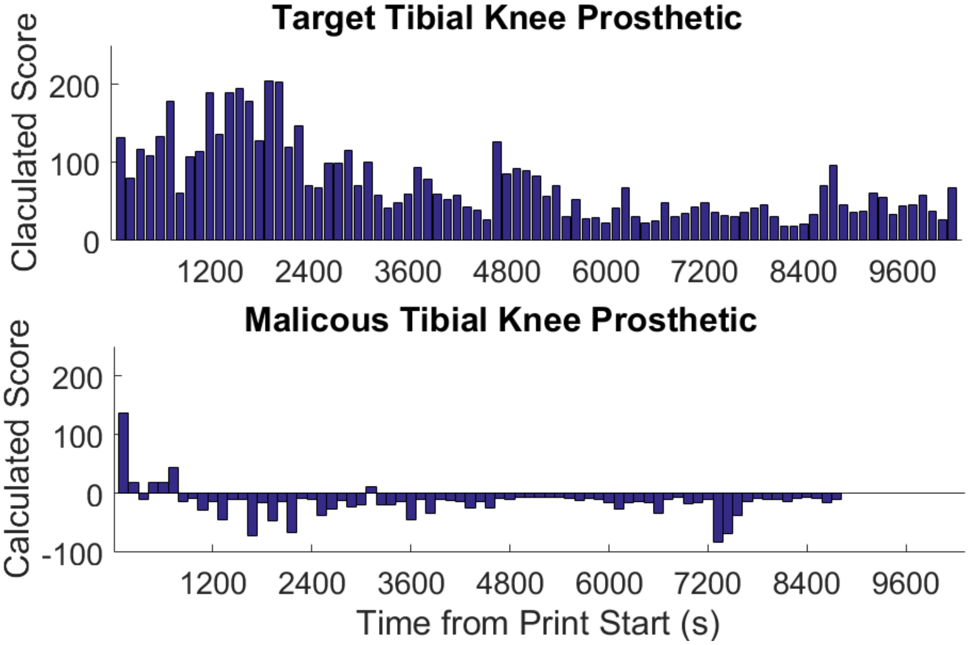


Figure 4.15: Comparison of benign and malicious prints. Comparison of target 60% Rectilinear Fill Tibial Prosthetic print acoustic classification (Top) vs. malicious 20% Honeycomb Fill (bottom). CTh = 0.

would take less 1% of the time of the total print to identify the erroneous pattern once it begins.

Real-Time Visualization. In this test, the target print uses a 60% Rectilinear fill and the malicious print uses a 20% Honeycomb fill. In the attack, the visualization of the intended G-code remains unaltered for the user while the instructions sent to the printer are altered. The consequences of this attack would be to cause accelerated wear in the implant causing pain and financial loss for the victim who has the implant. For the print identification and real-time visualization tests, a full sized prosthetic design is used. However, due to the size limitations of the MicroCT scanner, a significantly scaled down version of the same design is used.

The training, target, and attack prints were each recorded on the Lulzbot Taz6 printer. Due to the availability of the experimental setup, a single layer of each of these prints was performed by the Dobot Magician for the visualization tests. The exact same G-code was used for the Dobot prints as in the Taz6 with the exception of the extruder being disabled and the speeds decreased to suit the capabilities of Dobot. It

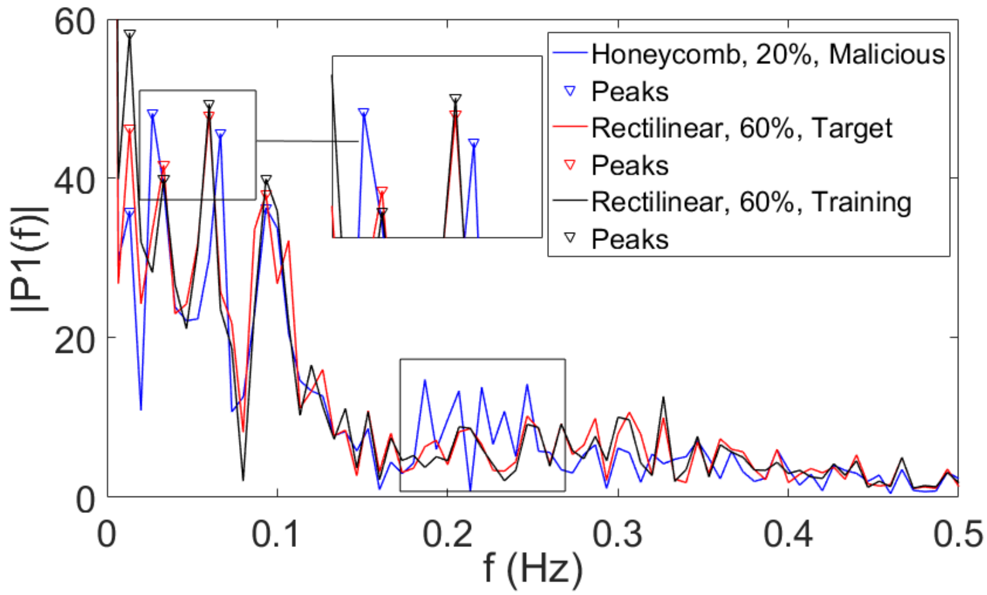


Figure 4.16: Comparison of x-axis frequency response for a layer of the tibial knee implant design.

should be noted that spatial verification testing is entirely plausible on the Taz6 which has a moving base because the measurements describe the relative position between the nozzle and the base. This is regardless of whether that base is a stationary table or a moving part of the printer. It should also be noted that both acoustic and spatial verification would ideally be performed in tandem, but for testing purposes here, they are not.

Figure 4.17 shows the spatial verification visualization of, in order of left to right, a G-code visualization of the training print, a spatial reconstruction of the target print, and a spatial reconstruction of the malicious print. It is clear that the recreated target print uses a rectilinear fill at approximately the correct density while the malicious print differs significantly from the intended G-code. Due to the warping that occurs in the spatial reconstruction, a user would not be made aware if the shape of the print were altered by using this method alone.

Post Production Visualization. We only considered the CT scan approach for the post production visualization as the Raman spectroscopy would not be able to verify the internal structure of the tibial prosthesis due to its depth limitations.

Figure 4.18 shows an X-ray scan of the front of a PLA tibial prosthesis with 2 infill

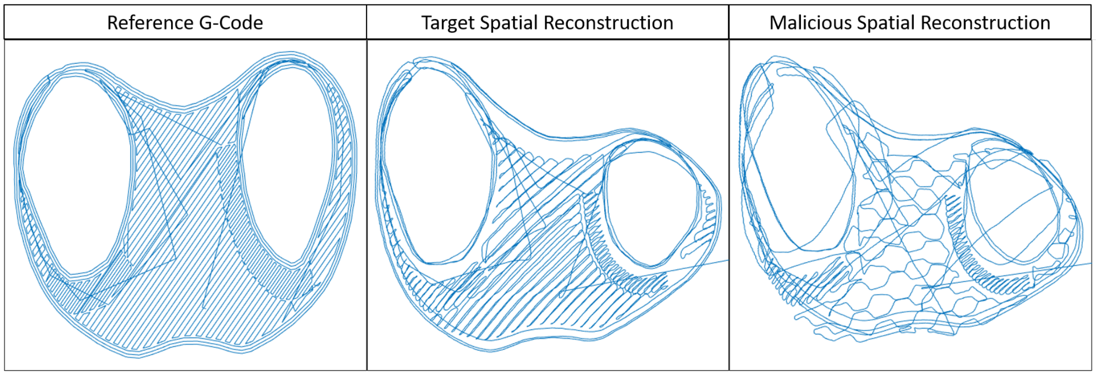

Reference G-Code
Target Spatial Reconstruction
Malicious Spatial Reconstruction

Figure 4.17: Comparison of target and malicious tibial knee implant prints. Left: G-code reconstruction of 60% Rectilinear fill, Middle: Spatial reconstruction of 60% Rectilinear fill, Right: Spatial reconstruction of malicious 20% Honeycomb fill.

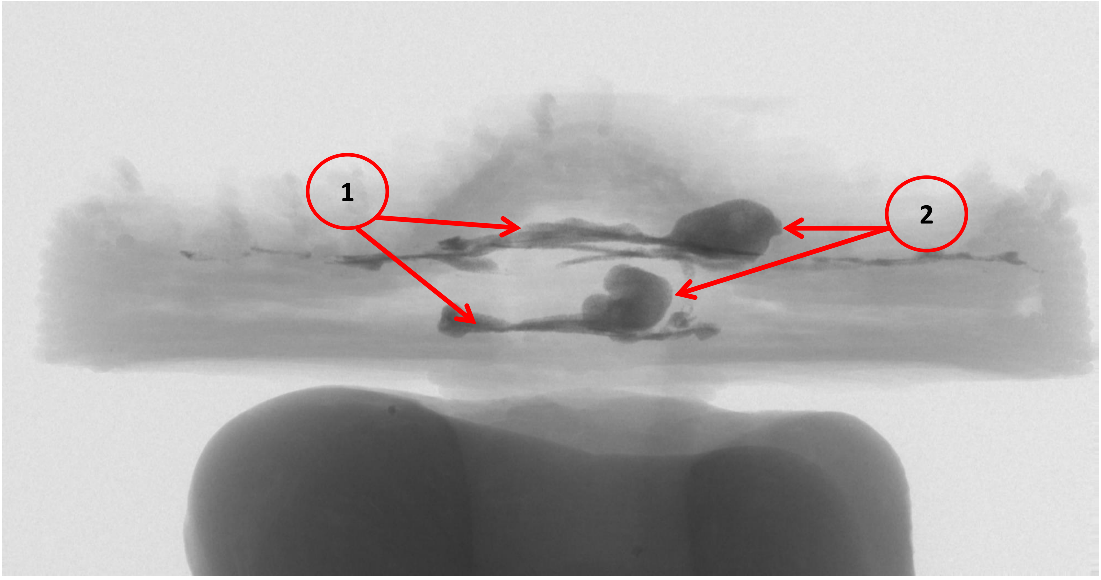


Figure 4.18: X-ray scan of front of PLA tibia with embedded stainless steel at a 15 μm/voxel size resolution. The first label shows the side view of the cross-sectional stainless steel infill, while the second label shows the two blotches where the stainless steel print began.

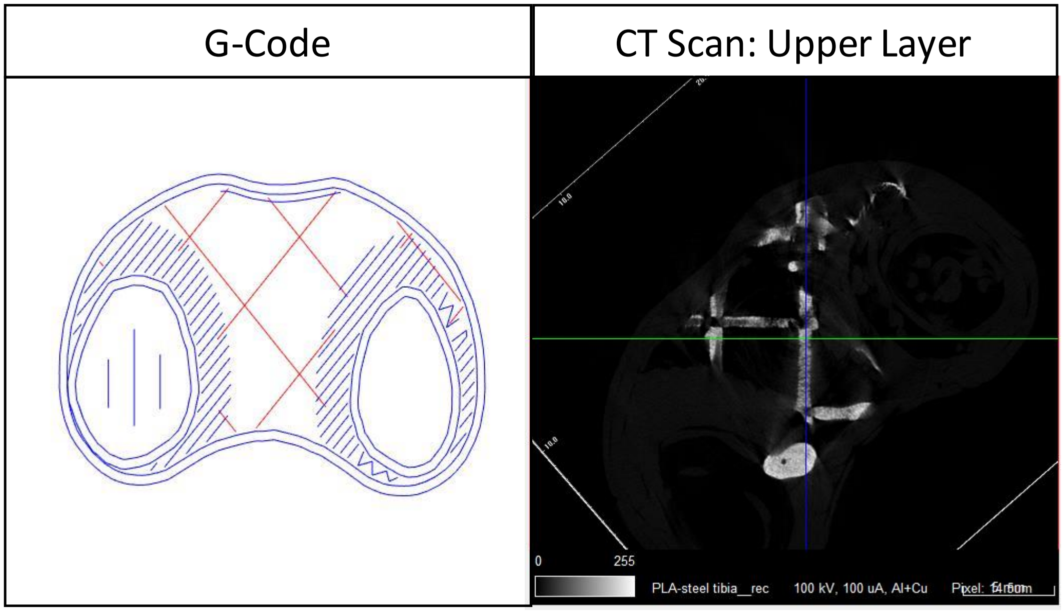


Figure 4.19: Comparison of G-code simulation of embedded steel (shown as red lines) versus CT scan of the printed model. The CT scan image is rotated about 45 degrees.

layers of steel. Because we had to use a MicroCT scanner, the part of the tibial insert was scaled down to fit within a diameter of about 30 mm. The two large blotches of stainless steel are simple imperfections that mark points where the second extruder began printing.

Figure 4.19 compares the G-Code representation of the intended print of the top stainless steel layer–with the stainless steel path highlighted in red–versus the CT scan of that layer at a 15 μm/voxel resolution. The CT scan image is rotated about 45 degrees in comparison to the intended print. Furthermore, the small model had to be mounted on a bed of silicone polymer to hold it in place, so it is not completely level. Despite the imperfections of the printed model and the scans, it can be seen that the steel was properly embedded within the walls of the model and is clearly detectable against the PLA filament.

5 Discussions

In this section, we discuss the various methods of implementing the proposed verification scheme. We then briefly discuss its limitations.

Implementation. The three layer verification and malicious print detection scheme described here is most readily suited for a mass production AM scenario. In this setting, many different standard designs may be produced using the same equipment. If each design is printed identically, then the acoustic layer, spatial sensing layer, and materials verification layer may be applied to each individual print.

In a setting such as the one described for the case study in Section 4.3, a base design may be modified for each print in order to adjust for biological parameters, etc. In this scenario, the user could train a known standard print and periodically test the printer for any malicious activity. This periodic test could include all three layers. Each specialized design, then, could be monitored using spatial and materials verification for real time and post production detection of malicious activity.

Finally, this verification scheme may be used in a scenario in which an end user sends a design to a third party to be printed. For the materials verification layer, she may send a specialized filament with embedded trackers to be used. If the object returns without the trackers or with trackers in the wrong locations, malicious activity may be detected. Also, using a secure live streaming connection, the user may receive data from the print in progress and perform any classification or analysis herself.

The experiments presented in this study focus primarily on on the detection of subtle changes in the internal fill pattern. Therefore, it is logical that more significant changes such as holes in the fill pattern or changes in the overall design will be easily detected.

Limitations. As with any verification schema, the system proposed here is not without limitations. The immediately obvious limitation is that the ability to detect a deviation from a training print decreases as the similarity to the print increases. However, drawn to its logical conclusion, this means that an attacker wishing to exploit this limitation would be forced to change the design in such a small way as to not affect its usefulness. Another limitation could be the need for a training print. This may be a minor issue in the mass production scheme described above. In a scenario such as the production of prosthetics, however, the periodic checks for malicious activity may be seen as time consuming. Finally, if a third party printing service implements these methods, some cost overhead will incur from the purchase of microphones, sensors, etc. However, these costs are relatively cheap considering that any major equipment such as a spectroscope or CT scanner would be in the domain of the end user.

6 Conclusions

Three layers of verification for AM are presented for a case in which either a control PC or printer firmware is compromised. Acoustic verification uses audio classification to determine whether a print matches a previously known print. Spatial verification provides a visualization of the print in real time along with data for frequency analysis of the printing process. Materials verification determines whether the correct materials were used and whether indicator patterns appear in the proper locations. Each layer is independent of firmware or a controller PC.

Acoustic and spatial verification are found to be useful for confirming the intended fill pattern and density in a print, and material verification is found to be most useful in determining that the correct material is used and that the design is free of tampering.

7 APPENDIX

7.1 Raman Spectroscopy Measurements

Figure 4.20 shows the Raman spectroscopy measurements of 3D printed disks of Raman scattering enhancers gold nanorods (GNRs), and Diethylthiatricarbocyanine iodide (DTTCI) embedded in acrylonitrile butadiene styrene (ABS) filament.

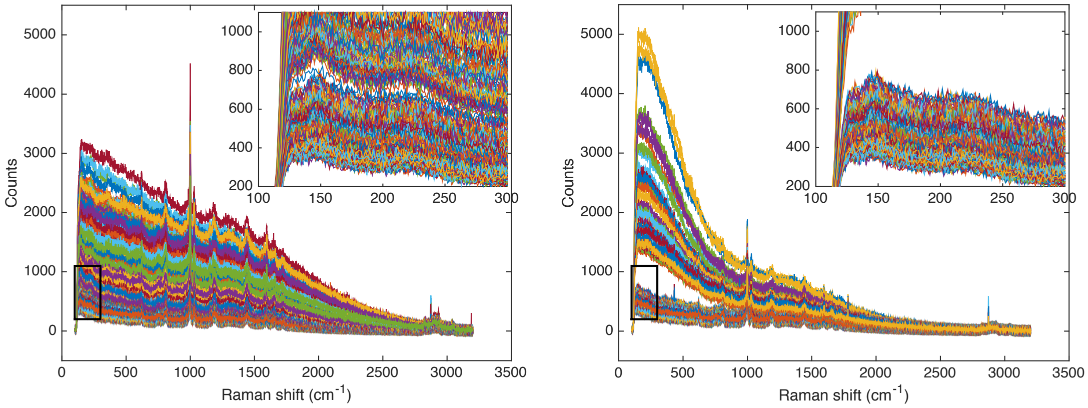
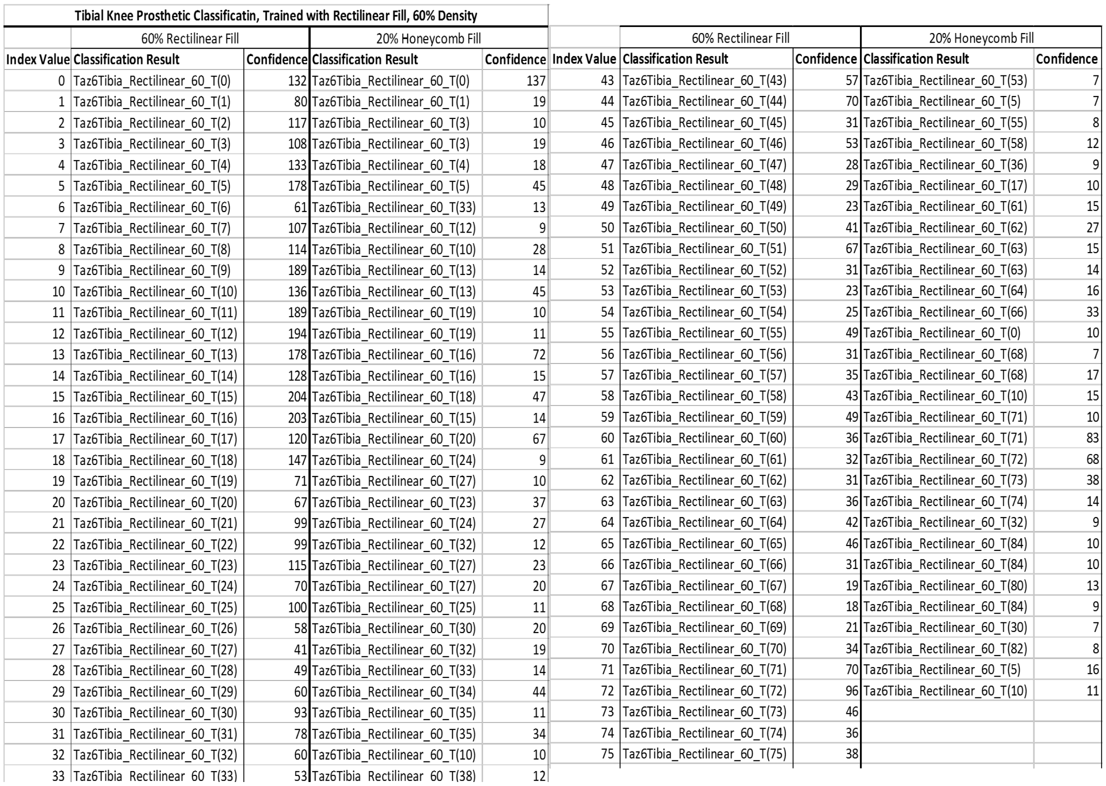


Figure 4.20: (a) Raman spectra GNRs embedded ABS filament. The GNRs amplifies Raman scattering of ABS. Inset figure shows the separation between the blank ABS and GNRs embedded ABS Raman spectra. (b) Raman spectra of ABS and DTTCI embedded ABS filaments. Large separation is due to the large quantity of enhancer embedded in ABS filament.

7.2 Results of Acoustic Classification on Tibial Knee Prosthetic



Tibial Knee Prosthetic Classificatin, Trained with Rectilinear Fill, 60% Density									
	60% Rectilinear Fill		20% Honeycomb Fill			60% Rectilinear Fill		20% Honeycomb Fill	
Index Value	Classification Result	Confidence	Classification Result	Confidence	Index Value	Classification Result	Confidence	Classification Result	Confidence
0	Taz6Tibia_Rectilinear_60_T(0)	132	Taz6Tibia_Rectilinear_60_T(0)	137	43	Taz6Tibia_Rectilinear_60_T(43)	57	Taz6Tibia_Rectilinear_60_T(53)	7
1	Taz6Tibia_Rectilinear_60_T(1)	80	Taz6Tibia_Rectilinear_60_T(1)	19	44	Taz6Tibia_Rectilinear_60_T(44)	70	Taz6Tibia_Rectilinear_60_T(5)	7
2	Taz6Tibia_Rectilinear_60_T(2)	117	Taz6Tibia_Rectilinear_60_T(3)	10	45	Taz6Tibia_Rectilinear_60_T(45)	31	Taz6Tibia_Rectilinear_60_T(55)	8
3	Taz6Tibia_Rectilinear_60_T(3)	108	Taz6Tibia_Rectilinear_60_T(3)	19	46	Taz6Tibia_Rectilinear_60_T(46)	53	Taz6Tibia_Rectilinear_60_T(58)	12
4	Taz6Tibia_Rectilinear_60_T(4)	133	Taz6Tibia_Rectilinear_60_T(4)	18	47	Taz6Tibia_Rectilinear_60_T(47)	28	Taz6Tibia_Rectilinear_60_T(36)	9
5	Taz6Tibia_Rectilinear_60_T(5)	178	Taz6Tibia_Rectilinear_60_T(5)	45	48	Taz6Tibia_Rectilinear_60_T(48)	29	Taz6Tibia_Rectilinear_60_T(17)	10
6	Taz6Tibia_Rectilinear_60_T(6)	61	Taz6Tibia_Rectilinear_60_T(33)	13	49	Taz6Tibia_Rectilinear_60_T(49)	23	Taz6Tibia_Rectilinear_60_T(61)	15
7	Taz6Tibia_Rectilinear_60_T(7)	107	Taz6Tibia_Rectilinear_60_T(12)	9	50	Taz6Tibia_Rectilinear_60_T(50)	41	Taz6Tibia_Rectilinear_60_T(62)	27
8	Taz6Tibia_Rectilinear_60_T(8)	114	Taz6Tibia_Rectilinear_60_T(10)	28	51	Taz6Tibia_Rectilinear_60_T(51)	67	Taz6Tibia_Rectilinear_60_T(63)	15
9	Taz6Tibia_Rectilinear_60_T(9)	189	Taz6Tibia_Rectilinear_60_T(13)	14	52	Taz6Tibia_Rectilinear_60_T(52)	31	Taz6Tibia_Rectilinear_60_T(63)	14
10	Taz6Tibia_Rectilinear_60_T(10)	136	Taz6Tibia_Rectilinear_60_T(13)	45	53	Taz6Tibia_Rectilinear_60_T(53)	23	Taz6Tibia_Rectilinear_60_T(64)	16
11	Taz6Tibia_Rectilinear_60_T(11)	189	Taz6Tibia_Rectilinear_60_T(19)	10	54	Taz6Tibia_Rectilinear_60_T(54)	25	Taz6Tibia_Rectilinear_60_T(66)	33
12	Taz6Tibia_Rectilinear_60_T(12)	194	Taz6Tibia_Rectilinear_60_T(19)	11	55	Taz6Tibia_Rectilinear_60_T(55)	49	Taz6Tibia_Rectilinear_60_T(0)	10
13	Taz6Tibia_Rectilinear_60_T(13)	178	Taz6Tibia_Rectilinear_60_T(16)	72	56	Taz6Tibia_Rectilinear_60_T(56)	31	Taz6Tibia_Rectilinear_60_T(68)	7
14	Taz6Tibia_Rectilinear_60_T(14)	128	Taz6Tibia_Rectilinear_60_T(16)	15	57	Taz6Tibia_Rectilinear_60_T(57)	35	Taz6Tibia_Rectilinear_60_T(68)	17
15	Taz6Tibia_Rectilinear_60_T(15)	204	Taz6Tibia_Rectilinear_60_T(18)	47	58	Taz6Tibia_Rectilinear_60_T(58)	43	Taz6Tibia_Rectilinear_60_T(10)	15
16	Taz6Tibia_Rectilinear_60_T(16)	203	Taz6Tibia_Rectilinear_60_T(15)	14	59	Taz6Tibia_Rectilinear_60_T(59)	49	Taz6Tibia_Rectilinear_60_T(71)	10
17	Taz6Tibia_Rectilinear_60_T(17)	120	Taz6Tibia_Rectilinear_60_T(20)	67	60	Taz6Tibia_Rectilinear_60_T(60)	36	Taz6Tibia_Rectilinear_60_T(71)	83
18	Taz6Tibia_Rectilinear_60_T(18)	147	Taz6Tibia_Rectilinear_60_T(24)	9	61	Taz6Tibia_Rectilinear_60_T(61)	32	Taz6Tibia_Rectilinear_60_T(72)	68
19	Taz6Tibia_Rectilinear_60_T(19)	71	Taz6Tibia_Rectilinear_60_T(27)	10	62	Taz6Tibia_Rectilinear_60_T(62)	31	Taz6Tibia_Rectilinear_60_T(73)	38
20	Taz6Tibia_Rectilinear_60_T(20)	67	Taz6Tibia_Rectilinear_60_T(23)	37	63	Taz6Tibia_Rectilinear_60_T(63)	36	Taz6Tibia_Rectilinear_60_T(74)	14
21	Taz6Tibia_Rectilinear_60_T(21)	99	Taz6Tibia_Rectilinear_60_T(24)	27	64	Taz6Tibia_Rectilinear_60_T(64)	42	Taz6Tibia_Rectilinear_60_T(32)	9
22	Taz6Tibia_Rectilinear_60_T(22)	99	Taz6Tibia_Rectilinear_60_T(32)	12	65	Taz6Tibia_Rectilinear_60_T(65)	46	Taz6Tibia_Rectilinear_60_T(84)	10
23	Taz6Tibia_Rectilinear_60_T(23)	115	Taz6Tibia_Rectilinear_60_T(27)	23	66	Taz6Tibia_Rectilinear_60_T(66)	31	Taz6Tibia_Rectilinear_60_T(84)	10
24	Taz6Tibia_Rectilinear_60_T(24)	70	Taz6Tibia_Rectilinear_60_T(27)	20	67	Taz6Tibia_Rectilinear_60_T(67)	19	Taz6Tibia_Rectilinear_60_T(80)	13
25	Taz6Tibia_Rectilinear_60_T(25)	100	Taz6Tibia_Rectilinear_60_T(25)	11	68	Taz6Tibia_Rectilinear_60_T(68)	18	Taz6Tibia_Rectilinear_60_T(84)	9
26	Taz6Tibia_Rectilinear_60_T(26)	58	Taz6Tibia_Rectilinear_60_T(30)	20	69	Taz6Tibia_Rectilinear_60_T(69)	21	Taz6Tibia_Rectilinear_60_T(30)	7
27	Taz6Tibia_Rectilinear_60_T(27)	41	Taz6Tibia_Rectilinear_60_T(32)	19	70	Taz6Tibia_Rectilinear_60_T(70)	34	Taz6Tibia_Rectilinear_60_T(82)	8
28	Taz6Tibia_Rectilinear_60_T(28)	49	Taz6Tibia_Rectilinear_60_T(33)	14	71	Taz6Tibia_Rectilinear_60_T(71)	70	Taz6Tibia_Rectilinear_60_T(5)	16
29	Taz6Tibia_Rectilinear_60_T(29)	60	Taz6Tibia_Rectilinear_60_T(34)	44	72	Taz6Tibia_Rectilinear_60_T(72)	96	Taz6Tibia_Rectilinear_60_T(10)	11
30	Taz6Tibia_Rectilinear_60_T(30)	93	Taz6Tibia_Rectilinear_60_T(35)	11	73	Taz6Tibia_Rectilinear_60_T(73)	46		
31	Taz6Tibia_Rectilinear_60_T(31)	78	Taz6Tibia_Rectilinear_60_T(35)	34	74	Taz6Tibia_Rectilinear_60_T(74)	36		
32	Taz6Tibia_Rectilinear_60_T(32)	60	Taz6Tibia_Rectilinear_60_T(10)	10	75	Taz6Tibia_Rectilinear_60_T(75)	38		
33	Taz6Tibia_Rectilinear_60_T(33)	53	Taz6Tibia_Rectilinear_60_T(38)	12					

Chapter 5

Malicious Materials Detection in Additive Manufacturing

1 Introduction

The flexibility of customization and rapid prototyping make additive manufacturing (or 3D printing) more applicable to critical application domains such as aerospace, automotive, and medical. Industries have integrated AM in the manufacturing process of critical components in major projects including those in the aerospace and military domains. For instance, General Electric (GE) Aviation plans to produce more than 100,000 additive parts for its LEAP and GE9X engines by 2020 [23]. SpaceX used 3D metal printing techniques to manufacture parts in SuperDraco, a hypergolic propellant liquid rocket engine designed and built by SpaceX [37]. Airbus puts over a thousand 3D printed parts in its A350 XWB airplane [88]. Naval Air Systems Command (NAVAIR) has marked its first successful flight demonstration of a titanium, 3D printed link and fitting assembly for the engine nacelle in MV-22B Osprey [52]. Oak Ridge National Laboratory's Manufacturing Demonstration Facility created the military's first 3D printed 30-foot proof-of-concept hull out of carbon fiber composite material [56]. Apart from aerospace, AM also has wide application in medical fields, such as tissue and organ fabrication, the creation of customized prosthetics, implants, and anatomical models [121].

The safety of the application of printed objects highly depends on the reliability of the printed objects. Howeve in recent development of 3D printing, the active material can be embedded within the 3D printed object to transform its structure when activated [21, 71, 86]. This poses a new challenge for 3D printing. The malicious materials can effect the structure and integerity of the 3D printed object when activated.

The materials used in 3D printing has yet to be scrutinized [131]. Detection of material changes is crutial to prevent the embedding of unknown materials within 3D printed objects. In this chapter, we propose a preliminary design and evaluation of portabe dielectric based sensor system to verify the materials in 3D printing.

2 Background

In this section, we describe the embedding of active materials in 3D printing for object's structure transformation. Furthermore, we describe lock-in amplifier architecture used in the proposed dielectric based sensor system for material verification.

2.1 Active Materials in 3D Printing

Active or programmable materials allow shape transformation under stimulations. Active material can change its properties and physical appearance considerably by swelling or shrinking with the external stimuli such as temperature changes, pH level of solvent, water, or humidity [74].

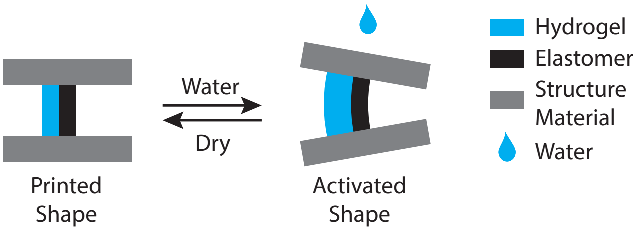


Figure 5.1: Hydrogel swells when contacting water. The swelling effect can be leveraged to control the shape change of a 3D printed object.

Hydrogel is one of the popular active materials. Hydrogel can absorb water and swell to increase its volume to 400 % [71]. On the other hand, when the environment is dry, water is lost and the hydrogel shrinks. By carefully design 3D structures with hydrogel, the desired structure change can be achieved when stimulated [10].

Figure 5.1 shows a simplified version of the design by Tibbits [116]. The object is composed of structural material, elastomer, and hydrogel. When the object in immersed in water, the hydrogel can swell up. The shape change can be predetermined by carefully arranging the distribution of the three components in the design.

Thermally induced polymers such as a blend of polylactic acid (PLA) and thermoplastic polyurethane (TPU) can also be considered active materials [67, 128]. To activate the material, the 3D printed object must be heated above critical temperature of the polymer, called glass transition temperature T_g. When the temperature is below T_g, the polymer is in a rigid state; whereas when the temperature is above T_g, the polymer is in elastic state, allowing for shape transformation of the structure of 3D printed object.

2.2 Lock-in Amplifier Architecture

In Chapter 2 and Chapter 3 , we introduced the information and user privacy protection via a physical design of a cytometry microfluidic device. The design of microfluidic device allows the encryption of information by reconfiguring the biosensor. The functionality of cytometry microfluidic device enables the embedding of authentication strings associate with the test results. The signal measurement in the cytometry microfluidic device is performed by the lock-in amplifier instrument Zurich HF2LI and current amplifier HF2TA.

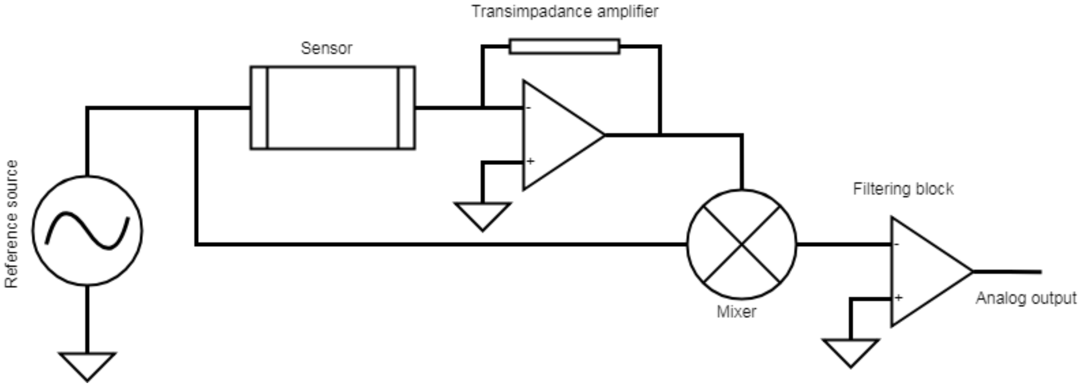


Figure 5.2: Simlified lock-in amplifier architecture.

Lock-in amplifier (LIA) intrument is the common system for detecting small signal below the noise floor using synchronous detection. This measurement technique promises the sensitivity thousand time lower than noise floor through a narrow band pass filter, which centeres around the carrier frequency [45, 40]. The performance of the

LIA has been demonstrated in various electronics sensing systems including the contactless sensing for capillary electronics micro-devices [76, 40, 27]. The high frequency reference sigal allows the bypass of coupling capacitive on the contactless sensors in microfluidic device; thus the ouptut signal can be linearly amplifed and detected using the lock-in amplification technique.

Figure 5.2 shows the simplified architecture of a LIA. The sinusoidal wave generator is used to modulate the sensor measurement with high frequency carrier signal. This gives the advantage of removing the intrinsic shot noise at baseband measuerement. The transimpedance amplifier converts sensing current to voltage signal. The output of transimpedance amplifier is demodulated using reference sinusoidal signal. The low pass filter coupling with amplifier block is used to amplify to signal to the detectable output signal. The more detail desciptions of design and analysis is shown in [113]. In this work, we present the preliminary application of the LIA for material detection in additive manufacturing.

3 Lock-in Amplifier System Design

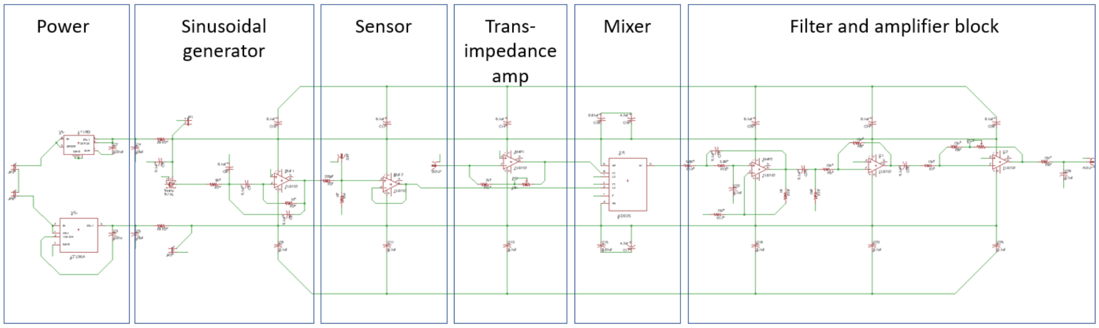
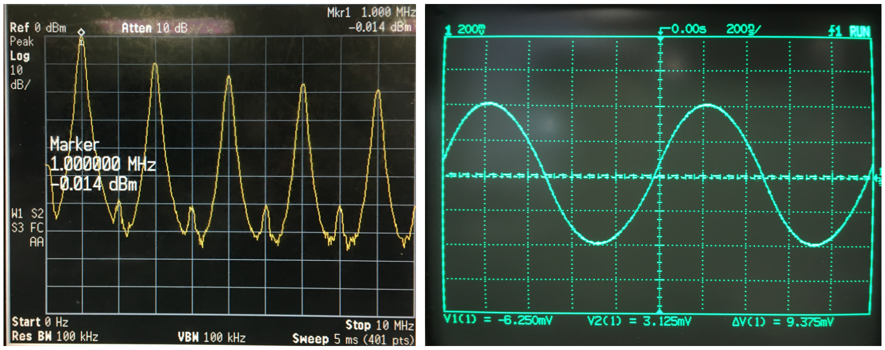


Figure 5.3: Lock-in amplifer schematics desing of the portable material detection in additive manufacturing. The design is completed with power source, sinusoidal signal generator, transimpedance amplifier, mixer, and the filtering block.

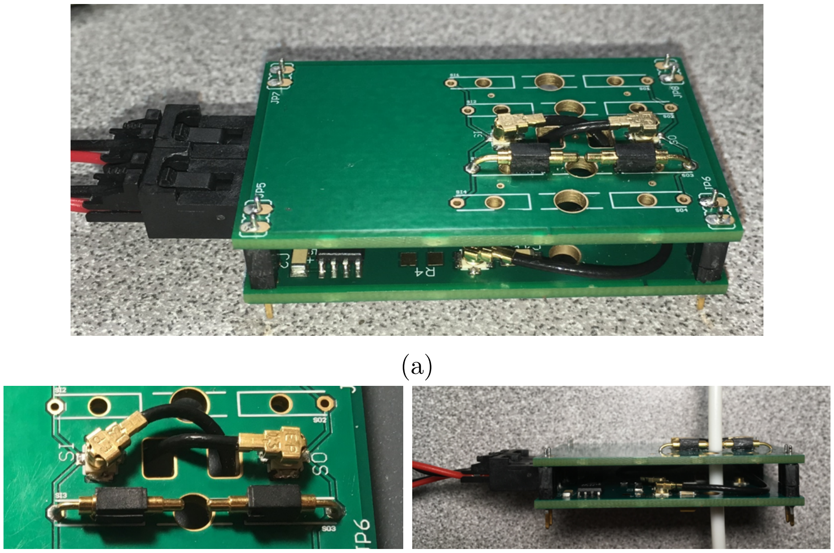
In this section, we present a portable material detection for additive manufacturing using an analog lock-in amplifier architecture design. Figure 5.3 describes the chematics of the LIA design. The system is completed with power source, sinusoidal signal generator, transimpedance amplifier, and filtering block. The power source consists of the 5 V and −5 V blocks. The sinusoidal signal generator uses the simple design of square



(a) (b)

Figure 5.4: Sinusoidal reference signal generator. (a) Spectrum of squarewave with odd harmonics. (b) Sinusoidal signal output after feeding squarewave through narrow bandpass filter.

wave clock filtering through a narrow band pass filter to remove the odd harmonics. Figure 5.4a shows the output of the1 MHz clock crystal and Figure 5.4b shows the output sinusoidal wave after feeding the squarewave through a narrow bandpass filter. The sinusoidal signal is used both as excitation of the measurement and reference signal in synchronous detection.



(a)

(b) (c)

Figure 5.5: Portable lock-in amplifier module. (a) Assembly of lock-in amplifier module. The portable device is powered with 5 V and −5 V power sources through voltage regulators. (b) Spring loaded contacts is used to perform dielectric measurement. The contact can change dimention for different filament diameters. (c) Filament is fed through the module for continuous monitoring.

The biosensor in microfluidic device is replaced by off-the-shelf (SoT) spring loaded contact as seen in Figure 5.5b. The printed circuit board (PCB) of the LIA is fabricated using the SoT components as seen in Figure 5.5. The sensor measures the filament dielectrics as it passes through the printer's extruder as in Figure 5.5c. In this system, the LIA is desinged to make the measurement at 1 MHz-1 V excitation. The portable device can be affixed to the 3D printer pernamently for continuous monitoring of the material while printing.

4 Evaluations

From the simplified capacitance formula,

$$C = \epsilon_o * A/d$$

where C is the capacitance, ϵ_o is the electric constant (which is the fiament in this evaluation), A is the area overlap of contact, and d is the distance between two measurement contacts (or diameter of filament), when comparing the same filament concentration of PLA/TPU with differnet diameters, the filament diameters would be inversely propotioned to the estimated capacitance value of the filament as seen in Figure 5.6.

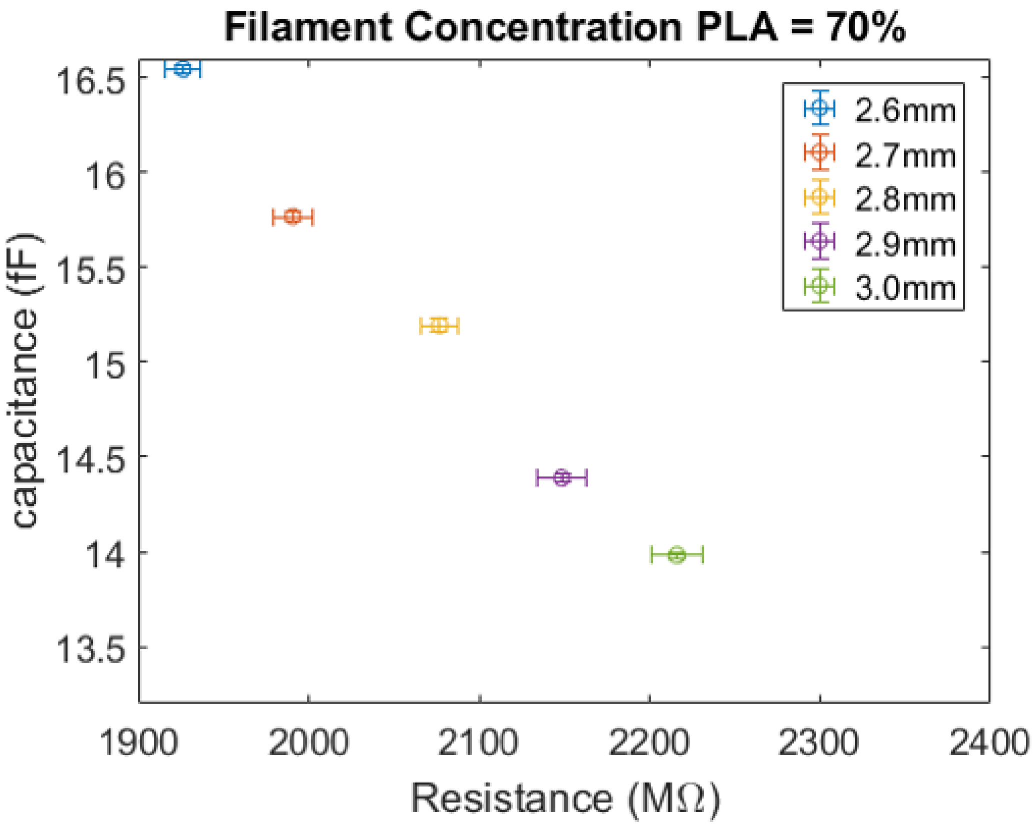


Figure 5.6: Quantifying filament diameter based on estimation of RC values using dielectric based sensor. *Top left* - Typical AC sweep response of filaments. The insert figure shows the equivalent RC model from DC to 10 MHz.

In this evaluation of the sensor and LIA system, we evaluation the ability of dielectric based sensor in detecting change in material and diameter of the filament. Figure 5.7 shows the detail of quantifying fialment diameters based on the estimation of RC values corresponding to diameters and concentrations of PLA/TPU change in fialment. The top left figure shows the typical AC sweep response of the filaments. The response has flat band at 5 kHz and steadily rises beyond 10 MHz with a single pole. This can be modeled as a simple RC network as inserted figure. Using two-point measurement at 5 kHz and 10 MHz, the RC values can be calculated according to the diameters and concentrations change in filaments. Figure 5.7 shows the RC-values as the results of filament diameter varying from 26 mm to 30 mm.

Figure 5.8 shows the measurement results of different filaments. In this assessment, we evaluate the ability of senor and LIA in differentiating PLA/TPU blend at different

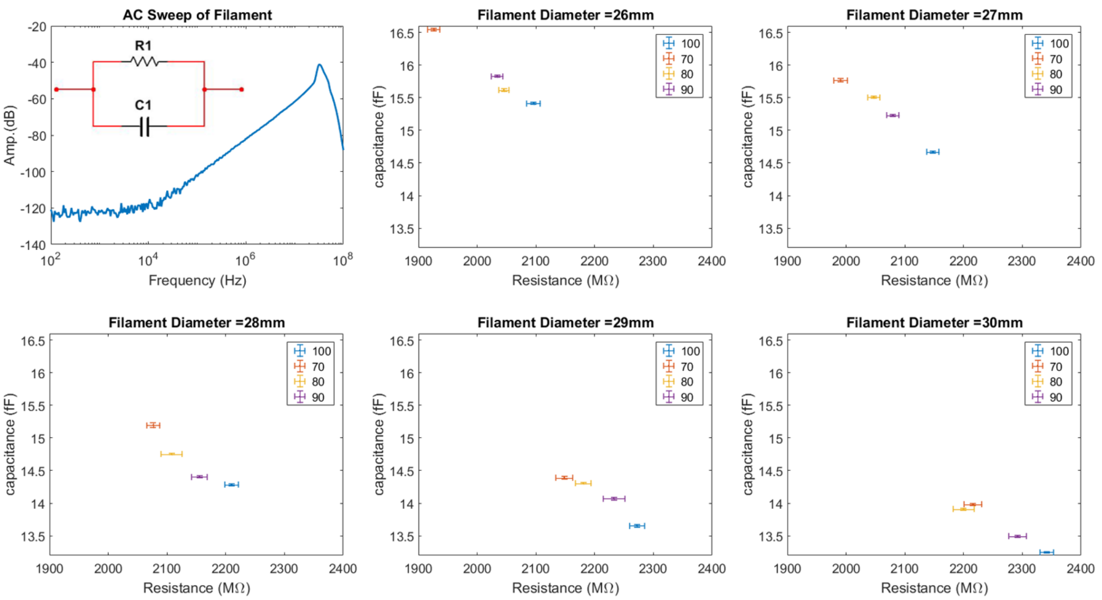


Figure 5.7: Quantifying filament diameter based on estimation of RC values using dielectric based sensor. *Top left* - Typical AC sweep response of filaments. The insert figure shows the equivalent RC model from DC to 10 MHz.

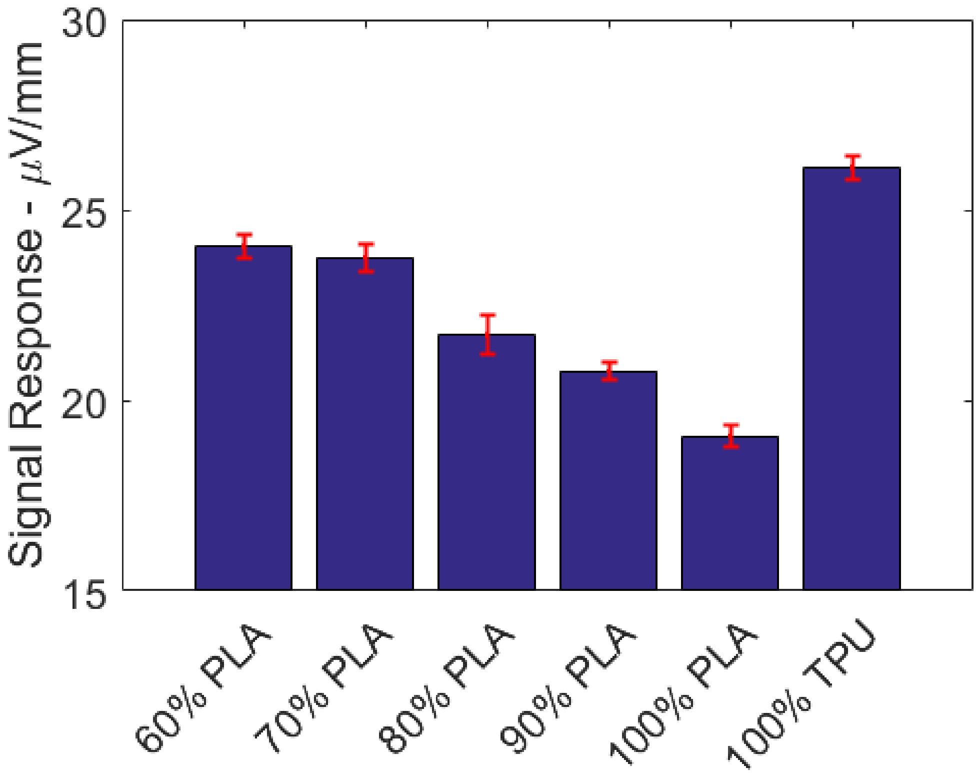


Figure 5.8: Dielectric properties measurement of filaments using lock-in amplifier.

concentations. The result shows that the portable device can detect the variations when changing from 60 %-100 % of PLA concentration at 10 % increasement.

5 Conclusions

The dielectric measurement technique using the lock-in amplifier (LIA) can be applied to monitor the filament in additive manufacturing. By replacing the biosensor in the typical application of the LIA with the spring loaded contacts, we can accomodate the measurement of filament diameter changes. Futhermore, the material detetion module can differentiate multiple PLA/TPU material bends. This portable device is applicable for continuous monitoring material in 3D printing, which is a crucial step for preventing malicious material embedding within the printed objects.

6 APPENDIX

6.1 Lock-in Amplifier Assembly Part List

This section lists the components used in assembling the lock-in amplifier. The ciruit is designed using EAGLE designing tool, version 9.2.0, 1988-2018 Autodesk, Inc.

Table 5.1: Lock-in amplifier components

Part	Value	Device	Package	Library
AMP1	TL071D	TL071D	SO08	linear
AMP2	TL071D	TL071D	SO08	linear
AOUT		734120110	734120110	con-coax
BUF1	TL071D	TL071D	SO08	linear
BUF2	TL071D	TL071D	SO08	linear
C1	0.1uF	C-USC1206	C1206	resistor
C2	0.01uF	C-USC1206	C1206	resistor
C3	0.01u	C-USC1206	C1206	resistor
C4	10uF	C-USC1206	C1206	resistor
C5	10uF	C-USC1206	C1206	resistor
C6	0.1uF	C-USC1206	C1206	resistor
C7	0.1uF	C-USC1206	C1206	resistor
C8	0.1uF	C-USC1206	C1206	resistor
C9	0.1uF	C-USC1206	C1206	resistor
C10	0.1uF	C-USC1206	C1206	resistor
C11	0.1uF	C-USC1206	C1206	resistor
C12	0.1uF	C-USC1206	C1206	resistor
C13	0.1uF	C-USC1206	C1206	resistor
C14	0.1uF	C-USC1206	C1206	resistor
C15	0.01uF	C-USC1206	C1206	resistor
C16	0.01uF	C-USC1206	C1206	resistor
C17	4.7uF	C-USC1206	C1206	resistor

C18	4.7uF	C-USC1206	C1206	resistor
C19	0.1uF	C-USC1206	C1206	resistor
C20	0.1uF	C-USC1206	C1206	resistor
C21	0.1uF	C-USC1206	C1206	resistor
C22	0.1uF	C-USC1206	C1206	resistor
C23	0.1uF	C-USC1206	C1206	resistor
C24	0.1uF	C-USC1206	C1206	resistor
C25	0.1uF	C-USC1206	C1206	resistor
C26	0.1uF	C-USC1206	C1206	resistor
C27	0.1uF	C-USC1206	C1206	resistor
C28	0.1uF	C-USC1206	C1206	resistor
C29	0.1uF	C-USC1206	C1206	resistor
G1	TL071D	TL071D	SO08	linear
G2	TL071D	TL071D	SO08	linear
PG	10k	POT	POT	NA
PG2	2k	POT	POT	NA
R1	9k	R-US_R1206	R1206	resistor
R2	1k	R-US_R1206	R1206	resistor
R3	220p	R-US_R1206	R1206	resistor
R4	1k	R-US_R1206	R1206	resistor
R5	15k	R-US_R1206	R1206	resistor
R6	15k	R-US_R1206	R1206	resistor
R7	15k	R-US_R1206	R1206	resistor
R8	15k	R-US_R1206	R1206	resistor
R9	15k	R-US_R1206	R1206	resistor
R10	15k	R-US_R1206	R1206	resistor
R14	5.6k	R-US_R1206	R1206	resistor
R15	5.6k	R-US_R1206	R1206	resistor
R16	1k	R-US_R1206	R1206	resistor
R17	15k	R-US_R1206	R1206	resistor

RFR1	NA	BLM15HB	0402	ferrite
RFR2	NA	BLM15HB	0402	ferrite
RG	2k	R-US_R1206	R1206	resistor
SIN		734120110	734120110	con-coax
SOUT		734120110	734120110	con-coax
V5+	LT1763	LT1763CS8-5	SOIC8	linear-technology
V5-	LT1964	LT1964ES5-5	SOT	LTC
XR	AD835	AD835ARZ	SOIC	AD835ARZ
XTAL	1MHz	SG-210STF20H	FA-20H	crystal

Chapter 6

Conclusions

The importance of portable diagnostic devices become more apparent in personal healthcare. The growing popularity PoC devices also increase the interests of cyber criminals in the budding technology. While showing great accuracy, flexibility among other potentials to be the counter part of the legacy healthcare management, it also creates significant concern over user's privacy and security.

The contributions of this thesis as follow.

- Chapter 2 provides the lightweight analog encryption scheme leveraging the design of microfluidic flow impedance cytometer to protect its measurement data. The hardware-level trusted sensing obfuscates the diagnostic information of the patient. This design guarantees the data protection by having small trusted computing base and considering the connecting mobile device and cloud servers untrusted. While the analysis can of information can be done on the honest but curious cloud server, the information discerned by the server cannot infer the diagnostic result.

- Chapter 3 presents the domain specific user authentication without using the private information. The synthetic micro-beads are used as the *characters* in the authentication string. By combining multiple bead sizes and concentrations, we can generate unique authentication string specific to a test result or user. This alternative method removes the authentication burdens from the users and protect patient privacy by preventing the directly linking of personal information with the diagnostic results.

- In Chapter 4, we develop the scheme of verification and intrusion detection that is independent of the device under test. Using the study of additive manufacturing the tibial knee implant, we incorporate both of the real-time verification and post production to verify the integrity of the 3D printed object. These verification methods can accurately verify the printing in real-time and stop the process in the event of discrepancy, and provide the non-destructive way to validate the internal structure of the 3D printed object.

- Chapter 5 presents malicious material detection in additive manufacturing. The full design of the test system addresses the portability, flexibility, and low cost of POC devices. The portable device can be used as a standalone unit for continuous monitoring of filament in additive manufacturing. As the reseulting application, the device can be used to detect and prevent the embedding of unknown or malicious materials within 3D printed structures.

Potential future works

Intrusion detection for additive manufacturing in real-time. As discussed in Chapter 4, the real-time malicious intrusion detection of the 3D printed object using acoustic signature relies on the training data of the same print over time. However, we can remove the need for training data and perform the intrusion detection in real-time using the live imaging of the printing process. As shown in Chapter 4, the movement of parts in the printer can be used to reconstruct the design of the object. By using the live imaging method, we can reconstruct the object while printing to verify with the design. While this method is very similar to the use of accelerometer, the advantages of the live imaging method are the monitoring of the filament while printing, monitoring the layer thickness, among others. The acceleromter data cannot be used to infer printing error in the event of no filament being extruded; whereas the live imaging can be used to construct the design to the design specifications such as layer thickness, filament type, printing temperature (for example, using infrared imaging).

In Chapter 4, we also mentioned that the supplier of the filament to be trusted in our threat model. In the future work, we can also add this entity to the threat model. In this event, we need to further verify the different materials detection of the prtable measurement device as presented in Chapter 5.

Portable and scalable test system. In Chapter 2, we used an analog multiplex device to select the sensors pairs in cytometry microfluidic device for encryption of diagnostics information. A similar design architecture can be employed to create a scalable system. Coupling with the design of the LIA, a large system can be created to monitor multiple 3D printers. Using time division multiplexing, the system can periodically check the materials feeding in each printer.

Bibliography

[1] Arconic strengthens 3d printing collaboration with airbus. *http://advancedmanufacturing.org/arconic-airbus-3d-printing-collaboration/*, Dec 2016. URL `http://advancedmanufacturing.org/arconic-airbus-3d-printing-collaboration/`.

[2] Hardware meets software in advanced manufacturing. *https://www.ge.com/stories/hardware-meets-software-advanced-manufacturing*, 2017. URL `https://www.ge.com/stories/hardware-meets-software-advanced-manufacturing`.

[3] Knee replacement implant materials. *https://bonesmart.org/knee/knee-replacement-implant-materials/*, 2017. URL `https://bonesmart.org/knee/knee-replacement-implant-materials/`.

[4] Natural machines: The makers of foodini - a 3d food printer making all types of fresh, nutritious foods. *http://www.naturalmachines.com/*, 2017. URL `http://www.naturalmachines.com/`.

[5] A. Adams and M. A. Sasse. Users are not the enemy. *Communications of the ACM*, 42(12):40–46, 1999.

[6] S. Akin and A. Kovscek. Computed tomography in petroleum engineering research. *Geological Society, London, Special Publications*, 215(1):23–38, 2003.

[7] Avery Li-Chun Wang. An industrial strength audio search algorithm.

[8] L. Aylmore. Use of computer-assisted tomography in studying water movement around plant roots. *Advances in Agronomy*, 49:1–54, 1993.

[9] M. Backes, M. Dürmuth, S. Gerling, M. Pinkal, and C. Sporleder. Acoustic side-channel attacks on printers. In *Proceedings of the 19th USENIX Conference on Security*, USENIX Security'10, pages 20–20. USENIX Association. URL `http://dl.acm.org/citation.cfm?id=1929820.1929847`.

[10] S. E. Bakarich, R. Gorkin III, M. I. H. Panhuis, and G. M. Spinks. 4d printing with mechanically robust, thermally actuating hydrogels. *Macromolecular rapid communications*, 36(12):1211–1217, 2015.

[11] P. Balakrishnan, M. Dunne, N. Kumarasamy, S. Crowe, G. Subbulakshmi, A. K. Ganesh, A. J. Cecelia, P. Roth, K. H. Mayer, S. P. Thyagarajan, and S. Solomon. An inexpensive, simple, and manual method of cd4 t-cell quantitation in hiv-infected individuals for use in developing countries. *JAIDS Journal of Acquired Immune Deficiency Syndromes*, 36(5):1006–1010, 2004.

[12] B. Berman. 3-d printing: The new industrial revolution. 55(2):155–162. ISSN 0007-6813. doi: 10.1016/j.bushor.2011.11.003. URL https://www.sciencedirect.com/science/article/pii/S0007681311001790.

[13] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *2012 IEEE Symposium on Security and Privacy*, pages 553–567. IEEE, 2012.

[14] F. M. Bui and D. Hatzinakos. Biometric methods for secure communications in body sensor networks: Resource-efficient key management and signal-level data scrambling. *EURASIP J. Adv. Signal Process*, 2008:109:1–109:16, Jan. 2008. ISSN 1110-8657. doi: 10.1155/2008/529879. URL http://dx.doi.org/10.1155/2008/529879.

[15] A. Campion and P. Kambhampati. Surface-enhanced raman scattering. *Chemical Society Reviews*, 27(4):241–250, 1998.

[16] X. Cheng, D. Irimia, M. Dixon, K. Sekine, U. Demirci, L. Zamir, R. G. Tompkins, W. Rodriguez, and M. Toner. A microfluidic device for practical label-free cd4+ t cell counting of hiv-infected subjects. *Lab on a Chip*, 7(2):170–178, 2007.

[17] X. Cheng, D. Irimia, M. Dixon, J. C. Ziperstein, U. Demirci, L. Zamir, R. G. Tompkins, M. Toner, and W. R. Rodriguez. A microchip approach for practical label-free cd4+ t-cell counting of hiv-infected subjects in resource-poor settings. *JAIDS Journal of Acquired Immune Deficiency Syndromes*, 45(3):257–261, 2007.

[18] K. Cheung, S. Gawad, and P. Renaud. Impedance spectroscopy flow cytometry: On-chip label-free cell differentiation. *Cytometry Part A*, 65(2):124–132, 2005.

[19] S. R. Chhetri, A. Canedo, and M. A. Al Faruque. Kcad: Kinetic cyber attack detection method for cyber-physical additive manufacturing systems. In *Proceedings of the 35th International Conference on Computer-Aided Design*, page 74. ACM, 2016.

[20] K. B. Chien, E. Makridakis, and R. N. Shah. Three-dimensional printing of soy protein scaffolds for tissue regeneration. *Tissue Engineering Part C: Methods*, 19 (6):417–426, 2012.

[21] J. Choi, O.-C. Kwon, W. Jo, H. J. Lee, and M.-W. Moon. 4d printing technology: A review. *3D Printing and Additive Manufacturing*, 2(4):159–167, 2015.

[22] V. Cnudde and M. N. Boone. High-resolution x-ray computed tomography in geosciences: A review of the current technology and applications. *Earth-Science Reviews*, 123:1–17, 2013.

[23] B. P. Conner, G. P. Manogharan, A. N. Martof, L. M. Rodomsky, C. M. Rodomsky, D. C. Jordan, and J. W. Limperos. Making sense of 3-d printing: Creating a map of additive manufacturing products and services. *Additive Manufacturing*, 1:64–76, 2014.

[24] A. J. Crosby and J.-Y. Lee. Polymer nanocomposites: the “nano” effect on mechanical properties. *Polymer reviews*, 47(2):217–229, 2007.

[25] J. Daemen and V. Rijmen. *The design of Rijndael: AES-the advanced encryption standard*. Springer Science & Business Media, 2013.

[26] A. Davies, . Feb. 28, and . 6. A swedish automaker is using 3d printing to make the world's fastest car. URL http://www.businessinsider.com/koenigsegg-one1-comes-with-3d-printed-parts-2014-2.

[27] A. De Marcellis, G. Ferri, P. Mantenuto, and A. D'Amico. A new single-chip analog lock-in amplifier with automatic phase and frequency tuning for physical/chemical noisy phenomena detection. In *5th IEEE International Workshop on Advances in Sensors and Interfaces IWASI*, pages 121–124. IEEE, 2013.

[28] K. Dheda, A. Lalvani, R. F. Miller, G. Scott, H. Booth, M. A. Johnson, A. Zumla, and G. A. Rook. Performance of a t-cell-based diagnostic test for tuberculosis infection in hiv-infected individuals is independent of cd4 cell count. *Aids*, 19(17): 2038–2041, 2005.

[29] J. M. Eisenberg. Can you keep a secret? *Journal of general internal medicine*, 16(2):131–133, 2001.

[30] S. Emaminejad, M. Javanmard, R. W. Dutton, and R. W. Davis. Microfluidic diagnostic tool for the developing world: Contactless impedance flow cytometry. *Lab on a Chip*, 12(21):4499–4507, 2012.

[31] N. Engel and N. Pant Pai. Qualitative research on point-of-care testing strategies and programs for hiv. *Expert review of molecular diagnostics*, (0):1–5, 2015.

[32] Equipment. Portable medical devices market; available at https://www.marketsandmarkets.com/Market-Reports/semiconductor-opportunities-mobile-healthcare-market-1204.html, 2013.

[33] D. Erickson, D. O'Dell, L. Jiang, V. Oncescu, A. Gumus, S. Lee, M. Mancuso, and S. Mehta. Smartphone technology can be transformative to the deployment of lab-on-chip diagnostics. *Lab on a Chip*, 14(17):3159–3164, 2014.

[34] M. Fleischmann, P. J. Hendra, and A. J. McQuillan. Raman spectra of pyridine adsorbed at a silver electrode. *Chemical Physics Letters*, 26(2):163–166, 1974.

[35] D. Florencio and C. Herley. A large-scale study of web password habits. In *Proceedings of the 16th international conference on World Wide Web*, pages 657–666. ACM, 2007.

[36] I. for Health Freedom. Public attitudes toward medical privacy. report submitted by the gallup organization; available at http://www.forhealthfreedom.org/Gallupsurvey/, 2001.

[37] J. Foust. Spacex unveils its 21st century spaceship. *NewSpace Journal*, 2014. URL http://www.newspacejournal.com/2014/05/30/spacex-unveils-its-21st-century-spaceship/.

[38] J. F. Fries, C. E. Koop, C. E. Beadle, P. P. Cooper, M. J. England, R. F. Greaves, J. J. Sokolov, and D. Wright. Reducing health care costs by reducing the need and demand for medical services. *New England Journal of Medicine*, 329(5):321–325, 1993.

[39] S.-Y. Fu, X.-Q. Feng, B. Lauke, and Y.-W. Mai. Effects of particle size, particle/matrix interface adhesion and particle loading on mechanical properties of particulate–polymer composites. *Composites Part B: Engineering*, 39(6):933–961, 2008.

[40] M. Gabal, N. Medrano, B. Calvo, P. Martínez, S. Celma, and M. Valero. A complete low voltage analog lock-in amplifier to recover sensor signals buried in noise for embedded applications. *Procedia Engineering*, 5:74–77, 2010.

[41] L. Garcia, F. Brasser, M. H. Cintuglu, A.-R. Sadeghi, O. Mohammed, and S. A. Zonouz. Hey, my malware knows physics! attacking plcs with physical model aware rootkit. In *24th Annual Network & Distributed System Security Symposium (NDSS)*, Feb. 2017.

[42] C. Gentry et al. Fully homomorphic encryption using ideal lattices. In *STOC*, volume 9, pages 169–178, 2009.

[43] G. Georgeson. A century of boeing innovation in nondestructive evaluation (nde). *Boeing Technical Journal*, 2016.

[44] A. Gernow, I. M. Lisse, B. Böttiger, L. Christensen, and K. Brattegaard. Determination of cd4+ and cd8+ lymphocytes with the cytosphere assay: a comparative study with flow cytometry and the immunoalkaline phosphatase method. *Clinical immunology and immunopathology*, 76(2):135–141, 1995.

[45] A. Gnudi, L. Colalongo, and G. Baccarani. Integrated lock-in amplifier for sensor applications. In *Proceedings of the 25th European Solid-State Circuits Conference*, pages 58–61. IEEE, 1999.

[46] F. T. Grampp and R. H. Morris. The unix system: Unix operating system security. *AT&T Bell Laboratories Technical Journal*, 63(8):1649–1672, 1984.

[47] J. A. Grande. Ultrasonic imaging finds voids, cracks and bonding defects. *PTOnline, February*, 1, 2007.

[48] B. Greve, R. Kelsch, K. Spaniol, H. T. Eich, and M. Götte. Flow cytometry in cancer stem cell analysis and separation. *Cytometry Part A*, 81(4):284–293, 2012.

[49] V. Gubala, L. F. Harris, A. J. Ricco, M. X. Tan, and D. E. Williams. Point of care diagnostics: status and future. *Analytical chemistry*, 84(2):487–515, 2011.

[50] M. Guri, Y. Solewicz, A. Daidakulov, and Y. Elovici. Fansmitter: Acoustic data exfiltration from (speakerless) air-gapped computers. URL `http://arxiv.org/abs/1606.05915`.

[51] J. Hainfeld, D. Slatkin, T. Focella, and H. Smilowitz. Gold nanoparticles: a new x-ray contrast agent. *The British journal of radiology*, 2014.

[52] N. Headquarters. Navair marks first flight with 3-d printed, safety-critical parts. *NAVAIR News*, 2016. URL `http://www.navair.navy.mil/index.cfm?fuseaction=home.NAVAIRNewsStory&id=6323`.

[53] J. Hicks. FDA approved 3d printed drug available in the US. URL `http://www.forbes.com/sites/jenniferhicks/2016/03/22/fda-approved-3d-printed-drug-available-in-the-us/`.

[54] A. Hojjati, A. Adhikari, K. Struckmann, E. Chou, T. N. Tho Nguyen, K. Madan, M. S. Winslett, C. A. Gunter, and W. P. King. Leave your phone at the door: Side channels that reveal factory floor secrets. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, pages 883–894. ACM. ISBN 978-1-4503-4139-4. doi: 10.1145/2976749.2978323. URL `http://doi.acm.org/10.1145/2976749.2978323`.

[55] X. Huang, I. H. El-Sayed, W. Qian, and M. A. El-Sayed. Cancer cells assemble and align gold nanorods conjugated to antibodies to produce highly enhanced, sharp, and polarized surface raman spectra: a potential cancer diagnostic marker. *Nano letters*, 7(6):1591–1597, 2007.

[56] T. Jackson. Navy partnership goes to new depths with first 3d-printed submersible. *Office of Energy Efficiency & Renewable Energy*, 2017. URL `https://energy.gov/eere/articles/navy-partnership-goes-new-depths-first-3d-printed-submersible`.

[57] A. Jain, L. Hong, and S. Pankanti. Biometric identification. *Communications of the ACM*, 43(2):90–98, 2000.

[58] G. D. Janaki Ram, Y. Yang, and B. E. Stucker. Effect of process parameters on bond formation during ultrasonic consolidation of aluminum alloy 3003. 25(3):221–238. ISSN 0278-6125. doi: 10.1016/S0278-6125(07)80011-2. URL `http://www.sciencedirect.com/science/article/pii/S0278612507800112`.

[59] A. Jayakumar. Cyberattacks are on the rise, and healthcare data is the biggest target; available at `http://www.washingtonpost.com/`, 2014.

[60] F. Jeff. SpaceX unveils its "21st century spaceship". URL `http://www.newspacejournal.com/2014/05/30/spacex-unveils-its-21st-century-spaceship/`.

[61] B. E. Jones, S. M. Young, D. Antoniskis, P. T. Davidson, F. Kramer, and P. F. Barnes. Relationship of the manifestations of tuberculosis to cd4 cell counts in patients with human immunodeficiency virus infection. *American Journal of Respiratory and Critical Care Medicine*, 148(5):1292–1297, 1993.

[62] B. E. Jones, M. M. Oo, E. K. Taikwel, D. Qian, A. Kumar, E. R. Maslow, and P. F. Barnes. Cd4 cell counts in human immunodeficiency virus—negative patients with tuberculosis. *Clinical Infectious Diseases*, 24(5):988–991, 1997.

[63] W. Jung, J. Han, J.-W. Choi, and C. H. Ahn. Point-of-care testing (poct) diagnostic systems using microfluidic lab-on-a-chip technologies. *Microelectronic Engineering*, 132:46–57, 2015.

[64] A. C. Kak and M. Slaney. *Principles of computerized tomographic imaging*. SIAM, 2001.

[65] D. Kilgus, J. Moreland, G. Finerman, T. Funahashi, and J. Tipton. Catastrophic wear of tibial polyethylene inserts. (273):223–231. ISSN 0009-921X.

[66] K. Kneipp, Y. Wang, H. Kneipp, L. T. Perelman, I. Itzkan, R. R. Dasari, and M. S. Feld. Single molecule detection using surface-enhanced raman scattering (sers). *Physical review letters*, 78(9):1667, 1997.

[67] S. M. Lai and Y. C. Lan. Shape memory properties of melt-blended polylactic acid (pla)/thermoplastic polyurethane (tpu) bio-based blends. *Journal of Polymer Research*, 20(5):140, 2013. ISSN 1572-8935. doi: 10.1007/s10965-013-0140-6. URL https://doi.org/10.1007/s10965-013-0140-6.

[68] O. Lazcka, F. Campo, and F. X. Munoz. Pathogen detection: A perspective of traditional methods and biosensors. *Biosensors and Bioelectronics*, 22(7):1205–1217, 2007.

[69] T. Le, G. Salles-Loustau, L. Najafizadeh, M. Javanmard, and S. Zonouz. Secure point-of-care medical diagnostics via trusted sensing and cyto-coded passwords. In *Dependable Systems and Networks (DSN), 2016 46th Annual IEEE/IFIP International Conference on*, pages 583–594. IEEE, 2016.

[70] E. C. Le Ru, M. Meyer, and P. G. Etchegoin. Proof of single-molecule sensitivity in surface enhanced raman scattering (sers) by means of a two-analyte technique. *The journal of physical chemistry B*, 110(4):1944–1948, 2006.

[71] A. Y. Lee, J. An, and C. K. Chua. Two-way 4d printing: A review on the reversibility of 3d-printed shape memory materials. *Engineering*, 3(5): 663 – 674, 2017. ISSN 2095-8099. doi: https://doi.org/10.1016/J.ENG.2017.05.014. URL http://www.sciencedirect.com/science/article/pii/S209580991730718X.

[72] S. Lee, V. Oncescu, M. Mancuso, S. Mehta, and D. Erickson. A smartphone platform for the quantification of vitamin d levels. *Lab on a Chip*, 14(8):1437–1442, 2014.

[73] R. L. Lemaster, L. Lu, and S. Jackson. The use of process monitoring techniques on a CNC wood router. part 2. use of a vibration accelerometer to monitor tool wear and workpiece quality. 50(9):59–64. ISSN 00157473. URL http://search.proquest.com/docview/214622388/abstract/AF151E1F83B2490BPQ/1.

[74] A. Lendlein and S. Kelch. Shape-memory polymers. *Angewandte Chemie International Edition*, 41(12):2034–2057, 2002.

[75] C. LeRouge, V. Mantzana, and E. V. Wilson. Healthcare information systems research, revelations and visions. *European Journal of Information Systems*, 16 (6):669–671, 2007.

[76] J. Lichtenberg, N. F. de Rooij, and E. Verpoorte. A microchip electrophoresis system with integrated in-plane electrodes for contactless conductivity detection. *Electrophoresis*, 23(21):3769–3780, 2002.

[77] D. Lin-Vien, N. B. Colthup, W. G. Fateley, and J. G. Grasselli. *The handbook of infrared and Raman characteristic frequencies of organic molecules*. Elsevier, 1991.

[78] H. Liu and T. J. Webster. Mechanical properties of dispersed ceramic nanoparticles in polymer composites for orthopedic applications. *Int J Nanomedicine*, 5: 299–313, 2010.

[79] X. Liu, T.-Y. Lin, and P. B. Lillehoj. Smartphones for cell and biomolecular detection. *Annals of biomedical engineering*, 42(11):2205–2217, 2014.

[80] C. Logan, M. Givens, J. T. Ives, M. Delaney, M. J. Lochhead, R. T. Schooley, and C. A. Benson. Performance evaluation of the mbio diagnostics point-of-care cd4 counter. *Journal of immunological methods*, 387(1):107–113, 2013.

[81] M. Mancuso, E. Cesarman, and D. Erickson. Detection of kaposi's sarcoma associated herpesvirus nucleic acids using a smartphone accessory. *Lab on a Chip*, 14 (19):3809–3816, 2014.

[82] D. Martin, J. Sim, G. Sole, L. Rymer, S. Shalekoff, A. Van Niekerk, P. Becker, C. Weilbach, J. Iwanik, K. Keddy, G. Miller, B. Ozbay, A. Ryan, T. Viscovic, and M. Woolf. Cd4+ lymphocyte count in african patients co-infected with hiv and tuberculosis. *JAIDS Journal of Acquired Immune Deficiency Syndromes*, 8 (4):386–391, 1995.

[83] F. E. McKenzie, W. A. Prudhomme, A. J. Magill, J. R. Forney, B. Permpanich, C. Lucas, R. A. Gasser, and C. Wongsrichanalai. White blood cell counts and malaria. *Journal of Infectious Diseases*, 192(2):323–330, 2005.

[84] J. W. Mellors, A. Munoz, J. V. Giorgi, J. B. Margolick, C. J. Tassoni, P. Gupta, L. A. Kingsley, J. A. Todd, A. J. Saah, R. Detels, et al. Plasma viral load and cd4+ lymphocytes as prognostic markers of hiv-1 infection. *Annals of internal medicine*, 126(12):946–954, 1997.

[85] A. M. Michaels, M. Nirmal, and L. Brus. Surface enhanced raman spectroscopy of individual rhodamine 6g molecules on large ag nanocrystals. *Journal of the American Chemical Society*, 121(43):9932–9939, 1999.

[86] F. Momeni, X. Liu, J. Ni, et al. A review of 4d printing. *Materials & Design*, 122:42–79, 2017.

[87] R. Morris and K. Thompson. Password security: A case history. *Communications of the ACM*, 22(11):594–597, 1979.

[88] A. Muller and S. Karevska. How will 3d printing make your company the strongest link in the value chain. *EY's Global 3D Printing Report*, 2016.

[89] S. V. Murphy and A. Atala. 3d bioprinting of tissues and organs. *Nature biotechnology*, 32(8):773, 2014.

[90] S. Nie and S. R. Emory. Probing single molecules and single nanoparticles by surface-enhanced raman scattering. *science*, 275(5303):1102–1106, 1997.

[91] B. Nikoobakht and M. A. El-Sayed. Surface-enhanced raman scattering studies on aggregated gold nanorods. *The Journal of Physical Chemistry A*, 107(18): 3372–3378, 2003.

[92] W. A. O'Brien, P. M. Hartigan, D. Martin, J. Esinhart, A. Hill, S. Benoit, M. Rubin, M. S. Simberkoff, and J. D. Hamilton. Changes in plasma hiv-1 rna and cd4+ lymphocyte counts and the risk of progression to aids. *New England Journal of Medicine*, 334(7):426–431, 1996.

[93] W. A. O'Brien, P. M. Hartigan, E. S. Daar, M. S. Simberkoff, and J. D. Hamilton. Changes in plasma hiv rna levels and cd4+ lymphocyte counts predict both response to antiretroviral therapy and therapeutic failure. *Annals of Internal Medicine*, 126(12):939–945, 1997.

[94] U. D. of Health and H. S. O. for Civil Rights. Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information. `https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf`, 2015. [Online; accessed 20-Mai-2016].

[95] C. J. Orendorff, L. Gearheart, N. R. Jana, and C. J. Murphy. Aspect ratio dependence on surface enhanced raman scattering using silver and gold nanorod substrates. *Physical Chemistry Chemical Physics*, 8(1):165–170, 2006.

[96] J. Parker Jr, D. Feldman, and M. Ashkin. Raman scattering by silicon and germanium. *Physical Review*, 155(3):712, 1967.

[97] D. Qi and A. J. Berger. Quantitative concentration measurements of creatinine dissolved in water and urine using raman spectroscopy and a liquid core optical fiber. *Journal of biomedical optics*, 10(3):031115–0311159, 2005.

[98] X. Qian, X.-H. Peng, D. O. Ansari, Q. Yin-Goen, G. Z. Chen, D. M. Shin, L. Yang, A. N. Young, M. D. Wang, and S. Nie. In vivo tumor targeting and spectroscopic detection with surface-enhanced raman nanoparticle tags. *Nature biotechnology*, 26(1):83–90, 2008.

[99] H. Richter, Z. Wang, and L. Ley. The one phonon raman spectrum in microcrystalline silicon. *Solid State Communications*, 39(5):625–629, 1981.

[100] Rick Smith. 8 Hot 3D Printing Trends To Watch In 2016. `http://www.forbes.com/sites/ricksmith/2016/01/12/8-hot-3d-printing-trends-to-watch-in-2016/`, 2016.

[101] R. A. Rueppel. Stream ciphers. In *Analysis and Design of Stream Ciphers*, pages 5–16. Springer, 1986.

[102] C. Schmidler. Knee joint anatomy, function and problems. *http://www.healthpages.org/anatomy-function/knee-joint-structure-function-problems/*, Dec 2016.

[103] P. Shekelle, S. C. Morton, and E. B. Keeler. Costs and benefits of health information technology. 2006.

[104] J. Soete, B. Badoux, Y. Swolfs, L. Gorbatikh, et al. Defect detection in 3d printed carbon fibre composites using x-ray computed tomography. *https://www. ndt. net/article/ctc2019/papers/iCT2019_Full_paper_62. pdf*, pages 1–8, 2019.

[105] C. Song, F. Lin, Z. Ba, K. Ren, C. Zhou, and W. Xu. My smartphone knows what you print: Exploring smartphone-based side-channel attacks against 3d printers. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, pages 895–907. ACM. ISBN 978-1-4503-4139-4. doi: 10.1145/2976749.2978300. URL `http://doi.acm.org/10.1145/2976749.2978300`.

[106] Sophos. The State of Encryption Today. Report by Sophos; available at `https://secure2.sophos.com/en-us/medialibrary/Gated%20Assets/white%20papers/the-state-of-encryption-today-wpna.pdf`, 2015.

[107] O. Stava, J. Vanek, B. Benes, N. Carr, and R. Měch. Stress relief: improving structural strength of 3d printable objects. *ACM Transactions on Graphics (TOG)*, 31(4):48, 2012.

[108] A. Sternstein. The fbi is getting its own, personal 3d printer for studying bombs. *Nextgov, June*, 13, 2014.

[109] A. Sternstein. Things can go kaboom when a defense contractor's 3-d printer gets hacked. *Nextgov, September*, 11, 2014.

[110] P. L. Stiles, J. A. Dieringer, N. C. Shah, and R. P. Van Duyne. Surface-enhanced raman spectroscopy. *Annu. Rev. Anal. Chem.*, 1:601–626, 2008.

[111] C. J. Strachan, T. Rades, K. C. Gordon, and J. Rantanen. Raman spectroscopy for quantitative analysis of pharmaceutical solids. *Journal of pharmacy and pharmacology*, 59(2):179–192, 2007.

[112] L. Sturm, C. Williams, J. Camelio, J. White, and R. Parker. Cyber-physical vunerabilities in additive manufacturing systems. *Context*, 7(2014):8, 2014.

[113] N. Talukder, A. Furniturewalla, T. Le, M. Chan, S. Hirday, X. Cao, P. Xie, Z. Lin, A. Gholizadeh, S. Orbine, et al. A portable battery powered microfluidic impedance cytometer with smartphone readout: Towards personal health monitoring. *Biomedical microdevices*, 19(2):36, 2017.

[114] W. Tang, D. Tang, Z. Ni, N. Xiang, and H. Yi. Microfluidic impedance cytometer with inertial focusing and liquid electrodes for high-throughput cell counting and discrimination. *Analytical chemistry*, 89(5):3154–3161, 2017.

[115] P. A. Temple and C. Hathaway. Multiphonon raman spectrum of silicon. *Physical Review B*, 7(8):3685, 1973.

[116] S. Tibbits. 4d printing: multi-material shape change. *Architectural Design*, 84 (1):116–121, 2014.

[117] E. van der Ryst, M. Kotze, G. Joubert, M. Steyn, H. Pieters, M. van der Westhuizen, M. van Staden, and C. Venter. Correlation among total lymphocyte count, absolute cd4+ count, and cd4+ percentage in a group of hiv-1-infected south african patients. *JAIDS Journal of Acquired Immune Deficiency Syndromes*, 19 (3):238–244, 1998.

[118] P.-J. T. K. Vandekerckhove, M. G. Teeter, D. D. R. Naudie, J. L. Howard, S. J. MacDonald, and B. A. Lanting. “the impact of coronal plane alignment on polyethylene wear and damage in total knee replacement: a retrieval study”. ISSN 0883-5403. doi: 10.1016/j.arth.2016.12.048. URL `http://www.sciencedirect.com/science/article/pii/S0883540316309342`.

[119] V. Velusamy, K. Arshak, O. Korostynska, K. Oliwa, and C. Adley. An overview of foodborne pathogen detection: in the perspective of biosensors. *Biotechnology advances*, 28(2):232–254, 2010.

[120] G. Veneziani, E. Corrêa, M. Potiens, and L. Campos. Attenuation coefficient determination of printed abs and pla samples in diagnostic radiology standard beams. In *Journal of Physics: Conference Series*, volume 733, page 012088. IOP Publishing, 2016.

[121] C. L. Ventola. Medical applications for 3d printing: current and projected uses. *Pharmacy and Therapeutics*, 39(10):704, 2014.

[122] R. S. Wallis, M. Pai, D. Menzies, T. M. Doherty, G. Walzl, M. D. Perkins, and A. Zumla. Biomarkers and diagnostics for tuberculosis: progress, needs, and translation into practice. *The Lancet*, 375(9729):1920–1937, 2010.

[123] D. Will. Dejavu; available at `https://github.com/worldveil/dejavu`, 2017.

[124] T. Wohlers. *Wohlers Report 2015: 3D printing and additive manufacturing state of the industry; annual worldwide progress report*. Wohlers Associates, 2015.

[125] D. Wolday, B. Hailu, M. Girma, E. Hailu, E. Sanders, and A. Fontanet. Low cd4+ t-cell count and high hiv viral load precede the development of tuberculosis disease in a cohort of hiv-positive ethiopians. *The International Journal of Tuberculosis and Lung Disease*, 7(2):110–116, 2003.

[126] C. L. Wu, M. Q. Zhang, M. Z. Rong, and K. Friedrich. Tensile performance improvement of low nanoparticles filled-polypropylene composites. *Composites Science and Technology*, 62(10):1327–1340, 2002.

[127] Y. Xia and G. M. Whitesides. Soft lithography. *Annual review of materials science*, 28(1):153–184, 1998.

[128] J. Xin, M. Hao-Yang, P. Xiang-Fang, and T. Lih-Sheng. The morphology, properties, and shape memory behavior of polylactic acid/thermoplastic polyurethane blends. *Polymer Engineering and Science*, 55(1):70–80, 2015. doi: doi:10.1002/pen.23873. URL `https://onlinelibrary.wiley.com/doi/abs/10.1002/pen.23873`.

[129] M. Yampolskiy, A. Skjellum, M. Kretzschmar, R. A. Overfelt, K. R. Sloan, and A. Yasinsac. Using 3d printers as weapons. 14:58–71. ISSN 1874-5482. doi: 10.1016/j.ijcip.2015.12.004. URL `http://www.sciencedirect.com/science/article/pii/S1874548215300330`.

[130] M. Yampolskiy, L. Schutzle, U. Vaidya, and A. Yasinsac. Security challenges of additive manufacturing with metals and alloys. In *International Conference on Critical Infrastructure Protection*, pages 169–183. Springer, 2015.

[131] M. Yampolskiy, W. E. King, J. Gatlin, S. Belikovetsky, A. Brown, A. Skjellum, and Y. Elovici. Security of additive manufacturing: Attack taxonomy and survey. *Additive Manufacturing*, 21:431–457, 2018.

[132] W. Zeng and S. Lei. Efficient frequency domain selective scrambling of digital video. *Multimedia, IEEE Transactions on*, 5(1):118–129, 2003.

[133] Q. Zhu, R. G. Quivey, and A. J. Berger. Raman spectroscopic measurement of relative concentrations in mixtures of oral bacteria. *Applied spectroscopy*, 61(11): 1233–1237, 2007.