WIRELESS META-SENSING FOR THE INTERNET OF THINGS SECURITY AND BEYOND

by

Zhengxiong Li

May 4th, 2021

A dissertation submitted to the
Faculty of the Graduate School of
the University at Buffalo, The State University of New York
in partial fulfilment of the requirements for the
degree of

Doctor of Philosophy

Department of Computer Science and Engineering

The thesis of Zhengxiong Li was reviewed by the following:

Dr. Wenyao Xu
Associate Professor of Computer Science and Engineering
Thesis Advisor, Chair of Committee

Dr. Lu Su
Associate Professor of Computer Science and Engineering
Committee Member

Dr. Karthik Dantu
Associate Professor of Computer Science and Engineering
Committee Member

Dedication

To my parents and friends, who have been always supporting me to move forward.

Acknowledgments

I would like to express my deepest gratitude to Dr. Wenyao Xu, my advisor, for his guidance, support, and patience throughout my Ph.D. study at the University at Buffalo, SUNY. Dr. Wenyao Xu brings me into the groundbreaking research world, and his insightful feedback pushed me to sharpen my thinking and brought my work to a higher level. I surely believe I cannot finish the Ph.D. study successfully without his supervision.

I also wish to thank Dr. Lu Su and Dr. Karthik Dantu as my dissertation committee member. They help me to extend my research scope and bring me the novel ideas to further enrich my research. Their valuable suggestions and supports are significant for my Ph.D. study.

Next, I will not forget the help and suggestions from Dr. Jeanne Langan, Dr. Changzhi Li, Dr. Jun Xia, Dr. Chi Zhou, Dr. Kun Wang, Dr. Lora Cavuoto, Dr. Jilong Kuang, and Dr. Li Zhu. I would also like to thank them for their valuable guidance throughout my studies. They provided me with the tools and resource that I needed to choose the right direction and successfully complete my dissertation.

Besides, I want to thank all my former and present labmates in Embedded Sensing and Computing group, Baicheng Chen, Aoseng Wang, Fen Lin, Chen Song, Jerry Ajay, Aditya Singh Rathore, Hanbin Zhang, Chenhan Xu, Huining Li, Xingyu Chen, Zhuolin Yang, and Wei Bo. I really enjoy the time we are working together and the wonderful team building activities in spare time. This memory will stay in my brain all the time. My thanks also extend to Kun Woo Cho, Matthew Stafford, Tri Vu, Mitchell Chudzik, Michael Brown, and Jasleen Alexis.

Further, I would like to express my great appreciation to all my colleagues and friends who supported me during Ph.D. study during these years. I have enjoyed the time we spent together, and they make my Ph.D. journey a pleasant and exciting one. In particular, I would like to thank Chris Xiaoxuan Lu, Chenglin Miao, Fenglong Ma, Yaqing Wang, Zheshuo Li, Wenjun Jiang, Hongfei Xue, Qiuling Suo, Di Wang, Zhengyu Peng, Ye Zhan, Yuehang Wang and those I have not included their names here, for the collaborations and helpful advice.

Last but not least, I would like to thank my parents for their endless love, support and understanding. During past years, they are with me all the time, sharing my pains and happiness. My degree is at the expense of their sacrifices.

Table of Contents

List of Tables

List of Figures

Abstract

The Internet of Things (IoT) is rapidly growing and has been widely recognized as the next revolution and promises to transform various realms of our daily lives. While the security and privacy threats (e.g., the IoT devices abuse, information theft, and sensor vulnerability) towards IoT devices are also increasing. These problems could lead to a series of catastrophic results, mainly severely increasing the risk of huge financial and health loss for both enterprises and individuals. However, due to the complexity of the surrounding occlusion, unavoidable variance in signal scaling, and privacy-preserving requirements, existing solutions yield unsatisfactory performance. First, most of the current wireless sensing approaches are based on the Huygens-Fresnel principle, which primarily focuses on the target exterior shape or object motion (e.g., appearance reflection information) and has limitations to assistant us to see-through the obstacles and explore the intrinsic secrets of the devices based on weak useful signal (e.g., structural components investigation and material characterization). Besides, the sensing data in the present methods (e.g., computer vision and voice recognition) inevitably contain sensitive information, which has a high risk of information leakage.

In this dissertation, we propose a novel wireless meta-sensing technology to secure and identify the vulnerabilities of IoT devices and further empower a new paradigm of IoT with wireless inkables. This dissertation is the first to explore the interconnection between wireless sensing, material and component, and security and privacy analysis for IoT. To begin with, we notice that hidden electronic devices (e.g., spy camera, bomb package, and bug) can cause life-threatening hazards, eavesdropping, and cheating or intrusion in private zones. Thus, we exploit the feasibility of hidden electronic device recognition under mmWave and investigate the unique properties in the nonlinear responses of electronic devices. The proposed approach offers a cost-efficient, portable and non-invasive manner to aid law enforcement in public inspections and ensure security. Further, we revisit a classic topic in the computer security community that how to mitigate risks of screen attacks, where many people believe it is ideal secure without device proximity, pre-installed malware, and occlusion to the outside. We reexamine this indispensable device and first identify and validate a new and yet practical side-channel

to remotely infer contents on digital display via the liquid crystal nematic state sensing with a novel end-to-end deep learning-based hierarchal system in isolation scenarios. This discovery suggests that the privacy-sensitive systems should pay considerable attention to this new side-channel and increase screen security. Finally, benefited from the wireless meta-sensing technology, we propose to explore a new paradigm of IoT with wireless inkables. Traditionally, IoT devices or sensors are based on microelectronic and semiconductor components, which are not cost-effective (e.g., a few dollars) and, more importantly, generate electronic wastes. Therefore, we explore and unveil a novel material mediated wireless meta-sensing technology via wireless inkables for the new tagging infrastructure and wireless temperature monitoring, which are extremely low-cost (e.g., under 1 cent per sensor), flexible (e.g., soft sensor material), remotely (e.g., distance up to several meters away) and ecological (e.g., environmentally friendly materials).

Chapter 1

Introduction

1.1 Overview

The Internet of Things (IoT) is rapidly growing and has been widely recognized as the next revolution and promises to transform various realms of our daily lives. The global market for Internet of things (IoT) end-user solutions is expected to grow to 212 billion U.S. dollars in size by the end of 2019 and is expected to reach 1.6 trillion by 2025 [40]. Besides, the IoT devices, as the fundamental base of IoT, are projected to amount to 21.5 billion units worldwide by 2025 [41].

However, the security and privacy threats towards IoT devices are also increasing. There are three significantly emerging types of threats in daily life. One of the threats is IoT device abuse, such as hidden electronic devices (hereafter, e-devices). E-devices bring both security and privacy threats to our daily life. For instance, explosion tragedies continuously occur due to the ineffective detection of remote-controlled disguised bombs [11, 13, 17, 24], which can be triggered by electronic initiators. Apart from these life-threatening hazards, e-devices (*e.g.*, smartphones and spy camera) can also be used for eavesdropping, cheating in private zones [23] or accessing other ar-

eas that restrict electronics [14, 25, 26]. The fact that these e-devices (hereafter, hidden e-devices) can be sealed in parcels or boxes, hidden insides in clothing, and disguised in appearance increases the risk that they can easily pass undetected through security checkpoints.

Besides, information theft is a substantial concern, such as information theft from the device screen, also known as screen attack. The digital screen is a pivotal output device, which delivers intended information to users in modern devices (e.g., smartphones, laptops, and access control). Due to the development of computer and networking cybersecurity services in core electronic devices, vulnerable computer accessories in physical worlds become a more effective and critical attack surface in practice, where digital screens are the most sought venue that adversaries can favorably leverage to steal information [70, 85, 96, 109]. Screen attacks can directly gain access to their organizational or personal resources and then pilfer the secrets (e.g., SSN, tax return, financial transactions, confidential data, and private communication), money (e.g., depository safe), and intellectual property (e.g., scientific research reports and blueprint). These leakages could lead to a series of catastrophic results, mainly severely increasing the risk of substantial financial and reputation loss for both enterprises and individuals [33, 34].

Last but not least, the device or sensor vulnerability also receives a lot of attention. Traditional IoT devices or sensors are made of microelectronic and semiconductor components with electrochemistry material. This kind of solution is highly dependent on the power grid and the chip supply chain. Additionally, due to the electricity working mechanism and imperfect manufacture, these IoT devices or sensors are inevitably suffered during analog-to-digital conversion [254], physical unclonable function (PUF) [140], or electromagnetic side-channel [109]. The attackers can confuse the perception ability of IoT sensors to mislead the IoT actuator (e.g., accelerate the autonomous vehicles before the obstacle), unveil the privacy of IoT users (e.g., monitoring the users' daily living trajectory), and steal sensitive information of IoT users. Moreover, these IoT devices are

usually not cost-effective (e.g., a few dollars) and, more importantly, generate electronic wastes.

These security and privacy problems could lead to a series of catastrophic results, mainly severely increasing the risk of enormous financial and intellectual loss for both enterprises and individuals. However, due to the complexity of the surrounding occlusion, unavoidable variance in signal scaling, and privacy-preserving requirements, existing solutions yield unsatisfactory performance. First, most of the current wireless sensing approaches are based on the Huygens-Fresnel principle [43], which primarily focuses on the target exterior shape or object motion (e.g., appearance reflection information) and has limitations to assistant us to see-through the common obstacles and explore the intrinsic secrets of the devices based on weak useful signal (e.g., structural components investigation and material characterization). Besides, the sensing data in the present methods (e.g., computer vision and voice recognition) inevitably contain sensitive information, which has a high risk of information leakage.

In this dissertation, to tackle these challenges in IoT devices, we propose a novel wireless meta-sensing technology, which can see through the obstacles and explore the inner characteristics of the targets in a cost-efficient, portable and privacy-preserving way. The foundation of this technology rests on the passive modulation response effect from the target when probed by the millimeter wave (mmWave). The intrinsic difference in target' hardware characteristics (e.g., a circuits' components and liquid crystal nematic pattern) generates a distinct nonlinear response, which can serve as the identity of a particular target and infer the related but unnoticeable credentials. Moreover, wireless meta-sensing not only can identify the vulnerabilities of IoT devices by analyzing the material or components in the current commercial devices, but also can promote the development of the new paradigm of IoT with new novel wireless-chem material. Here, we provide an overview of each work.

Hidden E-devices Recognition: We notice that hidden electronic devices (e.g., spy camera, bomb package, and bug) can cause life-threatening hazards, eavesdropping,

and cheating or intrusion in private zones. Thus, we exploit the feasibility of hidden electronic device recognition under mmWave and investigate the unique properties in the nonlinear responses of electronic devices [141]. The proposed approach offers a cost-efficient, portable, and non-invasive manner to aid law enforcement in public inspections and ensure security.

Screen Attack via mmWave Sensing: We revisit a classic topic in the computer security community that how to mitigate risks of screen attacks, where many people believe it is ideal secure without device proximity, pre-installed malware, and occlusion to the outside. We reexamine this indispensable device, and first identify and validate a new and yet practical side-channel to remotely infer contents on digital display via the liquid crystal nematic state sensing with a novel end-to-end deep learning-based hierarchal system in isolation scenarios [139]. This discovery suggests that the privacy-sensitive systems should pay considerable attention to this new side-channel and increase screen security.

A Paper-based mmWave-Scannable Tagging Infrastructure: Inventory management (e.g., product counting/identification) is pivotal in IoT, aiming to supervise the non-capitalized products and stock items. Currently, the most adopted inventory technologies are either entangled by an alignment issue (i.e., the laser reader must align with one laser-scannable barcode in line-of-sight), or is economically and environmentally unfriendly (i.e., the high-cost and not naturally disposable RFID). Benefited from the wireless meta-sensing, we propose a new paradigm of the tagging infrastructure [138]. It is a paper-based mmWave-scannable tagging infrastructure for the next-generation inventory management system, featuring ultra-low cost, environment-friendly, battery-free, and in-situ (i.e., multiple tags can be simultaneously processed outside the line-of-sight). It is on the basis of ferrofluidic ink on the paper print and its interference to the incoming mmWave signal, which has the potential to transform the sensing to new physical dimensions and serve as the object identity of the next-generation Internet.

Wireless Temperature Monitoring: Wireless temperature monitoring systems are one of the most widespread technologies in the IoT era and can drive mass applications in the fields of smart home, transportation, and logistics. The wireless temperature sensor is often made into tags with thermal-electric temperature sensors. Unfortunately, such technology associates with high cost, harms the environment, and lacks thermal imaging capability. Driven by the wireless meta-sensing, we propose a new paradigm of wireless temperature monitoring that is low-cost (e.g., under 1 cent per sensor), flexible (e.g., soft sensor material), remotely (e.g., distance up to several meters away), and ecological (e.g., environmentally friendly materials) [67]. It utilizes the thermal scattering effect on cholesteryl materials incited by mmWave signals, supporting both dot-wise temperature recognition and thermal imaging. Also, it complements the current wireless temperature sensing technology for IoT.

1.2 Contribution and Outline of Dissertation

In this dissertation, we propose a novel wireless meta-sensing technology to secure and identify the vulnerabilities of IoT devices, and further empower a new paradigm of IoT with wireless inkables. This dissertation is the first to explore the interconnection between wireless sensing, material and component, and security and privacy analysis for IoT. From the IoT security view, this dissertation uncovers the security and privacy analysis with wireless meta-sensing on the material or components in the current commercial devices. From the IoT paradigm view, this dissertation also facilities a new paradigm shift from passive wireless sensing and analysis on existing material or components to active new wireless-chem material design impelled by the next IoT.

Our contributions can be summarized in the following four chapters:

- In Chapter 3, we propose a novel form of recognizing hidden e-devices by exploring the nonlinear response effect of mmWave of e-devices. We find that the circuit inside the e-device acts as a passive signal modulator that reflects radio

frequency (RF) signals with intrinsic identity information. An end-to-end system, namely E-Eye, is developed to facilitate the low-cost, non-invasive, and robust hidden electronics recognition.

- In Chapter 4, to further explore the vulnerability in IoT devices, we discover a new side-channel to access the screen information from digital screens by exploiting the liquid crystal nematic response effect under the remote mmWave sensing. Then, to remotely monitor screen activities and retrieve screen, we also design and implement an end-to-end hierarchical system, namely WaveSpy, using a mmWave probe and a novel signal processing scheme. WaveSpy can launch a remote screen attack without using traditional emanation, such as EM and light. Finally, we discuss the effectiveness and study a set of passive and active countermeasures to prevent information leakage against this unprecedented information threat.

- In Chapter 5, to build a new paradigm of the tagging infrastructure, we first investigate the Ferrofluidic-RF (FerroRF) effects and discover the magnetic nanoparticles within the ferrofluidic ink modulates probing mmWave with classifiable characteristics. Besides, a new FerroRF infrastructure is modeled and advanced with an innovative nested tag pattern. Finally, we design and implement the FerroTag system with one working prototype machine.

- In Chapter 6, we propose to design a new paradigm of wireless temperature monitoring by investigating the thermal scattering effect that can cause a temperature-related frequency shift modulation in scattered RF signals. Subsequently, we study the mathematical model that captures and characterizes this change with low-cost and ecological cholesteryl materials. Then, we design and implement the Thermowave system, based on cholesteryl material's thermal scattering effect, to achieve dot-wise temperature monitoring and thermal image.

Chapter 2 is an overview of preliminaries. Chapter 3 presents an end-to-end system for hidden electronic devices recognition. Chapter 4 illustrates a new type of side-channel attacks towards the screen and proposes countermeasures to mitigate such attack. Chapter 5 introduces a new paradigm of IoT for the tagging infrastructure, and Chapter 6 shows one for the wireless temperature monitoring. Finally, Chapter 7 concludes this dissertation and discusses the future potential works.

Chapter 2

Preliminaries

2.1 Wireless Meta-sensing for IoT

Wireless sensing is becoming more and more important in the IoT era, however, most of the current wireless sensing approaches are based on the Huygens-Fresnel principle, which primarily focuses on the reflection signal from the target exterior shape or object motion (e.g., appearance reflection information). This type of signal has little information about the inner traits of the target, and limits us from exploring the intrinsic secrets of the hidden/blocked devices based on the weak useful signal. Therefore, to better understand the IoT device and the interaction between the IoT device and the ambient environment, we aim to break this sensing barrier and extend the wireless sensing technology into the intrinsic physical domain to seek IoT security and privacy analysis.

In this dissertation, we introduce a new wireless sensing technology, which especially aims to acquire internal information within the target even behind the occlusions in a non-contact way via a wireless signal. Wireless meta-sensing locates at the interaction of wireless sensing, material and component, and security and privacy analysis for IoT. Besides, the reflection signal, wireless meta-sensing utilizes comprehensive types of signal, especially the passive modulation response. The foundation of this framework rests on the passive modulation response effect from the target when probed by the

millimeter wave (mmWave). The intrinsic difference in target hardware characteristics (e.g., a circuits' components and liquid crystal nematic pattern) generates a distinct non-linear response, which can serve as the identity of a specific target and infer the related but unnoticeable credentials. Overall, wireless meta-sensing can identify the vulnerabilities of IoT devices by analyzing the material or components in the current commercial devices and promoting the development of the new paradigm of IoT with new novel wireless-chem material.

For the classic wireless sensing model, viewing from the fundamental analysis macroscopic Maxwell's equations, the constitutive relations in the frequency domain are [57]:

$$D(\omega) = \varepsilon_0 \varepsilon_\infty E(\omega), \tag{2.1}$$

$$B(\omega) = \mu_0 \mu_\infty H(\omega), \tag{2.2}$$

where ω is the angular frequency variable, E is the macroscopic electric field, and H is the macroscopic magnetic field in space and time with mmWave sources. D is the electric flux density, and B the magnetic flux density. ε_0 and μ_0 are the electrical permittivity and permeability of vacuum, respectively. ε_∞ and μ_∞ are the dimensionless dyadics corresponding to the reflection signal of an object to an input field. However, since most of targets in the IoT domain are made of the anisotropic material, the target exhibits responses to mmWave excitations [73, 228]. The wireless meta-sensing relations are expressed as in Equation 2.3 and 2.4 [107].

$$D(\omega) = \varepsilon_0(\varepsilon_\infty + \underbrace{\int_0^\infty z_{ee}(t) e^{j\omega t} dt}_{Parasitic\ Response}) \cdot E(\omega), \tag{2.3}$$

$$B(\omega) = \mu_0(\mu_\infty + \underbrace{\int_0^\infty z_{mm}(t) e^{j\omega t} dt}_{Parasitic\ Response}) \cdot H(\omega), \tag{2.4}$$

where j is the imaginary unit, z_{ee} and z_{mm} are dimensionless dyadics called susceptibility functions that constitute the convolution kernels specifying the target's response to an input field, which are related to the target's physical properties.

Then, we further explore the mechanism of wireless meta-sensing. When a continuous wave with transmitting frequency f_0 from the sensing probe is projected towards the target, the RF response is modulated with a set of sub-carrier frequencies due to the properties of the target (e.g., liquid crystal pattern, material reflection efficiency). Similarly, given that the target enters the RF beam field, the internal properties within the target are perceived as an array of antennas in the resolution of the mmWave [68, 83]. These antennas act as a passive processor and manipulate the transmit mmWave signals to generate a distortion formulated as:

$$z(t) = \phi(\varphi(t), \omega(t)) \otimes h_f(t), \tag{2.5}$$

where $\varphi(t)$ represents a collection of mmWave subcarriers for the response signals, $\phi(\cdot, \omega(t))$ is the modulation function of the internal properties within the target, $\omega(t)$ is the complex power-series for the internal properties (e.g., the equivalent dielectric constant, and molecular arrangement), $\otimes$ stands for convolution computing, and $h_f(t)$ is the ideal bandpass filter function for the carrier bandwidth. After the modulated signal radiates from the target, it is captured by the probe receive (Rx) antenna. Therefore, the response signal from the target incorporates profound information of the internal properties and can assist us for security and privacy analysis.

Next, to obtain the RF response with exceptional quality and promote the attack performance, it is critical to utilize a proper sensing frequency. Under the most common circumstances, the length of an equivalent half-wave resonant dipoles is l, and the effective dielectric constant of the target is ε. According to [119], the sensing frequency f_0 can be reckoned as:

$$f_0 = \frac{c}{2l\sqrt{\varepsilon}}, \tag{2.6}$$

where c is the propagation speed of a radar wave in air [63]. Therefore, we can select the sensing carrier frequency for the specific application. In this dissertation, we find 24GHz is most suitable to tackle these challenges, which can be approximately recognized as mmWave (the wavelength $\lambda = \frac{C}{f} = \frac{3*10^8}{24*10^9} = 0.0125m = 12mm$), in our study. In addition, we know mmWave can pass through most obstacles or coverings

(e.g., smoke, plastic, timber, and cardboard) in our daily life. Therefore, wireless meta-sensing can see-through the common obstacles and remotely explore the inner characteristics of the targets in an accurate and privacy-preserving way. This technology can enable IoT security and privacy analysis from the device material or components aspect, and furthermore, empower plentiful IoT applications (e.g., tagging infrastructure and wireless temperature monitoring) with a novel paradigm.

2.2 New Paradigm of IoT

Traditional IoT devices or sensors are made of microelectronic and semiconductor components with electrochemistry material, in which the electron is the transducer element [55, 103]. Inkjet-printed technology is a type of computer printing. It can achieve digital design by propelling droplets of ink onto paper substrates. In recent years, novel functional inks (e.g., nanoparticles-based [230]) with consumer inkjet printers enable a more disruptive potential for fabricating low-cost inkable electronics, also known as inkables. And the market for inkable sensors is predicted to reach $4.5 billion by 2030 [44]. In the past decade, the research on inkable sensors and circuits mainly focus on ink material and sensor prototype engineering. Many new kinds of sensory ink have been invented to provide prints with desired electronic properties, such as conductivity, insulation, hydrophobicity, and hydrophilicity [135, 153]. Besides, these inkables can be integrated into diverse sensing applications, such as humid monitoring [229], chemical analysis [46], and health [76]. However, limited to the nature of inkable systems, one of the significant challenges is how to let inkables interact with other electronic systems for functional integration. Currently, one of the widely adopted solutions is optical interfaces, such as cameras and smartphones [199], owing to the most inkables properties of color changing. Yet, this solution only works in the light of sight and is easily affected by the ambient environment.

In this dissertation, we introduce a new paradigm aiming to integrate functional inkable sensors with pervasive wireless signals for IoT. Rather than using direct/indirect electron transduction to transfer the signal, this paradigm will leverage the properties of wireless-chem material to modulate and interact with wireless signals. Compared to the electrochemistry material, the chem-wireless material is a type of material, which uses the changes or status of the material component structure and molecular arrangement to transfer the signal via wireless meta-sensing. This new paradigm of IoT is featured as: (1) Ultra-low cost: the ink and substrate are very accessible. The price for each sensor can be less than one cent, much lower than current chip-based sensors (0.18 - 30 US dollars); (2) Environment-friendly: the sensor doesn't use the conductive ink or the sophisticated toxic specific-designed chemical ink. It is ecological (e.g., organic, disposable, and recyclable material); (3) Battery-free: the tag/sensor is entirely passive, requiring no power supply; (4) In-situ: can work in a non-contact (distance up to hundreds of meter away), easy to be deployed and maintained, multiple tags are accurately read by a scanner outside the line-of-sight; (5) Flexible: This substrate of this sensor can be paper or thin film. And the sensor can be directly printed on the target object surface or manually suppressed to various shapes (e.g., bend, camber, curve, fold, wrap) without permanent deformation, opposite to other sensors on circuit boards have to be set in the rigid containers.

Chapter 3

E-Eye: Hidden Electronics Recognition through mmWave Nonlinear Effects

3.1 Introduction

Entry security check is the current method for defending against malicious, hidden e-devices requiring an X-ray machine [213] at safety-critical sites (*e.g.*, airports and embassy offices). Unfortunately, their expensive cost and poor portability make it an infeasible solution against the proliferation and the deployment of portable e-devices [178]. Moreover, the radiation emitted from X-rays is harmful to workers and persons passing through the checkpoints. Other scanning methods based on metal scanners can only detect the existence of the e-device rather than recognize the specific type directly (see Sec. 9.1). Conventional computer vision methods cannot be applied because the camera can not see through containers or bodies. Thermal imaging also fails because it only can detect the temperature of the hidden e-device [151], which can be easily interfered with by other heat sources. As a result, how to recognize hidden e-devices in a cost-efficient,

user-friendly and non-invasive manner remains an unsolved challenge for public security and privacy.

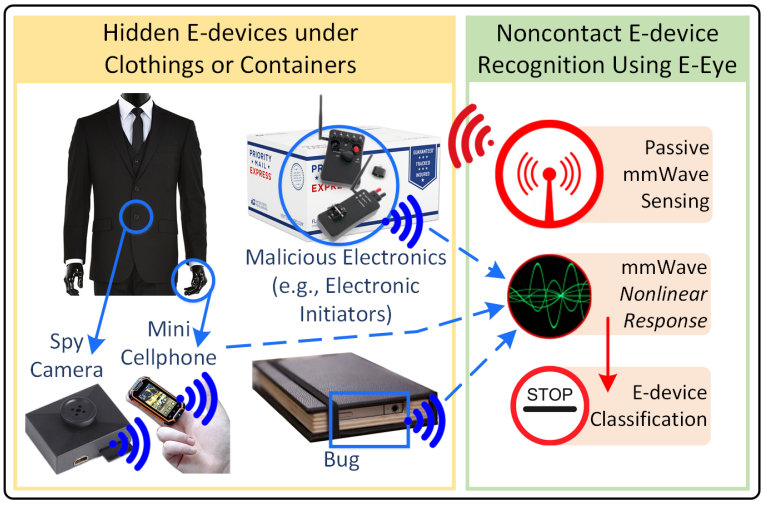


Figure 3.1: Examples of hidden electronics in different malicious applications. The proposed *E-Eye* system can detect and recognize hidden electronic devices under different circumstances in real world.

Recently, there is a rising trend of applying radio-frequency signals, such as millimeter wave (mmWave [20]), in sensing and tracking applications, because mmWave can penetrate obstacles and "image" hidden objects due to its highly-directional beamforming and strong reflection properties on objects [238]. For example, Adib *et al.* studied the possibility of sensing human occurrence and vitals through WiFi signals [47]. Zhu *et al.* developed a 60GHz mmWave imager for object detection and classification [259]. Wei *et al.* designed mTrack, a mmWave instrument for precision object tracking [238]. However, existing works mainly target either human or non-electronic object detection and tracking. The capability of accurately recognizing hidden electronic devices through mmWave sensing is unknown.

In this chapter, we propose our system, *E-Eye*, to facilitate hidden e-device recognition in public security inspections. Its features are (1) **cost-efficient**: the cost of the solution is affordable in daily life for large scale deployment; (2) **portable**: it is easy to use in the inspection of different containers (*e.g.*, delivery boxes, check-in luggages or

even human body) and various environments (*e.g.*, postal offices, airports or factories); (3) **non-invasive**: it can avoid the obtrusive (even illegal) opening of the container in real practice which sacrifices efficiency and may cause privacy issues.

The foundation of *E-Eye* rests on the *nonlinear response* effect from electronic circuits when probed by the mmWave. The intrinsic difference in circuits' hardware characteristics (*e.g.*, a circuits' components and circuit layout) generates a distinct nonlinear response, which can serve as the identity of a certain e-device brand. This way, we enable a novel sensing modality for non-invasive and cost-effective hidden e-devices recognition based on the mmWave field. Specifically, we design and prototype a portable ($11.8cm \times 4.5cm \times 1.8cm$) and light-weight ($45.4g$) 24GHz mmWave probe device which is enabled to probe the mmWave and capture the returned *nonlinear responses*. We address the challenges in noise isolation and coherence to achieve high-quality signal with low complexity and cost (less than US $\$100$). Afterward, the signal is transferred to the smartphone, and we propose the wavelet-based analysis module taking into consideration the unavoidable variance in the signal's scaling and magnitude in practical usage. Eventually, we develop a fine-tuned support vector machine (SVM) classifier for robust recognition under various conditions. In the experiment, we employ 46 e-devices, and the comprehensive results show that *E-Eye* can accurately recognize each e-device brand under different scenarios.

3.2 mmWave Nonlinear Effect: New concept and Preliminaries

3.2.1 Concept: Radio-Frequency Response of E-devices

There are usually two following forms of radio frequency (RF) response when probing a continuous wave (CW) with the transmit frequency f_0 towards a target.

Linear Effects: The main carrier frequency of the received signal is the same as that of the transmitted signal. The phase change in the linearly demodulated signals is related to the geometrical information, such as object distance, shape and size [163]. However, these linear effects do not reflect the material properties and we need to seek other information in the application of e-device detection and recognition.

Nonlinear Effects: Besides the main carrier frequency, the received signal wave is also modulated with a set of the sub-carrier frequencies with more side lobes in the spectrum. These sub-carrier frequencies are generated due to the nonlinear properties of the target (*e.g.*, material reflection efficiency) [187, 188]. In the remaining part of this section, we provide an in-depth analysis of non-linear effects in recognizing electronics.

Nonlinear Effects from E-device: As shown in Figure 3.2, when the e-device enters the RF beam field, chips, connectors and metal traces of printed circuit board (PCB) on an e-device are viewed as an array of antennas in the resolution of mmWave, and these antenna with inductance (L), capacitance (C) and resistance (R) act as a passive processor and manipulates the transmit mmwave signals. More specifically, antennas can conduct and transform the mmWave signal to a high-frequency current along the conductors between the electronic components within the device [38]. The components (*e.g.*, a diode) or parasitic parameters (*e.g.*, a parasitic circuit) on the PCB modulate the response signal and generate the nonlinear distortion [116], formulated as Equation (4.1):

$$r(t) = m(z(t), \hat{a}(t)) \otimes h_f(t), \tag{3.1}$$

where $z(t)$ is the response signal, $m(\cdot, \hat{a}(t))$ is the nonlinear modulation function of the PCB, $\hat{a}(t)$ is the complex power-series for the nonlinear system, $\otimes$ stands for convolution computing and $h_f(t)$ is the ideal bandpass filter function for the carrier bandwidth [95, 97]. After the modulated signal radiate from the e-device, they would be captured by the probe receive (Rx) antenna. Thus, this *nonlinear response* of the e-

device contains rich information of its physical characteristic and holds the potential to serve as the device's identity.

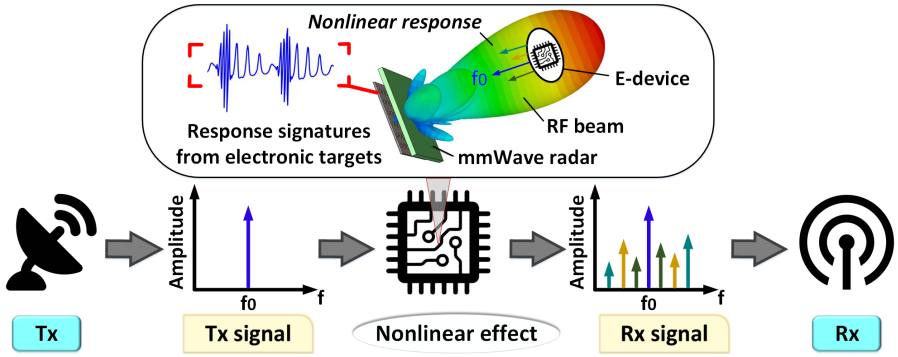


Figure 3.2: The e-device generates a *nonlinear response* signature under the RF beam. The response is determined by its intrinsic physical characteristics.

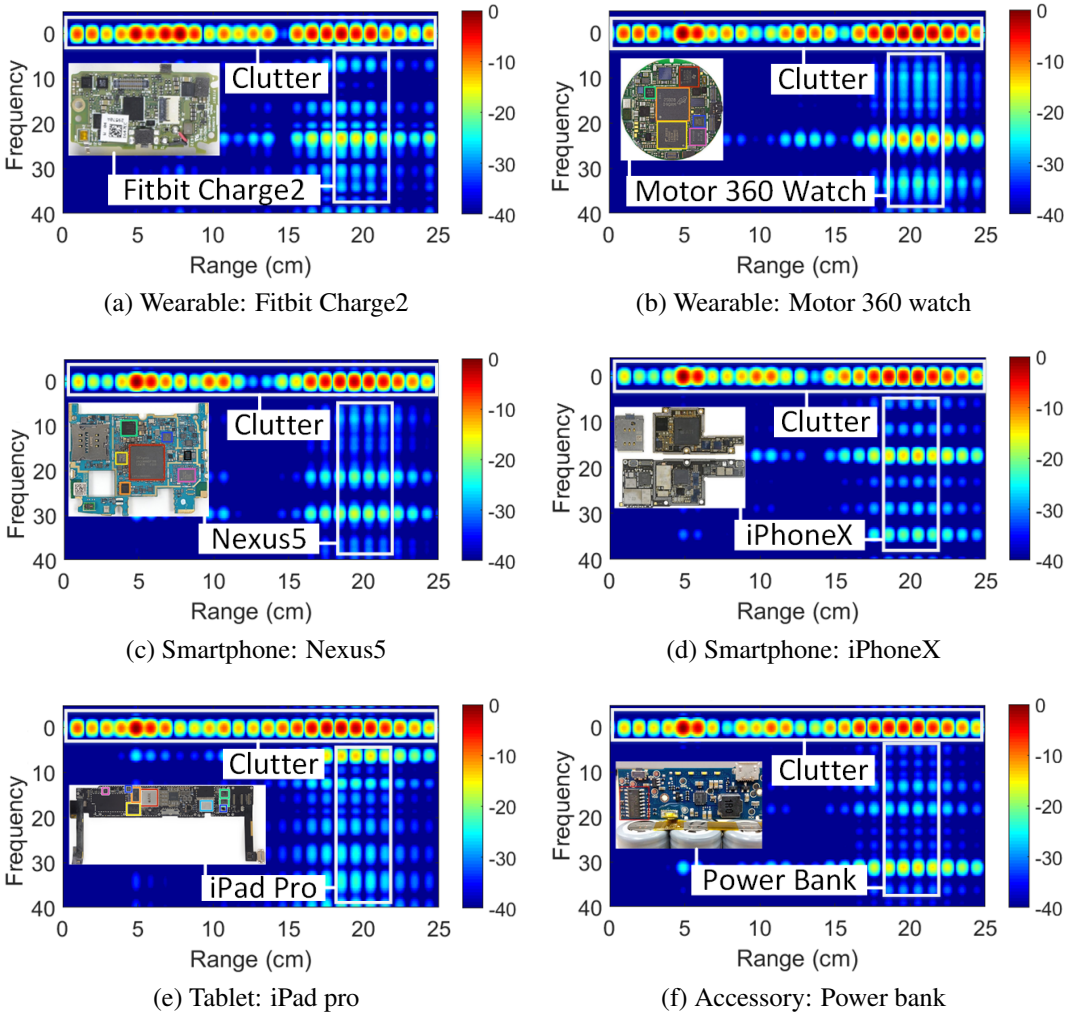
3.2.2 A Preliminary Study: mmWave Nonlinear Effects from Electronic Circuits

Carrier Frequency Selection: Selecting a transmit frequency (and consequently a receive frequency) requires all of the typical trade-offs associated with longer versus shorter wavelengths for radar, which include availability of components (*e.g.*, amplifiers and filters), realization of an acceptable gain for the antennas to achieve a sufficient signal-to-noise ratio (SNR) and exploitation of the radar cross-section (RCS) associated with a particular set of targets [98, 182].

If it is assumed, as a very rough approximation [162], that the length of a typical trace along a PCB is $l = 3mm$ on the High-frequency high-speed circuits (illustrated in Figure 3.3), and the effective dielectric constant of the board is close to $\varepsilon = 4$, the traces along the board become half-wave resonant dipoles ($l = \frac{\lambda}{2}$) at a frequency of $f_0 = \frac{c}{\sqrt{\varepsilon}\lambda} = \frac{3{\cdot}10^8 m/s}{\sqrt{4}{\cdot}2{\cdot}0.003m} \approx$24GHz, where c is the propagation speed of a radar wave in air. Thus, it is reasonable to expect that, for nonlinear effect, the radar will transmit frequencies in or near Super high frequency band, range from 3GHz to 30GHz [18, 197]. Considering the technology for 24GHz radar is significantly mature and 24GHz is unrestricted in

the industrial scientific medical (ISM) band [12], we apply the 24GHz as the transmit frequency, which is loosely known as mmWave.

Owing to different product design goals and the circuit IP protection, the circuits in different e-device brands are different. Thus, the amplitude, frequency and phase of the *nonlinear responses* are different among different e-devices. Therefore, it is possible to design a mmWave probe to force e-devices to radiate the *nonlinear response* signature that reflects their unique properties and can be used for recognition.



(a) Wearable: Fitbit Charge2

(b) Wearable: Motor 360 watch

(c) Smartphone: Nexus5

(d) Smartphone: iPhoneX

(e) Tablet: iPad pro

(f) Accessory: Power bank

Figure 3.3: Six different e-devices present different *nonlinear responses* (the spectrums in the white box are distinct in frequency and amplitude) when forced by the same mmWave probe. The main circuit board of each e-device is displayed on the left.

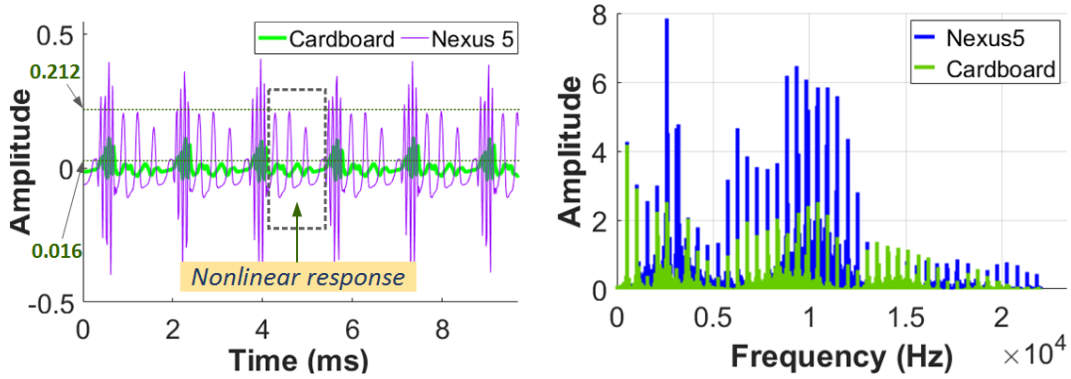
Proof-of-concept: Six different e-device types from four different representative device categories are stimulated with the mmWave probe fixed $20cm$ in distance from the devices. The main circuit board of each e-device is attached on the left. These circuits are different from aspects of the size, the components and layout. As shown in Figure 3.3, the x-axis is the sensing range, the y-axis is the frequency of the received signal and the color bar represents the amplitude of the signal. The varied sub-carrier frequencies can be clearly observed that their *nonlinear responses* are significantly distinct at the frequency, amplitude and phase, which matches Section 3.2.1. Given the huge amount of electric units integrated on the control board, parasitic variations have sufficient space to be served as powerful resources for device recognition.

A Study on Package Effects: In real-world applications, electronics can be placed inside the container or covered by different materials. As a result, we need to investigate whether the hidden materials will generate *nonlinear responses* or have a nonlinear effect [208]. It is proved in Figure 3.4a that within the area of the *nonlinear response*, there is little demodulated signal amplitude for cardboard (less than $0.016V$, ambient noise and thermal noise actually), while for Nexus 5, the demodulated *nonlinear response* signal is quite visible (more than $0.212V$, $13.5\times$ larger than cardboard's) (more detailed analysis about the *nonlinear response* in Section 3.5). In Figure 3.4b, we can observe their signal spectrum are significantly different, which proves the feasibility of unobtrusive hidden e-device recognition.

3.2.3 Practical Challenges

There are two technical challenges in our system design:

Low-cost and portable sensing modality: There are significant challenges in fulfilling such mmWave probe, especially in RF front-end, antenna, signal processing and manufacture craft parts. Moreover, to make the mmWave probe low-cost and compact with the portable size and excellent flexibility is arduous.



(a) The detected *nonlinear response* from the cardboard and Nexus 5.

(b) The significant difference of two responses in spectrum.

Figure 3.4: The cardboard's *nonlinear responses* are negligible when compared to Nexus 5's, indicating the feasibility of hidden e-device recognition.

Effective and robust recognition: Taking into account the ambient noise, unavoidable variance in signal's scaling as well as diverse intervention sources, it is not easy to accurately and efficiently discriminate the *nonlinear responses* from different e-devices in a limited time.

3.3 *E-Eye*: Hidden e-device Recognition System

We propose *E-Eye*, a portable, non-invasive and robust system to facilitate recognition of the hidden e-devices. Typically, we consider the real world practice where the inspector conducts the on-site inspection of the object for forbidden e-devices that may be contained in it. The end-to-end system overview is shown in Figure 3.5.

***E-Eye* Hardware:** A new mmWave probe with the smartphone is designed to remotely and robustly acquire the e-device's *nonlinear response* for recognition. Specifically, the probe transmits the continuous wave and process/demodulate the reflected signal. After that, the kilobyte (KB) size data is sent to smartphone for recognition via the line-in audio card converter [16].

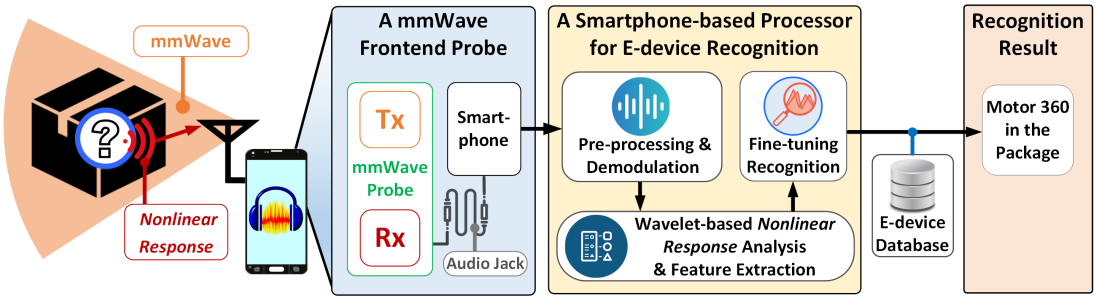


Figure 3.5: The system overview for *E-Eye* to non-invasively recognize the e-device hidden in the container. It comprises of a mmWave sensing module in the front-end and an e-device recognition module in the back-end.

***E-Eye* Software:** Once receiving the data, the e-device recognition module first performs the preprocessing and demodulation to filter the interference and noise. Then, it extracts the effective features from the *nonlinear responses* via wavelet-based analysis. After that, a fine-tuned classification algorithm is developed to recognize the e-device type. The result will eventually be displayed on the smartphone to the inspector.

3.4 A Portable and Cost-Effective mmWave Probe Design

In this section, we introduce the hardware design of *E-Eye*, which is capable of transmitting the 24GHz carrier signal and capturing the returned *nonlinear responses*.

3.4.1 Hardware Architecture

The schematic of the proposed mmWave probe is shown in Figure 3.6. It consists of a radio frequency board and a baseband board. The RF board includes a pair of array antennas (i.e., Tx and Rx), a voltage controlled oscillator (VCO), a pair of low noise amplifiers (LNA) and a six-port structure. The baseband board contains baseband amplifiers (BA) and an on-board sawtooth voltage generator (SVG).

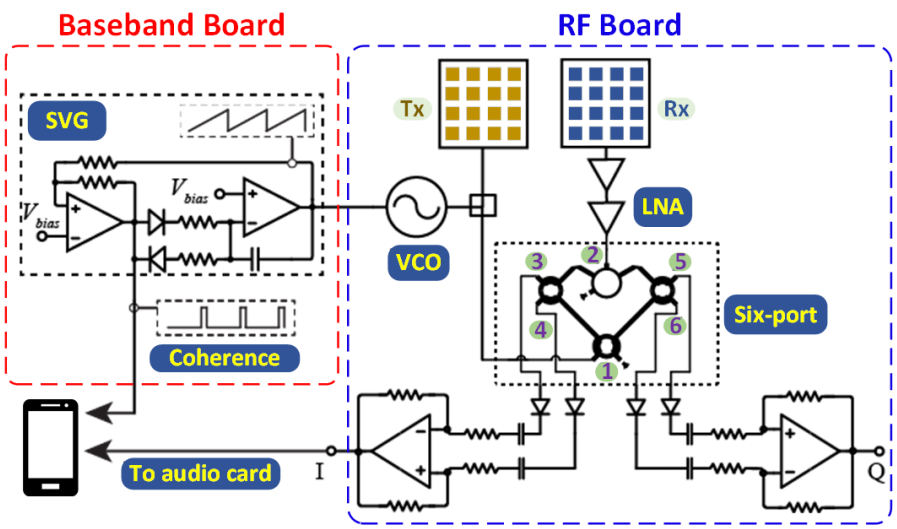


Figure 3.6: The hardware schematic for the cost-effective and portable 24GHz mmWave probe.

3.4.1.1 Six-port Structure

A six-port circuit is a simple structure, as a quadrature mixer, to down-convert RF signal into baseband, avoiding the use of expensive integrated mixer chips [218]. The six-port structure consists of three quadrature couplers and one rat-race coupler. Ports 1 and 2 of the six-port structure are the inputs for the local oscillator (LO) drive and the RF signal respectively. Four Schottky diodes are connected at ports 3, 4, 5 and 6. Ports 3 are 4 are for the I-channel differential baseband signal, and ports 5 and 6 are for the Q-channel differential baseband signal.

3.4.1.2 Coherence

Coherence is one of the most important requirements for the mmWave probe to obtain the effective information of the e-device [162,234]. Opposite to sharing the synchronous clocks at the signal generation and acquisition stages, which increases the complexity and cost of the system [183], in *E-Eye*, the coherence property of the mmWave probe is obtained by simultaneously sampling the reference signal and the baseband signal (see Section 3.5.1.2). In order to control the VCO, the reference signal is phase locked to

the sawtooth voltage signal. In the synchronization procedure, the phase of each beat-signal period is aligned in the digital domain after sampling the reference signal and the baseband signal. Thus, in this method, the synchronous clocks are not demanded to share between the generation and acquisition stages, which simplifies the hardware.

3.4.2 System Integration Design

3.4.2.1 System Parameters Consideration

Parameters in the mm-Wave probe design are significant and should be carefully selected. There are three key factors that determine the performance of the mmWave probe, detection range, range resolution and the maximum non-ambiguous wireless signal velocity as follows: $R_d = \frac{cf_sT}{4B}$, $\Delta_R = \frac{c}{2B}$ and $v_{max} = \frac{c}{4f_cT}$, where c is the speed of the light, f_s is the sampling frequency on the baseband board and f_c is the center frequency, which is 24GHz. A larger detection range R_d requires a longer frequency ramp repetition period T and smaller transmitted bandwidth B. However, the higher range resolution Δ_R requires the wider bandwidth B. At the same time, the faster non-ambiguous wireless signal velocity v_{max} requires the shorter T. Thus there exists a trade-off between the bandwidth and the frequency ramp repetition period in the *E-Eye* system design.

3.4.2.2 System Integration

The Federal Communications Commission (FCC) in the United States proposed that new flexible service among the 24GHz band is roughly in the 24-24.45GHz band [74]. Also, the wider bandwidth of the probe means more cost for the probe hardware. Thus, in *E-Eye*, the bandwidth of the transmitted signal (B) is $450MHz$ with a center frequency (f_c) of 24GHz, and the transmitted average power is around $8dBm$. The frequency ramp repetition period (T) is $6.45ms$. The sampling frequency on the baseband board (f_s) is $192KHz$. In addition, an operational-amplifier-based SVG is employed

to generate the sawtooth voltage to tune the free running VCO. The frequency of the sawtooth signal and the reference signal is $155Hz$.

3.5 E-device recognition

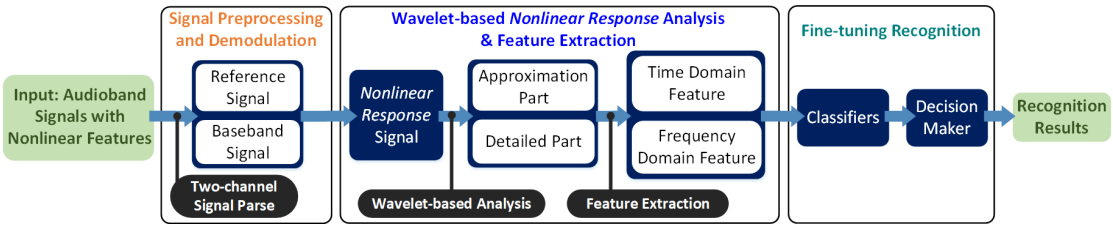


Figure 3.7: The flowchart of e-device recognition module, including three parts signal preprocessing and demodulation, wavelet-based *nonlinear response* analysis & feature extraction and fine-tuning recognition.

E-Eye listens to the *nonlinear response* reflected from the e-device and extracts unique identity from it. We first propose preprocessing and demodulation to extract the effective *nonlinear response* $y(t)$. Then, considering that $y(t)$ is irregular and asymmetric, we employ the wavelet decomposition to obtain the statistical features representing the device inner characteristics. In the end, a fine-tuning classifier is designed.

3.5.1 *Nonlinear Response* Preprocessing and Demodulation

3.5.1.1 Signal Preprocessing

As depicted in Figure 3.7, the data sensed by the mmWave probe is forwarded through the audio channel as two-channel signals. After parsing the audio signal, we get the baseband signal and the reference signal respectively. The reference signal is usually mixed with high frequencies from ambient noise and thermal noise. Thereby, we employ a filter to remove these components. However, filtering the reference signal of synchronous clock shape is difficult, which requires smoothing the shape and preserving the sharp edge at the same time. Specifically, we apply a Savizky-Golay and median combined filter [71]. Savitzky-Golay filter mainly fits successive sub-sets of adjacent

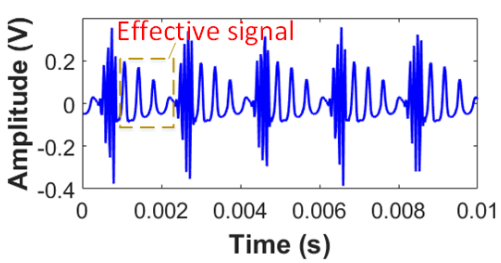
data points with a low-degree polynomial by the method of linear least squares. Although it is more effective at preserving the sharp edge for the pertinent high frequency components in the signal, it is less effective in noise filtering. Thus, the median filter is combined as it runs through the signal entry by entry, replacing each entry with the median of neighboring entries to remove the high frequency noise.

3.5.1.2 Signal Demodulation

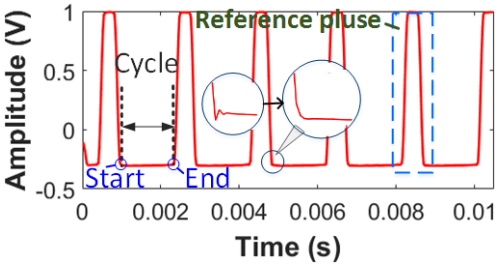
As shown in Figure 3.8a, we observe the reference signal has an edge effect on the baseband signal, making some parts distorted. Therefore, we utilize the reference signal to extract the effective parts in the baseband signal. First, we define that a *cycle* is the interval wave between the falling and rising edges of two adjacent pulses in the reference signal (see Figure 3.8b). Specifically, we use the falling and rising edges detection method to locate each *cycle* [193]. With the *cycle* information, we demodulate and extract the effective parts in the baseband signal based on the synchronized time. As a result, we obtain the effective *nonlinear response* signal consisting of N consecutive *cycles* in Figure 3.8c. Intuitively, the signal with more *cycles* will contain more unique physical characteristics of the e-device and thereby achieve better recognition accuracy. However, it also increases the computation overhead. To balance this trade-off, we empirically choose $N = 5$ and the corresponding original baseband signal has the length within $0.013s$ (we will investigate the performance of E-Eye with different N setups in Section 3.7.1.2).

3.5.2 Wavelet-based *Nonlinear Response* Analysis and Feature Extraction

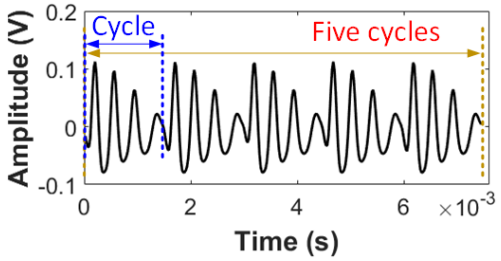
Given the *nonlinear response* signal, we find it is hard to classify them directly using the similarity distance because *nonlinear responses* have a large variation in magnitudes as



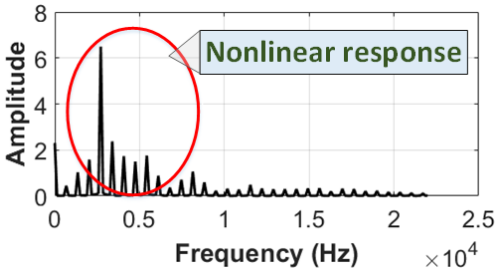
(a) The baseband signal parsed from the audio signal.



(b) The preprocessed reference signal.



(c) The *nonlinear response* signal after the signal demodulation.



(d) The spectrum for the *nonlinear response* signal.

Figure 3.8: A Nexus 5 smartphone is sensed within a USPS box at 20cm distance using the portable 24GHz mmWave probe. We preprocess and demodulate the raw sensing signal to extract the *nonlinear response*.

well as frequencies, which leads to irregularity and asymmetry. Therefore, we present the wavelet-based analysis which is resilient to the scale and magnitude variation.

3.5.2.1 Wavelet-based *Nonlinear Response* Analysis

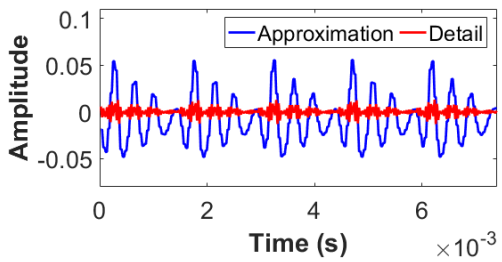
Wavelet transform (WT) is an effective multi-resolution analysis tool for signal decomposition [105, 157]. The WT approach can overcome the shortcoming of Fourier analysis, which only works in the frequency domain, not in the time domain [121]. The signal can be decomposed into many groups of coefficients in different scales with WT through different scaled versions. After removing the DC component, $y(t)$ becomes a signal with zero-mean and some variance and satisfies the following condition: $\int_{-\infty}^{\infty} f(t)dt = 0$, which indicates $y(t)$ is a waveform. WT uses $\psi_{a,b}$ and $\phi_{a,b}$, where $\phi_{a,b} = \frac{1}{\sqrt{a}}\phi(\frac{t-b}{a})$ and $\psi_{a,b} = \frac{1}{\sqrt{a}}\psi(\frac{t-b}{a})$, as the mother wavelet function that satisfies the condition of

dynamic scaling and shifting, where a and b are the scale and translation parameters accordingly [209]. In order to get high and low-frequency signal properties separately, the wavelet-based analysis is achieved as Equation (4.3):

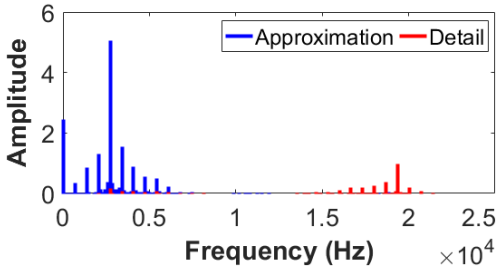
$$\underbrace{y(t)}_{\textit{Nonlinear response}} = \underbrace{\frac{1}{C_\phi}\int_{-\infty}^{\infty} F_W(a_0,b)\phi_{a_0,b}\frac{db}{\sqrt{a_0}}}_{\textit{The approximation part}} + \underbrace{\frac{1}{C_\psi}\int_{a_1}^{\infty}\int_{-\infty}^{\infty} F_W(a,b)\psi_{a,b}\frac{da}{a^2}\frac{db}{\sqrt{a}}}_{\textit{The detail part}}, \tag{3.2}$$

where $F_W(a_0,b)$ and $F_W(a,b)$ are the coefficients.

For the inverse transform to exist, we require that the analyzing wavelet satisfies the admissibility condition, given in the following: $C_\phi = 2\pi\int_{-\infty}^{\infty}\frac{|\hat{\phi}(\omega)|^2}{\omega}d\omega < \infty$ and $C_\psi = 2\pi\int_{-\infty}^{\infty}\frac{|\hat{\psi}(\omega)|^2}{\omega}d\omega < \infty$, where $\hat{\phi}(\omega)$ and $\hat{\psi}(\omega)$ are the Fourier transform of $\phi(t)$ and $\psi(t)$ respectively. Also, C_ϕ and C_ψ are constants for corresponding wavelets. Subsequently, we get the approximation signal as shown in Figure 3.9a and the detail signal in Figure 3.9b. Finally, for comprehensive characterization of the *nonlinear response*, we also get the spectral approximation and detail signals by Fast Fourier Transform (FFT) for further feature extraction.



(a) The approximation and detail parts of the Nexus 5 *nonlinear response* signal.



(b) The spectrum for the approximation and detail parts of the Nexus 5 *nonlinear response* signal.

Figure 3.9: The first level wavelet decomposition result of Nexus 5 *nonlinear response*. (a) and (b) represent its low and high frequency information respectively.

Table 3.1: List of Time Domain Features.

Name	Description
Mean Value	$\bar{x} = \frac{1}{N}\sum_{i=1}^{N} x(i)$
Standard Deviation	$\sigma = \sqrt{\frac{1}{N-1}\sum_{i=1}^{N}(x(i)-\bar{x})^2}$
* Skewness	$\gamma = \frac{1}{N}\sum_{i=1}^{N}(\frac{x(i)-\bar{x}}{\sigma})^3$
* Kurtosis	$\beta = \frac{1}{N}\sum_{i=1}^{N}(\frac{x(i)-\bar{x}}{\sigma})^4 - 3$
RMS Amplitude	$\lambda = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x(i))^2}$
Lowest Value	$l = \min_{i=1}^{N} x(i)$
Highest Value	$h = \max_{i=1}^{N} x(i)$

Table 3.2: List of Frequency Domain Features.

Name	Description
Mean Value	$\bar{y} = \frac{1}{N}\sum_{i=1}^{N} y(i)$
Standard Deviation	$\sigma = \sqrt{\frac{1}{N-1}\sum_{i=1}^{N}(y(i)-\bar{y})^2}$
* Skewness	$\gamma = \frac{1}{N}\sum_{i=1}^{N}\frac{y(i)-\bar{y}}{\sigma}^3$
* Kurtosis	$\beta = \frac{1}{N}\sum_{i=1}^{N}\frac{y(i)-\bar{y}}{\sigma}^4 - 3$
Crest Factor	$\varepsilon = 20\log(\frac{\max_{i=1}^{N}\lvert y(i)\rvert}{\sigma})$
* Flatness	$F_s = (\prod_{i=1}^{N} y_m(i))^{\frac{1}{N}} / ((\sum_{i=1}^{N} y_{m(i)}) / N)$

3.5.2.2 Spatial-temporal Domain Feature Extraction

As the above mentioned, the *nonlinear response* contains the unique identity of the device. As a result, we exploit the internal traits in the *nonlinear response* signal by extracting extract 13 scalar features in spatial-temporal domains. The feature names and descriptions are listed in Table 3.1 and 6.1. These features represent the *nonlinear response* signal shape from different aspects [62]. For example, *skewness* is a scale of symmetry to judge if a distribution looks the same to the left and right of the center point, *kurtosis* is to estimate whether the data are heavy-tailed or light-tailed relative to a normal distribution and *flatness* describes the degree to which they approximate the Euclidean space of the same dimensionality (marked with * in Table 3.1 and 6.1). Thus, in total, a feature vector containing these 26 features from the approximation and detail parts is formed.

3.5.3 Fine-tuning Recognition

Electronics recognition can be treated as a classification problem. *E-Eye* uses supervised learning to classify e-device types, beginning with a training phase followed by testing, as illustrated in **Algorithm 1**. However, it is possible that some e-devices (known as alien devices) are not included in the database before, which may spoof the check or cause false alarms. Therefore, to overcome this problem, we design the **Classifier** and the **Decision maker** to output the final recognition result.

During the training of the **Classifier**, n traces of *nonlinear response* signals from each e-device type are collected. For m e-device types in the database (namely, m pre-registered classes), $n \times m$ feature vectors are used to train the classifier altogether. In *E-Eye*, we employ SVM. The Gaussian radial basis function is selected as the kernel function to map the original data to a higher dimensional space [210]. During the testing phase, *E-Eye* collects a trace, extracts a feature vector, and inputs to the SVM model. The SVM model generates the probability set of classifying this test trace into each pre-trained class.

In the **Decision maker**, we define the maximum probability as the classification score. To distinguish an alien device, a threshold is applied: If the classification score is less than the threshold, the trace will be declared as an alien device with a second manual check; if not, the predicted type with the maximum probability will be regarded as the recognition result. In *E-Eye*, we select the threshold as 0.9 empirically.

3.6 System Prototype and Evaluation

3.6.1 *E-Eye* System Implementation and Integration

The prototype of the proposed mmWave probe is shown in Figure 4.11. The flexible RF board is based on a 0.245mm (0.0096in) thick substrate Rogers RT/duroid 5880 (Figure 3.10a). The rigid baseband board is fabricated on an FR4 substrate, which includes

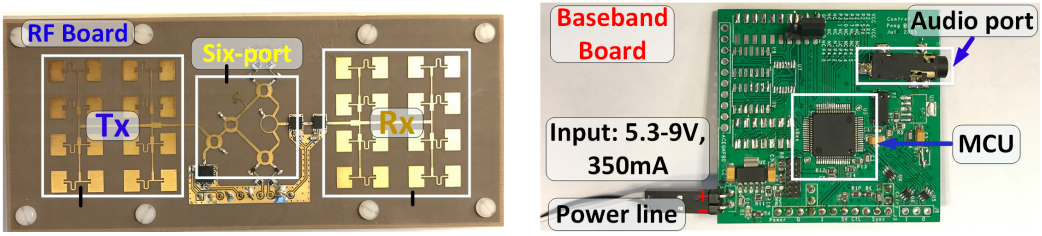
Algorithm 1: Fine-tuning Recognition

Input: $Q(n)$: n test nonlinear response traces from an e-device
Output: R: the predicted result

$E_i, S, R \leftarrow 0$;
Initialize T;
%Classifier:
for $i \in \{1, \ldots, n\}$ **do**
    $E(i) = Cls(Q(i))$;
    {*}[h]Classify m traces
end
%Decision maker:
$S = Tun(E)$;
%Make the classification score:
if $S < T$ **then**
    return *'Alien!'*;
    else
        $R = Rec(E)$;
        return R;
    end
end

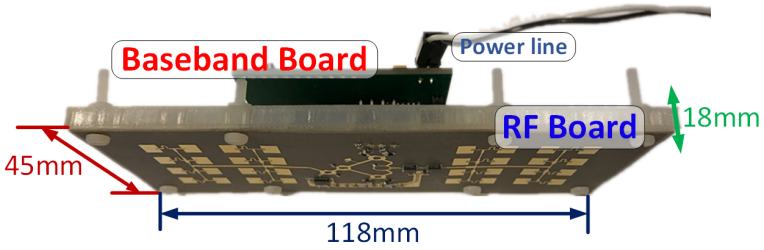
the SVG and the baseband amplifiers (Figure 3.10b). The Microprocessor Control Unit (MCU) is MSP430F2610, a widely used ultra low-power controller unit [15]. The baseband signals are fed to a 3.5mm audio jack directly supported by embedded MCU inner driver, which naturally has two channels for the reference signal and baseband signal without the extra need of the analog-to-digital converter or expensive communication chips. It can be easily connected to the audio interface of a smartphone or a tablet for signal processing.

The mmWave probe is $11.8cm$ $(4.65in)$ $\times$ $4.5cm$ $(4.65in)$ $\times$ $1.5cm$ $(0.59in)$ and weights only $45.4g$, which is lightweight for ease of adoption in security inspections. Moreover, it costs within 100 U.S. dollars. Figure 3.10c illustrates the integrated proposed mmWave probe. It typically has a 8dBm transmit power with a 3.7-$5V$ supply voltage and a $350mA$ maximum operating current under the $1.2W$ DC power consumption. The carrier frequency used in this work is 24GHz. To enhance the directivity, a



(a) RF board.

(b) Baseband board.



(c) The integrated mmWave probe with two boards.

Figure 3.10: The design of 24GHz mmWave front-end probe comprises two parts, i.e., (a) a radio-frequency Tx/Rx board and (b) a down-frequency baseband board. E-Eye probe integration is shown in (c).

Figure 3.11: Commodity electronic devices in our study.

pair of 4×4 antenna arrays are designed, offering an antenna directivity of $19.8dBi$. The received RF gain and baseband gain are $34dB$ and $26dB$, respectively.

3.6.2 Evaluation

Experiment Preparation: As shown in Table 3.3, we select 46 common e-devices and label them into 39 classes as we collect four duplicate Nexus 5 and three duplicate

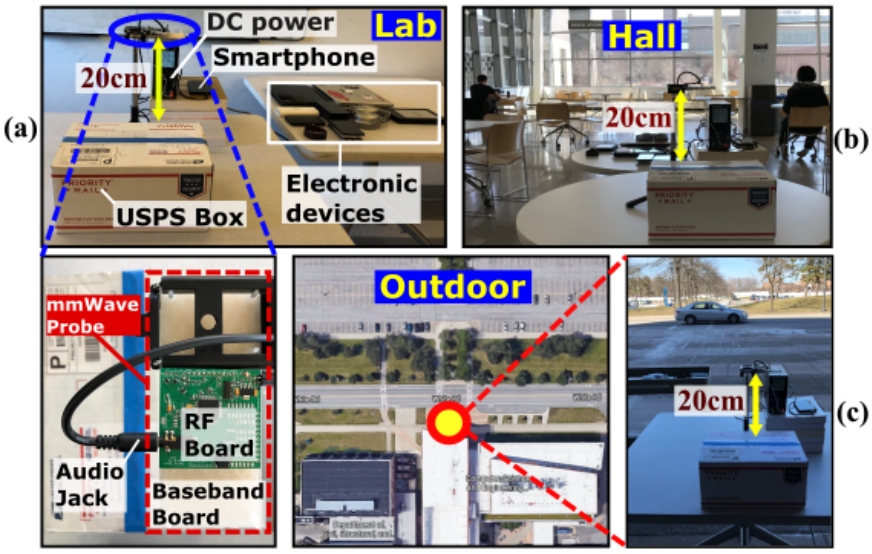


Figure 3.12: The setup for the evaluation: (a) in a controlled lab environment, (b) in an open hall at the first floor of the building, and (c) at the entrance of an outdoor public parking lot.

Uno R3. We also group them into seven categories based on their functions for ease of description. The corresponding circuit sizes range from $0.42in$ (diagonal) to $13.3in$ (diagonal). Without loss of generality, we employ two common containers to conceal the e-devices: a USPS package box (marked as Box1) and an Amazon package box (named as Box2).

Data Collection: During the experiment, the mmWave probe is placed $20cm$ from the container (see Figure 3.12). We record its initial position as $0°$ orientation in the horizontal plane. In every test trail, we conceal an e-device in one particular box and switch it on (if possible). We collect $10s$ sensing data with $44.1K$ sampling rate. In Section 3.5.1.2, we define one trace as the subsegment in the sensing data with the length of $0.013s$ ($13ms$), which contains $N = 5$ consecutive *cycles*. Eventually, we will randomly extract 100 traces for each device with regard to one container.

Data Partition: Unless specified, each time we randomly choose 70 out of 100 traces from each device as our training set and use the rest for testing. Thus, 3220 traces are used for training and 1380 traces are used for testing. Specifically, a 10-fold cross

Table 3.3: E-devices employed during experiments.

#	Device Category	Specific Device Brand
1	Laptop	Lenovo Xiaoxin310, Macbook Air, Asus LN4200, Macbook Pro, Mac mini
2	Tablet	iPad Pro, Asus ZenPad 3S, Nexus 10
3	Smartphone	Nexus 5*4, iPhone 6s, iPhone 6, iPhone X*2, iPhone 7plus, LG Leon, Nexus4, Smartisan T1*2, Jianguo Pro2, iPhone 4s, HTC One M8, Samsung S7
4	Wearable	Motor 360, Apple watch3, Fitbit Charge2, Mi band2
5	Mouse	Logitech M510, Rapoo 7200P, Dell MS111
6	Headphone	Bose QuietComfort 35, Status Audio CB-1, Air Pods
7	Others	Auduino Uno R3*3, iPhone Charger, Empty Box1, Empty Box2, Philips Sonicare 2 Series, Philips Norelco PQ208, Toshiba Canvio Basics, Kindle Paperwhite, Pisen power bank

validation method is employed in classification. It is worth mentioning that we conduct other types of cross validation experiments in Section 4.8 and 3.7.3 to examine the system performance under real-world environments.

Evaluation Metrics: We use accuracy, precision and recall as the performance metrics for evaluation [175]. Besides, we also adopt the Equal Error Rate (EER) and the Receiver Operating Characteristic (ROC). The lower the EER, the better the system performance [60].

3.7 Performance Evaluation

We evaluate the performance of *E-Eye* from three aspects:

- The control study validates the system under the ideal environmental condition, which proves the legitimacy of our system design.
- The field study considers the variation of system parameters in the practical usage and gives insights to how to achieve the best performance.
- The threat study exploits the vulnerability of the system from the attacker's perspective by examining more extreme conditions.

These three strategies serve different roles, which are complementary to each other.

3.7.1 *E-Eye* Control Study

3.7.1.1 Recognition Performance

We evaluate the ability of *E-Eye* to recognize the different e-devices in the optimal lab environment. First, we exploit the overall performance based on the training and testing data sensed from Box1 and Box2 respectively (denoted as Scheme1 and Scheme2). Then, we further apply the testing data from Box2 upon the training data from Box1 to study the system's universality (denoted as Scheme3). For each scheme, we make a comparison between two commonly used classifiers, SVM and KNN [219], to determine which classifier is more suitable.

The ROC results are shown in Figure 3.13. SVM achieves the EER of 0.0044, 0.0045 and 0.0111 respectively in three schemes. Correspondingly, KNN achieves the EER of 0.0647, 0.0669 and 0.0848 respectively. Both classifiers have excellent performance, which implies that the feature vector effectively reflects the unique *nonlinear response* characteristics in each e-device. The comparatively low EER in scheme3 indicates that our trained classifier does not have the over-fitting issue and can adapt to various usage scenarios.

Moreover, we conduct the McNemar test to determine if there is a significant difference in two classifiers [86]. McNemar test is a frequently used test for matched-pair

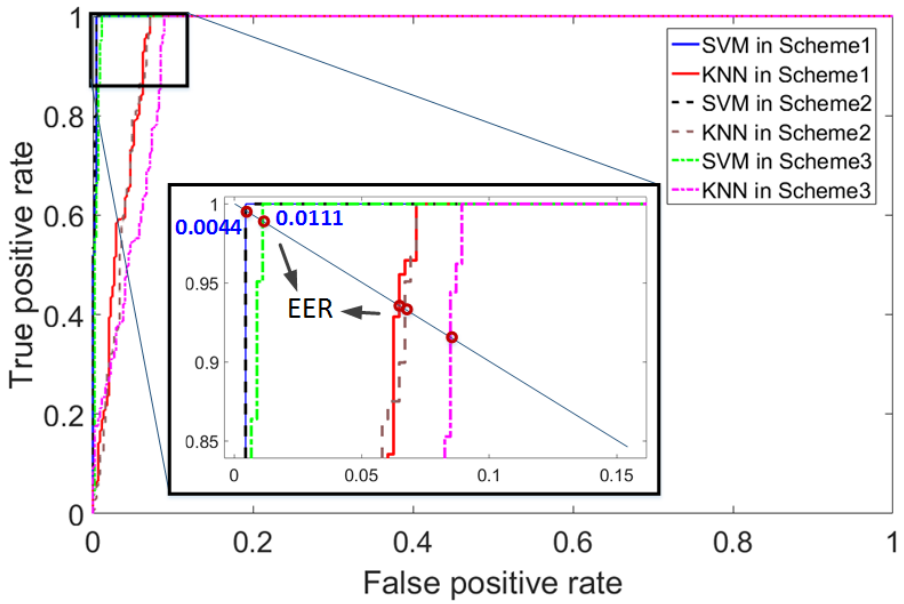


Figure 3.13: The overall performance of *E-Eye* with two different classification configurations.

data, with a significance level of $\alpha = 0.05$. Under the null hypothesis, the two classifiers have no significant difference. If the null hypothesis is rejected, the p value is below 0.05. In our test, the p value maintains around 0.01, which is less than 0.05 and thereby rejects the null hypothesis. Based on the above analysis, we prove that SVM has the better classifier and will employ SVM in the following evaluation unless otherwise specified. In conclusion, our results demonstrate that a hidden e-device can be precisely recognized by *E-Eye*.

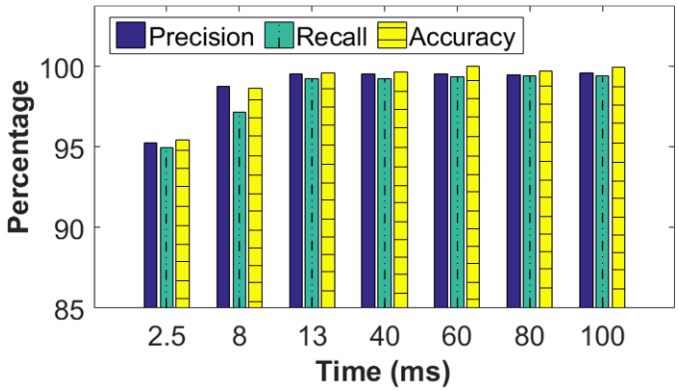


Figure 3.14: Recognition performance with seven different screening times.

3.7.1.2 Screening Time Efficiency

In public security, e-device screening tasks are challenging due to the limited time budgeted for efficiency. As a result, we are interested in analyzing the performance of *E-Eye* with regard to different time budgets. Specifically, considering that $2.5ms$ audio segment usually represents one *cycle*, we manually select seven different time settings between $2.5ms$ to $100ms$. For each time setting, we follow the same methodology described in Section 3.6.2 and re-prepare the training and testing set. Figure 3.14 shows the performance results. For the lowest budget of $2.5ms$, *E-Eye* only obtains 95.25% precision, 94.95% recall and 95.47% accuracy. These results are because the contained one *cycle* cannot comprehensively represent the characteristics of the e-device. After increasing the time, the performance gradually increases. Generally, we find a turning point at $13ms$ where the performance saturates afterwards (reaching 99.61% precision, 99.41% recall and 99.68% accuracy at $100ms$). This observation can guide us to the proper screening time setting to guarantee recognition accuracy without sacrificing screening efficiency.

3.7.1.3 Impact of Sensing Distance and Device Orientation

In practical scenarios, the inspector should be able to walk around with *E-Eye* according to different container shapes and inspection environments to accelerate inspection progress. Such a convenient practice, however, will lead to the changing distance and orientation between the hidden e-device and the mmWave probe. Therefore, it is important to investigate whether these aspects will affect system performance. Specifically, we measure the different device orientations (from 0° to 315°) at different distances (from $2cm$ to $100cm$). The results are shown in Figure 3.15. The average recognition accuracy over 46 devices remains high when the sensing distance varies within $80cm$ (above 99.5%). As for the orientation, although the reflected signal slightly changes due to the different probe angles for each e-device, the inter-device distinguishability among

46 devices is significant such that each device can be correctly recognized. Thereby, *E-Eye* can facilitate portable and convenient public screening in real practice.

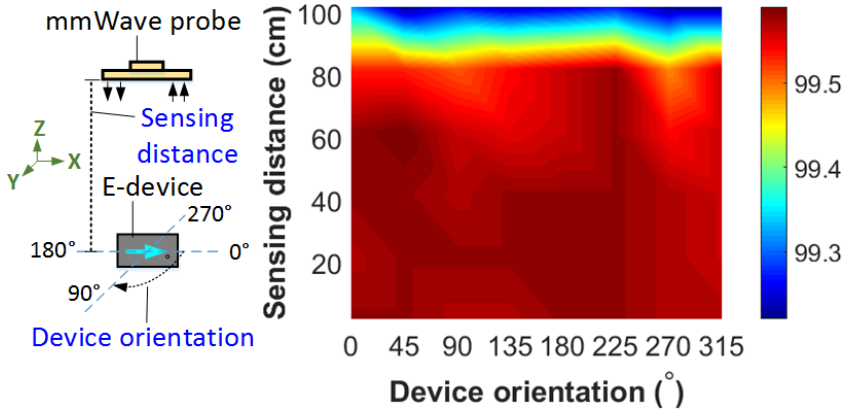


Figure 3.15: Measurement accuracy under different sensing distances.

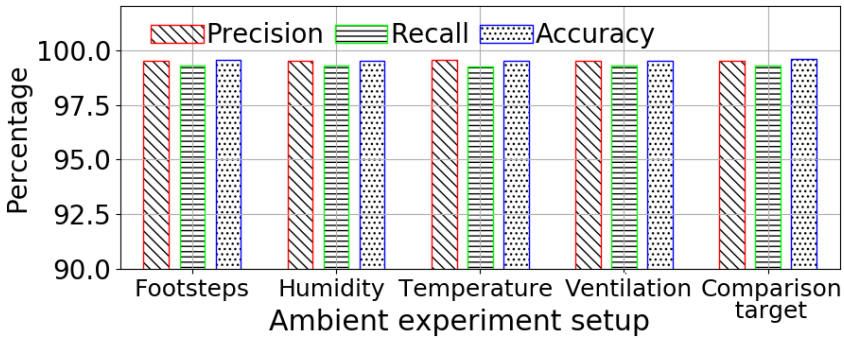


Figure 3.16: *E-Eye* recognition performance in different experiment setups.

3.7.2 Field Study

3.7.2.1 Robustness to Ambient Environment

The ambient environment can introduce random noises or even interfere with the probe hardware operation. We consider common noises in daily life in terms of human factors and ambient factors. Typically, we select four conditions where (1) five people are walking around the mmWave probe within 2 meters range; (2) the humidity of the testing location is controlled at 70%; (3) the environment temperature is 0°C (32°F); (4)

There is a working ventilation around. Moreover, we use the result of the optimal lab environment as the comparison target (humidity is 30% and the temperature is 20°C (68°F)). Again, we evaluate the above four conditions using 46 e-devices with scheme1. Figure 6.17 shows that their performances can achieve up to 99.6% precision, 99.3% recall and 99.6% accuracy. In conclusion, *E-Eye* presents a strong tolerance to different ambient environments.

3.7.2.2 Impact of Alien Devices

As discussed in Section 3.5.3, it is highly likely that *E-Eye* needs to classify the traces of the alien devices. In this section, we design an experiment to explore the ability of *E-Eye* to detect alien devices. In detail, we randomly include 9 out of 39 classes in the database as the training set as aforementioned (note that these data are never used for testing). Consequently, the remaining 30 classes are all regarded as the alien ones. Afterwards, we gradually increase the amount of alien devices from 5 to 30 and verify whether our specifically designed **Algorithm 1** can successfully identity them. For each amount, we report the average performance. As shown in Figure 3.17, the results remain stable in detection accuracy (*99.1%-100%*) showing no tendency to decrease in performance. In this way, we prove the effectiveness of fine-tuning the algorithm and the good scalability of *E-Eye* when used in real practice. Under these circumstances, the inspector can use the second check (*e.g., manual inspection*) for further security verification.

3.7.3 Threat Model Study

3.7.3.1 Human Body Intervention

Due to the advanced IC technology, e-devices are getting smaller in size such that they can be easily hidden upon the human body to bypass the security check. Therefore, we assume the attacker hides the device in different body positions, as listed in Figure 3.18. We specifically consider the devices in groups 3 and 4 as they are pervasive and

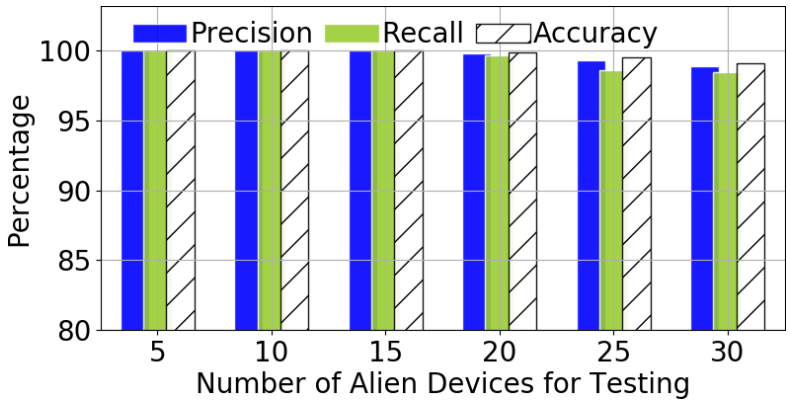


Figure 3.17: The alien device detection under six different alien device numbers.

can be used in multiple malicious activities (see Table 3.3). We recruit five participants carrying the device and we use *E-Eye* to scan them at target areas keeping an approximate distance of $50cm$. The reported average accuracy keeps higher than 97.7%, which implies that our system is resistant to human intervention.

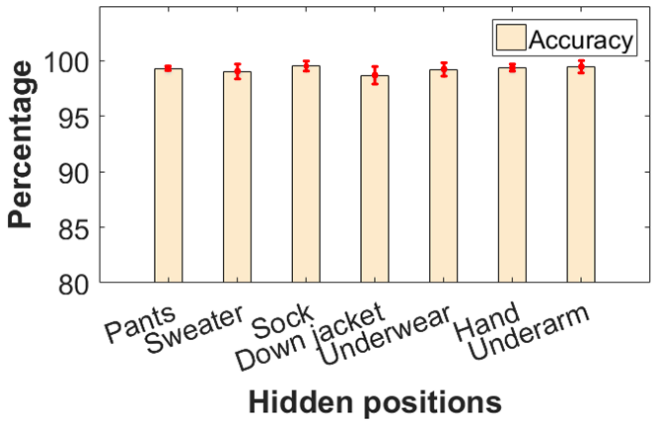


Figure 3.18: Detection accuracy under six different human interventions.

3.7.3.2 Impact of Cover Materials

We consider the scenario where the attacker intentionally hides the e-device in other materials to pass through screening. Particularly, we collect seven different daily-achievable materials as shown in Figure 3.19. We place the e-device inside each of them and evaluate the recognition accuracy for all 46 e-devices. The performance is reported

in the figure, where we can see that the overall accuracy for each is above 98%. Certain materials slightly affect the performance to some extent. This is because *E-Eye* utilizes high frequency signal and therefore, has small wavelength and limited penetration ability. As a result, it is prone to the scattering reflection upon some specific materials. But in general, *E-Eye* still provides reliable performance in device recognition.

Figure 3.19: Detection accuracy with six different cover materials.

3.7.3.3 Impact of Combined E-devices

In another scenario, the attack may know the benign devices registered in the database and try to physically stack the malicious device with the benign one to confuse the system. To explore whether *E-Eye* can still regard it as the alien device, we continue with the setup in Section 3.7.2.2. We randomly select 2 (labeled as No.1, No.2) devices from the 9 benign classes and 3 (labeled as No.3, No.4, No.5) from the remaining 30 alien classes. As shown in Figure 3.20, we enumerate all six combinations of the benign and alien devices and physically tap them together. For the sake of generality, we report the average and standard deviation of accuracy. From the results, we can observe that the average recognition accuracy are higher than 98%. This is owing to the fact that the equivalent circuit changes if we combine two devices together along with the *nonlinear response*.

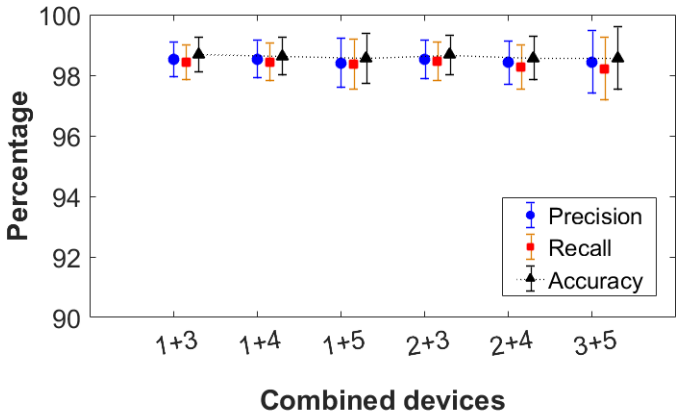


Figure 3.20: Detection of combined e-devices.

3.7.3.4 Impact of E-device Status

Considering the fact that many detection methods rely on the operation status of the hidden device (see Section 3.9.1), we simulate a scenario where the attacker wants to spoof the inspector by switching off the device or removing the battery. Thus, we repeat the experiment by shutting down all e-devices when collecting the data (as described in Section 3.6.2). Importantly, we still use the previously trained model where the devices were switched on. We apply the new 30 traces for each device for this test. Table 3.4 illustrates the precision, recall and accuracy for schemes 1 and 2, which are 99%. For scheme3, the accuracy is 98.75% which is in coherence with the results in Section 3.7.1.1. The high accuracy proves that *E-Eye* is not sensitive to the hidden device's operation status.

Table 3.4: System performance with the e-device status OFF at 50cm sensing distance.

Setup	**Precision**(%)	**Recall**(%)	**Accuracy**(%)
Scheme1	99.54	99.24	99.57
Scheme2	99.51	99.20	99.55
Scheme3	98.70	98.52	98.75

3.8 Discussion

Health Hazards: Compared to other security screening techniques (*e.g.*, Terahertz and X-ray imaging systems), *E-Eye* has a much smaller radiation factor, i.e., a 1.2W power consumption and an 8 dBm radio transmission power. Considering that typical public WiFi spots have about 20 to 30 dBm of output power, *E-Eye* is a considerably safe screening tool, even for cardiac device patients.

Metal Intervention: Metal has a stronger reflection on EM wave compared to other materials. We realize that a metal case shields a large portion of RF signals. By deploying an additional metal hidden material (*e.g.*, an e-device inside a metal box), it is difficult for *E-Eye* to recognize the covered e-device. This limitation can be solved by detecting the existence of metal [215].

Manual Check: We notice that mechanical motion in the electronic device and other intruders can affect the sensing performance. However, it is safe to assume that the security checker controls the environment thoroughly. If an unusual behavior happens, they initiate a manual check.

Database Storage: In this pioneering work, we have established 39 classes of an e-device database. Particularly, each feature vector has 26 dimensions data of size 0.2KB around. Thus, the template for each device seizes 14KB size data in the experiment setup. Therefore, it is practical to maintain a vast amount of templates on the mobile platform or the server (*e.g.*, 1,000 e-device types only require $13.67MB$ physical storage).

Multiple E-devices: Nowadays, it is normal for more than one e-device to be concealed in a container [21]. Therefore, it can bring huge convenience if *E-Eye* can automatically recognize each type when multiple devices are present. This problem can be further solved by employing the existing blind source separation and independent component analysis approaches in the speech processing domain [72, 250].

3.9 Related Work

3.9.1 Hidden E-device Detection

Currently, there are three main methods to detect hidden e-devices:

- **X-ray Imaging:** The X-ray baggage scanner operates based on the different X-radiation absorption rates of the penetrated objects and can accordingly produce the shape image of the objects [75]. The typical cost of such a scanner can reach US $50,000. Besides the undesired privacy concerns raised by the image of personal belongings [106], x-radiation also has harmful effects on human [106, 205].

- **Terahertz Imaging:** Terahertz (THz) imaging is also exploited in package screening by analyzing object transmissions or reflections of the THz electromagnetic wave. However, its optical image causes privacy issues and its resolution is too low for hidden e-devices recognition [148]. The current THz imaging systems have very low portability and extremely high cost (around US $25,000) [22, 88].

- **Electromagnetic Emission Sensing:** Studies find that e-devices transmit unintentional electromagnetic (UEM) radiations [195] when they are switched on. Many works [111, 212, 221] detect the existence of e-devices by analyzing their UEM waves. However, this technology is restricted and cannot be applied when the electronic device is powered off.

Therefore, we summarize that the current hidden e-devices recognition methods are either bulky, expensive or conditionally restrained, which cannot be directly applied in a regular and large-scale public security check. Other alternative handheld scanners [19, 106] can only provide the existence detection rather than accurately recognize the device type.

3.9.2 mmWave Sensing

mmWave radars have been studied in a variety of domains based on the detection of an object's inherent movements (*e.g.*, cardiorespiratory measurements and gesture sensing [115, 144, 145]) in the last decade. Soli [143] is a 60GHz mmWave radar gesture sensing system, which can detect all kinds of hand motions for the human-computer interface. In [167], a 94GHz mmWave radar is deployed to extract features of cardiorespiratory movements based on the reflected mmWave signals. These mmWave sensing applications mainly rely on the Doppler motion of the objects and cannot be applied to sense the target under clothings or obstacles (*e.g.*, packages and luggages). Although there are some recent applications to explore "through-wall" and "through-obstacle" sensing via mmWave [47, 238, 259], these techniques can only be applied for the target with specific mmWave-absorption characteristics. According to the literature, *E-Eye* is the first mmWave sensing application to explore nonlinear effects for hidden electronics recognition.

3.10 Conclusion

In this chapter, we proposed a hidden e-device recognition system *E-Eye* to aid law enforcement and ensure security. We started from the basics characteristics of the e-device and cover material under the nonlinear effect. Then, we proposed a portable 24GHz mmWave probe and the e-device recognition module to accurately recognize the hidden e-device type. Furthermore, extensive experiments indicated that our *E-Eye* could achieve more than 99% accuracy in less than 20ms response time and centimeter-level device physical size. Different levels of evaluation confirmed the effectiveness, reliability, and robustness of our proposed system. The research findings are an essential step for understanding the *nonlinear response* of hidden e-device and their applications at large.

Chapter 4

WaveSpy: Remote and Through-wall Screen Attack via mmWave Sensing

4.1 Introduction

Mitigating the risks of screen attacks has a long and rich history in the literature and is a core topic in the computer security community. Shoulder surfing, i.e., looking over the victim's shoulder, is one of the most investigated threats to user's screens [132]. With an increase in the user vigilance, however, adversaries have begun to exploit remote surveillance cameras to either directly or indirectly [70, 194] infer the screen content without line-of-sight assumptions. For example, it has been shown that various emanations from electronic displays, including ultrasound [87], electromagnetism (EM) [109], acoustic [96] and visible lights [131], can be leveraged to compromise the screen security. Therefore, one intuitive suggestion to enhance screen security is that people can place the screen in an enclosed location, e.g., no adversary-proximity/accessibility, no line-of-sight, and occluded to the outside. However, is this ideal scenario truly secure against attacks? Our answer is *no*.

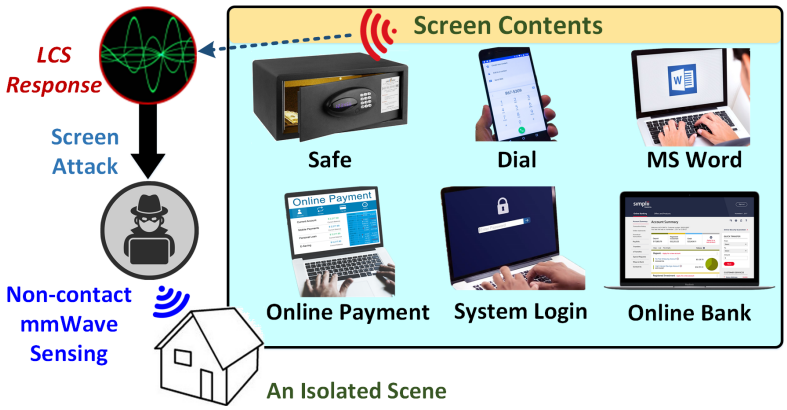


Figure 4.1: Examples of different screen contents in the screen attack applications. The WaveSpy system can infer the screen content and underlying sensitive information even in an isolated scene in the real world.

In this chapter, we discuss a new screen attack approach by exploiting the display mechanism using **liquid crystal** (LC) elements. Screen contents on displays (e.g., LCD) are generated by the states (e.g., shape distributions) of LC arrays behind the display panel [65]. In other words, there is a deterministic dependence between liquid crystal states (LCS) and screen contents. By utilizing this dependent relation, we discover a new and stealthy LC-based side-channel to remotely attack screens in real world. Specifically, we hypothesize that if an adversary can monitor either the state of each liquid crystal or their distribution in a display, it is possible to retrieve screen information by exploiting the LC dependent model. Because this new side-channel attack approach did not assume any traditional passive emanation (e.g., EM or light [109, 131]) to the outside world, the conventional wisdom on screen risk mitigation will fail, even in an isolated scene. If this hypothesis holds, there might be a novel screen attack approach which can change the conventional wisdom on screen risk mitigation and compromise screen security under an isolated scene mentioned above as shown in Figure 4.1.

There are multiple technical challenges to realize the new attack system. First, how can we obtain the information of a liquid crystal state on the targeted display? There are several recent studies on using radio frequency (RF) signals to characterize objects (i.e., shape, geometric features, and material types) [82, 141], however, sensing resolution of

a dot pitch (0.2-0.3mm) in an LCD display is still not reached. Second, to achieve a complete screen attack, the RF sampling frequency of liquid crystal states needs to be fast enough given that the modern screen flashes content every 4 to 10 milliseconds [84]. Lastly, it is critical to ensure the stealthiness of such an attack without creating noticeable disclosure when eavesdropping on the screen content using LCS remote sensing.

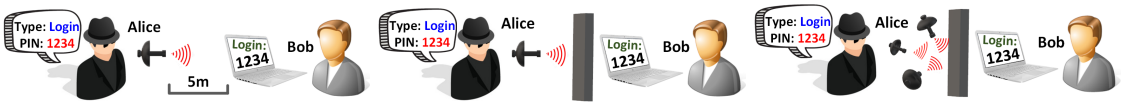
Our Work: In this chapter, we present WaveSpy, a new real-world screen attack system which rests on the concept of a liquid crystal nematic pattern inside the display panel which acts as a passive signal modulator and reflects RF signals, namely *LCS response*, containing the screen information. We first investigate the dependent relation between the reflected RF signal and the content displayed on the digital screens using a portable mmWave probe. Afterward, we develop an RF signal processing scheme, including a deep learning model, to investigate the internal traits in the *LCS response* signal through wavelet analysis, followed by the spectrogram feature augmentation while ensuring minimum time complexity. Subsequently, we conduct an extensive attack evaluation to assess the performance of our model in real-world applications. Eventually, we conclude the study by developing WaveSpy, a remote ($5m$ away, through-wall), low-cost, and stealthy screen inference system that precisely acquires the mmWave-based LCS response to facilitate two goals: (1) attack screens in a stealthy and through-wall manner; (2) retrieve the real-time sensitive information without the prior knowledge of their screen.

4.2 Attack Overview

4.2.1 Attack Scenario

We consider a scenario where a victim, namely Bob, utilizes common electronic devices (e.g., computer, mobile, smartwatch) in daily life. To ensure protection against attackers, Bob enables a password-based mechanism for every online activity including emailing, texting and monetary transactions and even facilitates an initial login screen for his

devices. Observing Bob's vigilance, an innovative attacker, hereafter Alice, aims to breach the established security and extract sensitive information without the victim's knowledge.



(a) Remote (b) Through-wall (c) Various angles

Figure 4.2: Three typical attack scenarios in daily life: (a) Alice infers the screen from a remote location; (b) Alice leverages the penetration properties of mmWave for through-wall inference; (c) Alice has the freedom to choose various sensing distance and angle to maximize the inference accuracy.

Scenario #1 (Privacy Invasion): To infer the type of screen content and user activity at a certain time, Alice intends to acquire information about the specific application initiated by Bob, usage statistics and the underlying content in real-time.

Scenario #2 (Security Attack): To compromise the personal security, Alice senses the information presented on the digital screen from a long distance or through-wall and reconstructs the sensitive information (e.g., PIN, password, lock pattern, words or sentences) without alerting Bob or his nearby surroundings, or even Bob in a closed room.

In contrast to prior work, we envision that the following constraints restrict Alice:

• **No Device Proximity:** Bob is alert to traditional shoulder-surfing or channel state information (CSI) attacks in terms that either Alice cannot get close or there is a blockage (e.g., wall) between Alice and Bob.

• **No Pre-installed Malware:** Assuming that Bob's electronic device is isolated from the Internet or any other communication channel, Alice is unable to directly compromise the electronic device from malware such as Trojans or malicious web scripts.

• **No Line-of-sight:** Alice cannot directly visualize the screen content or Bob's physiological attributes (e.g., hand motions, eye movement) during the activity phase

from any direction. Considering the alertness of Bob and real-world environments, there are no surveillance cameras that can remotely monitor digital screen contents.

Traditional EM-based, acoustic-based, CSI-based and vision-based screen attacks (e.g., [70, 87, 96, 109]) cannot work under an application scenario with the constraints mentioned above. However, screen security in this scene will not be necessarily guaranteed when we consider that Alice can leverage a tiny and cost-effective mmWave probe to perform real-time surveillance of screen information from an adjacent room and steal the information from the target victim, as shown in Figure 4.2.

4.2.2 Attack Application Study

In addition to the content type recognition, login authentication is one of the most fundamental types of security protection enabled by users in their personal devices. Moreover, this mechanism is increasingly deployed in other cyber-physical technologies such as Internet-of-Things (IoT), electronic depository safe, and smart homes. Figure 4.3 shows *three* attack applications in this study, including login using the virtual button, physical button and picture password. Based on the user acceptability and device operation, there are three primary categories of login methods:

4.2.2.1 Login Using Virtual Buttons

Presently, the most popular form of human-computer interaction is through the touchscreen via the virtual buttons. For different passwords, including *PIN*, *character password* and *pattern lock*, the user pauses for a brief moment in between subsequent inputs to recognize the user interface (UI) correspondence in the form of color change in the pressed buttons. The typical radius of each button on the screen can be small to $6mm$ (e.g., iPhone 7 Plus).

4.2.2.2 Login Using Physical Button

The non-touch based electronic devices (e.g., desktop monitor, laptop, cell phones and smart locks) require a user to input the password by pressing a physical button on the keyboard. This type of login has two categories. First, the password can appear as an asterisk character on the screen, similar to personal computer login. The second one can be found on some security devices where the password is visible on the screen as typed. The radius of each asterisk on the screen can be as small as $1mm$ (e.g., MacBook Pro). The typical size of each character on the screen can be $10mm$ by $6mm$ (e.g., security intercom system).

4.2.2.3 Login Using Picture Password

In contrast to the previous login methods, picture password offers the merit of unpredictability and superior usability. Rather than pressing the button on a virtual or physical keyboard, it allows a user to create three different gestures in a sequence on the specific position of the selected image and use those gestures as the password. The gesture can be any combination of circles, straight lines, and taps with predefined tolerances during the login process. The typical radius of each tap UI corresponding on the screen can be small to $6mm$ (e.g., Dell U2415).

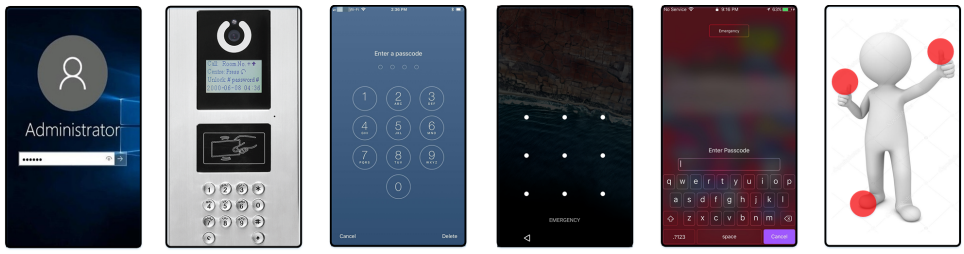


Figure 4.3: Six representative attack applications: (a) password length; (b) numeric password; (c) PIN; (d) pattern lock; (e) password; (f) picture password. The attack on each application is extensively evaluated in Section 4.6.2.

In the remainder of this paper, we present how WaveSpy performs the screen attack on aforementioned login-based authentications. The WaveSpy system also demon-

strates the significant promise in reconstructing critical information (e.g., words, sentences) in the digital screen as shown in Section 4.8.

4.3 Liquid Crystal State in Displays: A Closer Look

4.3.1 Background and Hypothesis

Presently, the liquid-crystal display (LCD) and organic light emitting diode (OLED) are the mainstream screen technologies adopted in the majority of electronic devices [90]. Our attack approach is applicable to both types of displays because they have the same LCS-based working principles. In the following part, we will review the display architecture and have a closer look at the LCS effects in modern displays.

Figure 4.4: The content displayed on the digital screen is determined by the arrangement of liquid crystal nematic patterns.

Working Principles of Displays: The LCD panel comprises a thin layer of glass substrate embedded with liquid crystals, while a white fluorescent backlight is positioned behind the screen to produce the images in color or monochrome. Each liquid crystal is aligned between two polarizing filters (parallel and perpendicular) as illustrated in Figure 4.4. Without the mentioned placement, light passing through the first filter would be blocked by the second (crossed) polarizer. The liquid crystal nematic pattern responds and changes its arrangement based on the voltage applied across the liquid crystal layer in each pixel, thereby altering the polarization of light. Besides, the variations in the liquid crystal nematic patterns lead to varying amounts of light to pass through, constituting different contents on the screen [65]. Note that the liquid crystal nematic pattern remains significantly stable under the probing of RF signals [220].

Liquid Crystal Nonlinear Effects: When a continuous wave with transmitting frequency f_0 from the mmWave probe is projected towards the target, the RF response is modulated with a set of sub-carrier frequencies due to the properties of the target (e.g.,

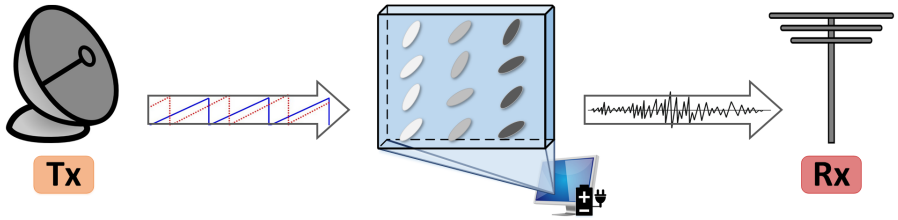


Figure 4.5: The liquid crystal nematic patterns on the digital screen incites a *LCS response* under the radio-frequency (RF) beam. Different liquid crystal nematic patterns cause different *LCS responses*.

liquid crystal pattern, material reflection efficiency). Similarly, given that the screen enters the RF beam field as shown in Figure 4.5, the liquid crystal nematic patterns are perceived as an array of antennas in the resolution of the mmWave [68,83]. These antennas act as a passive processor and manipulate the transmit mmWave signals to generate a distortion formulated as:

$$\begin{cases} Z(t) = \phi(\varphi(t), \triangle n, \kappa, \gamma, V_c) \otimes h_f(t), \\ \triangle n = \sqrt{\varepsilon_{\parallel}} - \sqrt{\varepsilon_{\perp}}, \end{cases} \tag{4.1}$$

where $\varphi(t)$ represents a collection of mmWave subcarriers for the response signals, $\phi(\varphi(t), \cdot)$ is the modulation function of the liquid crystal (LC) patterns, $\triangle n$ is the LC rotational viscosity, κ is LC the elastic constant, γ is the LC rotational viscosity, V_c is the LC threshold voltage, $\otimes$ stands for convolution computing, $h_f(t)$ is the ideal bandpass filter function for the carrier bandwidth, $\varepsilon_{\parallel}$ is the dielectric constant when the electrical field is parallel to the director of the liquid crystal molecules and $\varepsilon_{\perp}$ is the dielectric constant when the electrical field is perpendicular to the director [63, 189]. After the modulated signal radiates from the screen, it is captured by the probe receive (Rx) antenna. Therefore, *LCS response* of the digital screen incorporates profound information of the liquid crystal nematic patterns and holds the potential for monitoring the displayed content type or sensitive information.

Sensing Frequency Estimation: In order to obtain the RF response with exceptional quality and promote the attack performance, it is critical to utilize a proper sensing frequency. Under the most common circumstances, the length of a typical icon along a

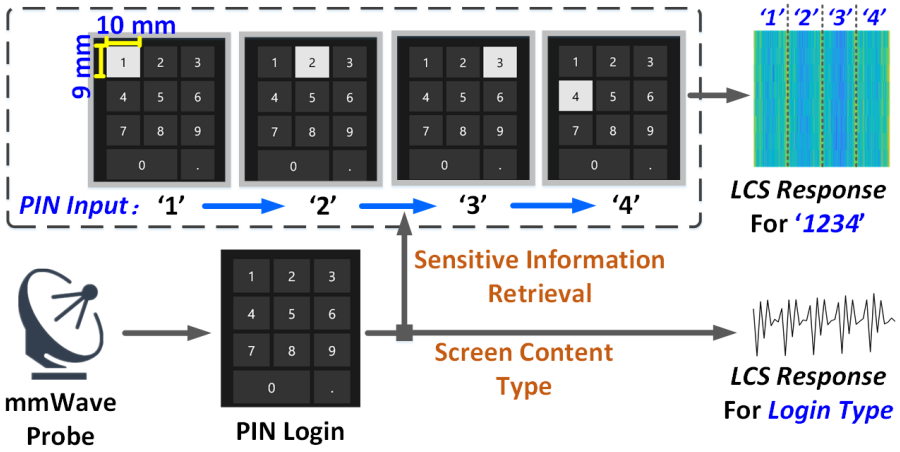


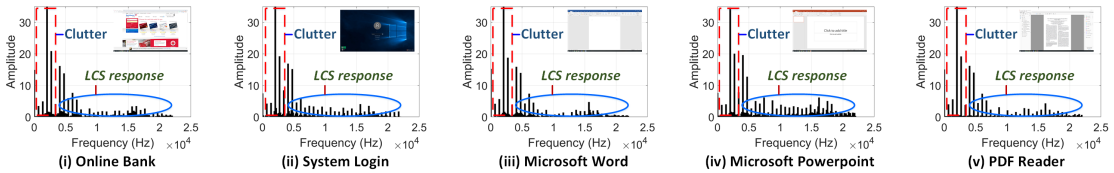
Figure 4.6: The *LCS response* illustration for PIN login mechanism with input '1234'. Every numeric input has a distinct *LCS response*, thereby enabling sensitive information retrieval.

screen is larger than $l = 3mm$, and the effective dielectric constant of the LC array is close to $\varepsilon = 3.66$ [247]. According to [119], the sensing frequency f_0 can be reckoned as

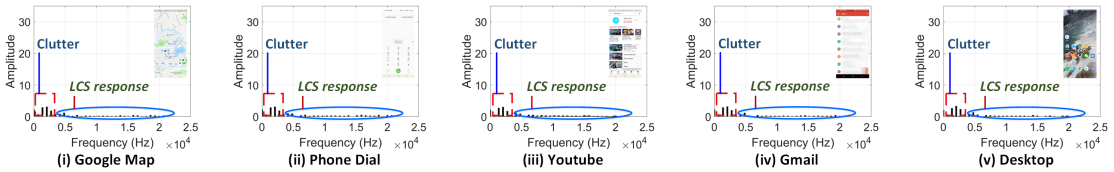
$$f_0 = \frac{c}{2l\sqrt{\varepsilon}} = \frac{3 \cdot 10^8 m/s}{2 \cdot 0.003m \cdot \sqrt{3.66}} \approx 24GHz, \tag{4.2}$$

where c is the propagation speed of a radar wave in air [63]. Therefore, we deploy the 24GHz sensing frequency, which can be approximately recognized as mmWave, in our study.

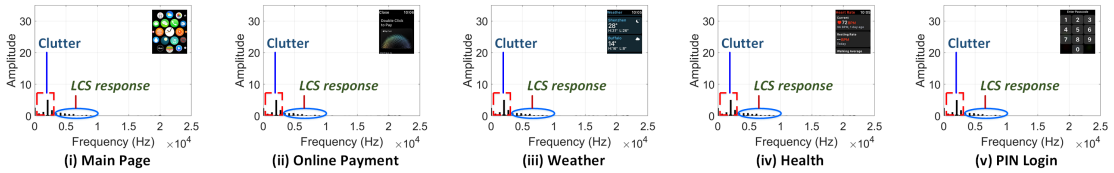
Hypothesis: Owing to the facts that the liquid crystal nematic pattern has a deterministic mapping to each displayed content and mmWave can remotely sense LC patterns, *there exists a unique and measurable connection between the displayed content and associated LCS response obtained under the mmWave beam reflectance of the liquid crystal layers*. Therefore, as shown in Figure 4.6, it is feasible to develop a portable mmWave probe with advanced signal processing techniques to capture this connection. The attacker can leverage the information for screen content type recognition and sensitive information retrieval, whose problem formulations are further discussed in Sections 4.4.4 & 4.4.5.



(a) *LCS responses* on Dell U2415 display with different content types.



(b) *LCS responses* on Samsung Galaxy S9 with different content types.



(c) The *LCS responses* on Apple Watch Series 3 with different content types.

Figure 4.7: Different screen content present different *LCS responses* (the spectrum in the red circles are distinct in frequency and amplitude) when forced by the same mmWave probe. The screen content on each screen is displayed on the left.

4.3.2 A Preliminary Study of LCS Response: A Side-channel on LCD Display

Proof-of-concept: To validate the above *hypothesis*, we conduct a preliminary experiment using *three* different mainstream off-the-shelf displays from representative device categories (i.e., Dell U2415 monitor, Samsung Galaxy S9, and Apple Watch Series 3) with different user activities. The spectrograms of *LCS responses* with associated content are shown in Figure 4.7. These devices are stimulated with the mmWave probe with a distance from the devices. The reflected signal profile is explored in the spectral domain. The x-axis represents the modulated frequency; y-axis describes the amplitude in the received signal. Given the vast contrast between the amplitude and the frequency of received *LCS response* marked in the blue circle, the liquid crystal nematic pattern variations have sufficient space to enable content recognition. Furthermore, we observe

that the response distributions among different devices are entirely distinct owing to the different device hardware structures and the screen designs.

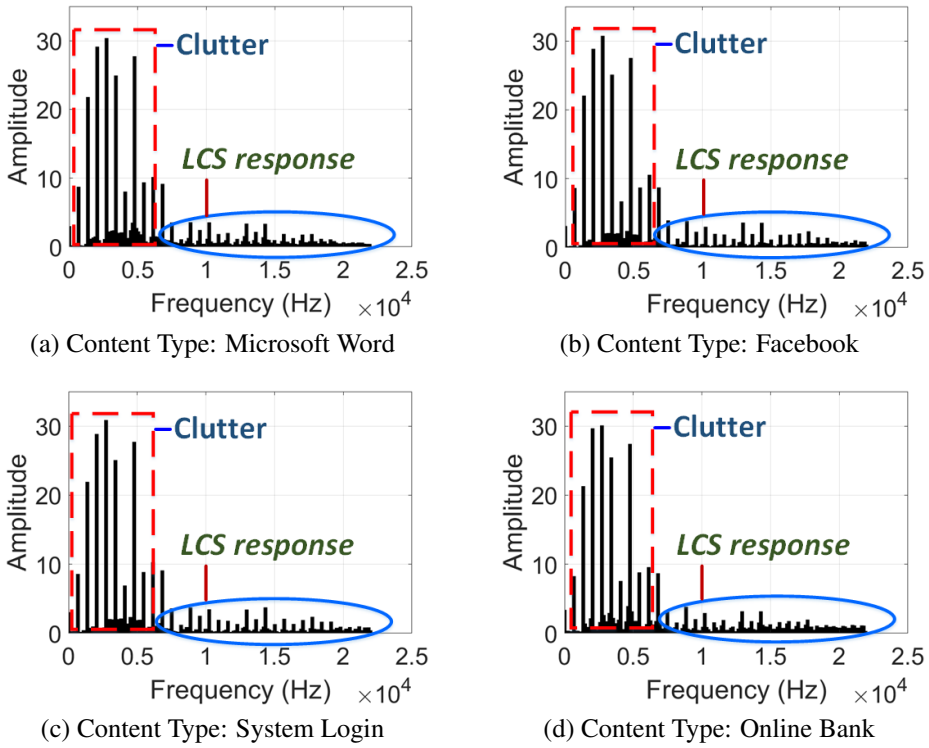
A Study on Wall Effects: In a real-world scenario, it is not uncommon for Bob to access his device in another room with the wall acting as an obstacle between the digital screen and attacker Alice. Therefore, it is crucial to investigate whether the material of the wall will block or interfere with the *LCS response* [208]. We conduct the experiment by positioning a $15cm$ thick wall between the mmWave probe and the digital screen of MacBook Pro. The sensing distance is $80cm$. Figure 4.8 demonstrates that in the overall signal spectrum, there is minute variation in the amplitude of low-frequency components from the wall and nearby objects. Upon closely analyzing the area within the *LCS response* (marked in the blue circle), there are observable variations in the high-frequency components among the different content displayed on the screen. However, this model is insufficient to precisely identify the liquid crystal nematic pattern as the differences between the *LCS responses* are not significant. Thus, we further develop the WaveSpy system for screen monitoring.

4.4 System Framework

4.4.1 WaveSpy: A Through-wall Screen Attack System

We propose a portable, unobtrusive and robust system to facilitate screen activity type recognition and sensitive information reconstruction as shown in Figure 4.9.

***LCS Response* Stimulation and Modeling:** We introduce the RF hardware in WaveSpy to stimulate and acquire the *LCS response* from electronics. Pulse-Doppler radar that emits a set of periodic powerful pulse signals has been largely used in airborne applications [154], such as the target range and shape detection. However, when a short-time pulse stimulus, which has an infinite frequency band, is applied to illuminate the electronics, the corresponding spectrum response will be overlapped with the stimulus signal and difficult to recognize. Therefore, WaveSpy selects a frequency-



(a) Content Type: Microsoft Word

(b) Content Type: Facebook

(c) Content Type: System Login

(d) Content Type: Online Bank

Figure 4.8: The non-linear response of the wall or surrounding objects is distinct in frequency and amplitude from the *LCS response* of digital screen in MacBook Pro, indicating the feasibility of indirect screen monitoring.

modulated continuous-wave (FMCW) radar with a narrow passband filter [184]. The FMCW radar continuously emits periodic narrow-band chirp signals whose frequency varies over time. The non-linear interrelation to these narrow-band stimuli will generate distinct frequency response, and the received signals will carry distinguishable *LCS responses* when the stimuli signals hit the target display. After the manipulated signal is radiated from the display, *LCS responses* will be captured by the RF probe receiver antenna (Rx).

Screen Monitoring: Once the data format obtained from the mmWave probe is demodulated to filter the interference and noise while guaranteeing the preservation of information. A wavelet-based response analysis is employed to extract a set of comprehensive features and formulate a sequence of multi-class deep neural networks based classifica-

Table 4.1: List of features extracted from the *LCS* response.

Category	Feature Names
Temporal Features	Mean Value, Standard Deviation, Skewness [160], Kurtosis [79], Lowest and Highest Value
Spectral Features	Mean Value, Standard Deviation, Kurtosis, Crest Factor [31], Flatness [136]
Others	*MFCC (12)* [191]

tion algorithm to obtain the content type and the sensitive information displayed on the digital screen.

Figure 4.9: The system overview for WaveSpy to non-invasively recognize the screen content type and retrieve the security information on the screen. It comprises of a mmWave sensing module in the front-end and a screen monitoring module in the back-end.

4.4.2 Screen Localization

Searching and localizing the display of interest is the first step in screen attack. In this section, we introduce the screen searching protocol to localize the screen position under the angular coordinates. First, WaveSpy steers the mmWave beams to sweep through all directions in the target areas. Second, considering the display will generate LCS which is significantly different from the background (e.g., LCS response), we utilize LCS-based features (see Table 4.1 with a threshold) to detect existence of display and estimate the orientation of the target screen. This process is efficient and can be finished within several milliseconds. Adaptive beam training protocols can be adopted to improve the accuracy in screen localization further [127]. Therefore, WaveSpy can pinpoint the screen and prepare for the *LCS response* analysis. Note that we evaluate the WaveSpy performance sensitivity to the probing orientation in Section VII (see Figure 14 in details).

4.4.3 The Wavelet Analysis on LCS Response

After removing the direct current (DC) component, modulated LCS signal $s(t)$ becomes a signal with zero-mean and some variance and satisfies the following condition: $\int_{-\infty}^{\infty} s(t)dt = 0$, which indicates $s(t)$ is a waveform. ***P()*** uses $\psi_{a,b}$ and $\phi_{a,b}$, where $\phi_{a,b} = \frac{1}{\sqrt{a}}\phi(\frac{t-b}{a})$ and $\psi_{a,b} = \frac{1}{\sqrt{a}}\psi(\frac{t-b}{a})$, as the mother wavelet function that satisfies the condition of dynamic scaling and shifting, where a and b are the scale and translation parameters accordingly [209]. In order to get signal properties at high frequency, the wavelet-based analysis is achieved as Eq. (4.3):

$$s(t) = P_0 + P_1 + P_2 + P_3, \tag{4.3}$$

where $s(t)$ is the LCS response, $P_0 = \frac{1}{C_\phi}\int_{-\infty}^{\infty} F_W(a_0, b)\phi_{a_0,b}\frac{db}{\sqrt{a_0}}$ is the approximation part, $P_1 = \frac{1}{C_\psi}\int_{-\infty}^{\infty} F_W(a_1, b)\psi_{a_1,b}\frac{da}{a_1^2}\frac{db}{\sqrt{a_1}}$ is the Level 1 detail part, $P_2 = \frac{1}{C_\psi}\int_{-\infty}^{\infty} F_W(a_2, b)\psi_{a_2,b}\frac{da}{a_2^2}\frac{db}{\sqrt{a_2}}$ is the Level 1 detail part, $P_3 = \frac{1}{C_\psi}\int_{-\infty}^{\infty} F_W(a_3, b)\psi_{a_3,b}\frac{da}{a_3^2}\frac{db}{\sqrt{a_3}}$ is the Level 3 detail part, $F_W(a_0, b)$, $F_W(a_1, b)$, $F_W(a_2, b)$ and $F_W(a_3, b)$ are the coefficients.

For the inverse transform to exist, we require that the analyzing wavelet satisfies the admissibility condition, given in the following: $C_\phi = 2\pi\int_{-\infty}^{\infty}\frac{|\hat{\phi}(\omega)|^2}{\omega}d\omega < \infty$ and $C_\psi = 2\pi\int_{-\infty}^{\infty}\frac{|\hat{\psi}(\omega)|^2}{\omega}d\omega < \infty$, where $\hat{\phi}(\omega)$ and $\hat{\psi}(\omega)$ are the Fourier transform of $\phi(t)$ and $\psi(t)$ respectively. Also, C_ϕ and C_ψ are constants for corresponding wavelets. Afterwards, the detail parts of the *LCS response* can help us to further achieve screen content type recognition and sensitive information retrieval.

4.4.4 Screen Content Type Recognition

Content type recognition can be formulated as a multi-class classification problem. We begin by defining the key terms and then formulate the content type recognition problem.

`Definition 1` *(The LCS Response Set on the Liquid Crystal Nematic Pattern by mmWave)*: For a mmWave sensing process, let ***s*** denote a mmWave response of

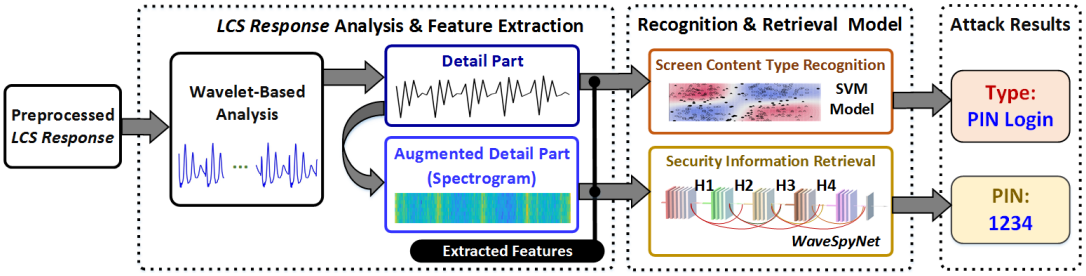


Figure 4.10: The flow chart of the screen monitor module, including two parts: (a) *LCS response* analysis & feature extraction, and (b) screen content type recognition & sensitive information retrieval model.

the liquid crystal nematic pattern that is attained by a certain sample method. $\boldsymbol{S}$ is defined as the response set, which contains every liquid crystal nematic pattern response. Specifically, we define s_0 as a complete sensing signal that has the entire information about characteristics of the source content on the screen. Therefore,

$$\forall s \in S, \emptyset \subset s \subseteq s_0. \tag{4.4}$$

Given the *LCS response* signals, it is hard to classify them using similarity and distance-based approaches directly. The reason is that *LCS responses* have a large variation in magnitudes as well as frequencies, which leads to irregularity and asymmetry. Therefore, we present the wavelet-based analysis which is resilient to the scale and magnitude variation.

`Definition 2` *(Feature Extraction from Wavelet-based Analysis)*: The response analysis function can be any function that demodulates the response, reflects the liquid crystal nematic characteristics, obtains the integration of content features, and outputs a feature vector. We use ***P()*** to represent the *LCS response* analysis function.

In this chapter, we use wavelet transform (WT) as ***P()***, which is an effective multi-resolution analysis tool for signal decomposition [105, 157]. The ***P()*** approach can overcome the shortcoming of Fourier analysis, which only works in the frequency domain, not in the time domain [121]. $s(t)$ matches the waveform and can be decomposed into many groups of coefficients in different scales with ***P()*** through differently scaled versions, as shown in Section 4.4.3.

Subsequently, we obtain the approximation and Level 1, 2 and 3 detail parts in Eq. (4.3) (in Section 4.4.3). As the above mentioned in Section 4.3, the unique characteristic information is hidden in the high-frequency range (i.e., the detail parts). Intuitively, the signal with more features in the high-frequency signal will contain more distinguishable characteristics of the screen content and thereby achieve a better recognition accuracy. However, it also increases the computation overhead. To balance this trade-off, we empirically choose the level 3 detail part (we will investigate the system performance with different $level$ setups in Section 4.6.1). As a result, we exploit the internal traits in the *LCS response* signal by extracting a 40-dimension feature vector in spectrum domains.

`Definition 3` *(Screen Content Type Classification)*: ***C()*** is the classification function that utilizes several response features to predict the screen content type. The specific implementation of ***C()*** responds to the real-world scenarios and the applied database mentioned in Section 4.4.4.

Formulation 1 *(User Activity Monitoring)*: The purpose of screen content type recognition is to identify the specific application and user online activity initiated by the mmWave response $\boldsymbol{s}$. We first extract its feature vector using ***P()***, and then recognize the application type with the screen content type classification function ***C()***. β is used to denote the result of the predicted specific application on the screen as follows:

$$\beta = C(P(s)). \tag{4.5}$$

In the WaveSpy system, we employ universal and easy-to-deploy classifiers, i.e., Support Vector Machine (SVM) and K-Nearest Neighbor (KNN) as the screen content type/user activity classification method $C()$, to identify content type based on the extracted features. Previously, SVM and KNN have been successfully applied in wireless sensing recognition [141] and physical cybersecurity [140], respectively. SVM locates an optimal hyperplane in high-dimensional space to perform the classification. The Gaussian radial basis function is selected as the kernel function to map the original data to a higher dimensional space. However, KNN stores all available cases and classifies

new cases based on a similarity measure. We opt to use SVM as the classifier after we compare their performances in Section 4.6.1.

WaveSpy uses a supervised approach to classify content types, beginning with a training phase followed by testing. During the training of the **Classifier**, n traces of *LCS response* signals from each content type are collected. For m content types in the database (namely, m pre-registered classes), $n \times m$ feature vectors are used to train the classifier altogether. During the testing phase, WaveSpy collects a trace, extracts a feature vector, and inputs to the classifier model. The classifier model generates the probability set of classifying this test trace into each pre-trained class. We output three candidates with the top three possibilities.

4.4.5 Sensitive Information Retrieval

4.4.5.1 Sensitive Information Retrieval Method

When the user presses a button on the screen, the pixel-level configuration of this button changes, showing the correspondence UI illumination and allowing the user to confirm the correctness of the input, which causes different *LCS responses* as shown in Figure 4.6. From a high-level point of view, WaveSpy infers password or sensitive information of the user by collecting and analyzing the *LCS response* sequence received on the mmWave probe. The sequence length is equal to the user's typing duration. When the screen content type is detected as the login interface, this sensitive information retrieval model is then activated to detect PIN passwords.

A traditional approach to address this problem is first to segment the input signals into N pieces, where N is the length of the PIN passwords, and then to classify each segmented piece as a digit. However, it is difficult for us to segment those signals manually. The other possible solution is to extract features for the whole signals first, and then to train a classifier for each PIN digit. However, we observe that the differences among those signals on different screen contents are significantly miniature. In other

words, the extracted features of different signals are nearly the same, which leads to the failure of both SVM and KNN.

To tackle this challenge, we employ deep neural networks (DNN) [112] in the WaveSpy System. The advantage of adopting DNN is that it is able to learn better feature representations automatically and further makes the signals distinguishable. Moreover, the DNN-based security inference framework can be easily applied to new scenarios without domain knowledge about the functioned sensors. Thus, we propose a novel end-to-end deep learning based approach, which takes the raw sensing data as the input and computes the most likely sensitive information that the users have entered.

First, sensitive information retrieval can be formulated as a sequence multi-class classification problem. However, the original sequence signal is too large to be considered the input of DNN. For example, the recording for PIN typing usually produces a four-second long audio containing about 176,400 samples in total. Thus, we utilize the technique of Joint Time-Frequency Analysis [192] to convert the sequence signal into a spectrogram.

`Definition 4` *(Feature Augmentation using Spectrogram)*: Let ***W()*** be the function to generate the spectrogram from the input signal, which is defined in Eq. (4.6) as follows:

$$\begin{cases} X(m,\omega) = \sum_{n=-\infty}^{\infty} x[n]w[n-m]\exp(-j\omega n), \\ W\{x(t)\}(m,\omega) \equiv |X(m,\omega)|^2. \end{cases} \tag{4.6}$$

Note that in our implementation, instead of using the original signal, we use the level 3 detail part from wavelet decomposition as the input of ***W()*** as shown in Figure 4.10, which reflects the internal trait in the *LCS response* signal (evaluated in Section 4.6.1). Finally, the converted spectrograms are the inputs of DNN.

`Definition 5` *(Sensitive Information Classification Function)*: ***V()*** is defined as the DNN model that utilizes several response-analysis to predict the sensitive information shown on the screen.

It is worth noting that for each real-world scenario mentioned in Section 4.2.2, we train a customized ***V()***. The details of the DNN model are further illustrated in Section 4.4.5.2.

`Formulation 2` *(Sensitive Information Retrieval)*: The final goal of sensitive information retrieval is to reconstruct the sensitive information from the input signal ***s*** using the response analysis function. Since there are N characters in the credential, for each reconstructed character, we train a specified DNN model. Let T_n be the candidate results of the sensitive information on the screen for the ***n***th character:

$$T_n = \mathbf{V}_n(\mathbf{W}(\mathbf{s})). \tag{4.7}$$

`Formulation 3` *(Ranking Sensitive Information Candidates)*: To deal with noisy mmWave signal traces and accommodate the input number allowed by the system, we need to rank the candidate credentials according to their possibilities. $R(n)$ is a function to obtain top ***k*** candidates for predicting the sensitive information shown on the screen:

$$\begin{cases} R(n) = f(T_n), & n = 1 \\ R(n) = f(R(n-1) \circ f(T_n)), & n \geq 2 \end{cases} \tag{4.8}$$

where the operation $\circ$ represents that all the data in one set are multiplied by all the elements in the other set, and $f(\circ)$ is the function to find the candidates with top ***k*** possibilities among the results. Thus, the algorithm for the screen attack in WaveSpy is established in Algorithm 2.

4.4.5.2 Sequence-to-Credential Model for General Security Information Inference

Though the original sequential signal can be transformed to the spectrogram using the time-frequency analysis technique, the transformed spectrograms are extremely similar as shown in Figure 4.7 and hard to be distinguished by traditional classification algorithms such as SVM and CNN. To make these spectrograms distinguishable, we design

Algorithm 2: The Screen Attack by WaveSpy

Input: $s(m)$: m *LCS response* traces from the screen
Output: β: the Screen content type recognition result
R: the sensitive information retrieval result

Initialize C, P, R, V, W, β, T;
%Screen content type recognition:
for $i \in \{1, \ldots, m\}$ **do**
    $\beta(i) = C(P(s(i))$;
    if $\beta(i) ==' Login'$ **then**
        %Sensitive information retrieval:
        $T(i) = V(W(s(i))$;
        return $R(T(i))$;
    end
    return $\beta(i)$;
end

WaveSpyNet, a Densely Connected Convolutional Networks (DenseNet) [114]-based classifier for the sensitive information retrieval, i.e., ***V()***. Besides perfectly guaranteeing the classification performance, WaveSpyNet also alleviates the vanishing-gradient problem, strengthens feature propagation, encourages feature reuse, and substantially reduces the number of parameters, which naturally satisfies the requirements of our problem. Next, the details of WaveSpyNet are introduced.

The WaveSpyNet consists of an initial layer, four dense blocks, three transition layers, and a prediction layer as shown in Figure 4.10. The initial layer aims to convert the transformed spectrogram $W(s) \in \mathbb{R}^{128\times128}$ into a latent space. The initial layer includes four consecutive operations: a convolution (Conv), followed by a batch normalization (BN), a rectified linear unit (ReLU) and a max pooling. Let $\mathbf{x}_0^1 \in \mathbb{R}^{128\times128}$ represent the output of the initial layer, which is the input of the first dense block.

Each dense block $b \in \{1, \cdots, \mathcal{B}\}$ comprises $\mathcal{L}^b$ layers, and each layer implements a non-linear transformation $H_\ell(\cdot)$, where ℓ indexes the layer. $H_\ell(\cdot)$ is defined as a composite function with three consecutive operations: BN-RELU-Conv. The most greatest advantage of WaveSpyNet is that for the ℓ-th layer ($1 \leq \ell \leq \mathcal{L}^b$ and $\ell \in \mathbb{R}^+$), the input of $H_\ell(\cdot)$ is the direct concatenation of all the previous layers, i.e., $[\mathbf{x}_0^b, \mathbf{x}_1^b, \cdots, \mathbf{x}_{\ell-1}^b]$.

The output of the ℓ-th layer is represented by:

$$\mathbf{x}_{\ell}^{b} = H_{\ell}([\mathbf{x}_{0}^{b}, \mathbf{x}_{1}^{b}, \cdots, \mathbf{x}_{\ell-1}^{b}]). \tag{4.9}$$

When the size of filters in convolutional layers changes, the concatenation operation used in Eq. (4.9) is not viable. Thus, a transition layer is designed to change the size of filters, which is between two consecutive dense blocks as shown in Figure 4.10. The transition layer consists of a batch normalization layer, a 1×1 convolutional layer followed by a 2×2 average pooling layer. The output of the transition layer is the first input of the next dense block.

The above two operations are repeatedly conducted until arriving at the last dense block. The output of the $\mathcal{B}$-th dense block is the input of the prediction layer. A simple linear function is used to produce a latent vector to represent the original input signal or the transformed spectrogram. Actually, each signal contains N characters. In the implementation, we train a separate WaveSpyNet with the cross-entropy loss, and we choose Adam, a light-weight stochastic function optimizer [128] to fine-tune the WaveSpyNet parameters.

4.5 Performance Prototype and Evaluation

4.5.1 WaveSpy System Implementation and Integration

WaveSpy utilizes an FMCW mmWave probe equipped with a pair of 4×4 antenna arrays. The transmission power is around one Millie Watt. The RF signal is processed using the novel mechanism of the inverse synthetic aperture radar [141]. Besides, the probe can be mounted on the wall or integrated with other portable devices like a laptop or smartphone. Therefore, WaveSpy can launch the attack with a convenient and user-friendly manner in real-world applications.

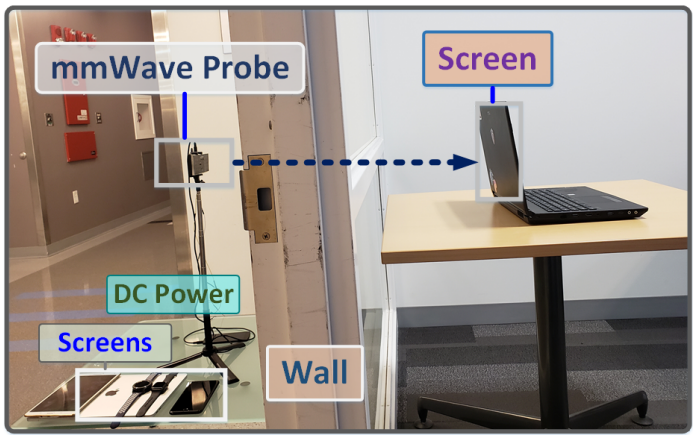


Figure 4.11: The setup for the evaluation mainly consists of three parts: a mmWave probe, screen, and wall.

4.5.2 Experiment Setup

4.5.2.1 Experiment Preparation and Data Collection

In order to comprehensively evaluate every possible form of the *LCS response*, we employ 30 digital screens and categorize them in six groups; specifically, nine monitors, five laptops, three tablets, six smartphones, four wearable devices, and three other electronic devices. Among these, 21 devices have LCD displays and 9 have OLED displays. All displays are well functioning with no defects. Their sizes vary between 1.5 inches to 70 inches while the usage time ranges from 1 to 11 years. All screens are under the default profile that is set to at the factory. The walls are made of wood and concrete, two mostly used in modern buildings. We recruit ten anonymous participants. It is ensured that every participant follows the host institute internal review board protocol. During the experiment, the mmWave probe is placed $80cm$ from the screen and its initial position is recorded as 0° orientation in the level plane. During the experimental phase, we position the screen behind the wall or obstacle (see Figure 4.11).

In general, we conduct two sets of experiments to enable screen content type recognition and sensitive information retrieval. We repeat each experiment for ten times for every participant. For the *content type recognition*, we prepare and label 100 screen

content types from common user activities, e.g., typing on Microsoft (MS) Word, and collect $2s$ of sensing data for the specific content type on each trial. As mentioned earlier, each participant is asked to repeat for 10 times. From the overall dataset, we randomly extract 100 traces for each content type (totaling 100 x 100 = 10,000 traces) with respect to an individual location. Unless specified, we randomly choose 7,000 out of 10,000 traces from each device as the training set and the remaining for testing.

For the *sensitive information retrieval*, the participants were asked to input a diverse set of sensitive information, including a PIN on the numeric keyboard. The official default interfaces are utilized here (e.g., system login), where only a certain region (system default size) is changed along with the input while other areas stay unaltered. For example, in *S2A: Password Length*, the font of a character is 10pt; in *S2E: Password*, the size of a virtual button is 70×50 pixels. For every piece of sensitive information listed above on each device, we collect more than 21,000 traces beforehand to train a DNN model. Notedly, the other 1,000 traces of data are utilized for the testing set.

4.5.2.2 Metrics

We employ **`Top-`**k ($k = 1$, 2 and 3) inference accuracy as the primary performance metric, which implies the candidates with top k possibilities. Specifically, the system generates a set of ranked candidates (i.e., PINs, lock patterns, or letters) for each trial. We claim that a trial succeeds if the true input appears in the Top-k candidates. Top-k inference accuracy is defined as the percentage of successful trials. Furthermore, to evaluate the picture password, we utilize *Distance Estimation Error (mm)* to measure the estimation error of the tapped position on the screen.

4.6 Evaluation I: A Control Study

In this section, we perform a control study to validate the legitimacy of our proposed system design under the ideal environmental condition.

4.6.1 The Performance of Screen Content Type Recognition

The performance of WaveSpy depends on the design of recognition approaches. To investigate the sensitivity of classification model and verify the capability our selected features, we perform a multi-level detail part (mentioned in Section 4.4.4) analysis, denoted as L1, L2 and L3, towards two mostly used classification configurations, i.e., SVM and KNN. The data are acquired from the database, hereafter Data Collection, built using our sensing system.

With respect to Top-3 inference, SVM achieves an accuracy of 90.71%, 94.13%, and 99.13% for L1, L2 and L3 schemes respectively. Correspondingly, KNN achieves 78.19%, 87.89%, and 93.98% for the three schemes as shown in Figure 4.12. The satisfactory performance on both classifiers indicates the effectiveness of our feature vector (see **`Definition 2`**) in reflecting the unique and salient characteristics of *LCS responses*, while the performance of SVM is superior compared to KNN for this application. It is worth mentioning that during the acquisition of traces, the content on the screen is not static because of several factors in the screen corner (e.g., UI animation, advertisements or updated news), which also increases the difficulty of this task. Against the original belief that this may severely interfere with recognition performance, WaveSpy maintains high inference accuracy, implying that the general layout (or template) of the application is static and unique.

4.6.2 The Performance of Sensitive Information Retrieval

To maximize the efficiency of WaveSpy in retrieving the sensitive information, the attacker may know the security mechanism employed by the victim on his electronic device prior to performing an attack. However, due to the increasing growth of smart devices supporting multiple login mechanisms, it would be ideal for the attacker if WaveSpy system can precisely retrieve the victim's input regardless of its length or type. While ensuring that all the credentials were only known by the participants, we

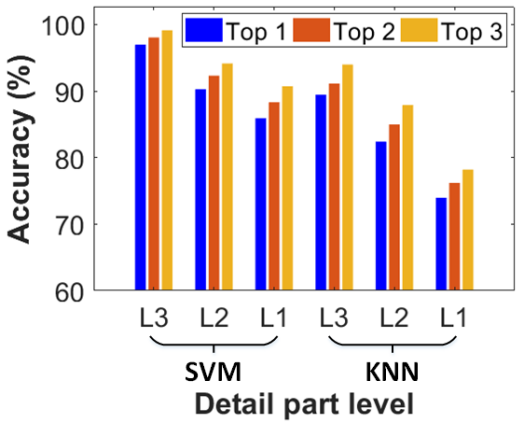


Figure 4.12: The overall performance for screen content type recognition (Scenario 1) with three different detail parts and two common classifiers.

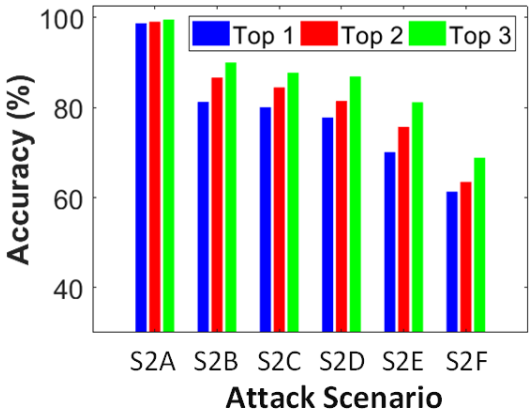


Figure 4.13: The overall performance of the sensitive information retrieval in six types of login information (S2A∼F described in Section 4.6.2).

investigate the realism of our attack model for three login methods and illustrate the results in Figure 4.13.

4.6.2.1 Overall Performance of Login Attack on Physical Button

This login usually has two aspects sorted by the information type.

S2A: Password Length: Each participant was asked to input the password on the system login of MacBook Pro. Notably, the resulting text on the screen is only shown as an asterisk character. Thus, this attack aims to evaluate the performance of WaveSpy in detecting the password length. The length of the password is within a typical range of 1 to 16 [87]. Our results demonstrate that WaveSpy can precisely infer the password length with an average Top-1, Top-2, Top-3 accuracy up to 98.73%, 99.09%, and 99.56%, respectively, leading to a drastic reduction in the recognition period for the key information. Moreover, we also can recover keystroke timings, that contains substantial information about the password being typed, by continually recording the change of the typed password length and the accuracy for the keystroke timing inference is 99.96%.

S2B: Numeric Password: We instruct the participants to press the respective key on the numeric keyboard (i.e., 0-9) of a security intercom system, where the resulting 4-digit

password is shown on the screen. In this attack, every password was input ten times. As observed in Figure 4.13, the average Top-1, Top-2 and Top-3 inference accuracy for the numeric password reaches up to 81.27%, 86.86%, and 90.03%, which significantly reduces the numeric password entropy, further discussed in Section 3.8.

4.6.2.2 Overall Performance of Login Attack on Virtual Button

The information from virtual button can be represented in three subtypes as follows.

S2C: PIN: A four-digit PIN was fed by each participant for ten times to the PIN keyboard of iPhone 7 Plus. The average inference accuracy of Top-1, Top-2 and Top-3 is up to 80.09%, 84.49%, and 87.77%, respectively. A typical mispredicted example is the PIN '1258' is wrongly considered as '1268'. The reason is that the '6' button is near to '5', causing the similar *LCS response*. A similar phenomenon can be observed in S2D and S2E. Upon careful analysis, we examine that the performance of this attack is inferior compared to the numeric password (S2B), due to the smaller display area (see Section 4.2.2) of the digital screen, which influences the characteristics of the received *LCS response*.

S2D: Pattern Lock: Each participant was required to draw 10 lock patterns on the pattern-lock keyboard of Nexus 5. The length of the lock pattern ranges from 1 to 6 units. For this attack, the average Top-1, Top-2 and Top-3 inference accuracy reaches to 77.81%, 81.49%, and 86.93%, respectively. The inference accuracy is slightly lower compared to previous four-digit PINs, as the UI correspondence of pattern locks changes little, increasing the challenge for WaveSpy to retrieve the sensitive information.

S2E: Password: A password generally comprises 26 letters and ten single-digit numbers. The participants were required to type on the alphabetical keyboard of MSI GL62. The length of the input varies from 1 to 8 characters. WaveSpy can infer passwords with the average Top-1, Top-2, Top-3 accuracy up to 70.12%, 75.72%, and 81.19%, respectively. In contrast to the PIN (S2C) and pattern lock (S2D), the password comprises numerous combinations of letters and numbers while having a longer character length,

which affects the system performance. However, the observed accuracy is still within an acceptable range considering that the attacker can utilize other learning techniques to guess the misclassified characters.

4.6.2.3 Overall Performance of Login Attack on Picture Password

For the attack on **S2F: picture password**, every participant clicked the specific locations on the digital screen of Dell U2415 using a cursor. The Top-1, Top-2 and Top-3 accuracy is 61.31%, 63.49%, and 68.86%, respectively. For more than 40% retrieval taps, the distance estimation error is less than $5mm$ (1.9% of the screen side length), which is within the UI correspondence area. Lower performance is observed due to the miniature radius of UI correspondence (i.e., $6mm$) and a high tolerance of the password mechanism, which provides the users more freedom in selecting the specific location on the screen as an input.

In conclusion, our results demonstrate the effectiveness of WaveSpy to facilitate screen content type recognition and sensitive information retrieval under ideal conditions. We further explore the system performance against varying sensing parameters and real-world scenarios in the remaining sections.

4.7 Evaluation II: Robustness Investigation

4.7.1 Impact of Sensing Distance and Device Orientation

In practical scenarios, the attacker should be able to keep a certain distance or an angle to avoid being discovered. Such a convenient practice, however, will lead to the changing distance and orientation between the screen and the mmWave probe. Therefore, it is important to investigate whether these aspects will affect system performance. Specifically, we measure the different device orientations (from 0° to 40°) at different distances (from $20cm$ to $180cm$). Following Section 4.5.2, we recollect the training and testing set. Three participants select 100 screen content types at a random sequence shown on

the Dell U2415. The results are shown in Figure 4.14. The average Top-3 inference accuracy remains high when the sensing distance varies within $180cm$ (above 99.5%). As for the orientation, although the reflected signal slightly changes due to the different probe angles for each content type, the inter-type distinguishability among 100 screen content types is significant such that each device can be correctly recognized. Thereby, WaveSpy can facilitate portable and convenient screen attack in real practice.

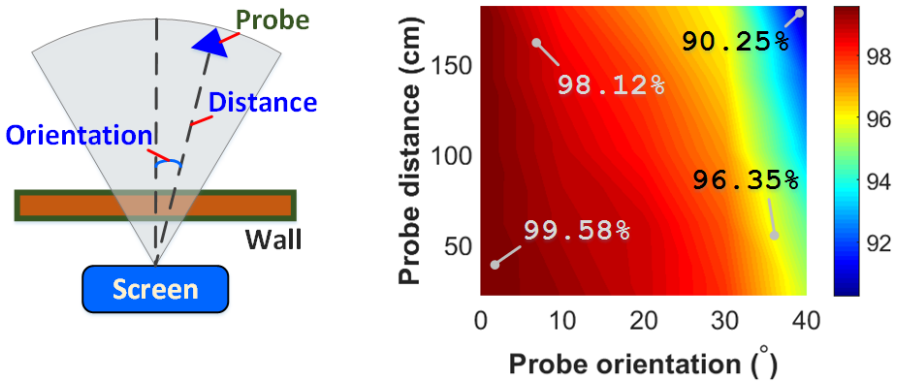


Figure 4.14: The attack accuracy according to sensing distance (from $20cm$ to $180cm$) and device orientation (from $0°$ to $40°$) keeps over 90.25%.

4.7.2 Impact of Display Resolution

The display resolution is a crucial consideration in a real application, which is related to the screen type. Specifically, we recruit five different screens with four different display resolutions between 800×600 (VGA) to 3840×2160 (4K) pixels. For each resolution setting, we evaluate the screen content type inference following the preparation in Section 4.5.2 and re-prepare the training and testing sets. Figure 4.15 manifests that their performance of average Top-3 accuracy can achieve up to 99.52%. Besides, the identification results all remain above 99.4%. Hence, WaveSpy can maintain a high success rate in attacking screens under different display resolution setups.

4.7.3 Impact of Screen Model

Due to the fact that many attacks rely on the screen model, we simulate a scenario where the attacker lacks this prior knowledge. In this section, we evaluate the attack performance under the impact of the screen model to verify the training data generalization. To address this concern, we employ four devices for testing, including iPhone 6, iPhone 6s, Pixel 2 and MacBook Pro. We repeat the experiment of the screen content type inference (as described in Section 4.5.2). Importantly, we still use the previous training data from iPhone 6. Notably, there are two iPhone 6 here, one for training, one for testing. As shown in Figure 4.16, the testing results illustrate the inference accuracy. We observe that the average Top-3 accuracy on iPhone 6 and iPhone 6s are the highest, 99.18% and 97.03% respectively, while others are both below 10%. The reason is that the tested iPhone 6 and iPhone 6s have an equal or similar hardware structure with the training device, which are entirely different from others. Moreover, the comparable accuracy on iPhone 6s testing indicates that our trained classifier does not have the over-fitting issue and can adapt to various usage scenarios. To sum up, results indicate that WaveSpy can work across different screens with the same or similar hardware structures (see a further discussion in Section 3.8).

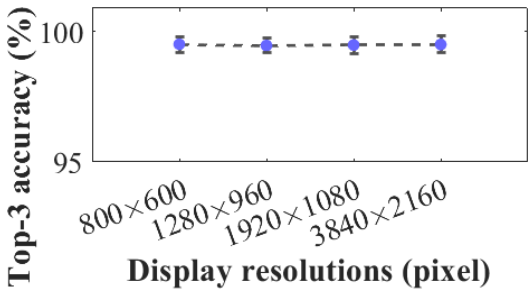


Figure 4.15: Inference performance under different display resolutions.

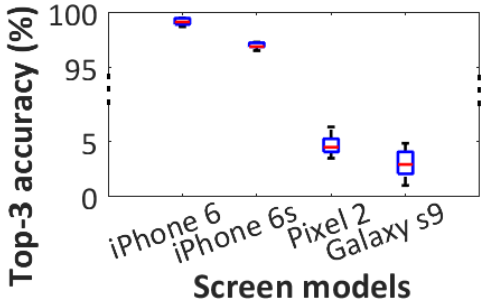


Figure 4.16: Inference performance under different screen models.

4.7.4 Impact of Cover Material

We consider the scenario where the user hides the screen in other materials to evade attacks. Particularly, we collect five different daily-accessible materials (i.e., brick, glass, plastic, wood, curtain, cardboard). We place the screen behind each of them and evaluate the screen content type inference accuracy for all nine monitors. The performance is reported in Figure 4.17, where we can see that the overall accuracy for each is above 98%. Certain materials slightly affect the performance to some extent. This is because WaveSpy utilizes a high-frequency signal and therefore has a small wavelength and limited penetration ability. As a result, it is prone to the scattering reflection upon some specific materials. Generally, WaveSpy still provides reliable performance in screen content type recognition.

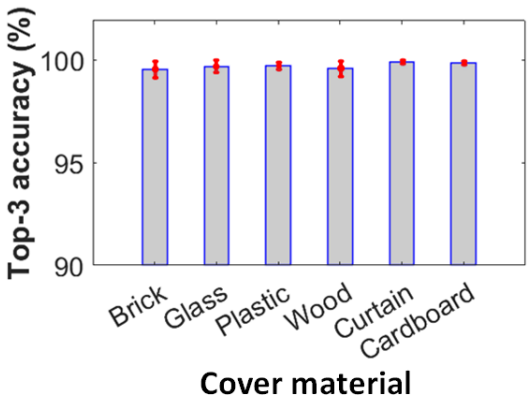


Figure 4.17: Evaluation to determine the influence of cover material on the screen content type recognition.

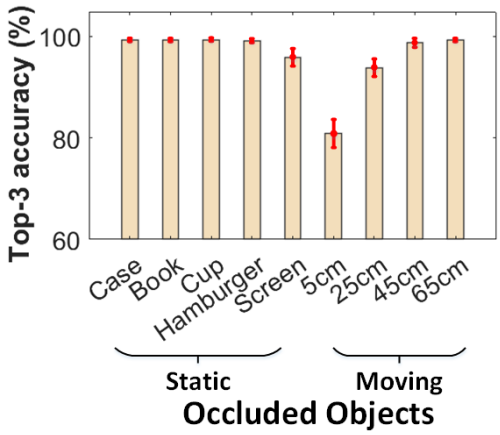


Figure 4.18: The system performance for screen content type recognition under the influence of different surrounding objects.

4.7.5 Impact of Occluded Objects

In this experiment, we investigate the influence of the *static and moving* surrounding objects that affect the mmWave signals on the inference accuracy of screen content type. For *static objects*, we select device case, book, cup, hamburger, and an extra screen. For

moving objects, we perform this experiment with two participants, i.e., a participant selects the screen content while another participant is moving with the same normal walking speed as the surrounding object at different distances away from the screen.

For *static objects*, the performance is reported in Figure 4.18, where we can see that the overall accuracy for each is above 98%, implying these surrounding objects have a limited effect on the performance. For *moving objects*, we can observe that the surrounding moving objects obviously affect the inference accuracy, but, the effect decreases as the distance increases. When the distance between the object and the screen exceeds $45cm$, the influence of surrounding objects becomes negligible. This is because the mmWave wave has a high directionality and controlled sensing angle, decaying exponentially with respect to distance from the screen to the surrounding objects. This experimental result demonstrates that it is not easy to disrupt WaveSpy using surrounding objects.

4.7.6 Impact of Open World Scenarios

In real practice, the attacker may also aim to extract text from the screen. By referring to a recently publish work on screen attack [96], we conduct an experiment on Dell U2415 under the open-world setting to verify whether we can extract content from the screen. We collect 30 paragraphs and each paragraph contains at least 60 words. In trace, each character lasts 0.5s, typed on the virtual keyboard. Following Section 4.5.2, we recollect the training and testing set. The results present the average Top-3 accuracy for word inference is 81.3%. For example, the word ”implicitly“ is incorrectly recognized as ”inplicitly“. Similar analysis is further discussed in Section 4.8. This performance can further improve by coordinating with the dictionary [70]. This experimental result demonstrates that WaveSpy can perform the screen attack under different open world setups.

4.8 Evaluation III: Real-world Screen Attacks

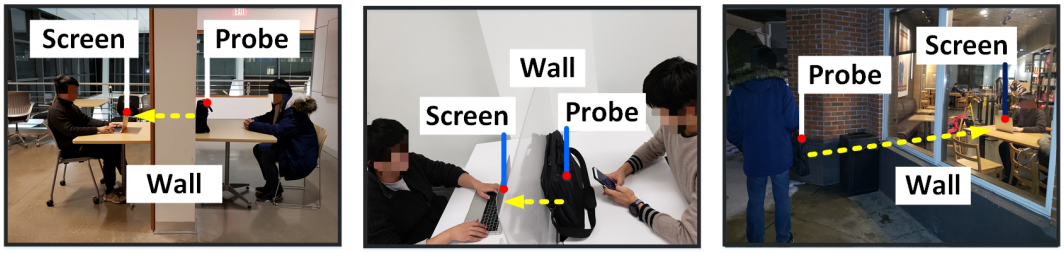


Figure 4.19: The carry on attacks are conducted in three locations, i.e., hall, office and cafeteria on the Macbook Pro. The probe is hidden in a normal handbag arousing no suspicion to victim and nearby surrounding.

Experimental Setup: Due to the portability and low cost of the setup, eavesdroppers can access a target screen used in public spaces. Therefore, we conduct a real-world screen attack. The studied sites involve three common locations in daily life (i.e., offices, hall and cafeteria) as shown in Figure 4.19. For each site, the participants were instructed to use the digital screen placed behind the wall or obstacle. The content type and the sensitive information are displayed on the screen at a default font (i.e., 9-12pt). It is important to note that these sites are different from the environments described in Section 4.3.2 where we collected the prior data and characterized the *LCS response*.

Evaluation Results: Table 4.2 shows case studies for four attack trials on the screen content type recognition and sensitive information retrieval, including their corresponding ground truths. We can see that, in MS Word types, it was wrongly recognized as MS Visio at the cafeteria location. The reason is that these two types have a considerably similar layout, confusing the classifier. The password mistake happens at the cafeteria, where recognizes the 'c' into 'v'. It is because these two characters have adjacent locations on the screen, leading to similar *LCS responses*. Although in the sentence retrieval, the results are not as good as a PIN, it still shows a huge potential for the sensitive sentence or content eavesdropping. Besides, we also conduct a sustained attack on the screen content type recognition, in an attempt to acquire the user activities usage

Table 4.2: Error Examples of the real-world attack at three different locations against the ground truth.

Attack Scenario	Attack Results on Different Locations			**Ground Truth**
	Hall	**Office**	**Cafeteria**	
#1	MS Word	MS Word	MS Visio	MS Word
#2	a1b2c3	a1b2c3	a1b2v3	a1b2c3
#2	Good Night	Good Night	Good Nitht	Good Night
	Have A mice Day	Have A Nict Day	Habe A Nocw Day	Have A Nice Day

statistics. The usage statistics analysis for three hours at the office location with Top-1 accuracy is shown in Figure 4.20. Note that our WaveSpy can be applied to monitor the user activities for a long time with high inference accuracy 96.2%. Though some performances appear lower than those of the above performance, we can improve them by adjusting the characteristics of the antenna according to the screen position. In contrast, if eavesdroppers identify the screen to be attacked in advance, they can optimize their setup according to profiling results. Moreover, an optimized antenna makes the maximum stealing distance much longer. Thus, the result suggests that our system provides reliable performance in real practice.

4.9 Countermeasures

Creating a large isolation zone (e.g., over ten thousands of square feet) is effective to defend most of the screen attacks, including WaveSpy. However, it is not practical (e.g., cost and usability) in real-world scenarios. In this section, we will discuss two sets of practical countermeasures against the WaveSpy attack. The first countermeasure set is cost-effective, altering either hardware or user behavior to mitigate the security risk.

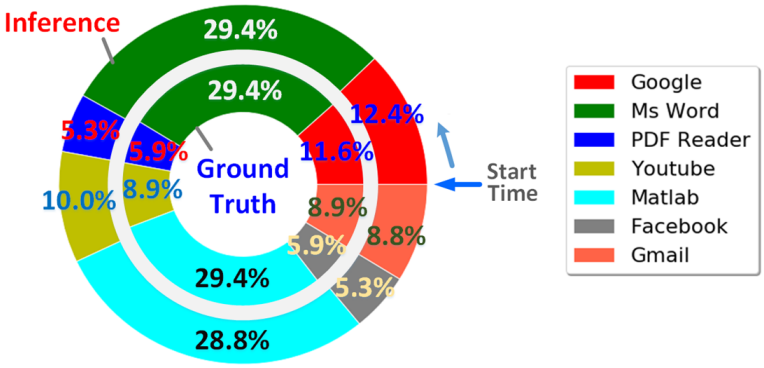


Figure 4.20: Usage statistic analysis of on-screen content type recognition for 3 hours at an office location. The inner loop indicates the ground truth while the outer loop demonstrates the usage statistics inferred from WaveSpy.

The second countermeasure set is zero-cost, a purely software-based solution with no hardware or user cooperation requirement.

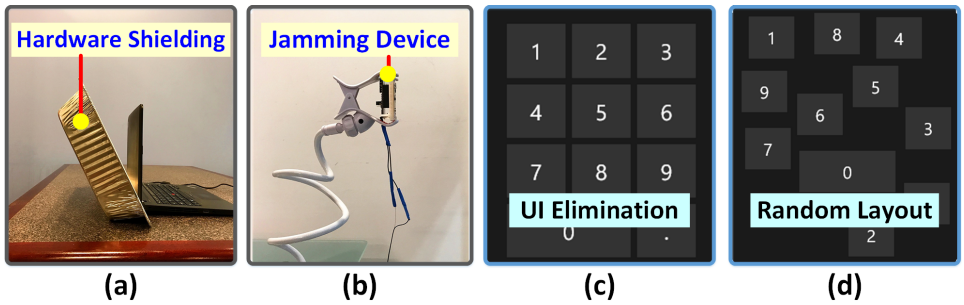
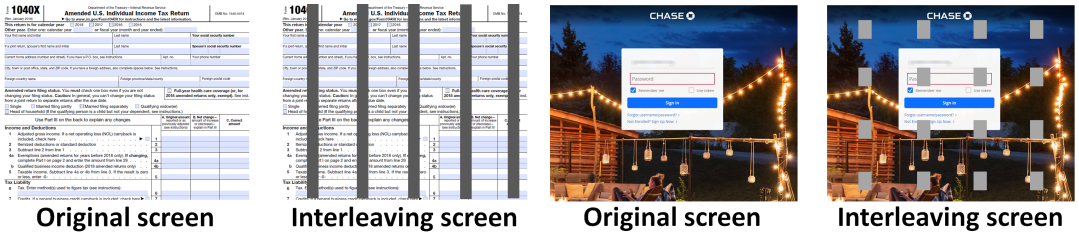


Figure 4.21: Examples of countermeasure solutions: (a) conductive hardware shielding; (b) side-channel inference with a jamming device; (c) corresponding UI elimination towards button touch; (d) randomized keyboard layout.

Cost-effective Approaches: To counter the attack, we introduce a cost-effective solution set including four protection strategies in Figure 4.21. In general, we explore the mmWave signal transmission drawback, and thus a shielding technique is proposed to isolate electrical devices from the "outside world" as shown in Figure 4.21(a). However, if the shield covers the full display surface, the usability of the screen drops significantly. Besides, deploying the shield needs extra human labor and increases the cost. Another possible way to avoid the attack from the mmWave is to make use of the receiving channel limitations. We employ a wireless jamming device that continuously transmits

noise signals to block the probe receiving channel as shown in Figure 4.21(b). Yet, in real practice, such an approach is hard to achieve, since the jamming device needs to know the attack frequency in advance. In addition, a straightforward countermeasure is to focus on the *LCS response* inhibition. We automatically prevent the usage of the UI reminder when inputting sensitive information, i.e., making no change on the screen, as shown in Figure 4.21(c). Also, another sophisticated defense exploits the same principle, which is to randomize the layouts of the keyboard grid as shown in Figure 4.21(d). However, both countermeasures can dramatically decrease the user experience.



(a) Tax return form (b) Credit card login

Figure 4.22: Two examples of the countermeasures with the interleaving screen.

Zero-cost Approach: Defense approaches above require either additional hardware or user behavior changes. In this part, we investigate a novel defense approach with zero cost, namely high-frequency interleaving screen. This approach exploits the display mechanism and leverages the RF probe sensing limitation. As indicated in Section 4.6, the least *LCS response* duration for attacking lasts from 40 to $100ms$, equal to 10-25Hz, while at the same time, the refresh rate on modern display is usual higher than $60Hz$. Since screen refresh rate is higher than probe sensing frame rate, we can scribble multiple frames (e.g., adding full-screen flicker marks) within the frame periods to deter attacking, while preserving viewing experience by taking advantage of human eyes' flicker fusion effects [253, 258]. Two examples of flicker marks are illustrated in Figure 4.22. We recollect 20 screen content types with the flicker makers as the testing data, combined with the training data in Section 4.5.2. The results with the flicker mark demonstrate the average Top-3 accuracy of 3.7%, which confirms the feasibility of this protection.

4.10 Related Work

Electronic Device Emanations: The electronic device functioning of various state-of-the-art sensors leaks critical information that can be acquired to infer application usage and screen activity. Previously, researchers have explored the threat of keystroke inference attacks based on observing the motion [56] or multiple sensor data in the device [149, 155, 156, 161, 248] and tablet backside motion patterns through vision-based monitoring [174, 214, 252]. Given the adversary has access to the target electronic device, the smudges on the screen can be investigated to construct critical information about recent user activity [51]. However, these attacking solutions cannot work in our attack model without line-of-sight. The intensity of light emitted from the cathode-ray tube (CRT) displays can be analyzed to reconstruct the text information shown on the display; however, it is only feasible in dark environments without the interference from other lighting sources [131]. Furthermore, the digital screens leak electromagnetic (EM) or other emanations that can be exploited by an adversary to steal the information displayed on the screen or from a login [87, 96, 109, 137, 257]. However, this type of attack highly depends on the power supply of the screen. Along with the power management development, there is a visible trend that the low-cost technology will be widely deployed in most screens, and thus the scaling of these emanations decrease dramatically making emanation-based attacks fail. In addition, in EM strategy, the attacker must be extremely close to the victim screen and acoustic-based solutions require no occlusion or obstacle, which hardly work under the setting of this chapter. Besides, it is worth mentioning that although some EM-based attacks have tried to visualize the results by combining the predicted results with the pre-capture screen image [109], the feasibility of the remote image visualization rests on the assumption that the attacker gets the pre-capture screen image of the victim, which is not the real image reconstruction. As aforementioned, these attacking strategies cannot work under the setting in this study.

Compromising Reflections: The sensitive information displayed on the digital screens to the user cannot be extracted from only be device side-channels, but also the screen's

optical emanations on nearby objects. A novel screen-based attack was presented which exploits the comprising reflections on the objects (e.g., eyeglasses, teapots) that are in proximity to the screen posing a significant threat to the privacy of the information displayed on the screen [53]. Even the diffused reflections from a wall or shirt can be employed from the reconstruction of the projected image using a digital camera [52]. Another form of compromising reflections can be obtained by tracking the diverging positions of victim's fingers during typing while they are reflected from proximity objects or even obtainable from long-distance view [48, 70, 194, 246]. All the work above is ineffective in our attack model.

Remote mmWave Sensing: In the last decade, mmWave radars have been extensively employed in both research and practice to detect the target's inherent motion (e.g., cardiorespiratory and gesture sensing [115, 144, 145]) for vital signs monitoring and user authentication. Studies have demonstrated the feasibility of remotely detecting the hand motions and physiological features, such as heart rate and breathing patterns [143, 167]. However, given that the underlying characteristics of the mentioned applications rely on Doppler motion, they cannot be directly applied to sense through the target or other obstacles (e.g., packages and luggage). While some researchers [47, 238, 259] explore the propagation of the mmWave through-wall and through-objects, the systems are still inapplicable for a target with specific mmWave-absorption characteristics. To the best of our knowledge, the proposed WaveSpy is the first non-contact mmWave sensing application that aims to exploit the *LCS response* to achieve the screen attack through the occlusion.

4.11 Conclusion

In this chapter, we first identified and validated a new and yet practical side-channel to infer contents on digital screens via the liquid crystal nematic state sensing in isolation scenarios. We started from the basic functioning mechanism and LC nonlinear effect in digital screens on the personal device and analyzed the *LCS response*. Then, we de-

signed a portable, low-cost, and energy-efficient 24GHz mmWave probe and proposed a novel end-to-end deep learning-based hierarchal module to recognize the screen content type and retrieve the sensitive information on digital screens. Furthermore, extensive experiments indicated that the proposed WaveSpy achieves more than 99% inference accuracy through-wall within $5m$ distance with a centimeter-level screen solution. The Top-3 sensitive information retrieval rate of the proposed WaveSpy is up to 87.77%. Various levels of evaluation proved the robustness, reliability, and efficiency of our proposed WaveSpy. Finally, we recommend that privacy-sensitive systems should pay considerable attention to this new side-channel and increase the screen security (e.g., flicker mark).

Chapter 5

FerroTag: A Paper-based mmWave-Scannable Tagging Infrastructure

5.1 Introduction

An impressive amount of capital in the U.S., about 1.1 trillion dollars in cash which are equivalent to 7% of the entire U.S. GDP, is tightly associated with inventories [3]. As a result, inventory management (i.e., the supervisory mechanism for tracking the flow of goods from manufacturers to warehouses and from storage to the point of sale) has become a critical component in the whole commercialized business. According to the newest 2019 report from Statista [36], business respondents, who are all manufacturers and retailers, rated warehouse management as the most important business investment in 2017 as 90% of the inventory are stationary (e.g., stored in warehouses) [35]. The reports also indicate that most companies are willing to upgrade the current existing inventory management systems to further promote efficiency in daily routines and manage business growth [104].

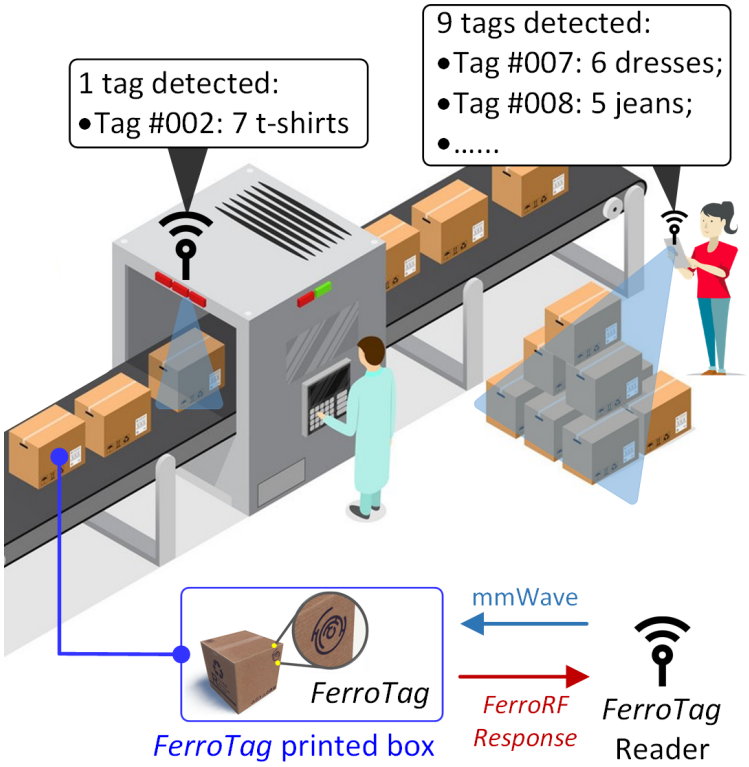


Figure 5.1: FerroTag, a paper-based mmWave-scannable tagging infrastructure, can replace the traditional tagging technologies for mass product counting and identification in inventory management.

Currently, there are two types of tagging technologies employed in most existing inventory management systems, i.e., barcode and radio-frequency identification (RFID) [37]. Barcode is a printed patternized identity which is read by a laser scanner [27]. However, since barcode technology relies on invisible/visible light (i.e., a medium can hardly travel through obstacles) for information acquisition, the scanner must align with the barcode in line-of-sight to recognize the identity [196]. In addition, ordinal scanners limit to processing one barcode at a time [69]. Different from the printable barcode, an RFID is an electronics consisting of a circuit and an antenna, which encodes and transmits the data/identity in RF wave (i.e., a medium can pass through barriers) [92]. Although RFID has the advantage over the barcode in terms of scanning efficiency, there is a significant hindrance causing the financial and environmental costs. One RFID tag costs from $0.18 - 30$ US dollars [6, 38]. Moreover, RFID tags cannot be naturally

degraded after use and become a kind of e-waste in most cases [176]. Giving the fact that the inventory system is essential for business growth, there is an urgent need to develop a better paradigm for tagging technologies.

In this chapter, we introduce FerroTag as an advanced tagging infrastructure to promote inventory management system, i.e., a critical part in the modern commercialized business. In particular, FerroTag is featured as **(1) Ultra-low cost:** the tag is highly affordable for large scale deployment; **(2) Environment-friendly:** the tag is based on ordinal papers and with non-toxic inks, which are safely disposable and naturally degradable; **(3) Battery-free:** the tag is completely passive requiring no power supply; **(4) In-situ:** multiple tags are accurately read by a scanner outside the line-of-sight. As shown in Figure 5.1, the application scenes of FerroTag include manufacturing factories, warehouses, and retail offices.

Specifically, FerroTag is a paper-based mmWave-scannable tagging infrastructure. A pattern printed by naturally degradable ink is served as an identity [185]. Thus, it is highly economical, environmentally harmless, and fully passive in its origin. In order to realize FerroTag, we need to address two technical challenges in this work: *(a) design and implement a paper-based mmWave-scannable tagging infrastructure for the inventory management system.* The foundation of FerroTag rests on the *FerroRF* effects. When RF signals meet surfaces and objects, a responsive RF signal will be generated [232]. In our application, when there is an RF signal passing through, a ferrofluidic ink print will generate a recognizable response (hereafter, the *FerroRF* response) which is associated with the ferrofluidic print pattern (i.e., the tag identity). To retrieve and recognize the identity, a fine-grained response analysis protocol is developed. First of all, to protect the *FerroRF* response from distortions, a range resolution analysis and an envelope correlation function are applied. Secondly, we extract a set of critical scalar features (n = 25), including ten most impactful ones based on Mel-frequency Cepstral Coefficients. In the end, the selected features are fed into a classifier containing a cluster of decision trees (m = 150) for identification. In addition, by analyzing the angle

of arrival, multiple tags can be simultaneously detected and identified. *(b) Model and optimization of the FerroRF effects for high capacity.* We first investigate and establish a mathematical model of the *FerroRF* effects. The *FerroRF* response is generated by the magnetic nanoparticles within the ferrofluidic ink. Since the quantity and the arrangement (i.e., three-dimensional locations) of particles are varying along with any variation in a ferrofluidic ink printed pattern, a unique pattern can be served as a non-contact retrievable identity as it can generate a unique *FerroRF* response. Secondly, with the in-depth modeling and understanding of the *FerroRF* effects and response, we study a systematic approach to optimize the variation of the *FerroRF* effects by designate tag patterns such that it contains only succinct geometric features but can be used to room high-capacity identities in the tagging infrastructure. More specifically, we investigate and evaluate an innovative nested pattern for tagging design in FerroTag, which can provide a large number of identities with regulations to a vast amount of products in inventories.

5.2 Background and Preliminaries

5.2.1 *FerroRF* Effects

Ferrofluidic ink is colloidal liquids, whose core components are magnetic nanoparticles (e.g., ferrite compound-Magnetite powder), carrier fluid that suspends the nanoparticles (e.g., organic solvent), and the surfactant that coats each magnetic nano-particles [230]. The quantity and the arrangement of these magnetic nanoparticles reflect into the unique characteristic frequency responses when tags are probed by broadband radio frequency (RF) signals as shown in Figure 5.2. When a fundamental tone is passed through the ferrofluidic ink, magnetic nanoparticles modulate the response signal and generate additional frequency tones besides the fundamental one as formulated in Section 5.2.2.

mmWave is an emerging technology (e.g., 5G network) and it is worth to mention that object (e.g., tags) presence detection, tracking and localization through mmWave

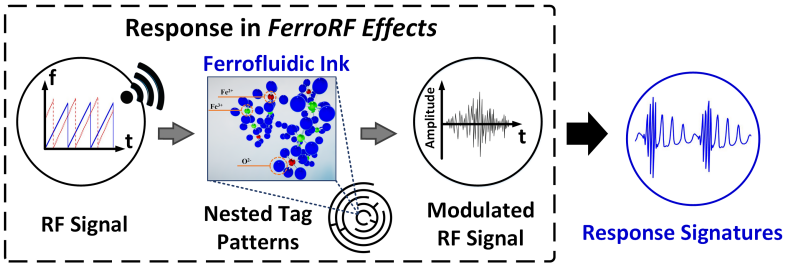


Figure 5.2: The ferrofluidic pattern generates a *FerroRF* response under the RF beam. The *FerroRF* response is associated with intrinsic physical characteristics of tag pattern.

signals are intensively studied in the past years [64, 225, 239, 242, 255]. In contrast to other RF sensing modalities such as WiFi [233] and acoustics [159], mmWave has an excellent performance in term of the directionality and owns the superiority in high tolerance to ambient noises (e.g., sound, light, and temperature) and less surface scattering. Furthermore, mmWave facilitates a micron-level shape change resolution making it feasible to monitor the pattern shape change, which in case of shape size occurs at the range of 2-3mm [202]. Considering that mmWave is becoming the key carrier in the next-generation wireless communication, we will investigate the *FerroRF* effects under the applications of mmWave signals.

Hypothesis: It is indeed the *FerroRF* response (i.e., harmonics or inter-modulation) that contains the unique characteristics of the tag, which can be treated as an intrinsic and persistent identity of the tag. Different geometric shapes and sizes of ink patterns on tags can be meticulously designed; these discrepancies are sufficient to alter the frequency responses and induce unique, measurable fingerprints which associate with the ink patterns. *Therefore, it is possible to utilize a mmWave probe to force tags to radiate the response signature that reflects their unique properties and can be used for object counting and identification.*

5.2.2 Modeling on *FerroRF* Effects

In this part, we further explore the *FerroRF* effects. Before completely understanding the tag modulation on the response signal, it is crucial to model the *FerroRF* effects.

When a fundamental tone is passed through the tags, the ferrofluidic patterns modulate the response signal and generate additional frequency tones besides the fundamental one as formulated in Equation (5.1):

$$r(f,\tau,t) = R_{f,t}(\tau) \bigotimes h_f(t), \tag{5.1}$$

where $r(f,\tau,t)$ is the signal modulation function of ferrofluidic due to the stimulation of millimeter wave [223]. $R_{f,t}(\tau)$ is the signal reflection function based on: τ-volume makeup of ferrofluidic, f-range of frequency, and t-time instant. $\bigotimes$ stands for convolution computing and $\mathrm{h}_{\boldsymbol{f}}$ (t) is the ideal band-pass filter function for the carrier bandwidth [141]. In the following equations, we model the relation between τ-volume makeup of ferrofluidic and signal modulation function, in which the volume makeup, consisting of three dimensions, is the geometric pattern that can be manipulated with tag pattern design.

$$\begin{cases} R_{f,t}(\tau) = \dfrac{R_{f,t}(\tau)_1}{R_{f,t}(\tau)_2}, \\ R_{f,t}(\tau)_1 = exp(2\gamma_d(\tau)L)(\gamma_d(\tau) - \gamma_0(\tau))(\gamma(\tau) + \\ \qquad \gamma_d(\tau)) + (\gamma_0(\tau) + \gamma_d(\tau))(\gamma(\tau) - \gamma_d(\tau)), \\ R_{f,t}(\tau)_2 = -exp(2\gamma_d(\tau)L)(\gamma_d(\tau) + \gamma(\tau))(\gamma_0(\tau) + \\ \qquad \gamma_d(\tau)) + (\gamma_0(\tau) - \gamma_d(\tau))(\gamma(\tau) - \gamma_d(\tau)), \\ \gamma^2(\tau) = \dfrac{\pi^2}{a^2} - \omega^2\epsilon_0\mu_0\epsilon\mu^*(\tau), \end{cases} \tag{5.2}$$

$R_{f,t}(\tau)$ has two parts in the mathematical presentation. γ_0 and γ are the propagation constants in the empty and ferrofluidic parts of the wave-guide, respectively; γ_d is the propagation constant of the wave in the dielectric. L is the thickness of dielectric insertion. d represents the diameter of the ferromagnetic particles; a is the size of the wide wall of the wave-guide; π is the ratio of a circle's circumference to its diameter. ϵ_0 and μ_0 are the electric and magnetic constants, respectively; ϵ and μ^* are the permittivity and the permeability of the medium that fills the wave-guide cross section, in which ferrofluidic presents, respectively. This shows the relationship between ferrofluidic's

permeability of millimeter wave and and the volume makeup, which we further model with Equation 5.3.

$$\begin{cases} \mu^* = 1 + \chi_m{}'(\tau) - j\chi_m{}''(\tau), \\ \chi_m{}'(\tau) = \dfrac{\gamma\tau ML(\sigma)}{\omega H_n} \dfrac{(1+\eta^2)^2 {H_n}^4 + (\eta^2-1){H_n}^2}{(1+\eta^2)^2 {H_n}^4 + 2(\eta^2-1){H_n}^2 + 1}, \\ \chi_m{}''(\tau) = \dfrac{\gamma\tau ML(\sigma)}{\omega H_n} \dfrac{\eta {H_n}^2 (1 + {H_n}^2(1+\eta^2))}{(1+\eta^2)^2 {H_n}^4 + 2(\eta^2-1){H_n}^2 + 1}, \end{cases} \tag{5.3}$$

where τ is the volume makeup of ferrofluid which is manipulated with our tag design, as shown in Figure 5.3. $\chi_m{}'$ and $\chi_m{}''$ are the real and imaginary parts of the magnetic susceptibility, respectively [223]. H_n is the reduced magnetic field $\eta = \xi(\frac{1}{L(\sigma)} - \frac{1}{\sigma})$; $\mathrm{H}_n = \gamma\frac{H}{\omega}$; $\sigma = \frac{\mu_0 M_d V}{kT} H$, σ is a combined parameter of the magnetic fluid; M_d is a saturation magnetization of the solid magnetic. $V = \frac{\pi d^3}{6}$ is the volume of a ferromagnetic particle; ξ is the damping constant of the electromagnetic wave in the magnetic fluid; For spherical ferromagnetic particles, it is assumed that the dielectric properties of the magnetic fluid are independent of the magnetic field [223, 224]. To summarize the foregoing exploration, *the FerroRF response can be affected by adjusting the ferrofluidic ink pattern shape and size*.

5.2.3 The *FerroRF* Effects on Tags

Proof-of-concept: To gain evidence on the validation of the *Hypothesis*, we conducted a preliminary experiment using 6 different tags with different patterns. Each tag pattern is attached to the right in Figure 5.3. These tag patterns are made by ferrofluidic ink with a regular copy paper following the Arabic numerals shapes of 1 to 6, which are different from aspects of the size and the shape. Six different tags are stimulated with the mmWave probe with a distance from the devices. The reflected signal profile is explored in the spectrum domain. As shown in the range frequency spectrum graph (see Figure 5.3), the x-axis is the frequency, and the y-axis is the amplitude of the received signal. The various sub-carrier frequencies can be clearly observed that, separated from

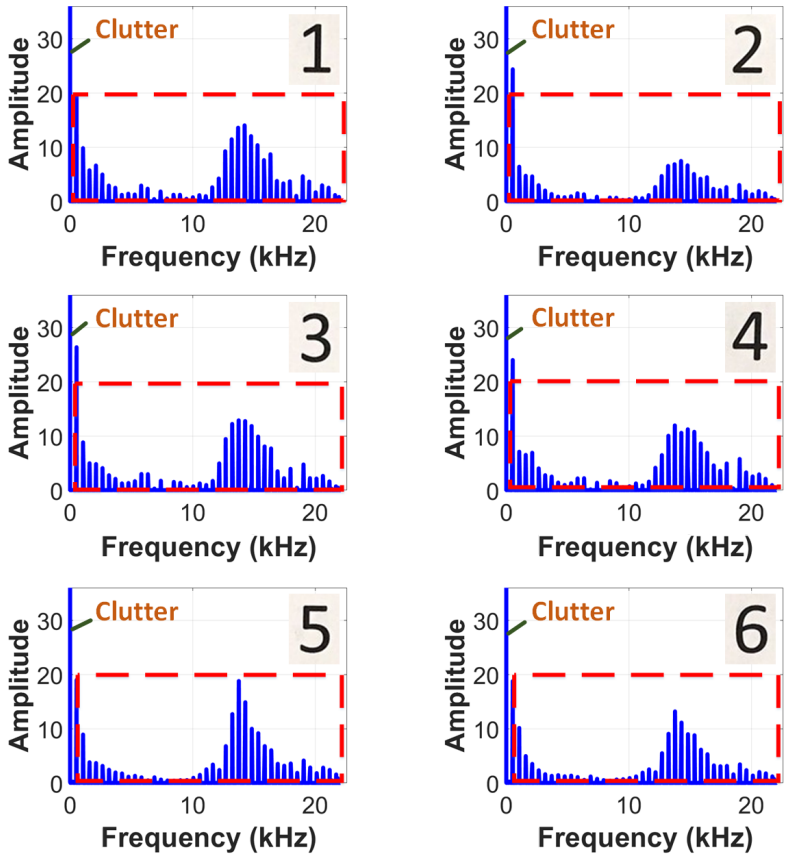
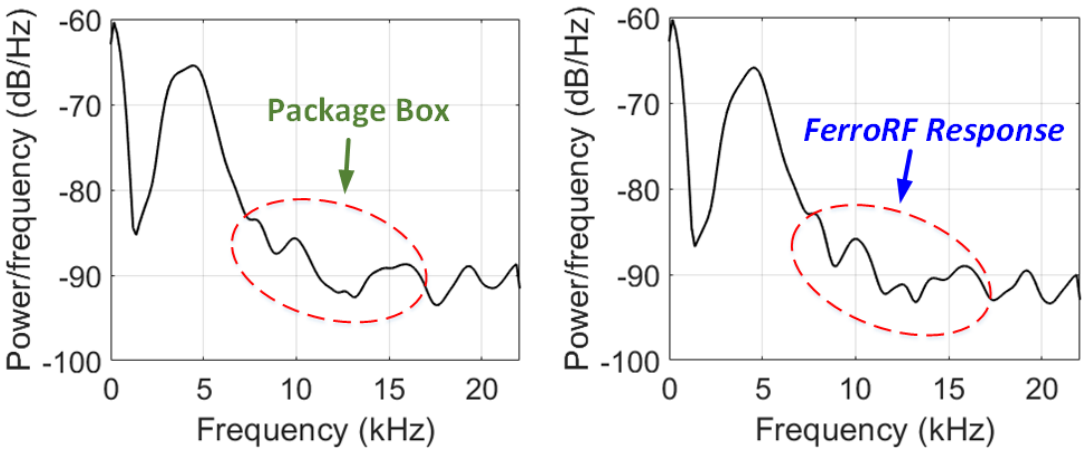


Figure 5.3: The *FerroRF* responses (in the red box) of six different patterns (in the upper right corner) are distinct in both frequency spectrum and amplitude after the modulation, indicating the feasibility of FerroTag counting and identification.

the clutter of the artifacts, their *FerroRF* responses are distinct at the frequency and amplitude. To conclude, the results are significantly promising, implying that given the massive amount of tags, variations have sufficient space to be served as powerful identity resources.

A Study on Package Box: After we confirm the *FerroRF* responses from different tag patterns are diverse, there is still one remaining challenge. In real-world applications, FerroTag can be placed on the package box. As a result, we need to investigate whether the surroundings, such as package box, will disturb the *FerroRF* response and interfere the tag identification. We investigate an example of the interference from the package box, when a mmWave signal comes through the tag, in Figure 5.4. We first put a pack-

age box without the tag before the mmWave probe. As shown in the range frequency spectrum graph (see Figure 5.4a), where the x-axis is the frequency of the received signal, the y-axis is the power spectral density (PSD) [240] of the received signal, we can observe that the reflective signal from the package box is stable and visible. Furthermore, we attach a tag on the package box, and then reacquire and analyze the mmWave signal as shown in Figure 5.4b. A comparison between these two trial results confirms that these two PSDs are significantly distinguishable, which proves the feasibility of the tagging infrastructure in real practice.



(a) The object package PSD analysis without the tag.

(b) The object package PSD analysis with the tag.

Figure 5.4: An example of the object package PSD estimation analysis without and with interference from FerroTag.

5.3 FerroTag System Overview

We introduce FerroTag, a paper-based mmWave-scannable tagging infrastructure to facilitate mass object counting/identification of the inventory management. The end-to-end system overview is shown in Figure 5.5.

Tag Fabrication: The primary physical components of FerroTag are a series of ferrofluid patterns printed on a normal substrate, e.g., copy paper. The tag patterns can

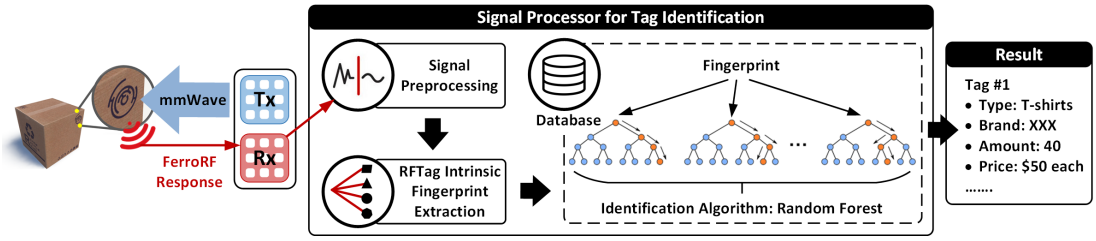


Figure 5.5: The system overview for FerroTag to in-situ identify the tag patterns. It comprises of the ultra-low cost tag with one mmWave sensing module in the front-end and one tag identification module in the back-end.

be highly customized. The tag can be manufactured via a variety of mass-produced, easy-to-use and widely accessible manufacturing methods.

Tag Scanning and Identification: A mmWave probe is proposed to remotely and robustly acquire the tag's *FerroRF* response for identification. Specifically, the probe transmits a mmWave signal and processes/demodulates the reflected response signal. Once receiving the data, the tag identification module first performs the preprocessing to correct the distortion and extracts the spatial-temporal features. After that, an effective classification algorithm is developed to count the tag number and recognize the tag identity.

5.4 Tag Design and Implementation

5.4.1 Basic Tag Pattern Study

To diffuse ferrofluidic materials in to the substrate, we print a ferrofluidic ink pattern directly on the substrate surface. In this process, the depth variation compared to its length and width is negligible (typically less than 0.1% on a tag that is 20x20mm), and the pattern can be considered pseudo-2D. As a result, we utilize 2D geometric shapes to characterize these ferrofluid printed pseudo-2D patterns and test the *FerroRF* response.

For designing an appropriate tag pattern, we analyze the area to perimeter ratios of some typical geometric shapes. The area to perimeter ratios of triangle, rectan-

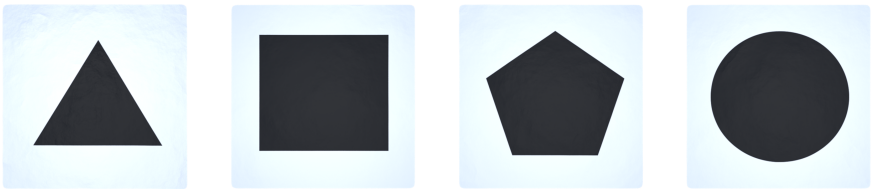


Figure 5.6: The design of four basic tag patterns.

gle/square, pentagon, and circle are around $0.14l$, $0.25l$, $0.2l$, and $0.25l$, respectively. It is worth to mention that other shapes (e.g., hexagon, octagon, and decagon) can be decomposed by two or more regular shapes. Among our design in Figure 5.6, both the square and the circle have the highest area to perimeter ratio, but the circle saves more than 21% space compared to the square. Also, we notice while the tag pattern is more complex, the pattern has more forms of presentation (i.e. more potential component combinations and identity capacity under certain layouts). We further introduce a formal approach to generating a nested geometric for robust and high-capacity tag design.

5.4.2 Prototyping of FerroTag

5.4.2.1 FerroTag Pattern Design Systemization

In order to better characterize the tag capacity, we propose the *pattern complexity score* $\phi(z)$ of a tag pattern to evaluate the pattern complexity. Specifically, $\phi(z)$ is estimated in Equation (5.4):

$$\begin{cases} \psi = \sum_{0}^{L-1} z_i p(z_i), \\ \phi(z) = \sum_{0}^{L-1} (z_i - \psi)^2 p(z_i), \end{cases} \tag{5.4}$$

where z is the grayscale of the image, $p(\cdot)$ is the histogram of the image, L is the grayscale level, ψ is the average of z, and $\phi(z)$ represents the complexity of the tag, which is also the variance of the histogram [186]. As shown in Figure 5.7, all scores of the basic patterns ((a)-(h)) are below 200. Besides, the complexity of a nested pattern (see Section 5.5) is at least twice than that of the basic pattern. Therefore, we define the

threshold as 400 empirically. When the score is larger than 400, the tag is treated as a nested one. Based on $\phi(z)$, the tag can then be categorized according to the corresponding rules in Section 5.4.1 and 5.5.

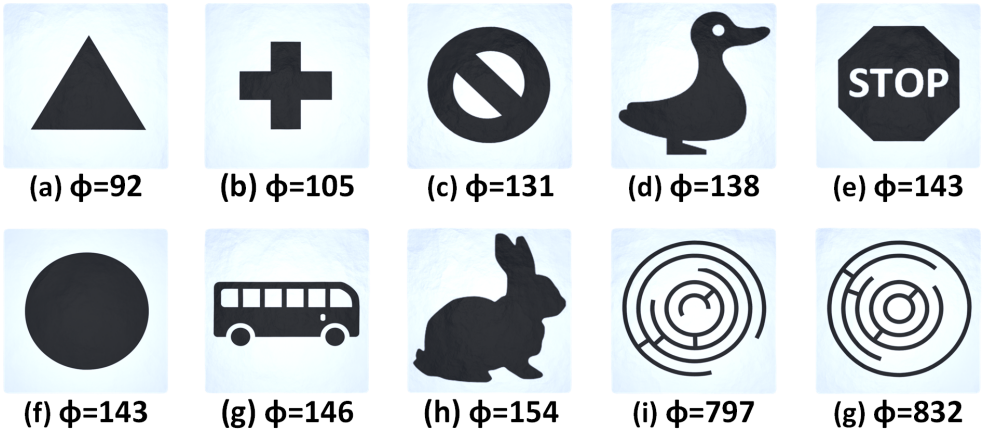


Figure 5.7: Representative tag designs with different complexity scores.

5.4.2.2 FerroTag Printing

FerroTag Substrate: A paper based ferrofluidic ink printed tag is selected to achieve ultra-low cost, wireless, and secure counting of target objects. Papers are extremely low cost nowadays, and its price can become minimal in mass production [2].

FerroTag Printing Machine: To rapidly prototype the tags, we design a new FerroTag printing machine that is capable of producing printed tags. The prototype is based on a commodity printer, including two system support components.

Hardware Development: For the ease of implementation, we employ the modal of inkjet printers as the base of our printing machine. The main task is to revitalize an ink cartridge for ferrofludic printing. As shown in Figure 5.8(a), in order to replace printer ink or refill with ferrofluidic ink, a syringe is used to transfer ferrofluidic ink from container to cartridge safely. Syringe with needle diameter greater than $3mm$ is preferred due to the sealing nature of ferrofluidic ink, which causes plunge from pushing it into a cartridge. The needle needs to be kept at least $1cm$ below the surface of container and cartridge, as the ferrofluidic ink tends to form bubbles and splash over

working area. In case that a cartridge is not revitalizable, we fabracate a 3D printable *Cartridge* that is physically compatible with manufacture's cartridge. After 3D printing the *Cartridge*, we inject the ferrofluidic ink without the need to remove ink residue, which is time-efficient and prevents the residue from contaminating ferrofluid. After injecting the ferrofluidic ink to the *Cartridge* and replacing manufacture cartridge with 3D printed *Cartridge*, procedures including print-head alignment, cleaning, and testing are carried out to remove ink residue in the printer. To prevent the printer from printing with an empty *Cartridge*, we design the ***Supply Manager*** module that estimates the ferrofluidic ink level in the printer based on *Cartridge*'s usage.

Software Development: To reduce the tag edit time, we develop a *FerroTag Generator* in the software stack that can efficiently generate tags in a mass scale, as shown in Figure 5.8(b). Users first input the number of tags to be printed, then the ***FerroTag Generator*** activates the *Randomizer* to generate parameters for the *Executor*. Afterwards, the *Executor* utilizes the parameters and follows Algorithm 3 (mentioned in Section 5.5) to generate tag image files.

After obtaining the generated patterns, we need a layout management to efficiently arrange tags on the substrate. Therefore, we add a custom-built *Layout manager* that transforms a set of tag images into a print-friendly printing layout, which is compatible with native printer drivers. The *Layout editor* first trims the tag images by removing white or transparent pixels, then, the size of each image is adjusted to user defined value from the *Size controller* via image processing technique such as bi-linear interpolation [158]. After that, the *Layout editor* concatenates images in a layout that best fits the paper size selected by users.

Alternative Fabrication Solution: With consumer-grade 3D printers becoming more pervasive, accessible, and reliable, users employ 3D printing technology to print FerroTag molds. As shown in Figure 5.9, we propose a new method of producing FerroTag utilizing the inexpensive, reusable, and durable 3D printed molds with basic geometric

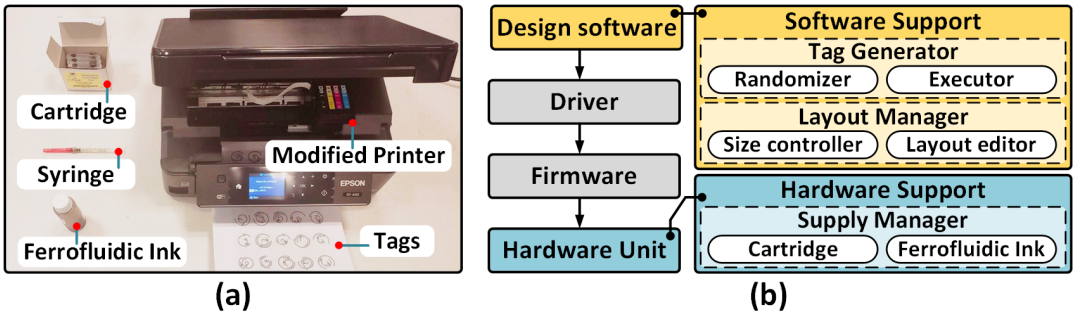


Figure 5.8: (a) shows the experimental setup for the retrofitted off-the-shelf printer employed for the mass manufacture. (b) illustrates the improved system architecture with hardware and software developments.

shape, as an alternative of modified inkjet printing. After the 3D printing stage, a firm tag can be drawn on the paper with a basic brush in seconds.

Figure 5.9: Several molds by 3D printing for the accessible manufacture.

Cost Analysis: The total printing costs originate from the printer and the consumable items. The commercial printer costs around $60 [32]. In our system, the 3D printing mold costs less than $1, the ferrofluidic ink costs around $9 for 60ml (around 0.15$/mL) [28], and the Staples copy paper we use costs $57 per 5000 sheets [29]. We find that per 10ml of ferrofluidic ink could produce more than 500 sheets and one sheet can carry more than 24 tag patterns. Therefore, the cost of one tag (i.e., ferrofluidic ink and paper) is less than *one cent*. Moreover, the cost can be further reduced under massive production.

5.5 FerroTag Advancement

In this section, we further investigate the advanced pattern design to enlarge the tag capacity and strengthen the robustness. The traditional approach is to utilize the stripe

pattern design [94], which has a fixed stripe layout and completes the tag pattern change through the line width. However, such design is not applicable for this application since the ink can expand and involve the adjacent lines, which can severely devastate the corresponding *FerroRF* response. Therefore, we develop an advanced nested geometric design. Inspired by the concentric zone model [42], the nested pattern is a multiple-layer pattern produced through a series of iterations of components. With this multiple-layer iteration mode, the nested pattern allows tag capacity to increase exponentially with respect to the increment in number of layers, which shows a huge capacity for this application. Besides, we introduce a component, Hollow, between layers to aid resisting the ink expansion interference. Furthermore, learned from our preliminary design exploration from the volume of ferrofluidic ink, the design complexity as shown in Figure 5.3 and Figure 5.7, respectively, we propose the design protocol, containing three key components: spiral line, hollow, connection as shown in Figure 5.10.

Figure 5.10: The illustration of the advanced tag pattern design, including three components: hollow, connection and spiral line.

Spiral Line: FerroTag is based on a set of nested circles that effectively utilizes two dimensional substrate surface space. To reduce ferrofluid usage on paper substrate, we apply a set of nested arcs (*i.e.,* spiral lines) to substitute nested circles. The parameters of spiral lines can be adjusted to manipulate the tag capacity. We first define the number of spiral line layers and the cardinality as N and C, respectively. $C_{startpos}$ is the cardinality of starting position of the spiral line in term of angle in degrees for each layer, given the ability to rotate $360°$, we set each possible starting position exactly $1°$ apart, resulting $C_{startpos}$ = 360. C_{endpos} is the cardinality of ending position relative to starting position

in degrees for any layer, this determines the length of the spiral line *length* = *endpos*.We set C_{endpos} = 361 to hold values 0 to 360, where 0 represents absence of spiral line and 360 represents a complete ring. In summary, the capacity contributed by spiral lines can be calculated as $(C_{startpos} \times (C_{endpos} - 2) + 2)^N$, where $(C_{endpos} - 2)$ acknowledges empty spiral line and full ring being same in any starting position.

Hollow: To allow a range of error tolerance, we develop hollow structure. As the ink takes time to sink into paper substrate, it can overlay with another line from the printer head, a hollow structure can reduce the probability that ink spreads and overlays on top of other undesired lines. In addition, enlarging hollow space can reduce ink usage and lower cost.

Connection: Adding connections increases tag capacity with the variations of connection between every two layers. We first define K, the number of connections between two layer, and C_K, the number of connections between adjacent layers. C_{KV} is the binary cardinality for each connection to be present or not, a connection is absent represented by KV = 0, and present presented with KV = 1. The capacity of connections alone can be calculated by ${C_{KV}}^{(C_K)^{(N-1)}}$.

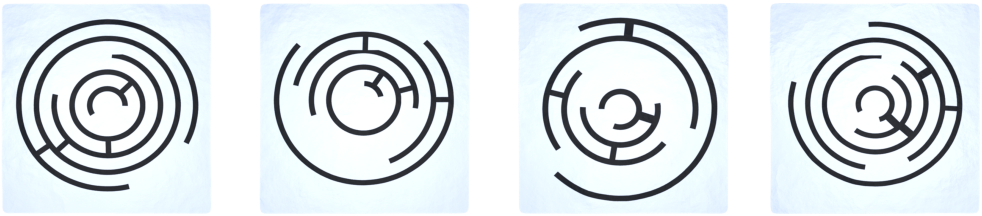


Figure 5.11: Four different advanced ferrofluidic nested tag patterns.

Tag Design: The design of ferrofluid nested pattern is illustrated in Algorithm 3. For a nested pattern (see Figure 5.11), the number of spiral line layers, radius of each spiral line, length of each spiral line, and starting position of each spiral line are preset by users or randomly distributed as input. We establish *SpiralLine()* and *Connection()* functions based on the preset parameters. By calling these functions, array of tuples that stores spiral line and connection points are generated. The algorithm iterates layers by layers to generate tag patterns. In detail, the algorithm first transforms between polar coordinate

Algorithm 3: Nested Pattern Design Generation in FerroTag

Input: N: The number of spiral line layer; R: Array of radius for spiral lines; L: Array of length of spiral lines; S: Array of starting point of spiral lines; K: Array of connection positions

Output: I: The generated tag pattern

```
Initialize N, R, L, S;
I.append(SpiralLine(index, 0, L, S));
index ← 1;
while index < N do
    I.append(SpiralLine(index, R, L, S));
    I.append(Connection(index, R, R_{-1}, K));
    index++;
end
return I;
```

and Cartesian coordinate, and then performs trigonometric calculations for each position such that pixel coordinates in the pattern are stored directly after calculation.

The Tag Capacity Estimation: We estimate the capacity of the tag with the model of Equation (5.5), where N is set as five for high capacity and proper size, and K is set as six to avoid overlapping connections as well as enable enough tag capacity. C_N is the total cardinality based on N. Based on these settings, the tag capacity can be mathematically modeled as follows:

$$\begin{cases} N > 1, C_K = 2, C_{KV} = 2, \\ C_{startpos} = 6, \\ C_{endpos} = 7, \\ C_N = (C_{startpos} \times (C_{endpos} - 2) + 2)^N \times {C_{KV}}^{(C_K)^{(N-1)}} \\ \quad = (6 \times (7-2))^5 \times (2^{2^4}) > 8.5 \times 10^{12}, \end{cases} \tag{5.5}$$

5.6 mmWave-Scannable Identification Scheme

5.6.1 *FerroRF* Response Signal Acquisition

We introduce the RF hardware in FerroTag to stimulate and acquire the *FerroRF* response from tags. Pulse-Doppler radar that emits a set of periodic powerful pulse signals has been largely used in airborne applications [154], such as the target range and shape detection. However, when a short-time pulse stimulus, which has an infinite frequency band, is applied to illuminate the electronics, the corresponding *FerroRF* response will be overlapped with the stimulus signal and difficult to recognize. Therefore, FerroTag selects a frequency-modulated continuous-wave (FMCW) radar with a narrow passband filter [184]. The FMCW radar continuously emits periodic narrow-band chirp signals whose frequency varies over time. Non-linear interrelation to these narrow-band stimuli will generate distinct frequency response, and the received signals will carry the distinguishable *FerroRF* responses when the stimuli signals hit the target tag. Specifically, the transmitted FMCW stimulation signal is formulated as Equation (5.6).

$$T(t) = e^{j(2\pi f_0 t + \int_0^t 2\pi\rho t \ dt)}, 0 < t < T_r, \tag{5.6}$$

where $T(t)$ is the transmitted signal, T_r is one chirp cycle, f_0 is the carrier frequency and ρ is the chirp rate. In our application, when $T(t)$ passes through the tag, the ferrofluidic patterns on the tag act as a passive convolutional processor (see Figure 5.2), and generates non-linear distortions to $T(t)$. After the manipulated signal radiates from the tag, the *non-linear spectrum response* will be captured by the RF probe receiver antenna (Rx). Once the *FerroRF* response signals are received, FerroTag will first preprocess the signal and extract the effective feature vector from the *FerroRF* response. After that, an identification model is developed to identify the tag.

Table 5.1: List of features extracted from the *FerroRF* response.

Category	Features
Temporal Feature	Mean Value, 50th percentile, 75th percentile, Standard Deviation, Skewness [160], Kurtosis [79], RMS Amplitude , Lowest Value, Highest Value
Spectral Feature	Mean Value, Standard Deviation, Skewness, Kurtosis, Crest Factor [31], Flatness [136]
Others	*MFCC-10* [191]

5.6.2 Signal Preprocessing

In practice, the received *FerroRF* response always contain the signal distortion. A natural countermeasure is to model a digital filter and compensate for the distortion accordingly. However, such a solution hardly handles cumulative errors over time that are unlikely to be accessible to end-users [171]. To address this issue, we employ the range resolution analysis solution [166]. The range resolution is $\Delta RES = \frac{c}{2B}$, where c is the light speed, and B is the bandwidth of one periodic chirp. This solution can automatically align the signal distortion based on different conditions. When the distortion displacement $< \Delta RES$, the signal has a minute frequency shift that is invisible on the *FerroRF response*. When the distortion displacement $> \Delta RES$, it will result in the misalignment issue of the *FerroRF response*. To align spectrum response $S(w)$, we utilize the envelope correlation function between the shifted spectrum and its corresponding reference spectrum $Q_(w)$, formulated as:

$$E(\tau) = \sum_{w} |Q(w)| \cdot |S(w - \tau)|, \tag{5.7}$$

where τ is the frequency shift. The optimal frequency shift can be calculated as:

$$\tau^{opt} = \arg\max E(\tau). \tag{5.8}$$

5.6.3 Spatial-temporal FerroTag Intrinsic Fingerprint Extraction

As the above mentioned, the *FerroRF* response contains the unique identity of the tag. As a result, we exploit the internal traits in the *FerroRF* response signal by extract-

ing scalar features in spatial-temporal domains. The feature are listed in Table 6.1. These features represent the *FerroRF* response signal from different aspects. Notably, we employ 10 features in Mel-Frequency Cepstral Coefficients (MFCC) [191]. MFCC are coefficients, which are based on a linear cosine transform of a log power spectrum on a nonlinear Mel scale of frequency as illustrated in Equation (5.9), (5.10), and (5.11) [200].

$$B_m[k] = \begin{cases} 0, k < f_{m-1} \; and \; k > f_{m+1}, \\ \dfrac{k - f_{m-1}}{f_m - f_{m-1}}, f_{m-1} \leq k \leq f_m, \\ \dfrac{f_{m+1} - k}{f_{m+1} - f_m}, f_m \leq k \leq f_{m+1}, \end{cases} \tag{5.9}$$

$$Y[m] = \log(\sum_{k=f_{m-1}}^{f_{m+1}} |X[k]|^2 B_m[k]), \tag{5.10}$$

$$c[n] = \frac{1}{M} \sum_{m=1}^{M} Y[m] \cos(\frac{\pi n(m - 0.5)}{M}), \tag{5.11}$$

where $X[k]$ is the input signal applied by the Fast Fourier Transform (FFT), $B_m[k]$ is the Mel filter bank, $Y[m]$ is the Mel spectral coefficients, m is the number of filter bank, n is the number of cepstral coefficients. Intuitively, the fingerprint with more MFCC coefficients will contain more unique physical characteristics of the tag. MFCC combines the advantages of the cepstrum analysis with a perceptual frequency scale based on critical bands, and can improve the tag recognition performance by boosting high-frequency energy and discovering more intrinsic information.

However, it also increases the computation overhead. To balance this trade-off, we empirically choose $n = 10$. Thus, MFCC-10 collectively make up the robust representation of the short-term power spectrum in the received signal, which is related to the tag pattern. Besides, apart from the MFCC-10, for example, the skewness is a scale of symmetry to judge if a distribution looks the same to the left and right of the center point, and flatness describes the degree to which they approximate the Euclidean space of the same dimensionality. Thus, after analyzing with the forward selection method

for the feature selection [59], a fingerprint containing 25 features from the temporal and spectral parts is formed.

5.6.4 FerroTag Identification Algorithm

After we obtain the input data, a 25-dimensional feature vector extracted from the *FerroRF* response, we use FerroTag for the tag identification. We utilize our FerroTag identification algorithm which can be formulated as a multi-class classification problem as shown in Algorithm 4. A traditional approach to address this problem is the Convolutional Neural Network (CNN) classification. Although some scholars adopted the CNN approach in their particular applications [243], the CNN is intractable requiring intricate network topology tuning, long training time and complex parameters selection. Moreover, CNN based solutions, which learn features automatically, are not always effective due to the local convergence problem. Thus, we employ a customized random forest method, which is an ensemble learning method for classification task that operates by constructing a multitude of decision trees at training time and outputting the class that is the mode of the classes of the individual trees [142]. The advantage of adopting the random forest is that it utilizes the unbiased estimate to achieve the generalization error, and subsequently has an outstanding performance in generalization. Moreover, the random forest can resist the overfitting, be implemented without massive deployment and has an excellent ability to be interpreted [91]. Therefore, we use an ensemble learning method for classification of the *FerroRF* response signal. Particularly, we deploy a random forest with 150 decision trees as a suitable classifier for our system. The set of features selected through Section 6.5.3 are used to construct a multitude of decision trees at training stage to identify the corresponding tags for every 20ms segment of the RF signal in the classification stage.

Algorithm 4: FerroTag Identification Algorithm

Input: γ: The *FerroRF* response traces from a tag
Output: R: The identification result

$\vartheta \leftarrow 150$;
$\delta \leftarrow 0$;
$\varrho(i) = Preprocessing(\gamma(i))$;
for $i \in \{1, \ldots, n\}$ **do**
    $\epsilon 1(i) = FeaturesTemp(\varrho(i))$;
    $\epsilon 2(i) = FeaturesFreq(\varrho(i))$;
    $\epsilon 3(i) = FeaturesMFCC(\varrho(i))$;
    $\epsilon(i) = [\epsilon 1(i), \epsilon 2(i), \epsilon 3(i)]$;
end
for $i \in \{1, \ldots, n\}$ **do**
    $R(i) = RandomForest(\epsilon(i), \vartheta)$;
    $\delta + +$;
end
return *R*;

5.6.5 Multiple Tags Counting and Identification

To further facilitate inventory management, FerroTag can count and identify multiple tags at the same time. This ability helps FerroTag with scanning multiple items in the same box or shelf, which can magnificently improve the scanning efficiency. To count the multiple tags, the spectral signature based solution is widely adopted [110]. The solutions detect if there are several wavelengths much greater than their footprints, when the designed tags resonate at frequencies. However, the resonation only occurs when the ink on the tag is conductive, while the ferrofluidic ink is the opposite. Thus, owing to multiple Rx on the probe, we employ the Angle of Arrival (AoA) to count the tags. The distances from the tags to different Rx (the distance of propagation) vary, which causes phase shifts among the received signal on multiple Rx. The AoA solution is to calculate these phase shifts to induce tag signal sources and count tags [198]. The phase shifts $\Delta\omega$ can be formulated by:

$$\Delta\omega = \frac{2\pi\Delta d \sin\theta}{\lambda}, \tag{5.12}$$

where Δd is the distances between two Rx and θ is the AoA. According to the above equation, we can get the AoA resolution $\Delta\theta$ as:

$$\Delta\omega_{RES} = \frac{2\pi\Delta d_{\max}}{\lambda}(\sin(\theta+\Delta\theta)-\sin\theta) > \frac{2\pi}{\nu} \xrightarrow{sin(\theta+\Delta\theta)-\sin\theta\approx\Delta\theta\cos\theta} \Delta\theta > \frac{\lambda}{\nu\Delta d_{\max}\cos\theta}, \tag{5.13}$$

where ν is the number of sample points.

5.7 System Prototype and Evaluation Setup

Experimental Preparation: The deployment of FerroTag is shown in Figure 5.12. The distance between the tag and the probe is denoted as D. Note that D is adjustable based on the requirement of real applications. In this setting, D is set as 60cm empirically. The corresponding tag sizes are made in 28mm ($1.11in$) (diagonal). Each tag is attached to three standard boxes for scanning: two USPS package boxes and an Amazon package box.

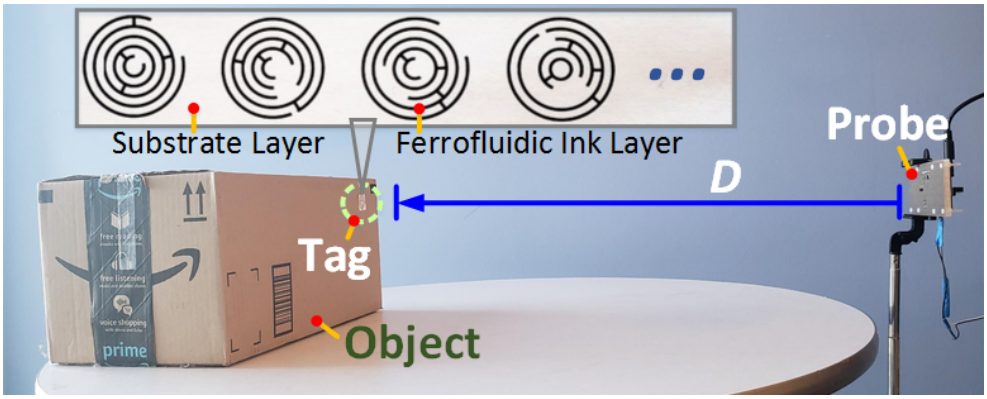


Figure 5.12: System implementation (designated FerroTags with a mmWave sensing probe).

FerroTag Fabrication: Without loss of the generality, we employ two off-the-shelf economic printers (i.e., Epson Expression Home XP-400 and Canon Pixma MG2922) and retrofit printers to produce massive tags with 201 different nested patterns in the

experiment. Each tag pattern is printed with different size (see Section 5.8.4 in detail). We collect a total of 300 traces with a 44.1K sampling rate for each tag, including 210 traces randomly selected for training and 90 traces for testing. As a result, there are entirely 42,210 traces for training and 18,090 for testing.

Application Protocol: FerroTag has the enrollment and identification mode. At the enrollment mode, FerroTag extracts features from tags introduced and stores them in a database. At the identification mode, FerroTag extracts features introduced and compares them to the template ones. FerroTag returns the tag ID and counts the object number.

Scanner Design: The FerroTag prototype employs an ordinal FMCW mmWave system [183]. The mmWave signal is processed using standard FMCW and antenna array equations to generate the *FerroRF* response, which is then utilized for the tag identification and counting. The transmission power is less than 1.2W. The cost is lower than $100. Besides, the probe can be easily mounted on the wall or integrated with other devices like laptops, smartphones, and mobile inspection instruments.

Performance Metric: To better evaluate the system performance, we adopted a confusion matrix, in addition to straightforward techniques such as accuracy, precision, and recall. In the confusion matrix plot, the darker the shade, the higher the classification performance [81].

5.8 FerroTag System Evaluation

5.8.1 Identification Performance

We evaluate the ability of FerroTag to recognize the different tags in the controlled lab environment. The resulting average classification performance for each tag is shown on a heat map (aka. a confusion matrix) in Figure 5.14. The rows represent the selected tag ID classified by the random forest classifier and the columns represent the actual tag ID. Evidently, the diagonal cells are the darkest blue, implying that the traces from

tag i were indeed classified as class i. While little light blue cells are appearing outside the diagonal cells, instances of misclassification are rare. The identification accuracy is 99.54%, with 99.52% precision and 99.49% recall, which implies that the feature vector effectively reflects the unique *FerroRF* response characteristics in each tag. To better illustrate the classification performance, we select ten types and enlarge their confusion matrices. Upon careful analysis, we notice that No.77 tag is misclassified as No.80 tag even though their shapes are significantly different. The reason is due to the nature of our algorithm which describes the *FerroRF* response, primarily based on the *FerroRF* effects, rather than their visual characteristics. In conclusion, our results demonstrate that paper-based printed tags can be precisely recognized by FerroTag.

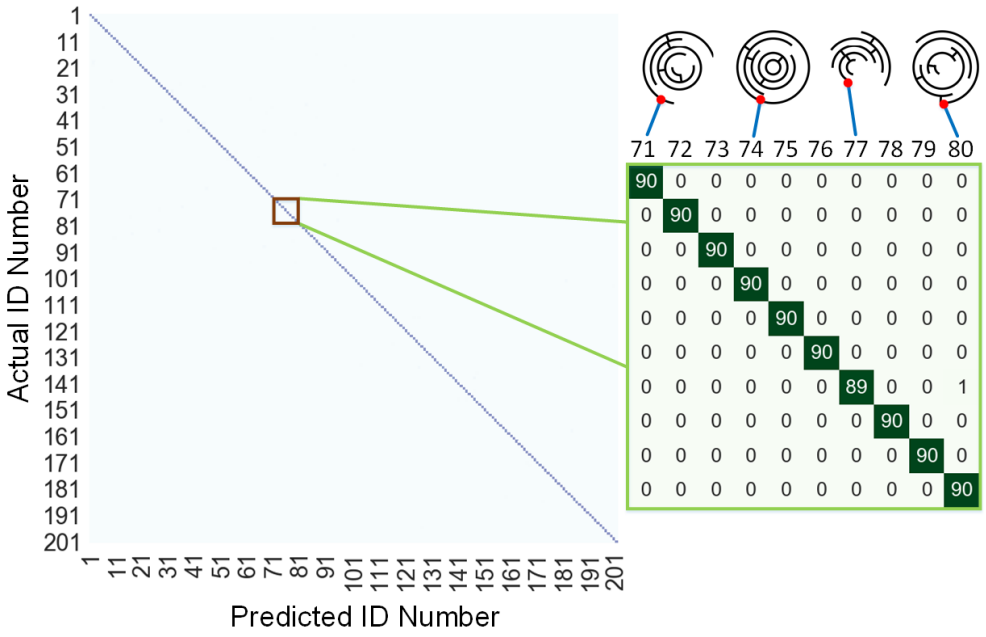


Figure 5.13: The identification performance for FerroTag with 201 different type tags. Confusion matrices of ten types are enlarged in the green box. These ten types are the same as others following the same pattern design. These ten types verify that most are classified correctly.

5.8.2 FerroTag Sensing Tests

It is essential to detect and recognize tag identifies in a tagging infrastructure. To evaluate this performance, we employ the radar cross-section (RCS), that is an important characteristic that indicates the power of the backward tag signal [177]. The RCS can be represented as:

$$\xi = \frac{P_r}{P_t G_t G_r} \frac{(4\pi)^3 d^4}{\lambda^2}, \tag{5.14}$$

where ξ is the RCS, P_r is the power of the received modulated tag signal, P_t is the power transmitted by the probe, G_t is the gain of the probe transmit antenna, G_r is the gain of the probe receive antenna, λ is the wavelength and d is the distance to the tag [66]. To evaluate the RCS of tags, we utilize 30 different tags. The RCS of the tags are between $-37dBsm$ to $-29dBsm$ under mmWave, which implies that the tag owns a similar exceptional performance to passive RFID tags [227].

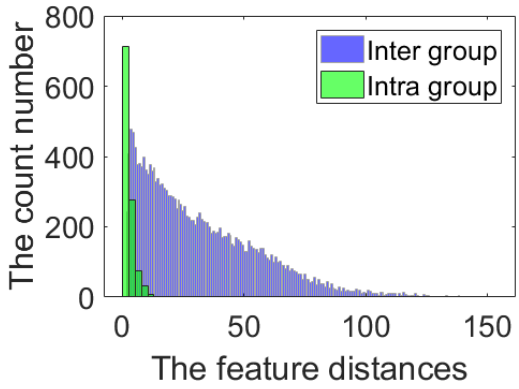


Figure 5.14: The tag uniqueness analysis

5.8.3 Tag Uniqueness

For a tagging infrastructure, it is essential to recognize the overall distinguishability of tags. In this evaluation, we employ 201 different fingerprints in Section 5.8.1 and differentiate the fingerprints into two groups, i.e., intra-group (within the same tag) and inter-group (among different tags). We leverage Euclidean distance, a widely used technique for measuring the fingerprint distance. The fingerprint distance between intra- and

inter-groups is illustrated in Figure 5.14. The average of intra group is 2.51, which is significantly smaller than the average of inter group 32.04. Also the results show the tags can be completely separated with little overlap. Thereby, we prove the independence between two tags, even with the similar pattern.

5.8.4 Performance Characterization of Different FerroTag Configurations

In this section, to further reflect the actual performance in real practice (e.g., the tag size, the tag ink intensity, the reading rate, the tag pattern complexity and substrate material), we conduct the following experiments.

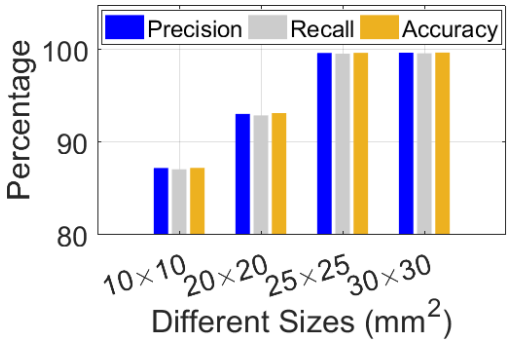


Figure 5.15: Tag detection and recognition with different sizes.

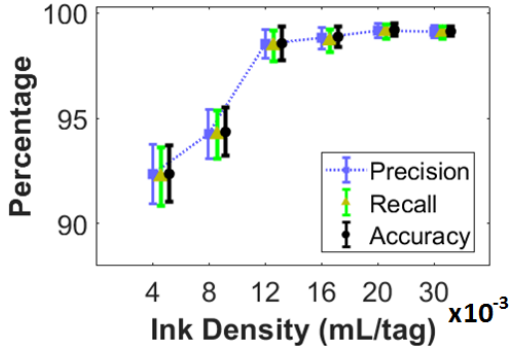


Figure 5.16: Performance under different ink densities.

Tag Size: The tag size is a crucial consideration in a real application, which is related to the tag cost and the occupancy. specifically, we design 50 different advanced tags with four different size settings between $10mm \times 10mm$ ($0.39in \times 0.39in$) to $30mm \times 30mm$ ($1.18in \times 1.18in$). For each size setting, we follow the same methodology described in Section 5.7 and re-prepare the training and testing set. Figure 5.15 shows the performance results. For the smallest size of $10mm \times 10mm$, FerroTag only obtains the accuracy of 87.22%. The results are because the ferrofluidic patterns are too small to be differentiated by the mmWave signal. After increasing the size, the performance gradually increases. Generally, we find that a turning point at $20mm \times 20mm$ where the

performance saturates afterward (reaching the accuracy of 99.54%). Considering the printed-based tag, e.g., barcode, whose width is at least 30mm [30], the results imply that FerroTag is applicable for various applications.

Tag Ink Density: Intuitively, it is well known that the ink density of tags profoundly affects the tag cost. Thus, we propose to measure the tag ink intensity (mL/tag) that shows the ink amount usage for making a tag. We design 50 different advanced tags with six different density settings varying from $0.004mL/tag$ to $0.030mL/tag$ and evaluate how it affects the accuracy of the tag identification. Figure 5.16 shows the accuracy is only 92.7%. For the lowest ink density of $0.004mL/tag$, FerroTag only obtains 92.74% precision,92.62% recall and 92.76% accuracy, which shows that lower ink density can diminish the accuracy. The performance improves, along the ink density grows until $0.020mL/tag$. Then the performance keeps constant around 99.57% precision,99.52% recall and 99.59% accuracy. This observation can guide us to select the proper density to ensure the identification accuracy with a minimal cost in specific applications.

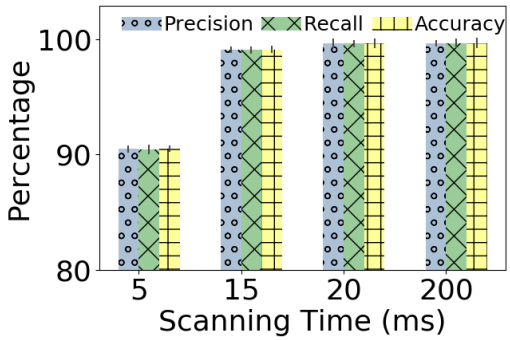


Figure 5.17: Tag identification with different scanning time.

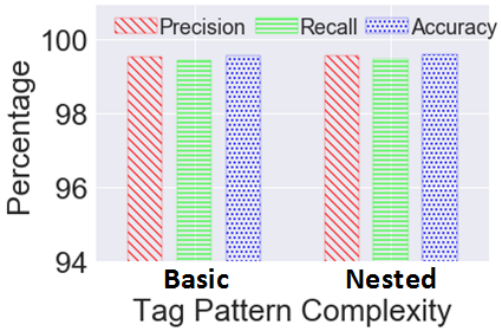


Figure 5.18: Performance under different tag complexities.

Scanning Time: We know that objects screening tasks are challenging due to concise budgeted time for efficiency. As a result, we are interested in analyzing the performance of FerroTag concerning different time budgets, *i.e.*, a different time needed for scanning one tag. Specifically, we select four different time settings between $5ms$ to $200ms$. For each time setting, we follow the same methodology described in Section 5.7 and re-prepare the training and testing set. Figure 5.17 shows the performance results. For

the lowest duration of $5ms$, FerroTag only obtains the accuracy of 90.17%. The results are because the contained information in traces with $5ms$ cannot comprehensively represent the characteristics of FerroTag. After increasing the scanning time, the performance gradually increases. Generally, we find that a turning point at $20ms$ where the performance saturates afterward (reaching 99.54% accuracy), which means we can scan 50 tags per second, which is a magnificent improvement in scanning speed compared to the optical-based solutions.

Tag Pattern Complexity: In the practical implementation, the tag pattern can be highly customized to satisfy different manufacture methods and appearance requirements. To understand its impact on the identification accuracy, we set *basic* group and *advanced* group according to the tag complexity and 50 different tags are employed for each. The results are shown in Figure 5.18. The identification accuracy for both groups remains high (above 99.1%), which implies that the system performance is insensitive to the tag pattern complexity.

Substrate Material: We consider the scenario where the user may use different substrates to build the tags according to various applications. Particularly, we collect four different daily-achievable materials as shown in Figure 5.19. The cumulative distribution function is plotted in the figure, where we can see that the overall identification error rate for each is less than 1%. Certain materials slightly affect the performance to some extent. This is because FerroTag utilizes high-frequency signal and therefore, has small wavelength and limited penetration ability. As a result, it is prone to the scattering reflection upon some specific materials. But in general, FerroTag still provides reliable performance in tag recognition.

5.9 Robustness Analysis

Performance in Different Distances: To validate the usability and effectiveness of FerroTag in the non-contact identification scenario, we set up the device to stimulate the operation distance from 30cm to 100cm considering the mmWave coverage of the

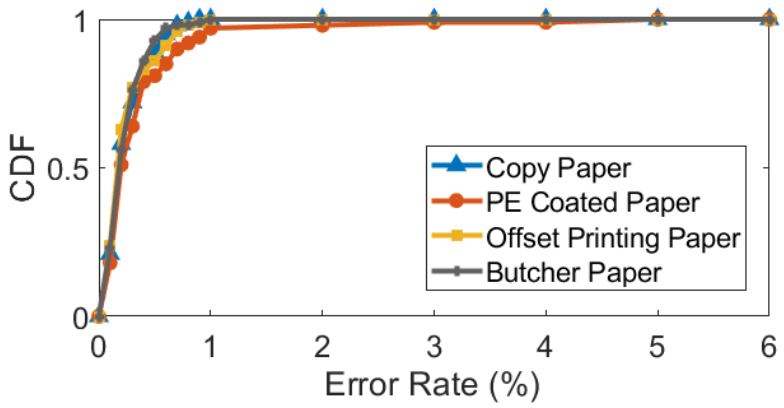


Figure 5.19: The objects detection under different substrate material.

tags in relation to their *response* magnitude. In this experiment, 50 different tags (see Section 5.7) are recruited. Figure 5.20 manifests that their performances can achieve up to 99.59% accuracy. Besides, the identification performance remains above 99% when the sensing distance varies within 1m. Thereby, FerroTag can facilitate in-situ and convenient tag scanning in real practice.

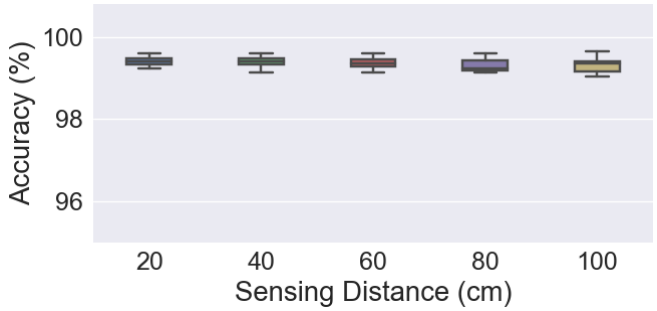


Figure 5.20: Performance under different sensing distances.

Impact of Environmental Dynamics: The ambient environment can introduce random noises or even interfere with the tag properties or the probe hardware operation. We consider common noises in the daily workplace in terms of human factors and ambient factors. Typically, we select four conditions where (1) the environment temperature is $10°C$ $(50°F)$; (2) the humidity of the testing location is controlled at 70%; (3) the magnetic field strength is set at $400\mu T$; (4) the light intensity is $1000Lux$. Moreover, we use the result of the optimal lab environment as the comparison target (the temperature,

the humidity, the magnetic field strength, the ultrasound wave and the light intensity are $20°C$ ($68°F$), 30%, $50\mu T$ and $300Lux$, respectively). Again, we evaluate the above four conditions using 50 tags. Figure 6.17 demonstrates that their performances all achieve above 99.14%. In conclusion, FerroTag presents a strong tolerance to different ambient environments.

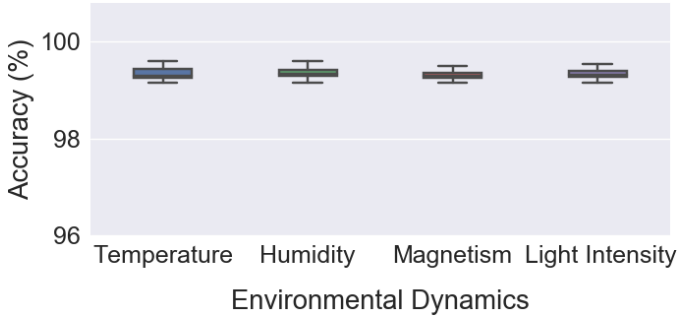


Figure 5.21: The tags detection under different environments.

Under Blockage: FerroTag usage scenarios may involve non-line of sight (NLOS) environment, e.g., in inventory management, where the object (and tag) may be placed inside a package. We mimic such NLOS cases by blocking the light of sight between the tag and probe using different materials: paper, wood, glass and plastic. Specifically, we evaluate the above four conditions using 50 tags. Figure 5.22 reveals that blockage has trivial impact on FerroTag's counting and identification. The experiment verifies that FerroTag works in NLOS scenarios where camera-based approaches will fail.

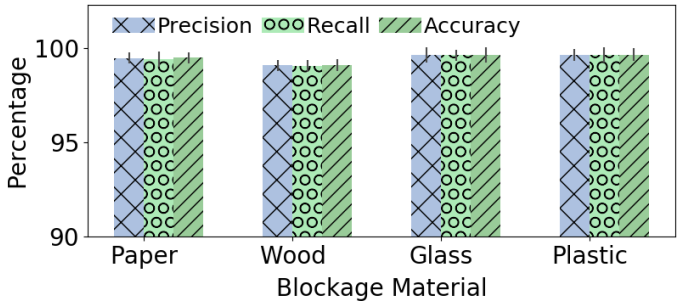


Figure 5.22: The tags detection under different occlusions.

Impact of Scanning Orientation: In practical scenarios, tags may place towards different orientations. Therefore, it is important to investigate whether the sensing angle will

affect system performance. Specifically, we measure the different tag orientations (from 0° to 180°). The results are shown in Figure 5.23. As for the orientation, the effective sensing range is among (60°-120°), since the mmWave has a narrow beam forming. Although the reflected signal slightly changes due to the different probe angles for each tag, the inter-device distinguishability among 30 tags is significant such that each tag can be correctly recognized. Thereby, FerroTag shows a strong capacity in real practice.

Durability Study: Proving the permanence of identification is crucial. Our generated dataset has included multiple sessions as part of a longitudinal approach to establishing a baseline comparison of long-term persistence. 30 different tags participated in the longitudinal study lasting three weeks as shown in Figure 5.24. Notably, this study has two phases: the enrollment phase and authentication phase. In the enrollment phase, training data were collected for each subject on the first day of this longitudinal study. Each tag finishes five trials in data collection events with the duration of each test set as 10 seconds. After that, the long-term authentication phase is carried out in the following three weeks. Each tag performed five identification trials every 2 days and each identification duration is 5 seconds in this study. The accuracy measurement is depicted in Fig 5.24. In the three weeks duration, mean values of accuracy measurement are between 99% and 100%, and standard deviations are between 0.22 and 0.51. We concluded that the accuracy has no significant performance decreasing or ascending tendency, which demonstrates FerroTag is robust against aging in time.

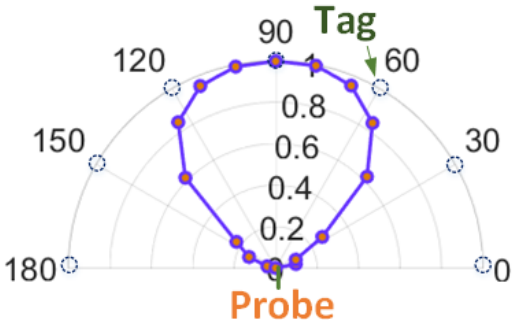


Figure 5.23: Impact of varying sensing angles.

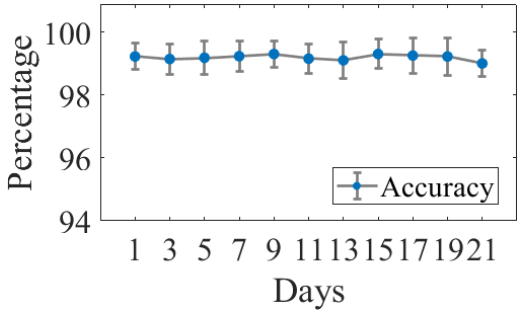


Figure 5.24: A three-week investigation on the accuracy stability of FerroTag.

5.10 A Case Study on Complex Scenes

As the application environments of tags are mainly in retail, warehouse or places where a large amount of coexisting tags hidden in the package under NLOS environment, we aim to count their number and know their types immediately and conveniently without opening the package and protecting the privacy. To achieve this goal, there are two existing primary concerns in practice: 1) the unavoidable variance in the signal's scaling and magnitude; and 2) the interference from the containing items and the ambient noises. To explore whether FerroTag can identify multiple hidden tags simultaneously, we continue with the setup in Section 5.7. Specifically, we employ 6 tags and select four conditions where: (i) and (iii) randomly select 2 tags, out of 6; (ii) and (iv) randomly select 3 tags, out of 6. In (i) and (ii), tags are attached to cardboard boxes within the package box, while in (iii) and (iv), tags are attached to T-shirts. This study is a 6-by-6 scanning with different combined. We enumerate all possible combinations in these conditions. Figure 5.25 shows the AoA range profile where the red color areas imply tag locations, and then we count the tags based on this range profile. The identification results are illustrated in Figure 5.26, showing that their performances keep between 97% to 99%. This is owing to the fact that the *FerroRF* effects change if we combine two tags along with the *FerroRF* response. To sum up, FerroTag suffices as an accurate and reliable way of ultra-low cost and in-situ tagging infrastructure in the real-world scene.

Figure 5.25: The graph shows the three tags counting.

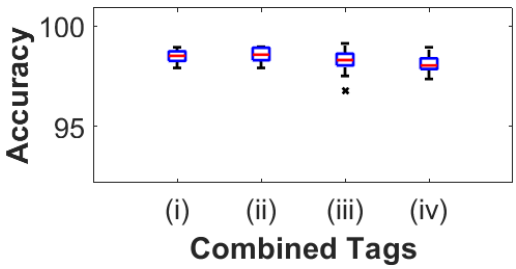


Figure 5.26: Identification of combined tags.

5.11 Discussion

Potential Health Hazard: There are two aspects for the potential health consideration: wireless sensing and ferrofluidic prints. Compared to other wireless sensing techniques (e.g., WiFi spots), FerroTag has a much smaller radiation factor, e.g., a 1.2W power consumption and an 8dBm radio transmission power. Besides, the ferrofluidic ink is not inherently dangerous or toxic and has been applied to the medical domain [50]. Moreover, the ferrofluidic print can be naturally degradable [122, 185]. Therefore, FerroTag is a considerably safe identification tool with limited health hazard concerns.

Security and Privacy: Privacy-preserving is another fundamental factor for the object counting and identification as many owners have extremely high requirements on their privacy protection. Our system only requires the *FerroRF* response with a small information disclosure (i.e., mmWave signal) of the corresponding tag.

Custom Designed Patterns: It is significant to customize the dimensions of patterns as well as the paper substrate in FerroTag, to satisfy different application requirements. The system robustness to the tag size and pattern is discussed in Section 5.8.4.

Future Applications: Beyond the use case of the mass objects counting and identification, owing to the concept of the *FerroRF* effects and the advantages of ultra-low cost and in-situ, FerroTag can serve as a generic solution to extend the interaction area of IoT devices, extend the network to new physical dimensions, or serve as the 'fingertips' of the next-generation Internet. It can also be applied to a variety of applications, *e.g.*, agricultural monitoring, cell tracking, monitoring patients, and anti-counterfeiting [100, 164, 190, 201].

5.12 Related Work

Paper-based (Chipless) Electronics: Paper-based electronics have been developed over the last few years. There are three categories in terms of the way to interact. The first one is the contact-based solution, that (e.g. microfluidic paper [206], wet sen-

sor [125], touch sensor [93, 123], ubiquitous device [101, 124, 173, 216], etc. However, they all need to measure the resistor, inductor, and capacitor (RLC) change in a contact manner, which are not convenient. The second category is based on a non-contact optical method. There are some research works, like linear barcode [27] and QR code [222]. However, these solutions are limited by the line of sight requirement. The solutions in the third category can work in a remote and invisible way, such as using the passive RFID [92, 108], ink-tattoo ID [100, 108] and mental-shape ID [80]. However, these solutions all employ the conductive ink or the complex toxic specific-designed chemical ink, which is neither low-cost nor environment-friendly. Up to date, no existing work utilizes the *FerroRF* effects to perform an ultra-low cost and naturally degradable tagging infrastructure.

mmWave Sensing: In recent years, mmWave has been utilized for the material characterization and object detection. There are two main mmWave sensing schemes. In the first category, these technologies are based on the detection of objects' geometry and micro-motion [115, 143–145, 167, 238, 260]. These mmWave sensing works mainly rely on analyzing the object boundaries and the Doppler effect of moving objects; thus their techniques cannot be applied to sense the intrinsic tag pattern. Second, there are some applications focusing on the material response for material component characterization [180, 181] and the non-linear response introduced by conductive components [139, 141] when stimulated by the mmWave signal. FerroTag is the first mmWave sensing work to combine the material response and the pattern design for identification.

5.13 Conclusion

In this chapter, we presented a paper-based and mmWave-scannable tagging infrastructure FerroTag, to promote the inventory management technologies. FerroTag is easy to use and low-cost, which is on the basis of ferrofluidic ink on the paper print and its interference to the mmWave signal. In this study, we modeled the *FerroRF* effects

to optimize the tag pattern design, prototyped an end-to-end FerroTag solution with a retrofitted paper printer, and a low-cost mmWave probe. Also, we developed a software framework for detecting and recognizing a newly designed nested tag pattern in practice. Extensive experiments, including one case study with complex scenes, imply that FerroTag can achieve the accuracy of 99.54% in a $20ms$ response time. Different levels of evaluation proved the effectiveness, reliability, and robustness of FerroTag. FerroTag has the potential to transform the sensing to new physical dimensions and serve as the object identity of the next-generation Internet.

Chapter 6

ThermoWave: A New Paradigm of Wireless Passive Temperature Monitoring via mmWave Sensing

6.1 Introduction

Temperature sensors are one of the most in-demand IoT technologies to monitor physical and environmental conditions in daily-life applications. For instance, temperature-sensitive products, including most foods and medicines, are required to be in a temperature-controlled environment to maintain the best possible quality in storage and transportation [8, 58, 120, 207]. Due to packaging and mobility considerations, wireless temperature systems are the essential solution to monitor thermal conditions and protect package integrity and quality in practice. In the landscape of temperature monitoring system markets, the wireless temperature sensor segment grows at the highest rate—15.09 million units generated in 2019 and is expecting to reach 23.45 billion units by 2025 [1, 9, 204]. Currently, updating the existing infrastructure to support low-cost and ecological wireless temperature monitoring has been the primary trend impacting multiple industries, such as smart cities and cold chain logistics [54].

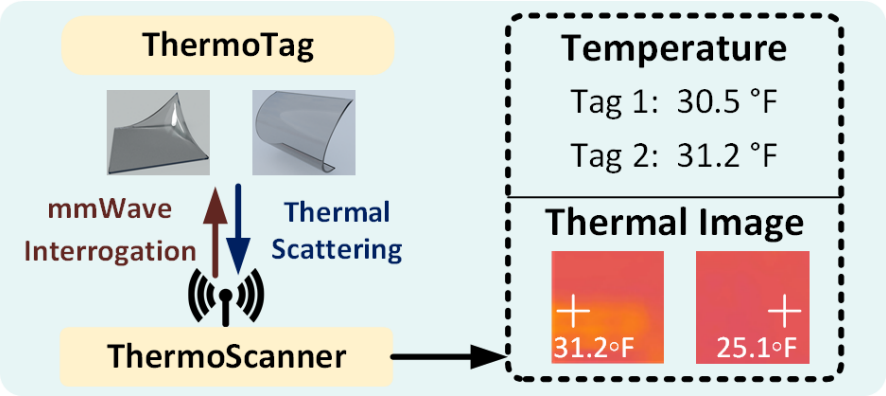


Figure 6.1: ThermoWave: a new ultra-low cost mmWave-scannable temperature monitoring paradigm capable of thermal imaging that utilizes flexible materials.

There is a set of rich literature and commercial products about wireless temperature monitoring technologies developed in two directions (i.e., wireless temperature sensors and thermal-imaging devices). Wireless temperature sensor is often made into tags with thermal-electric temperature sensors [165, 211, 226]. Unfortunately, such technology associates with high cost, harms the environment and lacks thermal imaging capability. On the other side, thermal imaging devices read temperature distribution across space in front of the sensor [151, 168]. However, such a mechanism fails to read temperature from the target object with as little as a thin sheet of paper in between. Given the fact that temperature monitoring is a high demand industry that impacts every second of our daily life, a more powerful wireless temperature sensing paradigm is in urgent need for future temperature monitoring applications in scientific (e.g., material research), industrial (e.g., smart city), and medical fields (e.g., body temperature sensing).

In this chapter, we explore and unveil a novel material-mediated wireless temperature sensing technology, using mmWave sensing. This technology aims to empower extremely low-cost (e.g., under 1 cent per sensor), flexible (e.g., soft sensor material), and ecological (e.g., environmentally friendly materials) temperature monitoring for both dot-wise and fine-grained thermal imaging results under NLOS scenario. The design rationale bases on the cholesteryl material's thermal scattering effects. When the ambient temperature changes, the molecular alignment of cholesteryl material alters accordingly

due to thermal expansion of inter-molecular distance, and thereby impacting scattering properties when it is probed by broad-band (e.g., 250 MHz) radio frequency (RF) signals. Motivated by such a thermal scattering effect, we utilize cholesteryl materials to fabricate a film-shaped temperature tag that can change and modulate the scattered RF signals with temperature change characteristics. To exploit stronger scattering properties, we investigate the high-frequency RF signaling technologies, such as the millimeter wave (mmWave) probes, to effectively interrogate the thermal scattering effects and infer the temperature information. As shown in Fig. 6.1, this technology can enable low-cost, out-of-sight, accurate temperature monitoring in environmentally restricted scenes, such as medicine storage and transportation logistics.

To this end, we present ThermoWave, a new mmWave technology based paradigm to facilitate fully passive temperature monitoring. There are three parts to the ThermoWave paradigm. (1) We first design the ThermoTag based on a thin layer of cholesteryl material stabilized on top of a thin polyvinyl chloride sheet with adhesives, which can characterize the thermal scattering effect as temperature changes. (2) We prototype a mmWave based ThermoScanner to continuously interrogate the ThermoTag and capture frequency shift of thermal scattering response in contrast to the transmitted signal. (3) The scattering response signals are input to ThermoSense, which is a software mechanism for temperature inference. For dot-wise temperature recognition, the input signals are first decomposed into a combination of wavelets via Empirical Wavelet Transform for extracting spectral features. Then, we apply a regression-based ThermoDot model that utilizes extracted features in order to determine the single dot-wise temperature value. Toward thermal imaging results, we first transform the input signals into a spectrogram image using continuous-time short-time Fourier Transform. After that, the spectrogram images are fed to a customized ThermoNet (i.e., an image-to-image GAN) model for reconstructing thermal images. As a first exploration study, we use a set of metrics to evaluate ThermoWave performance (e.g., temperature inference accuracy and image structural similarity index). We evaluate the robustness of

ThermoWave under different sensing distances, scanning orientations, and occlusions to show its superior performance for temperature inference. In our study, ThermoWave can measure the dot-wise temperature change from 30F to 120F with the precision of $\pm$1.0F and thermal imaging in the same temperature range with a $\pm$3.0F precision.

6.2 Background and Preliminaries

6.2.1 Thermal Scattering Effect

The crux of the proposed wireless temperature sensing paradigm is to leverage temperature-sensitive physical characteristics of specific material to retrieve temperature information via RF probing. Among existing wireless temperature sensing solutions, our method presents the benefit of highly low-cost, flexibility, environment friendliness and advanced thermography functions. Due to cholesteryl material's temperature sensitive molecular alignment pattern [113], we select cholesteryl materials as the sensing media to convey the temperature information of the target object. When cholesteryl ma-

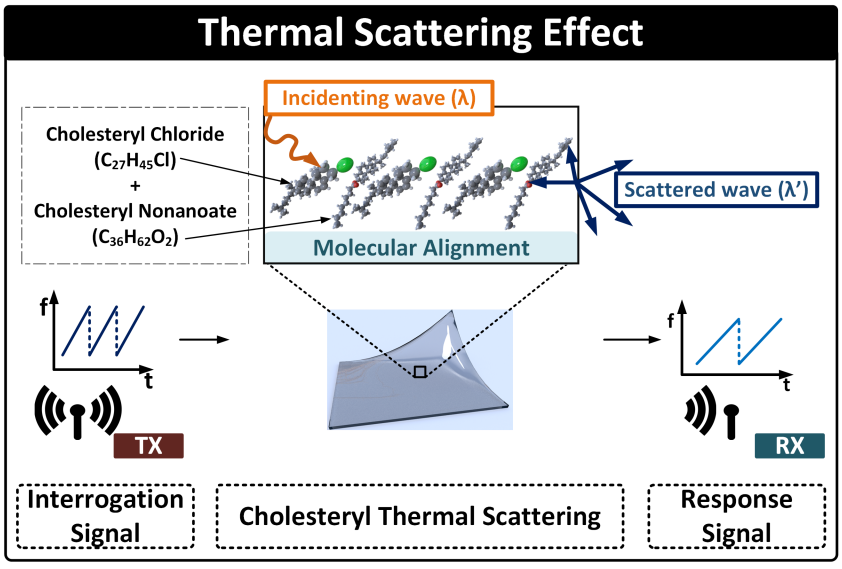


Figure 6.2: Cholesteryl material's temperature dependent molecular alignment directly impacts the frequency of scattering response under the illumination of mmWave.

terial is attached to the target object, it will immediately reach the same temperature as the target object and keep thermal equilibrium according to the theory of thermodynamics [129]. This theory suggests that the level of average kinetic energy (i.e., temperature) of an object tends to balance with the contacting objects. When the temperature of cholesteryl material changes, its underlying structure, which contains polymersome (i.e., vessels), will alter its molecular alignment due to thermal expansion [89]. This molecular alignment directly impacts the scattering angle when such cholesteryl material is probed by broadband RF signals. Specifically, as the RF signal arrives at the location of interest, in-placed cholesteryl material scatters a response RF signal with a modulated frequency shift. The frequency shifted signal is then scattered in all directions, allowing signature capturing for temperature inference. The process of this so-called Thermal Scatter Effect is visualized in Fig. 6.2.

6.2.2 A Preliminary Study: Cholesteryl Material based mmWave Sensing

Hypothesis: The thermal scattering effect of cholesteryl material that contains a unique RF scattering response from temperature caused molecular alignment can be treated as an intrinsic thermal feature. Thereby, it is possible to leverage a mmWave probe that stimulates the cholesteryl material for a frequency-shifted scattering, which contains temperature-induced modulation and contributes toward object temperature detection.

Proof-of-concept: To prove the Hypothesis, we designed and conducted a preliminary experiment using a prototype of cholesteryl material as a temperature sensing media. Specifically, our preliminary experiment is conducted in a well temperature monitored room to ensure that the environment temperature does not change while the tag changes temperature with controlled air-based heating. To simulate a temperature sensing scenario, we use a table as the sensing target, and place the tag on top of the table edge to act as a temperature sensing media. Then, we place a heater on the side of the table to manually control the material temperature from 70 F (i.e., room temperature) to 90 F for

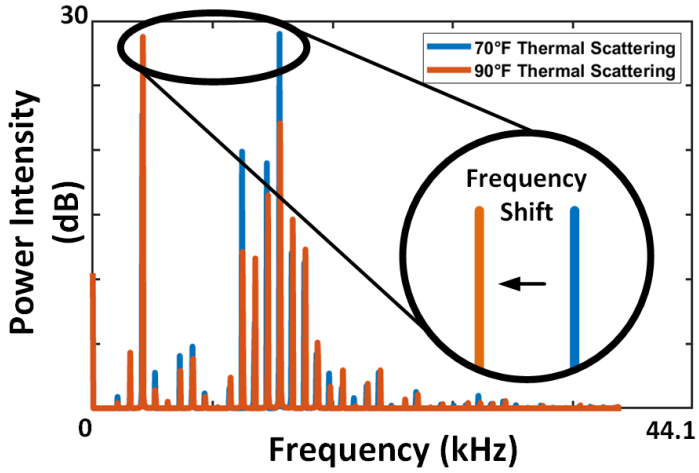


Figure 6.3: Thermal scattering responses from cholesteryl material show evident frequency shift in spectrum analysis. Compared to response at 70 F, the frequency shifted response at 90 F have a tone that is few kHz lower.

theoretically distinct data points as we attempt to visualize the thermal scattering effect in Fig. 6.3. To eliminate the ground truth temperature sensor (e.g., digital thermometer) from interfering with the interrogation signal from the mmWave probe or response signal from the tag, we adopt an infrared camera that can read tag temperature while placed behind the mmWave probe. To illuminate the cholesteryl material, we utilize a 24GHz frequency modulated continuous wave (FMCW) radar with a 250MHz bandwidth. After obtaining the thermal scattering response from the material, we analyze the signal utilizing the spectral plot that presents a direct connection between temperature difference and frequency shift of the scattered signal. As shown in Fig. 6.3, the thermal scattering responses of cholesteryl material at $70F vs. 90F$ are uniquely different. This proves that cholesteryl material can be used to perform temperature monitoring, which further verifies the feasibility and effectiveness of obtaining temperature value via material-mediated temperature sensing.

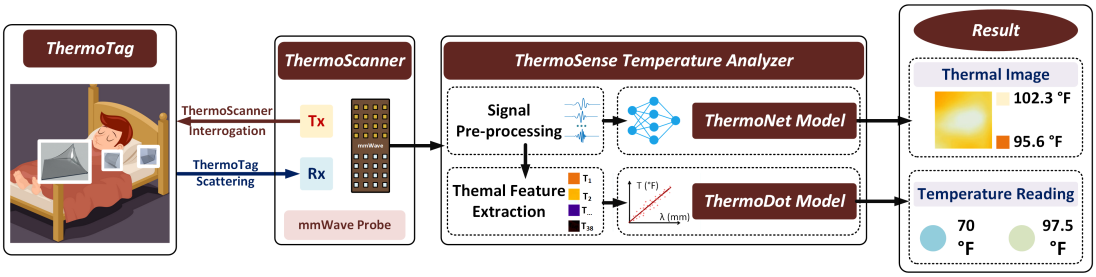


Figure 6.4: We present the ThermoWave paradigm with its three core modules (i.e., ThermoTag,ThermoScanner,and ThermoSense). ThermoTag can be placed on be wrist for skin temperature, bed for ambient temperature, and bed sheet for body thermal imaging. ThermoScanner continuously interrogates ThermoTag to capture temperature cased thermal scattering response, then, the response signals are sent to ThermoDot model and ThermoNet model to obtain dot-wise temperature reading and thermal imaging, respectively.

6.3 ThermoWave Overview

The ThermoWave paradigm comprises three main modules: ThermoTag, ThermoScanner, and ThermoSense to realize material-mediated wireless temperature sensing (see the illustration in Fig. 6.4).

ThermoTag: ThermoTag is a Cholesteryl material-based passive wireless temperature sensor that attaches to the surface of the target object for wireless temperature sensing. As the target object's surface temperature changes, ThermoTag's temperature will instantly follow and alter its cholesteryl molecular alignment accordingly. As ThermoTag's molecular alignment changes, its mmWave scattering properties will also change as shown in Fig. 6.3. The resulting mmWave scattering properties can be captured by the customized ThermoScanner for temperature inference.

ThermoScanner: Considering the prospect of mmWave with a 5G technology in wireless communication as well as its large bandwidth opportunities, we prototype a tag scanner based on 24Ghz FMCW radar, namely ThermoScanner. It is worth mentioning that the cost for a mmWave radar sensor is below $24 and a mmWave radar modality is below $50, which is projected to keep decreasing along with infrastructural deployment [7, 45]. To localize the ThermoTag, the ThermoScanner employs

a pair of four by four antenna arrays with antenna directivity of 19.8 dBi to enhance the precision. While the ThermoScanner continuously interrogates ThermoTag, the thermal scattering response is recorded continuously for temperature inference. Without further adieu, ThermoScanner sends recorded signal to ThermoSense for both dot-wise temperature inference and thermal imaging.

ThermoSense: ThermoSense is a software mechanism to facilitate both dot-wise temperature recognition and thermal image inference. However, the result from dot-wise temperature recognition is a single value while a thermal image is multi-dimensional. Thus, we allocate two models to perform the two specific temperature inference tasks.

For dot-wise temperature recognition, we first convert the scattering signals from a time domain to frequency domain via Empirical Wavelet Transform, then, a feature extractor is developed to reduce data dimension to an array of 38 features from each pre-processed signal, after that, we use a regressor based **ThermoDot** model to map the feature array to a specific temperature value. In order to achieve thermal imaging, we first transform thermal scattering response into spectrogram image using continuous-time short-time Fourier Transform. Then, we develop a **ThermoNet** model based on a generative adversarial network (GAN) to reconstruct thermal images from spectrogram input data.

6.4 ThermoTag Design

6.4.1 ThermoTag Implementation

In order to sustain temperature sensing capability, ThermoTag is manufactured from cholesteryl materials (e.g., cholesteryl benzoate) that can withstand temperature up to 149 C (i.e., 300 F) without being damaged [4, 118]. This facilitates a wide range of applications, such as high-temperature chamber monitoring, boiling liquid sensing, and heating radiator monitoring. During the manufacturing process, we stabilize a thin layer of cholesteryl material on top of a thin substrate layer of polyvinyl chloride sheet with

adhesives, which enables high elasticity [241] of ThermoTag. As a result, ThermoTag can be manually suppressed to various shapes (e.g., bend, camber, curve, fold, wrap) without permanent deformation as shown in Fig. 6.5. In this way, it is flexible to deploy ThermoTag in many complicated scenarios, such as high voltage electric cable temperature monitoring within a power cage over the length of the cord, cold chain transportation with non-rigid medicine containers, and vehicle tire temperature monitoring while inflated [133, 172, 203]. It is worth mentioning that ThermoTag is very lost-cost. In contrast to commodity RFID temperature tags with a price of 1.99 dollars in bulk order, one functional slice of ThermoTag (1cm x 1cm square shaped film) costs less than one US cent, which is a significant reduction [10, 150].

6.4.2 ThermoTag Modeling

The temperature variation of Cholesteryl material based ThermoTag can disturb its thermal scattering of mmWave signals. In this subsection, we establish a physical model to illustrate the thermal scattering effect of ThermoTag.

ThermoTag is designated to be a temperature sensing media that attaches to a target surface. When the target's temperature changes, ThermoTag's temperature inevitably follows. As the temperature of cholesteryl material-based ThermoTag varies, its inner molecular alignment (i.e., three-dimensional geometry shown in Fig. 6.2) will alter due

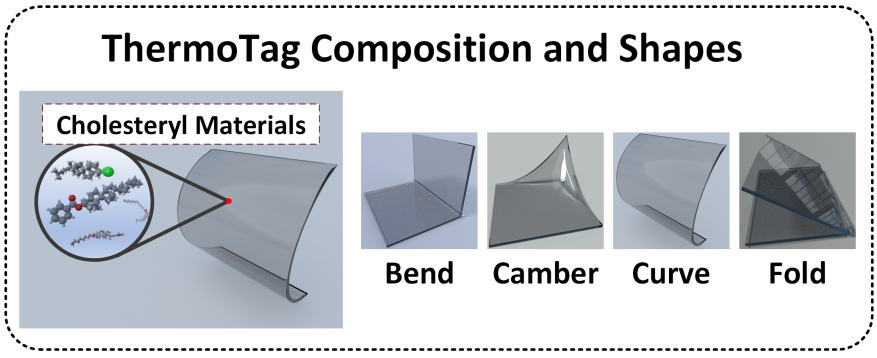


Figure 6.5: ThermoTag utilizes soft cholesteryl material that can be manufactured and stressed into various shapes for complex deployment scenarios.

to the Flory−Huggins parameter χ [77], expressed as:

$$\chi(T) = \frac{v_0}{kT}(\delta_1 - \delta_2)^2, \tag{6.1}$$

where T is temperature, and $\chi(T)$ is the Flory−Huggins parameter as a function of temperature, v_0 is the volume of the cholesteryl mixture, δ_1 and δ_2 are the solubility constants for the cholesteryl material polymers in the mixture, k is the real gas constant. The above presents a crucial monotonous relationship between the temperature of ThermoTag and the Flory−Huggins parameter of the material, which generalizes the underlying molecular alignment pattern, This facilitates further interpretation of temperature through the physical trait using wireless means.

When the interrogation mmWave signal reaches ThermoTag (i.e., cholesteryl material mixture), the tag will generate a frequency-shifted scattering based on temperature as shown in Fig. 6.4. The temperature-induced frequency shift relationship is formulated in Eq. (6.2):

$$\lambda_r(\lambda_i, T) = \lambda_i cos\frac{1}{2}[(sin^{-1}(\frac{l}{l'}sin(\Phi_i)) + sin^{-1}(\frac{l}{l'}sin(\Phi_r(\chi(T)))], \tag{6.2}$$

where l is the index of refraction of the environment (e.g., air), and $l^{'}$ is the index of refraction of cholesteryl mixture. Assuming the relative location and orientation between the ThermoTag and ThermoScanner does not change during the period of sensing, Φ_i being the angle of entrance for the incident wave, can be replaced with a constant. Φ_r is the angle of exit for the return wave as a function of the temperature dependent Flory-Huggins parameter χ, which bases on temperature T. Upon removing potential constant values, a lean model is derived in Eq. (6.3),

$$\lambda_r(\lambda_i, T) = \lambda_i cos[\Phi_r(\chi(T))], \tag{6.3}$$

where T is the temperature, λ_i is the frequency of the incident wave, and $\lambda_r(\lambda_i, T)$ is the frequency of the response wave [89, 113]. It is noteworthy that thermal scattering emits a frequency modulated response signal at all directions, allowing flexible deployment of ThermoTag in various scenarios.

To summarize, ThermoTag's underlying molecular alignment is changed by the variation of temperature, such alignment variation further affects thermal scattering properties for mmWave.

6.4.3 ThermoTag Ecology Analysis

ThermoTag is an organic tag based on cholesteryl materials which is biodegradable [231]. ThermoTag is also highly reusable due to the relatively low melting point and can be used to forge a new tag with different shapes without losing significant volume. ThermoTag's ecological life cycle begins with cholesteryl materials being mixed by heating the solid mixture into liquid, the liquid is then poured to mold for shaping. During the molding and shaping stage, it is important that the mixture is kept at a high temperature (around 300 F) which allows the liquid to keep flowing and change shape. The resulting tag can be reused immediately after cooling. Any residue without contamination can be collected and melted for another reuse cycle. Therefore, ThermoTag allows the reuse and safe disposal of cholesteryl material and is an ecological sensor.

6.5 ThermoDot Sensing Scheme

6.5.1 Thermal Scattering Response Acquisition

ThermoTag scatters frequency-shifted response signal with modulated temperature information as the intrinsic property. It is essential to ensure that ThermoScanner receives and parses different frequency shifts that occur at different temperatures. Most of the mmWave radars support both pulse and continuous wave modes. High amplitude pulse waves can undermine the thermal scattering effect in return, making temperature prediction difficult. The continuous wave mode allows continuous reception of thermal scattering from ThermoTag, which enables a higher sampling rate. Therefore, the ThermoWave design selects the continuous wave mode with a frequency modulated

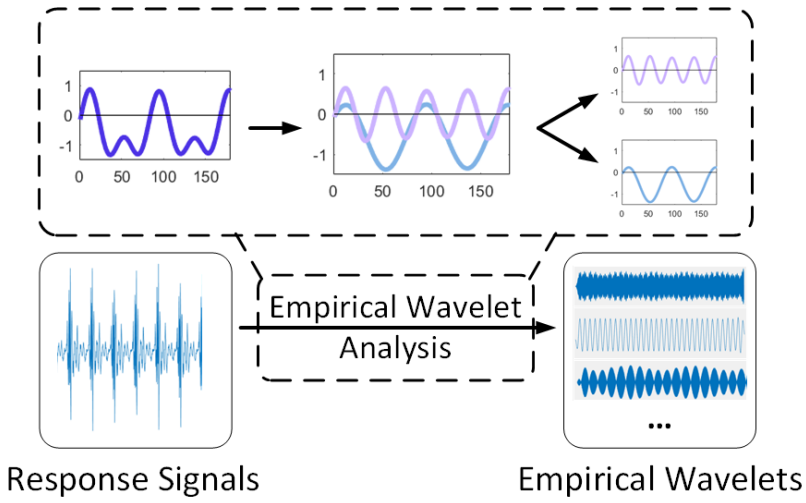


Figure 6.6: Empirical wavelet analysis transforms acquired signal into a series of wavelets for frequency analysis.

continuous wave (FMCW) radar. When ThermoScanner emits the interrogation signal from TX terminal to illuminate ThermoTag, ThermoTag undergoes the thermal scattering effect. This allows ThermoScanner RX terminal to receive the response with intrinsic thermal scattering effects. It is worth mentioning that such sensing mechanism is not restricted by the orientation setup as the scattering of ThermoTag's modulated response signal occurs in all directions. Finally, the thermal scattering response encapsulating temperature characteristics is acquired and passed to the ThermoSense module.

6.5.2 Scattered Signal Transformation

To perform the effective temperature estimation, there are critical pre-processing and transformation operations (i.e., filtered, decomposed) to facilitate an accurate frequency shift analysis. Since the frequency shift characteristic is crucial in thermal scattering response yet highly complex (i.e., variance in thermal scattering response's amplitude and frequency is non-memorizable due to large bandwidth), we propose to utilize a signal decomposition technique that separate thermal scattering signals into a set of wavelets to allow effective and efficient amplitude-frequency spectral analysis. Thus, we

utilize Empirical Wavelet Transform (EWT) [99] to perform frequency domain analysis by detecting local maxima in the wavelet spectrum in our application.

To formulate EWT, we show the reconstruction of the ThermoTag response signal that is separated into a series of wavelets by EWT, whose sum infinitely approaches the original thermal scattering response:

$$f(t) = W_f^{\epsilon}(0,t) \star \phi_1(t) + \sum_{n=1}^{N} W_f^{\epsilon}(n,t) \star \psi_n(t), \tag{6.4}$$

$$f(t) = (\hat{W_f^{\epsilon}}(0,\omega)(\hat{\phi_1}(\omega) + \sum_{n=1}^{N} (\hat{W_f^{\epsilon}}(n,\omega)(\hat{\psi_n}(\omega))^{\vee}, \tag{6.5}$$

where $f(t)$ is the synthesized signal that infinitely approaches original ThermoTag's thermal scattering response, t is time, ω is a wavelength, which is inversely proportional to frequency, $\phi_n(\omega)$ is the empirical scaling function, $\psi_n(\omega)$ is the empirical wavelets, N is the number of wavelets in total. $W_f^{\epsilon}(0,t)$ is the approximation coefficients, and $W_f^{\epsilon}(n,t)$ is the detail coefficients given by the inner products with the empirical wavelets. Eq. (6.5) is the representation of Eq. (6.4) wavelet reconstruction in terms of fourier transform that displays frequency-domain wavelet summation. To this end, the signal is decomposed into a series of empirical wavelets as shown in Fig. 6.6 for feature extraction.

Table 6.1: Feature List in the ThermoDot model

Types	**Features**
Spectral	Crest Factor [31], RMS Amplitude, Flatness [136], Skewness [160], Kurtosis [79], PNCC-20, MFCC-5
Temporal	Lowest Value, 50th percentile, Mean Value, 75th percentile, Highest Value, Standard Deviation, Kurtosis, Skewness

6.5.3 Feature Extraction

Thermal scattering response is characterized by the frequency shift alone with amplitude variations, making simple model-driven approaches quickly fail due to the complexity of spectral data in a bandwidth of 250MHz. Thus, we implement feature extraction from the wavelets that can accurately and effectively describe the frequency-shifted signals without concern from noisy signal impacting sensing accuracy. To comprehend the thermal scattering response, we enlist features in two types, i.e., spectral and temporal features. It is noteworthy that we employ spectral analysis that takes the signal to filter, then analyze the distribution of signal intensity. For instance, mel-frequency cepstral coefficients (MFCC) [152, 191, 200, 256] and power-normalized cepstral coefficients (PNCC) [49, 126, 170] are exceptional power-frequency distribution analyzers that provide detailed comprehension of the frequency shift and is capable of reducing noise impacts in the later prediction. Notably, PNCC are scalar coefficients based on gammatone channel filtering. The channel bias minimization is used to suppress the noise effects as shown in Eqs. (6.6) and (6.7) [217]:

$$V[f,c] = (\frac{kP[f,c]\widetilde{S}[f,c]}{\mu[f]})^{1/15}, \tag{6.6}$$

where $V[f,c]$ is the power function non-linearity, f and c are the frame and channel indices, respectively. k is the DFT size, empirically determined to be 1024. $P[f,c]$ is the result of the signal after Pre-emphasis, Short-Time Fourier Transform, Magnitude Squared, and Gammatone Frequency Integration. $\widetilde{S}[f,c]$ is the result of $P[f,c]$ after medium-time power calculation, asymmetric noise suppression with temporal masking, and weight smoothing. $\mu[f]$ is the mean power estimate of frame f formulated in Eq. (6.7):

$$\mu[f] = \lambda_\mu \mu[f-1] + \frac{(1-\lambda_\mu)}{C} \sum_{C-1}^{c=0} T[f,c], \tag{6.7}$$

where C represents the total number of frequency channels. λ_μ is empirically determined to be 0.999 as the forgetting factor. $T[f,c]$ is the the result of $\widetilde{S}[f,c]$ after time-

frequency normalization by elementary multiplication of $P[f, c]$ and $\widetilde{S}[f, c]$. The initial value of $\mu[f]$, $\mu[0]$, is determined to be 16161 dB/Hz based on the mean power of signals using the data set in our preliminary study.

The power function non-linearity then goes through a discrete cosine transform. The resulting matrix is converted into a one-dimensional array to reduce the feature count for better efficiency, i.e., generating 20 coefficients from 20 Gammatone channels, respectively. The origin of PNCC work includes the operation of mean normalization, considering that the feature coefficients are used for the regression analyzes. Note that mean normalization is opted out because this operation will not provide further benefits in thermal analysis. Up to this point, scalar coefficients are effectively collected for regression. The complete feature list categorized into two types(i.e., Spectral, Temporal) is shown in Table 6.1.

6.5.4 ThermoDot Regression Model

The feature array of 38 scalar values are extracted from each segment of RF signals, and we feed the feature arrays with one temperature label (i.e., the ground truth) into a regression model to solve the prediction modeling problem as shown in Algorithm

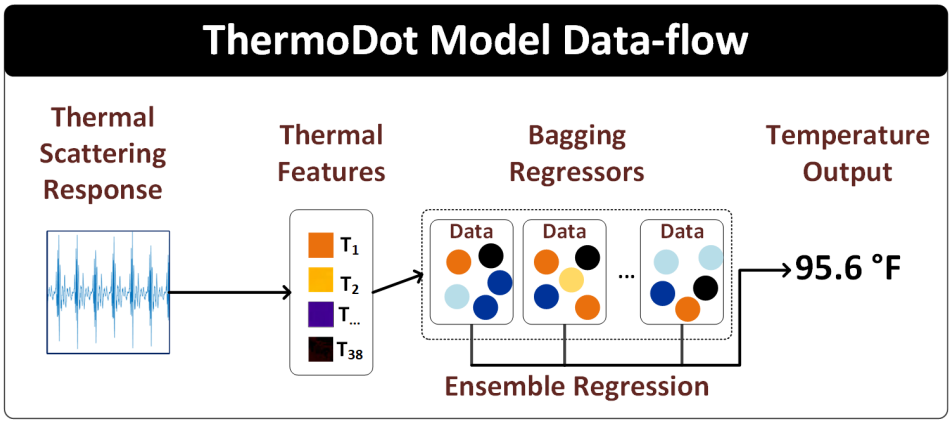


Figure 6.7: ThermoDot model data flow from thermal scattering response to exact temperature value.

5. We start with choosing a meta-algorithm to perform the task. There are two major advantages for employing the bootstrap aggregation (bagging) method [142]. 1) Ensemble learning allows multiple regressors to generate independent prediction results and aggregate them into the final decision with better confidence. Weighting is given by the accuracy of each separate regressor to boost the accuracy of the final decision, enabling higher accuracy. 2) Bagging allows a low variance value that makes the output more stable in temperature prediction, which prevents overfitting. The series of feature arrays are fed into a bagging model that utilizes the ThermoDot model in Algorithm 5 to perform the regression prediction and return temperature estimation corresponding to the feature arrays. After feeding the bagging regressor with a list of feature vectors as input and a list of temperature values as the ground truth, the regressor solves the discrete parameters to fit training data. The resulting ThermoDot model will then take in thermal scattering response and return a single value temperature output as shown in Fig. 6.7.

Algorithm 5: ThermoDot Algorithm

Input: S: mmWave signal; L: Signal segment count; K: Feature count; M: Trained regression model; ε: Number of trees
Output: T: Point Temperature Prediction Results

```
Initialize T = [ ];
M = loadModel();
S_w = EWT(S);
for i = 1, 2, ..., L do
    ϱ = S_w(i);
    Initialize features = [ ];
    for j = 1, 2, ..., K do
        ϑ = featureFunction_j(ϱ);
        features.append(ϑ);
    end
    t = M.Regression(features, ε);
    T.append(t);
end
return T;
```

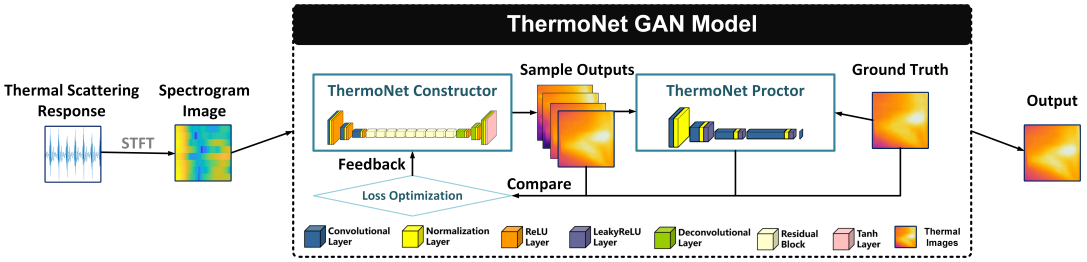


Figure 6.8: ThermoNet leverages spectrogram image from thermal scattering response and its corresponding ground truth thermal image to train the image-to-image neural network model, the resulting model has the capability to generate thermal images from spectrogram images. The ThermoNet Constructor keeps generating sample outputs based on spectrogram image while the ThermoNet Proctor decides whether the sample output is close enough to the ground truth. When the ThermoNet Proctor denies the sample output, the results are compared and sent to Loss Optimization for ThermoNet Constructor to generate better (i.e., more accurate) output in the future.

6.6 ThermoNet Sensing Scheme

6.6.1 Thermal Scattering Response to Spectrogram Transformation

The objective of thermal imaging is the retrieval of surface temperature in the form of a thermal image from a thermal scattering response. To realize it, the first step is to transform a thermal scattering response signal from one-dimensional spectral-temporal function, into a two-dimensional spectral-image function. Based on the advantage that continuous-time short-time Fourier Transform (STFT) is more applicable for real-time processing compare to two-dimensional wavelet transform's high computation overload, we adopt STFT [61] for converting the spectrogram signal into a three-dimensional representation, formulated as Eq. (6.8):

$$STFT\{x(t)\}(\tau,\Omega) = \int_{-\infty}^{\infty} x(t)\Omega(t-\tau)e^{-j\lambda t}dt, \tag{6.8}$$

where $\Omega(\tau)$ is the Gaussian window function, $x(t)$ is the signal to be transformed, λ is the frequency and $STFT\{x(t)\}(\tau,\Omega)$ is the resulting spectrogram image that captures

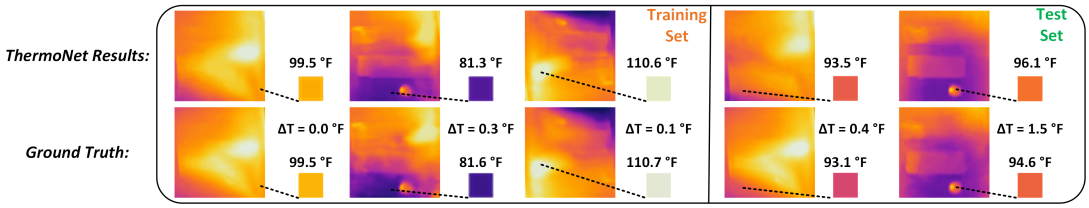


Figure 6.9: Comparison between thermal images generated by ThermoNet and ground truth. ThermoNet is capable of capturing the details on thermal image and regenerating them in prediction, making target detection possible using edge detection. With a large amount of training samples, ThermoNet meets the expectation of generating thermal images in untrained (test set) scenarios that are also extremely close to the ground truth in terms of both image structure, and image detail.

essence of thermal scattering response. The result is a three-dimensional data, we map one of the dimensions to color space in order to generate a temperature image. At this point, the problem is reduced to mapping a spectrogram image to a correct thermal image.

6.6.2 ThermoNet Model Construction

In order to solve the spectrogram image to thermal imaging mapping problem, pixels in spectrogram image must be mapped to pixels in thermal image. Such mapping must not only capture the general color to color relationship, but the image structure, which encapsulates the temperature distribution over the thermal image. However, a typical thermal image have over 65,536 pixels (256x256), which can lead to four billion links to a 65,536 pixel spectrogram image, making it nearly impossible to compute over short period of time in temperature sensing applications. Thus, we implement a neural network to solve the image to image mapping problem. We employ the Pix2pix model [117], which is a Generative Adversarial Network (GAN) [102] model specifically designed for image-to-image transformation tasks. Different from Convolutional Neural Network (CNN)'s dependency on a fixed loss function to optimize the neural network, GAN implements an adaptive loss function, this allows GAN to solve problem of neural network generation without a cumbersome loss function design. We formulate

the ThermoNet model as follows:

$$\min_G \max_D V(D,G) = E_{\zeta \sim p_{data}(\zeta)}[logD(\zeta)] + E_{z \sim p_z(z)}[log(1 - D(G(z)))], \tag{6.9}$$

$$\max_D V(D) = E_{\zeta \sim p_{data}(\zeta)}[logD(\zeta)] + E_{z \sim p_z(z)}[log(1 - D(G(z)))], \tag{6.10}$$

$$\min_G V(G) = E_{z \sim p_z(z)}[log(1 - D(G(z)))], \tag{6.11}$$

where G is the generator (i.e., constructor) function, D is the discriminator (i.e., proctor) function, z is the input data being our image from spectrogram transform, and ζ is the training data being temperature image from IR camera. To achieve an ideal transformation result, *ThermoNet* requires a Constructor and a Proctor to collaborate and compete against each other.

(a) Constructor is a network of "encoder-decoder" structure. The encoder has a three-layer convolution structure with a first layer depth of 64, the second layer depth of 128, and the third layer depth of 256. Each layer is followed by a ReLU activation function. In order to abstract and retain more information, we add more weighted layers between the encoder and the decoder. We use nine residual blocks because the residual blocks contain skip connections which can concatenate all channels between layers. To capture the details in image, the decoder is designed with three layers of deconvolution layers that upsamples the image by eight times larger, magnifying small differences in the image.

(b) Proctor is a network of "encoder" structures that contains four layers of convolution. The other three convolutions use LeakyReLU, except that the first layer uses the ReLU activation function [244]. The proctor is capable of determining whether the image from the constructor is similar enough compared to the ground truth. The binary

decision generated by the proctor is then sent to an optimizer that allows the constructor to generate better results.

The workflow is shown in Fig. 6.8, as the constructor produces batches of thermal images as sample output, the proctor determines if the generated thermal image outputs are close enough to the ground truth thermal image. The output thermal images from the proctor and the losses were sent to the optimizer, then, the optimizer enhances the weights in the constructor. In the end, the trained ThermoNet model is able to produce temperature images given the input of spectrogram image without the exact temperature image in training database as shown in Fig. 6.9.

6.7 Evaluation setup

6.7.1 Experimental preparation

To evaluate the system, we conduct controlled experiments in a lab condition. The experiment setup is shown in Fig. 6.10. We fabricate the ThermoTag using a square thin film with a side length of 15 cm and a thickness of approximately 0.01 cm. The ThermoTag is attached to the inner wall of the cabinet, while ThermoScanner is

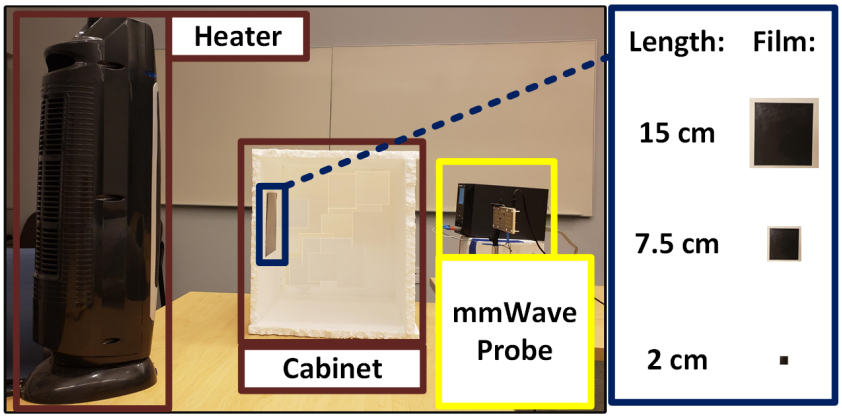


Figure 6.10: The film shaped ThermoTag is attached to the left wall inside the cubic foam cabinet, ThermoScanner is placed on the outer of right wall of the cabinet. The heater heats up the air in the cabinet, and thus heating up ThermoTag.

placed outside the cabinet. We then align the ThermoScanner to the direction of the ThermoTag starting from a distance of 25 cm. Note that there is no physical blockage between ThermoTag and ThermoScanner except the wall of cabinet box in the overall performance study. Room air temperature is held constant at 70 F to eliminate variation in heat dissipation across different evaluation experiments. To collect ground truth , we utilize a wired thermometer with precision of $\pm 1.0F$ and an IR camera with precision of $\pm 3.0F$ to compare with results from ThermoDot and ThermoNet, respectively [5, 39]. We evaluate the system performance under the temperature ranging from 30F to 120 F for all experiments that can satisfy various scenarios such as room temperature monitoring and food/medicine package temperature monitoring.

Application Protocol: To make ThermoWave easily deployable, the system employs a ready to sense protocol that automatically performs a scan for ThermoTags in the environment. After a ThermoTag is localized, ThermoScanner will continuously interrogate the tag for thermal scattering response, and perform temperature inference using ThermoDot and ThermoNet.

Data Collection and Preparation: Due to ThermoWave's paradigm containing two modules with unique output, two separate groups of ground truth data are collected for ThermoDot and ThermoNet. Utilizing the digital thermometer, a camera is placed to record the continuous temperature change of ThermoTag and the temperature values are obtained using optical character recognition. As a result of high-speed continuous data collection from ThermoScanner, 90,000 lines of feature array is collected, and a 75%-25% split is utilized to separate the training and testing data. For the IR camera, its seven frames per second video frame rate forced ThermoNet's sampling rate to seven Hz with alignment. ThermoNet is a data-intensive model, we collected 105,790 thermal images and generated the same number of spectrogram images for ThermoNet model training and testing. To effectively assess the performance of the two models, we collect a single group of data for training, and test it against different scenarios that were not trained.

6.7.2 Performance Metrics

To analyze the ThermoWave performance in both dot-wise sensing and thermal imaging, we introduce performance metrics tailoring to ThermoDot and ThermoNet's output data format.

6.7.2.1 ThermoDot Metrics

In order to assess ThermoDot's ability to correctly derive a single temperature value from a specific location using mmWave signal, we prepared three numerical metrics to evaluate the performance of dot temperature sensing, including percentage accuracy, maximum error, and correlation coefficient.

Percentage accuracy: Correct temperature prediction is defined as value predicted within the precision tolerance (i.e., threshold) of ground truth value.

Maximum error: Average of the top 1% error between the predicted value and ground truth value.

Correlation coefficient: To have a general grasp on how close is the predicted temperature value to ground truth temperature value, the correlation coefficient is employed [134]. A higher value (with a maximum value of 1) indicates better routine system performance.

6.7.2.2 ThermoNet Metrics

The metrics for ThermoNet need to consider the two-dimension characteristics of the output and ground truth. Since thermal imaging is commonly done by IR systems as a two-dimensional image reading with each pixel containing RGB components, we used the IR imaging system FLIR ONE PRO with approximately $\pm$ 3.0 F precision as our ground truth. To evaluate the thermal imaging performance at both macro and micro levels, we utilize a total of three metrics that can effectively compare the similarity between two images.

Structural Similarity Index: We utilize Structural Similarity Index (SSIM) [236, 237] for the thermal image structural comparison between prediction and ground truth. SSIM is based on three measures of two thermal images, i.e., luminance, contrast, and structure, which correlates to intensity, distribution, and target location in the thermal image. The SSIM we used is formulated as:

$$SSIM(p, g) = [l(p, g)] * [c(p, g)] * [s(p, g)], \tag{6.12}$$

where p and g are the predicted thermal image and ground truth thermal image, respectively. When the value of $SSIM\ (p, g)$ reaches 1, p and g shares the highest similarity, which means the predicted thermal image is nearly identical to the ground truth. $l(p, g)$, $c(p, g)$, and $s(p, g)$ are the individual measure of the similarity in luminance, contrast, and structure, respectively.

Peak Signal to Noise Ratio: We use an MSE based peak signal to noise ratio (PSNR) to verify the estimated thermal image quality as calculated below:

$$MSE = \frac{\sum_{a=1,b=1}^{A,B}[I_1(a, b) - I_2(a, b)]^2}{A * B}, \tag{6.13}$$

where a and b are indices of 2-D image under the thermal image resolution (A,B) pixels in horizontal and vertical axis, respectively. I_1 is the ground truth, and I_2 is the generated thermal image. Based on MSE, the PSNR is formulated as:

$$PSNR = 10 \log_{10} \frac{R^2}{MSE}, \tag{6.14}$$

where R is the maximum value of each pixel value in I_1 and I_2 (i.e., R is 255 if I_1 and I_2 is read as uint8 format and R is 1 if I_1 and I_2 is read as floating point format).

Percentage Accuracy: Percentage accuracy is calculated via counting the number of pixels in the generated thermal image (I) that are within Δ distance from ground truth thermal image (T) and dividing by the total number of pixels in the thermal image.

Percentage Accuracy can be expressed as:

$$Accuracy = \frac{count(|I - T| < \Delta)}{count(I)} * 100\%, \tag{6.15}$$

6.8 ThermoWave Evaluation

6.8.1 Overall Performance

We evaluate the temperature inference accuracy from multiple aspects for both dot-wise temperature sensing and thermal imaging.

Dot-wise Performance. ThermoDot shows reliable performance in dot-wise temperature sensing by accurately reading the temperature values of ThermoTag. As shown in Fig. 6.11, the bagging algorithm shows the best performance compare to LSBoost and Random Forest. By comparing the prediction results of ThermoDot to the ground truth temperature values, the correlation coefficient is determined to be 0.99993. This means that ThermoDot's prediction result is extremely close to the actual temperature value if not exactly the same. With the maximum error being $\pm$0.97 F, ThermoDot's precision in temperature inference can be determined to be $\pm$1.0 F, which is exactly the same as the ground truth temperature measuring device. In other words, ThermoDot's exceptional temperature inference performance is not over-fitted, and arguably bottle-necked by the ground truth sensing device. For percentage accuracy, ThermoDot is capable of returning 99.9% of temperature readings under the precision of $\pm$1.0 F. For all subsequent evaluations, the highest accuracy possible would be the 100% with the standard precision of $\pm$1.0 F.

Thermal Imaging Performance. ThermoWave system relies on ThermoNet module to produce thermal images, and the temperature image can be analyzed two-fold. First, in a two-dimensional temperature matrix perspective, each pixel is changed to temperature based on color, ThermoWave achieves an overall accuracy of 99.16% under the precision of $\pm$3.0F across the two-dimensional sensing range with MSE is calculated to

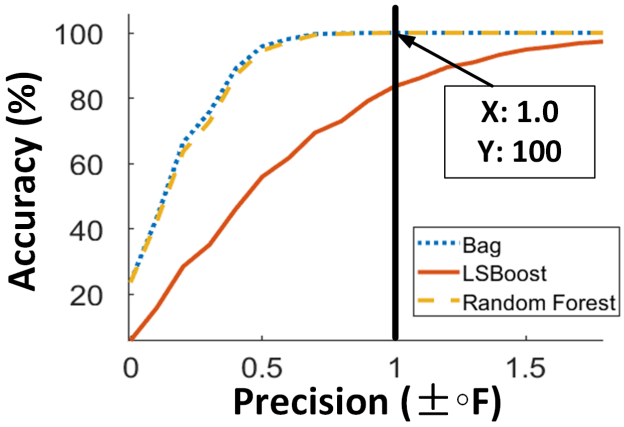


Figure 6.11: Micro-benchmark of temperature recognition accuracy versus precision tolerance comparing three typical regressor algorithm.

be 2.2351. At around 85 F, the temperature imaging device has a precision of approximately ±5F, which states that given a more accurate ground truth device, ThermoNet's performance in per pixel temperature accuracy can be higher than the IR imaging device. On the other hand, the two-dimensional data is viewed as a stand-alone image, PSNR is calculated based on the prediction result from ThermoNet to ground truth IR image. Examples of the image-to-image comparison are shown in Fig. 6.9. PSNR is determined to be 23.9872 for the collection of the standard data set. The SSIM from generated temperature image to the ground truth temperature image is determined to be 0.9439, with SSIM being close to 1, meaning the generated image and ground truth image is very close, ThermoWave proves to be an accurate system.

6.8.2 Performance of Different Configurations

When ThermoWave system is applied in different scenarios, it is common that parameters such as sensing distance will vary from experiment condition. We evaluate ThermoWave system with different parameter variations to assess the reliability.

ThermoTag Shape. When ThermoTag is shaped to conform with the sensing target's surface, the shape alone might have an impact in the temperature recognition. Thus, we

test ThermoTag in irregular shapes such as bend, camber, curve, and fold to simulate various conditions such as sensor taped to the wall, fixed into corners, and tied to cables. The result shows ThermoWave system remains in high performance with dot-wise temperature inference score averaging to 99.9 % accuracy, ± 1.4522 F max error, and 0.9993 correlation coefficient. ThermoNet scores average to 23.5174 PSNR and 0.9407 SSIM. In conclusion, ThermoWave is able to retain 99% accuracy at all four tag shapes for both dot-wise temperature sensing and thermal imaging. The performance is shown in Fig. 6.12, results have proven that ThermoWave system is fully functional with different tag shapes.

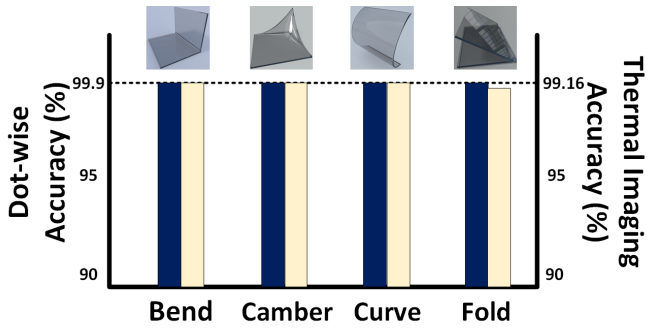


Figure 6.12: Performance for both dot-wise temperature and thermal imaging under different ThermoTag shapes.

ThermoTag Size. A crucial parameter of the sensor is its physical size (i.e., surface area in thin-film format), which directly contributes to the occurrence rate of thermal scattering effect. Thus, it is necessary to examine the impact of ThermoTag size to ThermoWave system performance. We used three sizes of square-shaped sensors with length 15 cm, 7.5 cm, and 2 cm as shown in Fig. 6.10. Performance scores are shown in Table 6.2 and 6.3 for dot-wise temperature sensing and thermal imaging, respectively. It

Table 6.2: Dot-wise evaluation performance of different ThermoTag sizes.

Sensor length	Accuracy (%)	Maximum error (F)
2 cm	**99.8**	1.5
7.5 cm	**99.9**	1.2
15 cm	**99.9**	1.0

is also noteworthy that the distance capacity of ThermoTag in relation to the size is expected to exhibit a positive correlation. Our intuition is to use radar cross-section (RCS) to estimate the distance capacity in free space. However, the thermal scattering effect is different from the material's reflection property, making RCS an inaccurate description. Thus, we empirically determine the distance capacity of a ThermoTag with a 2 cm side length to be 50 cm. The overall high sensing accuracy result proves ThermoWave system is highly reliable with different sensor sizes for various application scenarios.

6.9 Robustness Analysis

6.9.1 Impact of Occlusion

One critical feature of ThermoWave system is passive wireless and functions in NLOS scenarios. Thus, we chose four universal occlusion scenarios in such packaging material occlusion, the thickness for bubble bag, foam, paper, wood subjects are 1.0 cm, 1.0 cm, 0.01 cm, 6.35 cm, and 2.54 cm, respectively. Among the thermal imaging assessments, ThermoWave system keeps PSNR above 22.5 and 0.95 SSIM for all four occlusions as shown in Fig. 6.13, proving its usability. Without surprise, the IR camera's result showed a thermal image for the blocking object instead of ThermoTag during the heating and cooling period, which stayed the same throughout the experiment session. This result shows ThermoWave's a crucial advantage over existing IR cameras that utilizes mmWave as media to communicate with ThermoTag that achieves thermal imaging in NLOS scenarios.

Table 6.3: Thermal imaging evaluation performance of different ThermoTag sizes

Sensor length	Accuracy (%)	PSNR	**SSIM**
2 cm	97.7	21.1184	**0.9435**
7.5 cm	99.1	23.5449	**0.9436**
15 cm	99.2	23.9872	**0.9439**

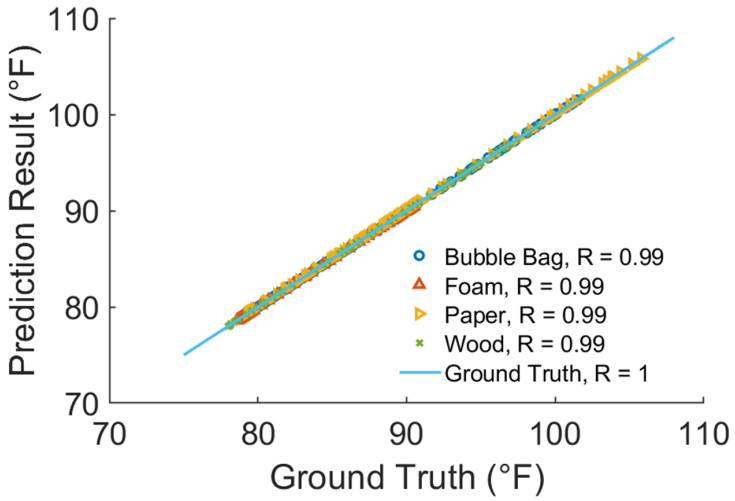


Figure 6.13: Dot-wise Performance under occlusion.

6.9.2 Impact of Sensing Distance

To validate ThermoWave's usability in contact-less (i.e., zero to ten cm) and wireless (above 50 cm) application scenarios, we performed a series of experiments with sensing distance ranging from 0.25 m to 2 m. Results have shown minimum accuracy change (i.e., above 99%) as the ThermoTag with side length 15cm moved up to two meters. Based on the sensing capacity of mmWave, ThermoWave system is expected to perform highly accurate temperature sensing with a further distance than two meters. Thus, ThermoWave is capable and suitable for many industrial applications such as cold chain transportation in logistics.

6.9.3 Impact of Scanning orientation

The impact of sensing angle is a common concern when testing wireless communication, and it is important to have a device that works with various sensing angles to be robust. Therefore, we measure the dot-wise performance of ThermoWave by having a ThermoTag fixed on top of the sensing target, and ThermoScanner to move around the sensing target for angular adjustments. Due to the fact that the film shaped Thermo-

Tag is symmetrical on all axis, we measure angles from 0 degrees to 90 degrees with 15 degrees of increment. Based on performance results shown in Fig. 6.14, the percentage accuracy was in the high 90s from 45 to 90 degrees with a correlation coefficient averaging to 0.9985, proving ThermoWave is strong with different sensing angles for various sensing applications.

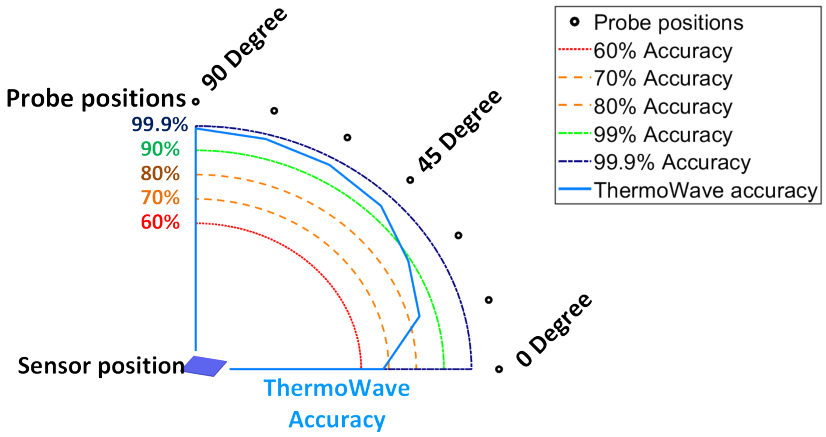


Figure 6.14: ThermoDot performance under different scanning orientations with ThermoTag fixed in location and ThermoScanner rotating around.

6.9.4 Impact of Sampling Rate

It is very worthy to mention the importance of the time that ThermoWave takes to acquire a signal, which is directly proportional to the temporal efficiency in applications. Thus, we assess ThermoWave's performance under various sampling rates for both dot-wise and thermal imaging models. While the wired thermometer can give continuous readings for ThermoDot ground truth, the IR camera has a limitation of around seven frames per second, limiting the sampling rate for ThermoNet's ground truth. Thereby, we examine ThermoWave's sampling rate from one Hz to seven Hz. Results show that ThermoWave can achieve a 7 Hz sampling rate without significant loss of accuracy, as shown in Fig. 6.15.

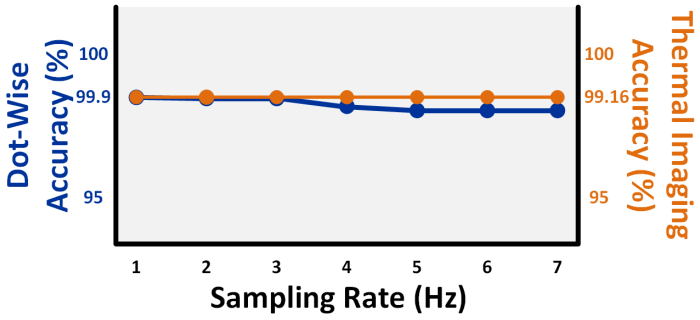


Figure 6.15: Both ThermoDot and ThermoNet's accuracy performance at sampling rates from one Hz to seven Hz.

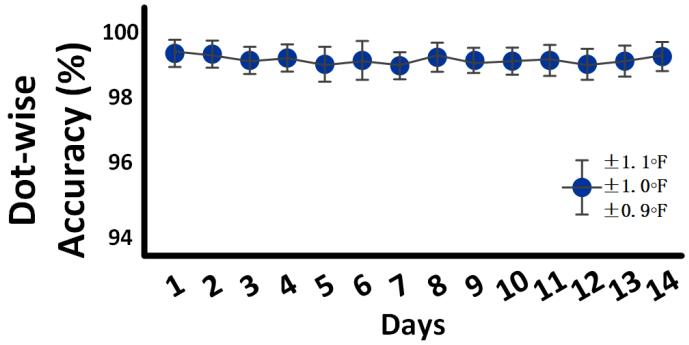


Figure 6.16: Plot of accuracy against time in days into permanence experiment across two weeks of testing period.

6.9.5 Permanence Analysis

To investigate the permanence of ThermoWave, we collected multiple sessions of dot-wise temperature data on a single ThermoTag across three weeks. In the first week, approximately ten samples of data (i.e., temperature value ranged $35F$ to $80F$ with $0.1F$ resolution) is collected each day to train a ThermoDot model. In the next two weeks, two samples of untrained data are collected each day for testing the pre-trained ThermoDot model, and the predicted temperature vs. ground truth temperature is used to measure the accuracy. As shown in Fig. 6.16, ThermoDot model delivered over 99% of prediction is within the $\pm 1.0F$ precision, proving the ability to sustain a long period with high accuracy.

6.9.6 Environmental Dynamics

To determine whether ThermoWave can function under different environmental interferences such as humidity and vibration, a ThermoTag's thermal imaging performance is tested in simulated conditions. For the humidity simulation, a humidifier is placed in front of the cabinet, and air at near dew point is blown into the cabinet to ensure ThermoTag is surrounded with humid air. For the vibration simulation, an actuator is placed on top of the cabinet vibrating consistently to introduce pseudo-random vibration to the ThermoTag. The result in Fig. 6.17 proves that ThermoWave can maintain high accuracy while under humid and shaking conditions.

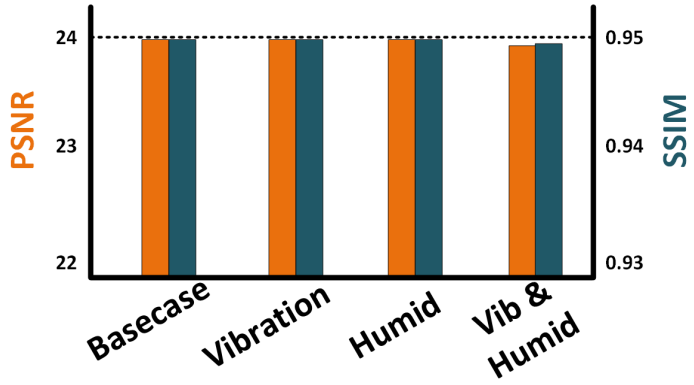


Figure 6.17: ThermoWave thermal imaging performance under environment interferences.

6.10 Real World Test

To ensure that ThermoWave system remains accurate temperature sensing performance when it leaves lab condition, thus, we deploy ThermoWave in a complex scenario where multiple tags exist in a compact and NLOS setting with environmental disturbances. To determine ThermoWave's capability of recognizing multiple ThermoTags in a complex scenario, we attach two ThermoTags to the back of a storage box that is 20 cm away from each other (i.e., on the upper left corner and the lower right corner

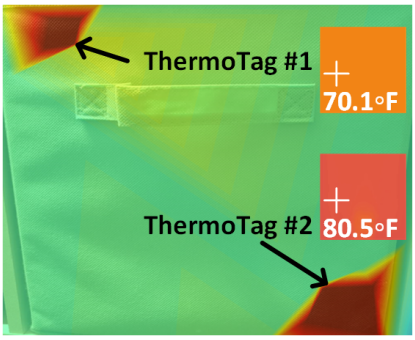


Figure 6.18: Two ThermoTags in the shelf box for thermal imaging.

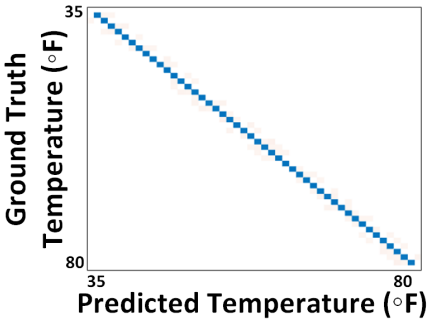


Figure 6.19: Dot-wise temperature performance for the two ThermoTags in the box.

of the box) for sensing. Next, to determine its resistance toward environmental dynamics such as vibration and humidity, arbitrary water vapor in heated air is blown into the box while an actuator is generating arbitrary vibration inside the box. As shown in Fig. 6.18 and 6.19, ThermoWave is capable of identifying the positions of each ThermoTag and accurately reading thermal images. The confusion matrix consists of dot-wise temperature prediction accuracy for both of the ThermoTags. The average accuracy is determined to be 97.7% with $\pm$1.0F precision. In conclusion, ThermoWave system is capable of accurately recognizing ThermoTags position as well as inferring each of their temperature for both dot-wise and thermal imaging.

6.11 Discussion and Limitations

ThermoNet modeling: It is ideal to have a model that specifies which segment of thermal scattering response corresponds to a specific pixel in the resulting thermal image. Thus, it is appealing to utilize ThermoDot's model and expand feature extraction upon multiple frequencies to a dimension that matches the number of pixels in the ground truth. However, this technique is hindered by the computational overload and mmWave beam-forming precision, which is too costly and too blurred at long distance, real-time sensing. Thus, the current data-driven GAN methodology is applied.

Potential Medical Applications: ThermoTag's cholesteryl material is a common steroid chemical in mammalian organism's body [147, 169], meaning it is not inherently toxic and is often researched in the medical domain. Beyond the experimentation of this chapter, it is foreseeable that ThermoTag will be applied to human body for medical purposes and possibly in the human body for fine-grained temperature monitoring. In addition, ThermoScanner's electromagnetic radiation is powered at 1.2 W with 8dBm radio transmission power at the range of two meters, which is insignificant when compared to modern wireless communication infrastructure, such as Wi-Fi. Moreover, the power can be further reduced in surgical application scenarios where the sensor is placed closer to the body. Thus, ThermoWave is a safe and ecological technology for medical applications in the near future.

Aging effect of film: It is common that material in the shape of film experience degradation(i.e., aging from wear, tear, or erosion). Preserving the shape of the sensor is also an important task in protecting the system. We came up with two solutions to protect ThermoWave film from the aging effect. **(i)** Cover the film with a protective material such as a thin sheet of PVC, which is tested in our evaluation experiments that have little effect on the overall ThermoWave system's overall sensing ability. **(ii)** Design a calibration protocol such that accuracy is tested periodically. Once the accuracy falls below a threshold, replace the ThermoTag.

Metallic Occlusion: It is worth to mention that metallic objects are excellent at reflecting radio frequency waves, making wireless communication difficult with metallic occlusion. Consequently, when a sheet of metal lays in between ThermoTag and ThermoScanner, the thermal scattering response is unlikely to be generated considering the blockage.

6.12 Related Work

Wireless Temperature Monitoring: Existing wireless temperature monitoring technology can be placed into two categories based on their output (i.e., dot-wise temperature and thermal image). The core of dot-wise temperature sensing systems [130, 179, 226, 235, 249, 251] is the thermal-electric sensor that delivers a temperature value. Such a solution associates with high cost (i.e., a single passive RFID temperature tag is at least $\$1.00$) and harms the environment with heavy metal in its circuity. Moreover, wireless temperature sensor such as the RFID tags are usually one-time use and create unsalvageable electronic waste [78]. On the other hand, thermal imaging devices reads temperature matrices by measuring the amplitude of electromagnetic wave in front of the imaging sensor, which fails if there is occlusion such as a piece of paper (e.g., infrared [151], mmWave [168]). Up to date, no wireless temperature monitoring technology is capable of ultra-low cost and ecological temperature sensing, as well as thermal imaging with occlusion.

mmWave Sensing: mmWave sensing has been growing popularity in different fields (e.g., 5G in telecommunication, object detection in autonomous driving, etc.) in recent years. Many focus on macro motion and three-dimensional geometry of target object such as electronic identification, human gesture recognition, heart motion sensing, and tag pattern identification [141, 143, 146, 238, 245, 260], while others focus on micro-motion and internal characteristic such as liquid classification and liquid crystal phase recognition [139, 180, 181]. To this date, ThermoWave is the first mmWave sensing system to perform ultra-low cost, ecological, and flexible temperature sensing using thermal scattering effect that achieves thermal imaging.

6.13 Conclusion

In this chapter, we develop a novel mmWave technology-based paradigm, ThermoWave, for wireless temperature monitoring. The ThermoWave design exploits the

thermal scattering effect, i.e., the changing ambient temperature can impact the scattering characteristics of the cholesteryl material when it is probed by RF signals. We fabricate a film-based temperature tag (i.e., ThermoTag) using cholesteryl material, which is attached to the target object. Then, we prototype a mmWave based ThermoScanner for interrogating thermal scattering response from ThermoTag. Finally, the response signals are fed to ThermoDot and ThermoNet model for dot-wise temperature recognition and thermal imaging, respectively. ThermoWave is capable of achieving the precision of $\pm 1.0°$F in the range of 30°F to 120°F for dot-wise temperature and $\pm 3.0°$F precision in thermal imaging. ThermoWave is promising to enable wireless signals to sense environmental and object temperature without the infrastructure support. Various experiments also proved the robustness of ThermoWave, demonstrating its potential to serve as the next-generation temperature sensing technology.

Chapter 7

Conclusion

7.1 Summary

In this dissertation, we propose a novel wireless meta-sensing technology to secure and identify the vulnerabilities of IoT devices and further empower a new paradigm of IoT with wireless inkables. This dissertation is the first to explore the connection between wireless sensing, material and component, and security and privacy analysis for IoT. From the IoT security view, this dissertation uncovers the security and privacy analysis with wireless meta-sensing on the material or components in the current commercial devices. From the IoT paradigm view, this dissertation also facilities a new paradigm shift from passive wireless sensing and analysis on existing material or components to active new wireless-chem material design impelled by the next IoT.

Our contributions can be summarized in the following four chapters:

- In Chapter 3, we proposed a hidden e-device recognition system E-Eye, to aid law enforcement and ensure security. We started from the basics characteristics of the e-device and cover material under the nonlinear effect. Then, we proposed a portable 24GHz mmWave probe and the e-device recognition module to accurately recognize the hidden e-device type. Furthermore, extensive experiments indicated that E-Eye could achieve excellent performance in hidden e-device recog-

nition with a millisecond-level response time for the security check and law enforcement.

- In Chapter 4, we first identified and validated a new and yet practical side-channel to infer contents on digital screen via the liquid crystal nematic state sensing in isolation scenarios. A novel end-to-end deep learning-based hierarchal module was designed to recognize the screen content type and retrieve the sensitive information on digital screens. Furthermore, extensive experiments indicated that the proposed WaveSpy achieves high inference accuracy through-wall within a middle distance with a centimeter-level screen solution, which can significantly reduce the attack cost.

- In Chapter 5, we presented a paper-based and mmWave-scannable tagging infrastructure FerroTag, to promote inventory management technologies. FerroTag is easy to use and low-cost, which is on the basis of ferrofluidic ink on the paper print and its interference to the mmWave signal. An end-to-end prototype based on a commercial inject printer and a software framework of detecting and recognizing a newly designed nested tag pattern are designed and implemented in practice. Extensive experiments, including one case study with complex scenes, imply that FerroTag can achieve superior accuracy in tag identification within a quick response time.

- In Chapter 6, we developed a novel mmWave technology-based paradigm for wireless temperature monitoring. The ThermoWave design exploits the thermal scattering effect, i.e., the changing ambient temperature can impact the scattering characteristics of the cholesteryl material when it is probed by RF signals. We fabricated a film-based temperature tag (i.e., ThermoTag) using cholesteryl material, which can be attached to the target surface. ThermoDot and ThermoNet models are designed for dot-wise temperature recognition and thermal imaging. The

experiments indicated that ThermoWave could greatly work for passive wireless temperature monitoring with high precision as a new paradigm of IoT.

7.2 Future Scope

In the near future, our research will continue to focus on hardware and software integration systems designs for high-impact social applications via wireless meta-sensing. There are also some potential directions to continue this dissertation.

Wireless Meta-sensing for Autonomous Vehicles Security: Autonomous vehicles, including aerial, ground, sea, and underwater vehicles, are becoming an integral part of our life. Compared to daily IoT devices (e.g., smartphones and smartwatches), autonomous vehicles have significantly powerful actuation, which can cause much more severe disasters after affected. The question of the security and privacy of autonomous vehicles rises rapidly. Wireless meta-sensing can detect the unique internal traits of the target autonomous vehicles to address abundant concerns about autonomous vehicle security, such as the in-situ drone authentication and adversarial attack on the autonomous vehicle.

Wireless Meta-sensing for Multi-functional Inkable Sensors: Inkable sensor is a new paradigm of IoT and AI Sensors. However, to build such powerful and versatile inkable sensors, there are still huge urgent needs for more wireless-chem material. Therefore, another promising direction is to embed the state-of-the-art multi-functional material into inkable sensors. We envision our system can achieve more sensing functionalities via wireless meta-sensing, such as monitoring air quality, pressure, and moisture.

Bibliography

[1] *TEMPERATURE SENSORS MARKET - GROWTH, TRENDS, AND FORECASTS (2020 - 2025)*. https://www.mordorintelligence.com/industry-reports/temperature-sensors-market-industry.

[2] *Printing Cost Calculator - Calculate Your Cost of Printing*. https://www.uniprint.net/en/printing-cost-calculator-calculate-cost/, Jul 2018.

[3] *10 Shocking Inventory Management Statistics*. https://blog.capterra.com/inventory-management-statistics, 2019.

[4] *Cholesteryl benzoate*. https://pubchem.ncbi.nlm.nih.gov/compound/Cholesteryl-benzoate, 2019.

[5] *FLIR ONE PRO*. https://www.flir.com/products/flir-one-pro/, 2019.

[6] *RFID vs Barcode: Comparison, Advantages & Disadvantages*. https://www.peak-ryzex.com/articles/rfid-vs-barcode-comparison-advantages-disadvantages, 2019.

[7] *Single-chip 76-GHz to 81-GHz automotive radar sensor integrating DSP and MCU*. https://www.ti.com/product/AWR1642#order-quality, 2019.

[8] *Temperature-sensitive foods: focus on packaging*. https://www.ups.com/us/es/services/knowledge-center/article.page?kid=a0e0087b, 2019.

[9] *Temperature Sensor Market*. https://www.marketsandmarkets.com/Market-Reports/temperature-sensor-market-522.html, 2019.

[10] *UHF 915 MHz Temperature Sensing RFID Tags*. https://www.rfidinc.com/uhf-915-mhz-temperature-sensing-rfid-tags, 2019.

[11] *IS turns hobby drones into remote-control bombs*. https://nakedsecurity.sophos.com/2017/01/19/is-turns-hobby-drones-into-remote-control-bombs/, Accessed: 2018-1-11.

[12] *ISM band*. https://en.wikipedia.org/wiki/ISM_band, Accessed: 2018-1-11.

[13] *ISIS' Online 'Training Manual' Teaches Sympathizers How to Disguise Themselves as Westerners and Build Bombs to Carry Out Attacks*. https://www.christianpost.com/news/isis-training-manual-teaches-sympathizers-how-to-disguise-themselves-as-westerners-and-build-bombs-to-carry-out-terror-attacks-139253/, Accessed: 2018-1-21.

[14] *Mobile-phone cheating in exams on the rise*. https://www.cnet.com/news/mobile-phone-cheating-in-exams-on-the-rise/, Accessed: 2018-1-21.

[15] *MSP430 Microcontrollers With CapTIvate Touch Technology*. http://www.ti.com/lit/wp/slay044/slay044.pdf, Accessed: 2018-2-19.

[16] *Sound card*. https://en.wikipedia.org/wiki/Sound_card, Accessed: 2018-3-13.

[17] *Bombs disguised as rocks in Yemen reportedly show Iran aid*. https://www.defensenews.com/global/mideast-africa/2018/03/26/bombs-disguised-as-rocks-in-yemen-reportedly-show-iran-aid/, Accessed: 2018-3-21.

[18] *International Telecommunication Union*. https://www.itu.int/en/Pages/default.aspx, Accessed: 2018-3-22.

[19] *Millimeter Scanning at Airports: Is It Worth the Cost?* https://www.securitymagazine.com/articles/79508-millimeter-scanning-at-airports-is-it-worth-the-cost-1, Accessed: 2018-3-23.

[20] *5G mmWave: the next frontier in mobile broadband*. https://www.qualcomm.com/invention/technologies/5g-nr/mmwave, Accessed: 2018-3-31.

[21] *Digital Consumers Own 3.2 Connected Devices*. https://blog.globalwebindex.net/chart-of-the-day/digital-consumers-own-3-point-2-connected-devices/, Accessed: 2018-3-31.

[22] *Features of the Terahertz technology in security applications*. http://terasense.com/news/thz-in-security/, Accessed: 2018-3-31.

[23] *Geddes town supervisor's secretary faces felony for eavesdropping on co-workers*. http://www.syracuse.com/crime/index.ssf/2016/12/geddes_town_supervisors_secretary_faces_felony_for_evesdropping_on_co-workers.html, Accessed: 2018-3-31.

[24] *Package Explosion in Austin*. https://www.washingtonpost.com/news/morning-mix/wp/2018/03/20/package-believed-to-be-bound-for-austin-explodes-at-texas-\fedex-facility-police-say/?utm_term=.8b593439781e, Accessed: 2018-3-31.

[25] *Phone and Electronic Device Policy*. https://collegereadiness.collegeboard.org/sat/taking-the-test/phone-electronic-device-policy, Accessed: 2018-3-31.

[26] *Use of Cell Phones, Laptops, and Other Electronic Devices by Visitors*. https://www.cadc.uscourts.gov/internet/home.nsf/Content/VL+-+Courthouse+-+Cell+Phones+Laptops+and+Other+Electronic+Devices, Accessed: 2018-3-31.

[27] *GS1 BARCODE CHART*. http://www.gs1us.org/resources/standards/ean-upc-visuals, Accessed: 2019-1-13.

[28] *MakingCosmetics - Triethanolamine - 2.0floz / 60ml - Cosmetic Ingredient*. https://www.amazon.com/MakingCosmetics-Triethanolamine-2-0floz-60ml/dp/B01GDZYRK4/ref=sr_1_fkmrnull_1?, Accessed: 2019-1-3.

[29] *Staples Copy Paper Multi-Purpose Copier and Fax Machine Carton, Letter Size, Acid Free, 92 Bright, 20 lb, White, 5000 Sheets/Case*. https://www.amazon.com/Staples-Multi-Purpose-Copier-Machine-Carton/dp/B00FGIFL0A/ref=sr_1_3?, Accessed: 2019-1-9.

[30] *Barcode Dimensions*. https://worldbarcodes.com/barcode-standards/, Accessed: 2019-2-15.

[31] *Crest factor*. https://en.wikipedia.org/wiki/Crest_factor, Accessed: 2019-2-16.

[32] *Epson Expression Home XP-440 Wireless Color Photo Printer with Scanner and Copier, Amazon Dash Replenishment Enabled*. https://www.amazon.com/gp/product/B06W9K5FD2/ref=oh_aui_search_asin_title?ie=UTF8&psc=1, Accessed: 2019-2-3.

[33] *2017 Data Breaches - The Worst Breaches, So Far*. https://www.identityforce.com/blog/2017-data-breaches, Accessed: 2019-3-11.

[34] *2018 Identity Fraud: Fraud Enters a New Era of Complexity*. https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity, Accessed: 2019-3-14.

[35] *Everything You Need to Know About Inventory Management*. https://www.warehouseanywhere.com/resources/inventory-management/, Accessed: 2019-4-5.

[36] *Which area are you investing in most heavily to evolve your inventory management practices?* https://www.statista.com/statistics/780763/inventory-management-investments-retailers-manufacturers/, Accessed: 2019-4-5.

[37] *4 Types of Inventory Control Systems*. https://www2.camcode.com/asset-tags/inventory-control-systems-types/, Accessed: 2019-5-3.

[38] *YARONGTECH UHF tag*. https://www.amazon.com/YARONGTECH-860-960MHZ-Alien-73-5x21-2mm-Adhesive/dp/B01L97ULR4/[2], Accessed: 2019-8-10.

[39] *MLX90614 temperature sensor*. https://www.sparkfun.com/datasheets/Sensors/Temperature/MLX90614_rev001.pdf, Accessed: 2020-10-2.

[40] *Forecast end-user spending on IoT solutions worldwide from 2017 to 2025*. https://www.statista.com/statistics/976313/global-iot-market-size/, Accessed: 2020-10-30.

[41] *Internet of Things - active connections worldwide 2015-2025*. https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/, Accessed: 2020-10-30.

[42] *The Burgess Urban Land Use Model*. https://transportgeography.org//?page_id=4908, Accessed: 2020-11-20.

[43] *Huygens–Fresnel principle*. https://en.wikipedia.org/wiki/Huygens%E2%80%93Fresnel_principle, Accessed: 2020-11-20.

[44] *Printed and Flexible Sensors 2020-2030: Technologies, Players, Forecasts*. https://www.idtechex.com/en/research-report/printed-and-flexible-sensors-2020-2030-technologies-players-forecasts/755#, Accessed: 2020-5-15.

[45] *Digitimes Research: 79GHz to Replace 24GHz for Automotive Millimeter-Wave Radar Sensors.* https://www.digitimes.com/news/a20170906PD208.html, Accessed: 2020-9-2.

[46] Koji Abe, Koji Suzuki, and Daniel Citterio. Inkjet-printed microfluidic multianalyte chemical sensing paper. *Analytical chemistry*, 80(18):6928–6934, 2008.

[47] Fadel Adib and Dina Katabi. *See through walls with WiFi!*, volume 43. ACM, 2013.

[48] Ahmed Al-Haiqi, Mahamod Ismail, and Rosdiadee Nordin. The eye as a new side channel threat on smartphones. In *Research and Development (SCOReD), 2013 IEEE Student Conference on*, pages 475–479. IEEE, 2013.

[49] Musab TS Al-Kaltakchi, Wai Lok Woo, Satnam Singh Dlay, and Jonathon A Chambers. Study of fusion strategies and exploiting the combination of mfcc and pncc features for robust biometric speaker identification. In *2016 4th international conference on biometrics and forensics (IWBF)*, pages 1–6. IEEE, 2016.

[50] Christoph Alexiou, Roland Jurgons, Roswitha J Schmid, Christian Bergemann, Julia Henke, Wolf Erhard, Ernst Huenges, and Fritz Parak. Magnetic drug targeting - biodistribution of the magnetic carrier and the chemotherapeutic agent mitoxantrone after locoregional cancer treatment. *Journal of drug targeting*, 11(3):139–149, 2003.

[51] Adam J Aviv, Katherine L Gibson, Evan Mossop, Matt Blaze, and Jonathan M Smith. Smudge attacks on smartphone touch screens. *Woot*, 10:1–7, 2010.

[52] Michael Backes, Tongbo Chen, Markus Duermuth, Hendrik PA Lensch, and Martin Welk. Tempest in a teapot: Compromising reflections revisited. In *Security and Privacy, 2009 30th IEEE Symposium on*, pages 315–327. IEEE, 2009.

[53] Michael Backes, Markus Dürmuth, and Dominique Unruh. Compromising reflections-or-how to read lcd monitors around the corner. In *Security and Privacy, 2008. SP 2008. IEEE Symposium on*, pages 158–169. IEEE, 2008.

[54] Ricardo Badia-Melis, Ultan Mc Carthy, Luis Ruiz-Garcia, J Garcia-Hierro, and JI Robla Villalba. New trends in cold chain monitoring applications-a review. *Food Control*, 86:170–182, 2018.

[55] Eric Bakker and Martin Telting-Diaz. Electrochemical sensors. *Analytical chemistry*, 74(12):2781–2800, 2002.

[56] Davide Balzarotti, Marco Cova, and Giovanni Vigna. Clearshot: Eavesdropping on keyboard input from video. In *Security and Privacy, 2008. SP 2008. IEEE Symposium on*, pages 170–183. IEEE, 2008.

[57] H Banks and N Gibson. Electromagnetic inverse problems involving distributions of dielectric mechanisms and parameters. *Quarterly of Applied Mathematics*, 64(4):749–795, 2006.

[58] Rafik H Bishara. Cold chain management–an essential component of the global pharmaceutical supply chain. *American Pharmaceutical Review*, 9(1):105–109, 2006.

[59] F Guillaume Blanchet, Pierre Legendre, and Daniel Borcard. Forward selection of explanatory variables. *Ecology*, 89(9):2623–2632, 2008.

[60] Ruud M Bolle, Jonathan H Connell, Sharath Pankanti, Nalini K Ratha, and Andrew W Senior. *Guide to biometrics*. Springer Science & Business Media, 2013.

[61] Ronald Newbold Bracewell and Ronald N Bracewell. *The Fourier transform and its applications*, volume 31999. McGraw-Hill New York, 1986.

[62] Jamie Bullock and UCEB Conservatoire. Libxtract: a lightweight library for audio feature extraction. In *ICMC*, 2007.

[63] Robert Camley, Zbigniew Celinski, Yuriy Garbovskiy, and Anatoliy Glushchenko. Liquid crystals for signal processing applications in the microwave and millimeter wave frequency ranges. *Liquid Crystals Reviews*, pages 1–36, 2018.

[64] Christian Carlowitz, Axel Strobel, Tobias Schäfer, Frank Ellinger, and Martin Vossiek. A mm-wave rfid system with locatable active backscatter tag. In *2012 IEEE International Conference on Wireless Information Technology and Systems (ICWITS)*, pages 1–4. IEEE, 2012.

[65] Joseph A Castellano. *Liquid gold: the story of liquid crystal displays and the creation of an industry*. World Scientific, 2005.

[66] Luca Catarinucci, Danilo De Donno, Matteo Guadalupi, Fabio Ricciato, and Luciano Tarricone. Performance analysis of passive uhf rfid tags with gnu-radio. In *2011 IEEE International Symposium on Antennas and Propagation (APSURSI)*, pages 541–544. IEEE, 2011.

[67] Baicheng Chen, Huining Li, Zhengxiong Li, Xingyu Chen, Chenhan Xu, and Wenyao Xu. Thermowave: A new paradigm of wireless passive temperature monitoring via mmwave sensing. In *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking*, MobiCom '20, New York, NY, USA, 2020. Association for Computing Machinery.

[68] Robert H Chen. *Liquid crystal displays: fundamental physics and technology*. John Wiley & Sons, 2011.

[69] Shilin Chen, Hui Yao, Jianping Han, Chang Liu, Jingyuan Song, Linchun Shi, Yingjie Zhu, Xinye Ma, Ting Gao, Xiaohui Pang, et al. Validation of the its2 region as a novel dna barcode for identifying medicinal plant species. *PloS one*, 5(1):e8613, 2010.

[70] Yimin Chen, Tao Li, Rui Zhang, Yanchao Zhang, and Terri Hedgpeth. Eyetell: Video-assisted touchscreen keystroke inference from eye movements. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 144–160. IEEE, 2018.

[71] Chedsada Chinrungrueng. Combining savitzky-golay filters and median filters for reducing speckle noise in sar images. In *Systems, Man and Cybernetics, 2003. IEEE International Conference on*, volume 1, pages 690–696. IEEE, 2003.

[72] Seungjin Choi, Andrzej Cichocki, Hyung-Min Park, and Soo-Young Lee. Blind source separation and independent component analysis: A review. *Neural Information Processing-Letters and Reviews*, 6(1):1–57, 2005.

[73] Anthony P Colombo, Yan Zhou, Kirill Prozument, Stephen L Coy, and Robert W Field. Chirped-pulse millimeter-wave spectroscopy: Spectrum, dynamics, and manipulation of rydberg–rydberg transitions. *The Journal of chemical physics*, 138(1):014301, 2013.

[74] Federal Communications Commission et al. Use of spectrum bands above 24 ghz for mobile radio services. *Fed Regist*, 81(164):58270–58308, 2016.

[75] Christine Connolly. X-ray systems for security and industrial inspection. *Sensor Review*, 28(3):194–198, 2008.

[76] Benjamin Stassen Cook, Atif Shamim, and MM Tentzeris. Passive low-cost inkjet-printed smart skin sensor for structural health monitoring. *IET Microwaves, Antennas & Propagation*, 6(14):1536–1541, 2012.

[77] Crow. Polymer properties database.

[78] Seyde Daniel and Suga Tadatomo. Perspectives for the application of rfid on electric and electronic waste. In *Advances in Life Cycle Engineering for Sustainable Manufacturing Businesses*, pages 359–364. Springer, 2007.

[79] Robert I Davis, Wei Qiu, Nicholas J Heyer, Yiming Zhao, MS Qiuling Yang, Nan Li, Liyuan Tao, Liangliang Zhu, Lin Zeng, Daohua Yao, et al. The use of the kurtosis metric in the evaluation of occupational hearing loss in workers in china: Implications for hearing risk assessment. *Noise and Health*, 14(61):330, 2012.

[80] Gerald DeJean, Vasileios Lakafosis, Anya Traille, Hoseon Lee, Edward Gebara, Manos Tentzeris, and Darko Kirovski. Rfdna: A wireless authentication system on flexible substrates. In *2011 IEEE 61st Electronic Components and Technology Conference (ECTC)*, pages 1332–1337. IEEE, 2011.

[81] Sanorita Dey, Nirupam Roy, Wenyuan Xu, Romit Roy Choudhury, and Srihari Nelakuditi. Accelprint: Imperfections of accelerometers make smartphones trackable. In *NDSS*, 2014.

[82] Ashutosh Dhekne, Mahanth Gowda, Yixuan Zhao, Haitham Hassanieh, and Romit Roy Choudhury. Liquid: A wireless liquid identifier. In *Proceedings of the 16th Annual International Conference on Mobile Systems, Applications, and Services*, MobiSys '18, pages 442–454, New York, NY, USA, 2018. ACM.

[83] Evangelos C Economou. *Liquid Crystal Based Tunable Bandpass and Bandstop Filters for Millimeter Wave Signal Processing Applications*. PhD thesis, University of Colorado at Colorado Springs, 2017.

[84] Robert Efron. Conservation of temporal information by perceptual systems. *Perception & Psychophysics*, 14(3):518–530, 1973.

[85] Miro Enev, Sidhant Gupta, Tadayoshi Kohno, and Shwetak N Patel. Televisions, video privacy, and powerline electromagnetic interference. In *Proceedings of the 18th ACM conference on Computer and communications security*, pages 537–550. ACM, 2011.

[86] Morten W Fagerland, Stian Lydersen, and Petter Laake. The mcnemar test for binary matched-pairs data: mid-p and asymptotic are better than exact conditional. *BMC medical research methodology*, 13(1):91, 2013.

[87] Song Fang, Ian Markwood, Yao Liu, Shangqing Zhao, Zhuo Lu, and Haojin Zhu. No training hurdles: Fast training-agnostic attacks to infer your typing. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pages 1747–1760. ACM, 2018.

[88] John F Federici, Brian Schulkin, Feng Huang, Dale Gary, Robert Barat, Filipe Oliveira, and David Zimdars. Thz imaging and sensing for security applications: explosives, weapons and drugs. *Semiconductor Science and Technology*, 20(7):S266, 2005.

[89] James L Fergason. Liquid crystals in nondestructive testing. *Applied Optics*, 7(9):1729–1737, 1968.

[90] María Rodríguez Fernández, Eduardo Zalama Casanova, and Ignacio González Alonso. Review of display technologies focusing on power consumption. *Sustainability*, 7(8):10854–10875, 2015.

[91] Jerome Friedman, Trevor Hastie, and Robert Tibshirani. *The elements of statistical learning*, volume 1. Springer series in statistics New York, 2001.

[92] Chuhan Gao, Yilong Li, and Xinyu Zhang. Livetag: Sensing human-object interaction through passive chipless wifi tags. In *15th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 18)*, pages 533–546, 2018.

[93] Chuhan Gao, Xinyu Zhang, and Suman Banerjee. Conductive inkjet printed passive 2d trackpad for vr interaction. In *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking*, pages 83–98. ACM, 2018.

[94] Jerry Zeyu Gao, Lekshmi Prakash, and Rajini Jagatesan. Understanding 2d-barcode technology and applications in m-commerce-design and implementation of a 2d barcode processing solution. In *31st Annual International Computer Software and Applications Conference (COMPSAC 2007)*, volume 2, pages 49–56. IEEE, 2007.

[95] Kevin G Gard, Lawrence E Larson, and Michael B Steer. The impact of rf front-end characteristics on the spectral regrowth of communications signals. *IEEE Transactions on Microwave Theory and Techniques*, 53(6):2179–2186, 2005.

[96] Daniel Genkin, Mihir Pattani, Roei Schuster, and Eran Tromer. Synesthesia: Detecting screen content via remote acoustic side channels. *arXiv preprint arXiv:1809.02629*, 2018.

[97] Khaled M Gharaibeh. *Nonlinear distortion in wireless systems: Modeling and simulation with MATLAB*. John Wiley & Sons, 2011.

[98] Franco Giannini and Giorgio Leuzzi. *Nonlinear microwave circuit design*. John Wiley & Sons, 2004.

[99] Jerome Gilles. Empirical wavelet transform. *IEEE transactions on signal processing*, 61(16):3999–4010, 2013.

[100] Moshe Glickstein. Firewall protection for paper documents. *RFID Journal internet article, Feb*, 2004.

[101] Nan-Wei Gong, Steve Hodges, and Joseph A Paradiso. Leveraging conductive inkjet technology to build a scalable and versatile surface for ubiquitous sensing. In *Proceedings of the 13th international conference on Ubiquitous computing*, pages 45–54. ACM, 2011.

[102] Ian Goodfellow, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, and Yoshua Bengio. Generative adversarial nets. In *Advances in neural information processing systems*, pages 2672–2680, 2014.

[103] Dorothee Grieshaber, Robert MacKenzie, Janos Vörös, and Erik Reimhult. Electrochemical biosensors-sensor principles and architectures. *Sensors*, 8(3):1400–1458, 2008.

[104] David Griggs, Mark Stafford-Smith, Owen Gaffney, Johan Rockström, Marcus C Öhman, Priya Shyamsundar, Will Steffen, Gisbert Glaser, Norichika Kanie, and Ian Noble. Sustainable development goals for people and planet. *Nature*, 495(7441):305–307, 2013.

[105] U Gudaru and Vishal B Waje. Analysis of harmonics in power system using wavelet transform. In *Electrical, Electronics and Computer Science (SCEECS), 2012 IEEE Students' Conference on*, pages 1–5. IEEE, 2012.

[106] S. Hantscher, B. Schlenther, M. Hagelen, S. A. Lang, H. Essen, A. Tessmann, A. Hulsmann, A. Leuther, and M. Schlechtweg. Security pre-screening of moving persons using a rotating multichannel w -band radar. *IEEE Transactions on Microwave Theory and Techniques*, 60(3):870–880, March 2012.

[107] Andreas Hartman. *Electromagnetic Modeling with Complex Dielectrics: A Partial Element Equivalent Circuit Approach*. PhD thesis, Luleå University of Technology, 2019.

[108] Takahiro Hashizume, Takuya Sasatani, Koya Narumi, Yoshiaki Narusue, Yoshihiro Kawahara, and Tohru Asami. Passive and contactless epidermal pressure sensor printed with silver nano-particle ink. In *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, pages 190–195. ACM, 2016.

[109] Yuichi Hayashi, Naofumi Homma, Mamoru Miura, Takafumi Aoki, and Hideaki Sone. A threat for tablet pcs in public space: Remote visualization of screen images using em emanation. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 954–965. ACM, 2014.

[110] Cristian Herrojo, Jordi Naqui, Ferran Paredes, and Ferran Martín. Spectral signature barcodes implemented by multi-state multi-resonator circuits for chipless rfid tags. In *2016 IEEE MTT-S International Microwave Symposium (IMS)*, pages 1–4. IEEE, 2016.

[111] J. Hertenstein and S. Jagannathan. Simulation and detection of unintended electromagnetic emissions from super-regenerative receivers. *IEEE Transactions on Instrumentation and Measurement*, 62(7):2093–2100, July 2013.

[112] Geoffrey Hinton, Li Deng, Dong Yu, George Dahl, Abdel-rahman Mohamed, Navdeep Jaitly, Andrew Senior, Vincent Vanhoucke, Patrick Nguyen, Brian Kingsbury, et al. Deep neural networks for acoustic modeling in speech recognition. *IEEE Signal processing magazine*, 29, 2012.

[113] Sabrina Hocine, Annie Brûlet, Lin Jia, Jing Yang, Aurélie Di Cicco, Laurent Bouteiller, and Min-Hui Li. Structural changes in liquid crystal polymer vesicles induced by temperature variation and magnetic fields. *Soft Matter*, 7(6):2613–2623, 2011.

[114] Gao Huang, Zhuang Liu, Laurens Van Der Maaten, and Kilian Q Weinberger. Densely connected convolutional networks. In *CVPR*, volume 1, page 3, 2017.

[115] M. C. Huang, J. J. Liu, W. Xu, C. Gu, C. Li, and M. Sarrafzadeh. A self-calibrating radar sensor system for measuring vital signs. *IEEE Transactions on Biomedical Circuits and Systems*, 10(2):352–363, April 2016.

[116] Handan Ilbegi, Harun Taha Hayvaci, Imam Samil Yetik, and Asim Egemen Yilmaz. Distinguishing electronic devices using harmonic radar. In *Radar Conference (RadarConf), 2017 IEEE*, pages 1527–1530. IEEE, 2017.

[117] Phillip Isola, Jun-Yan Zhu, Tinghui Zhou, and Alexei A Efros. Image-to-image translation with conditional adversarial networks. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 1125–1134, 2017.

[118] Toshio Itahara, Shushi Furukawa, Kaoru Kubota, Mayumi Morimoto, and Miho Sunose. Cholesteryl benzoate derivatives: synthesis, transition property and cholesteric liquid crystal glass. *Liquid Crystals*, 40(5):589–598, 2013.

[119] David R Jackson, Arthur A Oliner, and C Balanis. Modern antenna handbook. In *Leaky-Wave Antennas*. Wiley, 2008.

[120] SJ James and C James. The food cold-chain and climate change. *Food Research International*, 43(7):1944–1956, 2010.

[121] Jianhua Jia, Zi Liu, Xuan Xiao, Bingxiang Liu, and Kuo-Chen Chou. ippi-esml: an ensemble classifier for identifying the interactions of proteins by incorporating their physicochemical properties and wavelet transforms into pseaac. *Journal of theoretical biology*, 377:47–56, 2015.

[122] Robert Kaiser. Ferrofluid composition, October 24 1972. US Patent 3,700,595.

[123] Çağdaş Karataş and Marco Gruteser. Printing multi-key touch interfaces. In *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, pages 169–179. ACM, 2015.

[124] Yoshihiro Kawahara, Steve Hodges, Benjamin S Cook, Cheng Zhang, and Gregory D Abowd. Instant inkjet circuits: lab-based inkjet printing to support rapid prototyping of ubicomp devices. In *Proceedings of the 2013 ACM international joint conference on Pervasive and ubiquitous computing*, pages 363–372. ACM, 2013.

[125] Yoshihiro Kawahara, Hoseon Lee, and Manos M Tentzeris. Sensprout: Inkjet-printed soil moisture and leaf wetness sensor. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, pages 545–545. ACM, 2012.

[126] Chanwoo Kim and Richard M Stern. Power-normalized cepstral coefficients (pncc) for robust speech recognition. *IEEE/ACM Transactions on Audio, Speech and Language Processing (TASLP)*, 24(7):1315–1329, 2016.

[127] Joongheon Kim and Andreas F Molisch. Fast millimeter-wave beam training with receive beamforming. *Journal of Communications and Networks*, 16(5):512–522, 2014.

[128] Diederik P Kingma and Jimmy Ba. Adam: A method for stochastic optimization. *arXiv preprint arXiv:1412.6980*, 2014.

[129] Dilip Kondepudi and Ilya Prigogine. *Modern thermodynamics: from heat engines to dissipative structures*. John Wiley & Sons, 2014.

[130] R. Kuchta and R. Vrba. Wireless temperature sensor system. In *International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL'06)*, pages 163–163, April 2006.

[131] Markus G Kuhn. Optical time-domain eavesdropping risks of crt displays. In *Security and Privacy, 2002. Proceedings. 2002 IEEE Symposium on*, pages 3–18. IEEE, 2002.

[132] Manu Kumar, Tal Garfinkel, Dan Boneh, and Terry Winograd. Reducing shoulder-surfing by using gaze-based password entry. In *Proceedings of the 3rd symposium on Usable privacy and security*, pages 13–19. ACM, 2007.

[133] Toshio Kurashima, Tsuneo Horiguchi, and Mitsuhiro Tateda. Distributed-temperature sensing using stimulated brillouin scattering in optical silica fibers. *Optics letters*, 15(18):1038–1040, 1990.

[134] I Lawrence and Kuei Lin. A concordance correlation coefficient to evaluate reproducibility. *Biometrics*, pages 255–268, 1989.

[135] Hsien-Hsueh Lee, Kan-Sen Chou, and Kuo-Cheng Huang. Inkjet printing of nanosized silver colloids. *Nanotechnology*, 16(10):2436, 2005.

[136] Benjamin L'Huillier and Arman Shafieloo. Model-independent test of the flrw metric, the flatness of the universe, and non-local estimation of h0 rd. *Journal of Cosmology and Astroparticle Physics*, 2017(01):015, 2017.

[137] Mengyuan Li, Yan Meng, Junyi Liu, Haojin Zhu, Xiaohui Liang, Yao Liu, and Na Ruan. When csi meets public wifi: Inferring your mobile phone password via wifi signals. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 1068–1079. ACM, 2016.

[138] Zhengxiong Li, Baicheng Chen, Zhuolin Yang, Huining Li, Chenhan Xu, Xingyu Chen, Kun Wang, and Wenyao Xu. Ferrotag: a paper-based mmwave-scannable tagging infrastructure. In *Proceedings of the 17th Conference on Embedded Networked Sensor Systems*, pages 324–337, 2019.

[139] Zhengxiong Li, Fenglong Ma, Aditya Singh Rathore, Zhuolin Yang, Baicheng Chen, Lu Su, and Wenyao Xu. Wavespy: Remote and through-wall screen attack via mmwave sensing. In *To appear in IEEE Symposium on Security and Privacy 2020*, S&P'20, 2020.

[140] Zhengxiong Li, Aditya Singh Rathore, Chen Song, Sheng Wei, Yanzhi Wang, and Wenyao Xu. Printracker: Fingerprinting 3d printers using commodity scanners. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pages 1306–1323. ACM, 2018.

[141] Zhengxiong Li, Zhuolin Yang, Chen Song, Changzhi Li, Zhengyu Peng, and Wenyao Xu. E-eye: Hidden electronics recognition through mmwave nonlinear effects. In *Proceedings of the 16th ACM Conference on Embedded Networked Sensor Systems*, pages 68–81. ACM, 2018.

[142] Andy Liaw, Matthew Wiener, et al. Classification and regression by randomforest. *R news*, 2(3):18–22, 2002.

[143] Jaime Lien, Nicholas Gillian, M. Emre Karagozler, Patrick Amihood, Carsten Schwesig, Erik Olson, Hakim Raja, and Ivan Poupyrev. Soli: Ubiquitous gesture sensing with millimeter wave radar. *ACM Trans. Graph.*, 35(4):142:1–142:19, July 2016.

[144] F. Lin, Y. Zhuang, C. Song, A. Wang, Y. Li, C. Gu, C. Li, and W. Xu. Sleepsense: A noncontact and cost-effective sleep monitoring system. *IEEE Transactions on Biomedical Circuits and Systems*, 11(1):189–202, Feb 2017.

[145] Feng Lin, Chen Song, Yan Zhuang, Wenyao Xu, Changzhi Li, and Kui Ren. Cardiac scan: A non-contact and continuous heart-based user authentication system. In *Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking*, MobiCom '17, pages 315–328, New York, NY, USA, 2017. ACM.

[146] Feng Lin, Yan Zhuang, Chen Song, Aosen Wang, Yiran Li, Changzhan Gu, Changzhi Li, and Wenyao Xu. Sleepsense: A noncontact and cost-effective

sleep monitoring system. *IEEE transactions on biomedical circuits and systems*, 11(1):189–202, 2016.

[147] Shan-Yang Lin, Chia-Jen Ho, and Mei-Jane Li. Precision and reproducibility of temperature response of a thermo-responsive membrane embedded by binary liquid crystals for drug delivery. *Journal of controlled release*, 73(2-3):293–301, 2001.

[148] Hai-Bo Liu, Hua Zhong, Nicholas Karpowicz, Yunqing Chen, and Xi-Cheng Zhang. Terahertz spectroscopy and imaging for defense and security applications. *Proceedings of the IEEE*, 95(8):1514–1527, 2007.

[149] Xiangyu Liu, Zhe Zhou, Wenrui Diao, Zhou Li, and Kehuan Zhang. When good becomes evil: Keystroke inference with smartwatch. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 1273–1285. ACM, 2015.

[150] Llc. *Mood Sheet*. 2019.

[151] J Michael Lloyd. *Thermal imaging systems*. Springer Science & Business Media, 2013.

[152] Beth Logan et al. Mel frequency cepstral coefficients for music modeling. In *ISMIR*, volume 270, pages 1–11, 2000.

[153] Hanbin Ma, Yang Su, Chen Jiang, and Arokia Nathan. Inkjet-printed ag electrodes on paper for high sensitivity impedance measurements. *RSC advances*, 6(87):84547–84552, 2016.

[154] Bassem R Mahafza. *Introduction to radar analysis*. Chapman and Hall/CRC, 2017.

[155] Anindya Maiti, Oscar Armbruster, Murtuza Jadliwala, and Jibo He. Smartwatch-based keystroke inference attacks and context-aware protection mechanisms. In *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*, pages 795–806. ACM, 2016.

[156] Anindya Maiti, Murtuza Jadliwala, Jibo He, and Igor Bilogrevic. Side-channel inference attacks on mobile keypads using smartwatches. *IEEE Transactions on Mobile Computing*, 2018.

[157] Stephane G Mallat. A theory for multiresolution signal decomposition: the wavelet representation. *IEEE transactions on pattern analysis and machine intelligence*, 11(7):674–693, 1989.

[158] Heikki Mannila and Pekka Orponen. *Algorithms and Applications*. Springer, 2010.

[159] Wenguang Mao, Mei Wang, and Lili Qiu. Aim: Acoustic imaging on a mobile. In *Proceedings of the 16th Annual International Conference on Mobile Systems, Applications, and Services*, MobiSys '18, pages 468–481, New York, NY, USA, 2018. ACM.

[160] Kanti V Mardia. Measures of multivariate skewness and kurtosis with applications. *Biometrika*, 57(3):519–530, 1970.

[161] Philip Marquardt, Arunabh Verma, Henry Carter, and Patrick Traynor. (sp) iphone: decoding vibrations from nearby keyboards using mobile phone accelerometers. In *Proceedings of the 18th ACM conference on Computer and communications security*, pages 551–562. ACM, 2011.

[162] Gregory J Mazzaro, Anthony F Martone, Kenneth I Ranney, and Ram M Narayanan. Nonlinear radar for finding rf electronics: System design and recent advancements. *IEEE Transactions on Microwave Theory and Techniques*, 65(5):1716–1726, 2017.

[163] Gregory J Mazzaro and Kelly D Sherbondy. Combined linear and nonlinear radar: waveform generation and capture. Technical report, ARMY RESEARCH LAB ADELPHI MD SENSORS AND ELECTRON DEVICES DIRECTORATE, 2013.

[164] Moataz M Mekawy, Atsushi Saito, Akira Sumiyoshi, Jorge J Riera, Hiroaki Shimizu, Ryuta Kawashima, and Teiji Tominaga. Hybrid magneto-fluorescent nano-probe for live apoptotic cells monitoring at brain cerebral ischemia. *Materials Science and Engineering: C*, 2019.

[165] Gerard Rudolph Mendez, Mohd Amri Md Yunus, and Subhas Chandra Mukhopadhyay. A wifi based smart wireless sensor network for monitoring an agricultural environment. In *2012 IEEE International Instrumentation and Measurement Technology Conference Proceedings*, pages 2640–2645. IEEE, 2012.

[166] Adriano Meta, Peter Hoogeboom, and Leo P Ligthart. Signal processing for fmcw sar. *IEEE Transactions on Geoscience and Remote Sensing*, 45(11):3519–3532, 2007.

[167] I. V. Mikhelson, S. Bakhtiari, T. W. Elmer II, and A. V. Sahakian. Remote sensing of heart rate and patterns of respiration on a stationary subject using 94-ghz millimeter-wave interferometry. *IEEE Transactions on Biomedical Engineering*, 58(6):1671–1677, June 2011.

[168] Koji Mizuno, Yoshihiko Wagatsuma, Hideo Warashina, Kunio Sawaya, Hiroyasu Sato, Seiko Miyanaga, and Yukio Yamanaka. Millimeter-wave imaging technologies and their applications. In *2007 IEEE International Vacuum Electronics Conference*, pages 1–2. IEEE, 2007.

[169] Jacek W Morzycki and Andrzej Sobkowiak. Electrochemical oxidation of cholesterol. *Beilstein journal of organic chemistry*, 11(1):392–402, 2015.

[170] Lindasalwa Muda, Mumtaj Begam, and Irraivan Elamvazuthi. Voice recognition algorithms using mel frequency cepstral coefficient (mfcc) and dynamic time warping (dtw) techniques. *arXiv preprint arXiv:1003.4083*, 2010.

[171] José M Muñoz-Ferreras and Félix Pérez-Martínez. Subinteger range-bin alignment method for isar imaging of noncooperative targets. *EURASIP Journal on Advances in Signal Processing*, 2010:14, 2010.

[172] Manoj V Murhekar, Srihari Dutta, Ambujam Nair Kapoor, Sailaja Bitragunta, Raja Dodum, Pramit Ghosh, Karumanagounder Kolanda Swamy, Kalyanranjan Mukhopadhyay, Somorjit Ningombam, Kamlesh Parmar, et al. Frequent exposure to suboptimal temperatures in vaccine cold-chain system in india: results of temperature monitoring in 10 states. *Bulletin of the World Health Organization*, 91:906–913, 2013.

[173] Koya Narumi, Steve Hodges, and Yoshihiro Kawahara. Conductar: an augmented reality based tool for iterative design of conductive ink circuits. In *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, pages 791–800. ACM, 2015.

[174] Matei Negulescu and Joanna McGrenere. Grip change as an information side channel for mobile touch interaction. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pages 1519–1522. ACM, 2015.

[175] Phuc Nguyen, Hoang Truong, Mahesh Ravindranathan, Anh Nguyen, Richard Han, and Tam Vu. Matthan: Drone presence detection by identifying physical signatures in the drone's rf communication. In *Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services*, pages 211–224. ACM, 2017.

[176] Pavel V Nikitin, Sander Lam, and KVS Rao. Low cost silver ink rfid tag antennas. In *2005 IEEE Antennas and Propagation Society International Symposium*, volume 2, pages 353–356. IEEE, 2005.

[177] Pavel V Nikitin, KVS Rao, and Roberto D Martinez. Differential rcs of rfid tag. *Electronics Letters*, 43(8):431–432, 2007.

[178] Amy Nordrum. Popular internet of things forecast of 50 billion devices by 2020 is outdated. *IEEE Spectrum*, 18, 2016.

[179] Karn Opasjumruskit, Thaweesak Thanthipwan, Ohmmarin Sathusen, Pairote Sirinamarattana, Prachanart Gadmanee, Eakkaphob Pootarapan, Naiyavudhi Wongkomet, Apinunt Thanachayanont, and Manop Thamsirianunt. Self-powered wireless temperature sensors exploit rfid technology. *IEEE Pervasive computing*, 5(1):54–61, 2006.

[180] Turgut Ozturk. Characterization of liquids using electrical properties in microwave and millimeter wave frequency bands. *Journal of Nondestructive Evaluation*, 38(1):11, 2019.

[181] Turgut Ozturk. Classification of measured unsafe liquids using microwave spectroscopy system by multivariate data analysis techniques. *Journal of hazardous materials*, 363:309–315, 2019.

[182] J Pedro and N Carvalho. Intermodulation distortion in microwave and wireless circuits. norwood, ma: Artech house, 2003.

[183] Zhengyu Peng, José-María Muñoz-Ferreras, Roberto Gómez-García, Lixin Ran, and Changzhi Li. 24-ghz biomedical radar on flexible substrate for isar imaging. In *Wireless Symposium (IWS), 2016 IEEE MTT-S International*, pages 1–4. IEEE, 2016.

[184] Zhengyu Peng, Lixin Ran, and Changzhi Li. A 24-ghz low-cost continuous beam steering phased array for indoor smart radar. In *2015 IEEE 58th International Midwest Symposium on Circuits and Systems (MWSCAS)*, pages 1–4. IEEE, 2015.

[185] R Perez-Castillejos, J Esteve, MC Acero, and JA Plaza. Ferrofluids for disposable microfluidic systems. In *Micro Total Analysis Systems 2001*, pages 492–494. Springer, 2001.

[186] Jukka Perkiö and Aapo Hyvärinen. Modelling image complexity by independent component analysis, with application to content-based image retrieval. In *International Conference on Artificial Neural Networks*, pages 704–714. Springer, 2009.

[187] Adam C Polak, Sepideh Dolatshahi, and Dennis L Goeckel. Identifying wireless users via transmitter imperfections. *IEEE Journal on selected areas in communications*, 29(7):1469–1479, 2011.

[188] Adam C Polak and Dennis L Goeckel. Rf fingerprinting of users who actively mask their identities with artificial distortion. In *Signals, Systems and Computers (ASILOMAR), 2011 Conference Record of the Forty Fifth Asilomar Conference on*, pages 270–274. IEEE, 2011.

[189] Anastasis C Polycarpou, Marios A Christou, and Nectarios C Papanicolaou. Tunable patch antenna printed on a biased nematic liquid crystal cell. *IEEE Transactions on Antennas and Propagation*, 62(10):4980–4987, 2014.

[190] Stevan Preradovic, Isaac Balbin, and Nemai Karmakar. The development and design of a novel chipless rfid system for low-cost item tracking. In *2008 Asia-Pacific Microwave Conference*, pages 1–4. IEEE, 2008.

[191] Zakariya Qawaqneh, Arafat Abu Mallouh, and Buket D Barkana. Deep neural network framework and transformed mfccs for speaker's age and gender classification. *Knowledge-Based Systems*, 115:5–14, 2017.

[192] Shie Qian and Dapang Chen. Joint time-frequency analysis. *IEEE Signal Processing Magazine*, 16(2):52–67, 1999.

[193] Lawrence R Rabiner and Bernard Gold. Theory and application of digital signal processing. *Englewood Cliffs, NJ, Prentice-Hall, Inc., 1975. 777 p.*, 1975.

[194] Rahul Raguram, Andrew M White, Dibyendusekhar Goswami, Fabian Monrose, and Jan-Michael Frahm. ispy: automatic reconstruction of typed input from compromising reflections. In *Proceedings of the 18th ACM conference on Computer and communications security*, pages 527–536. ACM, 2011.

[195] C.J. Reddy. Control and measurement of unintentional electromagnetic radiation. *IEEE Antennas and Propagation Magazine*, 40(2):88–89, 1998.

[196] Jie Ren, Lin Wang, Yuefeng Mo, Chen Feng, Yunxin Ouyang, Hui Li, and Jun Yin. Illuminator for a barcode scanner, February 21 2019. US Patent App. 16/055,776.

[197] Matteo Rinaldi, Chiara Zuniga, Chengjie Zuo, and Gianluca Piazza. Super-high-frequency two-port aln contour-mode resonators for rf applications. *IEEE transactions on ultrasonics, ferroelectrics, and frequency control*, 57(1), 2010.

[198] Peng Rong and Mihail L Sichitiu. Angle of arrival localization for wireless sensor networks. In *2006 3rd annual IEEE communications society on sensor and ad hoc communications and networks*, volume 1, pages 374–382. Ieee, 2006.

[199] Giulio Rosati, Marco Ravarotto, Matteo Sanavia, Matteo Scaramuzza, Alessandro De Toni, and Alessandro Paccagnella. Inkjet sensors produced by consumer printers with smartphone impedance readout. *Sensing and Bio-Sensing Research*, 26:100308, 2019.

[200] Md Sahidullah and Goutam Saha. Design, analysis and experimental evaluation of block based transformation in mfcc computation for speaker recognition. *Speech Communication*, 54(4):543–565, 2012.

[201] Adeel Saleem, Atif Iqbal, Adnan Sabir, and Adil Hussain. Real-time physical changing 3d display using magnetic liquid technology for visually impaired patients. In *2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, pages 1–5. IEEE, 2019.

[202] S. Scherr, S. Ayhan, B. Fischbach, A. Bhutani, M. Pauli, and T. Zwick. An efficient frequency and phase estimation algorithm with crb performance for fmcw radar applications. *IEEE Transactions on Instrumentation and Measurement*, 64(7):1868–1875, July 2015.

[203] G Schimetta, F Dollinger, G Scholl, and R Weigel. Wireless pressure and temperature measurement using a saw hybrid sensor. In *2000 IEEE Ultrasonics Symposium. Proceedings. An International Symposium (Cat. No. 00CH37121)*, volume 1, pages 445–448. IEEE, 2000.

[204] Esther Shaulova and Lodovica Biagi. Smart home report 2019 - energy management.

[205] D. M. Sheen, D. L. McMakin, and T. E. Hall. Three-dimensional millimeter-wave imaging for concealed weapon detection. *IEEE Transactions on Microwave Theory and Techniques*, 49(9):1581–1592, Sep 2001.

[206] Hiroyuki Shibata, Yuki Hiruta, and Daniel Citterio. Fully inkjet-printed distance-based paper microfluidic devices for colorimetric calcium determination using ion-selective optodes. *Analyst*, 2019.

[207] Mary Shomon. Variations in temperature may be hazardous to your drugs, Jun 2019.

[208] Aditya Singh and Victor Lubecke. A heterodyne receiver for harmonic doppler radar cardiopulmonary monitoring with body-worn passive rf tags. In *Microwave Symposium Digest (MTT), 2010 IEEE MTT-S International*, pages 1600–1603. IEEE, 2010.

[209] Satish Sinha, Partha S Routh, Phil D Anno, and John P Castagna. Spectral decomposition of seismic data with continuous-wavelet transform. *Geophysics*, 70(6):P19–P25, 2005.

[210] Chen Song, Aosen Wang, Kui Ren, and Wenyao Xu. Eyeveri: A secure and usable approach for smartphone user authentication. In *Computer Communications, IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on*, pages 1–9. IEEE, 2016.

[211] Nadarajah Sriskanthan, F Tan, and Advait Karande. Bluetooth based home automation system. *Microprocessors and microsystems*, 26(6):281–289, 2002.

[212] C. Stagner, A. Conrad, C. Osterwise, D. G. Beetner, and S. Grant. A practical superheterodyne-receiver detector using stimulated emissions. *IEEE Transactions on Instrumentation and Measurement*, 60(4):1461–1468, April 2011.

[213] Colin Blake Stagner. Detecting and locating electronic devices using their unintended electromagnetic emissions. *Doctoral Dissertations*, 2013.

[214] Jingchao Sun, Xiaocong Jin, Yimin Chen, Jinxue Zhang, Yanchao Zhang, and Rui Zhang. Visible: Video-assisted keystroke inference from tablet backside motion. In *NDSS*, 2016.

[215] J Svatoš, J Vedral, and P Nováček. Metal object detection and discrimination using sinc signal. In *Electronics Conference (BEC), 2012 13th Biennial Baltic*, pages 307–310. IEEE, 2012.

[216] Tung Ta, Masaaki Fukumoto, Koya Narumi, Shigeki Shino, Yoshihiro Kawahara, and Tohru Asami. Interconnection and double layer for flexible electronic circuit with instant inkjet circuits. In *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, pages 181–190. ACM, 2015.

[217] Mohamed Tamazin, Ahmed Gouda, and Mohamed Khedr. Enhanced automatic speech recognition system based on enhancing power-normalized cepstral coefficients. *Applied Sciences*, 9(10):2166, 2019.

[218] Serioja O Tatu and Ke Wu. Six-port technology and applications. In *Telecommunication in Modern Satellite, Cable and Broadcasting Services (TELSIKS), 2013 11th International Conference on*, volume 1, pages 239–248. IEEE, 2013.

[219] Phan Thanh Noi and Martin Kappas. Comparison of random forest, k-nearest neighbor, and support vector machine classifiers for land cover classification using sentinel-2 imagery. *Sensors*, 18(1):18, 2017.

[220] Dane C Thompson, John Papapolymerou, and Manos M Tentzeris. High temperature dielectric stability of liquid crystal polymer at mm-wave frequencies. *IEEE Microwave and wireless components letters*, 15(9):561–563, 2005.

[221] V. Thotla, M. J. Zawodniok, S. Jagannathan, M. T. A. Ghasr, and S. Agarwal. Detection and localization of multiple r/c electronic devices using array detectors. *IEEE Transactions on Instrumentation and Measurement*, 64(1):241–251, Jan 2015.

[222] Iuliia Tkachenko, William Puech, Christophe Destruel, Olivier Strauss, Jean-Marc Gaudin, and Christian Guichard. Two-level qr code for private message sharing and document authentication. *IEEE Transactions on Information Forensics and Security*, 11(3):571–583, 2016.

[223] DA Usanov, Al V Skripal, An V Skripal, and AV Kurganov. Determination of the magnetic fluid parameters from the microwave radiation reflection coefficients. *Technical Physics*, 46(12):1514–1517, 2001.

[224] DA Usanov, AV Skripal, and SA Ermolaev. Microwave and ultrasound methods for determining the size of ferromagnetic particles and magnetic fluid agglomerates. *MAGNETOHYDRODYNAMICS C/C OF MAGNITNAIA GIDRODINAMIKA*, 32:481–486, 1996.

[225] Marco Vari and Dajana Cassioli. mmwaves rssi indoor network localization. In *2014 IEEE International Conference on Communications Workshops (ICC)*, pages 127–132. IEEE, 2014.

[226] Alexander Vaz, Aritz Ubarretxena, Ibon Zalbide, Daniel Pardo, Héctor Solar, Andrés Garcia-Alonso, and Roc Berenguer. Full passive uhf tag with a temperature sensor suitable for human body temperature monitoring. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 57(2):95–99, 2010.

[227] Arnaud Vena, Etienne Perret, Smail Tedjini, Guy Eymin Petot Tourtollet, Anastasia Delattre, Frédéric Garet, and Yann Boutant. Design of chipless rfid tags printed on paper by flexography. *IEEE Transactions on Antennas and Propagation*, 61(12):5868–5877, 2013.

[228] Ville Viikari, Kimmo Kokkonen, and Johanna Meltaus. Optimized signal processing for fmcw interrogated reflective delay line-type saw sensors. *IEEE transactions on ultrasonics, ferroelectrics, and frequency control*, 55(11):2522–2526, 2008.

[229] Juha Virtanen, Leena Ukkonen, Toni Bjorninen, Atef Z Elsherbeni, and Lauri Sydänheimo. Inkjet-printed humidity sensor for passive uhf rfid systems. *IEEE Transactions on Instrumentation and Measurement*, 60(8):2768–2777, 2011.

[230] W Voit, DK Kim, W Zapka, M Muhammed, and KV Rao. Magnetic behavior of coated superparamagnetic iron oxide nanoparticles in ferrofluids. *MRS Online Proceedings Library Archive*, 676, 2001.

[231] Tao Wan, Tao Zou, Si-Xue Cheng, and Ren-Xi Zhuo. Synthesis and characterization of biodegradable cholesteryl end-capped polycarbonates. *Biomacromolecules*, 6(1):524–529, 2005.

[232] Anran Wang, Vikram Iyer, Vamsi Talla, Joshua R Smith, and Shyamnath Gollakota. {FM} backscatter: Enabling connected cities and smart fabrics. In *14th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 17)*, pages 243–258, 2017.

[233] Chen Wang, Jian Liu, Yingying Chen, Hongbo Liu, and Yan Wang. Towards in-baggage suspicious object detection using commodity wifi. *2018 IEEE Conference on Communications and Network Security (CNS)*, pages 1–9, 2018.

[234] Guochao Wang, Jose-Maria Munoz-Ferreras, Changzhan Gu, Changzhi Li, and Roberto Gomez-Garcia. Application of linear-frequency-modulated continuous-wave (lfmcw) radars for tracking of vital signs. *IEEE Transactions on Microwave Theory and Techniques*, 62(6):1387–1399, 2014.

[235] Ya Wang, Yi Jia, Qiushui Chen, and Yanyun Wang. A passive wireless temperature sensor for harsh environment applications. *Sensors*, 8(12):7982–7995, 2008.

[236] Zhou Wang, Alan C Bovik, Hamid R Sheikh, Eero P Simoncelli, et al. Image quality assessment: from error visibility to structural similarity. *IEEE transactions on image processing*, 13(4):600–612, 2004.

[237] Zhou Wang, Eero P Simoncelli, and Alan C Bovik. Multiscale structural similarity for image quality assessment. In *The Thrity-Seventh Asilomar Conference on Signals, Systems & Computers, 2003*, volume 2, pages 1398–1402. Ieee, 2003.

[238] Teng Wei and Xinyu Zhang. mtrack: High-precision passive tracking using millimeter wave radios. In *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*, pages 117–129. ACM, 2015.

[239] Teng Wei and Xinyu Zhang. Gyro in the air: tracking 3d orientation of batteryless internet-of-things. In *Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking*, pages 55–68. ACM, 2016.

[240] Peter Welch. The use of fast fourier transform for the estimation of power spectra: a method based on time averaging over short, modified periodograms. *IEEE Transactions on audio and electroacoustics*, 15(2):70–73, 1967.

[241] Charles E Wilkes, James W Summers, Charles Anthony Daniels, and Mark T Berard. *PVC handbook*, volume 184. Hanser Munich, 2005.

[242] Klaus Witrisal, Paul Meissner, Erik Leitinger, Yuan Shen, Carl Gustafson, Fredrik Tufvesson, Katsuyuki Haneda, Davide Dardari, Andreas F Molisch, Andrea Conti, et al. High-accuracy localization for assisted living: 5g systems will turn multipath channels from foe to friend. *IEEE Signal Processing Magazine*, 33(2):59–70, 2016.

[243] Lauren J Wong, William C Headley, Seth Andrews, Ryan M Gerdes, and Alan J Michaels. Clustering learned cnn features from raw i/q data for emitter identification. In *MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM)*, pages 26–33. IEEE, 2018.

[244] Bing Xu, Naiyan Wang, Tianqi Chen, and Mu Li. Empirical evaluation of rectified activations in convolutional network. *arXiv preprint arXiv:1505.00853*, 2015.

[245] Chenhan Xu, Zhengxiong Li, Hanbin Zhang, Aditya Singh Rathore, Huining Li, Chen Song, Kun Wang, and Wenyao Xu. Waveear: Exploring a mmwave-based noise-resistant speech sensing for voice-user interface. In *Proceedings of the 17th Annual International Conference on Mobile Systems, Applications, and Services*, pages 14–26, 2019.

[246] Yi Xu, Jared Heinly, Andrew M White, Fabian Monrose, and Jan-Michael Frahm. Seeing double: Reconstructing obscured typed input from repeated compromising reflections. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pages 1063–1074. ACM, 2013.

[247] Mani Yazdanpanahi, Senad Bulja, Dariush Mirshekar-Syahkal, Richard James, Sally E Day, and F Anibal Fernandez. Measurement of dielectric constants of nematic liquid crystals at mm-wave frequencies using patch resonator. *IEEE Transactions on Instrumentation and Measurement*, 59(12):3079–3085, 2010.

[248] Guixin Ye, Zhanyong Tang, Dingyi Fang, Xiaojiang Chen, Kwang In Kim, Ben Taylor, and Zheng Wang. Cracking android pattern lock in five attempts. In *The Network and Distributed System Security Symposium*, 2017.

[249] Daniel Yeager, Fan Zhang, Azin Zarrasvand, and Brian P Otis. A 9.2 μa gen 2 compatible uhf rfid sensing tag with- 12dbm sensitivity and 1.25 μvrms input-referred noise floor. In *2010 IEEE International Solid-State Circuits Conference-(ISSCC)*, pages 52–53. IEEE, 2010.

[250] Ozgur Yilmaz and Scott Rickard. Blind separation of speech mixtures via time-frequency masking. *IEEE Transactions on signal processing*, 52(7):1830–1847, 2004.

[251] Jun Yin, Jun Yi, Man Kay Law, Yunxiao Ling, Man Chiu Lee, Kwok Ping Ng, Bo Gao, Howard C Luong, Amine Bermak, Mansun Chan, et al. A system-on-chip epc gen-2 passive uhf rfid tag with embedded temperature sensor. *IEEE Journal of Solid-State Circuits*, 45(11):2404–2420, 2010.

[252] Qinggang Yue, Zhen Ling, Xinwen Fu, Benyuan Liu, Kui Ren, and Wei Zhao. Blind recognition of touched keys on mobile devices. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 1403–1414. ACM, 2014.

[253] Lan Zhang, Cheng Bo, Jiahui Hou, Xiang-Yang Li, Yu Wang, Kebin Liu, and Yunhao Liu. Kaleido: You can watch it but cannot record it. In *Proceedings of*

the 21st Annual International Conference on Mobile Computing and Networking, pages 372–385. ACM, 2015.

[254] Youqian Zhang and KB Rasmussen. Detection of electromagnetic interference attacks on sensor systems. In *IEEE Symposium on Security and Privacy (S&P)*, 2020.

[255] Mingmin Zhao, Yonglong Tian, Hang Zhao, Mohammad Abu Alsheikh, Tianhong Li, Rumen Hristov, Zachary Kabelac, Dina Katabi, and Antonio Torralba. Rf-based 3d skeletons. In *Proceedings of the 2018 Conference of the ACM Special Interest Group on Data Communication*, pages 267–281. ACM, 2018.

[256] Fang Zheng, Guoliang Zhang, and Zhanjiang Song. Comparison of different implementations of mfcc. *Journal of Computer science and Technology*, 16(6):582–589, 2001.

[257] Man Zhou, Qian Wang, Jingxiao Yang, Qi Li, Feng Xiao, Zhibo Wang, and Xiaofen Chen. Patternlistener: Cracking android pattern lock using acoustic signals. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pages 1775–1787. ACM, 2018.

[258] Shilin Zhu, Chi Zhang, and Xinyu Zhang. Automating visual privacy protection using a smart led. In *Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking*, pages 329–342. ACM, 2017.

[259] Yanzi Zhu, Yibo Zhu, Ben Y Zhao, and Haitao Zheng. Reusing 60ghz radios for mobile radar imaging. In *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*, pages 103–116. ACM, 2015.

[260] Yibo Zhu, Yanzi Zhu, Zengbin Zhang, Ben Y Zhao, and Haitao Zheng. 60ghz mobile imaging radar. In *Proceedings of the 16th International Workshop on Mobile Computing Systems and Applications*, pages 75–80. ACM, 2015.