FakeGuard: Exploring Haptic Response to Mitigate the Vulnerability in Commercial Fingerprint Anti-Spoofing

Aditya Singh Rathore[†¶], Yijie Shen[§¶], Chenhan Xu[†], Jacob Snyderman[†], Jinsong Han[§], Fan Zhang[§], Zhengxiong Li[ζ], Feng Lin[§*], Wenyao Xu[†], Kui Ren[§]
[†] University at Buffalo, SUNY, [§] Zhejiang University, [ζ] University of Colorado Denver
{asrathor, chenhanx, jacobsny, wenyaoxu}@buffalo.edu, {shenyijie, hanjinsong, fanzhang, flin, kuiren}@zju.edu.cn, {zhengxiong.li}@ucdenver.edu

***Abstract*—How to defend against presentation attacks via artificial fake fingers is a core challenge in fingerprint biometrics. The trade-off among security, usability, and production cost has driven researchers to reach a common standpoint, i.e., integrate the commercial fingerprint technology with anti-spoofing detection (e.g., ridge traits). These anti-spoofing solutions are perceived as *sufficiently resilient* under the assumption that a fake finger can never closely relate to a live finger due to either composition of spoofing materials or non-automated manufacturing errors. In this paper, we first identify the vulnerability of in-practice anti-spoofing solutions in commercial fingerprint products. Instead of using expensive 3D fake fingers [1] (above USD $1000), we mimic a more realistic scenario where an attacker fabricates high-precision fake fingerprints using low-cost polyvinylacetate materials [2] (less than USD $50). Building on this, we introduce a practical and secure countermeasure, namely *FakeGuard*, to overcome the exposed vulnerability. We examine the nature of 3D haptic response effect that arises when a fingertip epidermis interacts with a tactile surface and reflects the disparate anatomy of live and fake fingers. Unlike the previous mitigation strategies, *FakeGuard* offers both hardware and software compatibility with existing fingerprint scanners. As the first exploration of haptic-based anti-spoofing solution, we demonstrate the capability of *FakeGuard* to prevent known and unknown fake finger attacks with an average detection error of 1.4%. We also examine and prove *FakeGuard* resilience against seven different physical attacks, e.g., brute-force through pressure variations or partial fingerprints, haptic response alteration via advanced spoofing materials or side-channel interference, and denial-of-service attacks by manipulating the moisture, lighting, and temperature of the ambient environment.**

I. Introduction

Automated fingerprint recognition systems (AFRS) are designed to protect against unauthorized access by linking the user's unique fingerprint to safeguarded information [9]. As AFRS continues to grow in critical applications from gate access, law enforcement, identity management to mobile authentication, adversaries discover innovative ways to bypass fingerprint-based security [10], [11], [12]. The vulnerability of AFRS was not considered a major threat until it was shown possible to hack the 2D images of German minister's fingerprint as well as bypass Apple's TouchID sensors [13]. Since then, different attacks have surfaced, e.g., using 3D artificial fake fingers to bypass Samsung S10 smartphone [14] or fingerprint cloning via glue gun to hack 500 bank accounts [15]. Realizing the threat, researchers have proposed promising mitigation strategies [16], [17], [18], [19] using customized hardware or software-based solutions. These anti-spoofing solutions are actively integrated into commercial AFRS products to trace the millimeter-scale artifacts [20], [21] on fake fingers. Given the maturity of fingerprint domain, existing AFRS are perceived as sufficiently resilient against non-automated, error-induced fake fingers; however, their effectiveness against emerging attacks [22], [23] remains undetermined.

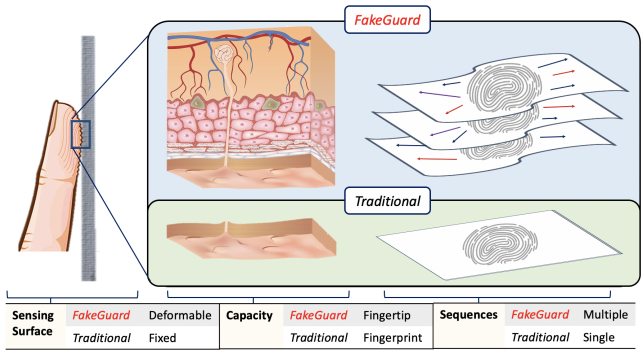

Fig. 1. *FakeGuard* offers a multi-dimensional representation of biological network within a human fingertip and exploits the fundamental anatomical difference between live fingertip and fake fingers made from diverse spoofing materials for anti-spoofing.

Are the latest AFRS resilient against fake fingers? To answer this, we perform an exploratory investigation on the anti-spoofing mechanism in commercial AFRS through high-precision fake finger attacks. In contrast to recent studies utilizing expensive 3D printers in their attack model [24], we leverage low-cost and highly accessible materials to fabricate high-resolution fake fingers with an error margin of a sub-

¶ The first two authors contribute equally to this work.
* The corresponding author.

Network and Distributed Systems Security (NDSS) Symposium 2022
24-28 April 2022, San Diego, CA, USA
ISBN 1-891562-74-6
https://dx.doi.org/10.14722/ndss.2022.24082
www.ndss-symposium.org

TABLE I. COMPARISON BETWEEN TRADITIONAL HARDWARE-BASED ANTI-SPOOFING SOLUTIONS VS PROPOSED *FakeGuard*.

Reference	*Technology*	*Hardware*	*Target*	*Spoofing Material*	*Performance (ACE)*	*Cost*
Goicoecha-Telleria et al. [3]	Optical	Lighting Microscopes	2D Fingerprint, color, edges	PlayDoh, Latex, Gelatin, White Glue, Nail polish	1.51%	>$1000
Sousedik et al. [4]	Optical	Optical Coherence Tomography (OCT)	3D Fingerprint	Gelatin, Silicone, Latex, Paint, Wood Glue	7.42%	>$1000
Baldisserra et al. [5]	Electrical	Electronic Nose	Odor	Latex, Silicone, Gelatin	6%	<$25
Kolberg et al. [6]	Electrical	Thin Film Transistor	Impedance	Glue, Gelatin, PlayDoh, Wax, Latex, Paint and others	2.89%	<50
Parthasaradhi et al. [7]	Capacitive Electro-optical	Precise Biometrics, Ethenticator USB 2500	Perspiration	PlayDoh, Putty	4.8%	$100 - $200
Galbally et al. [8]	Thermal	Yubee Atmel's Fingerchip	2D Fingerprint	Silicone	8.09%	<$50
Proposed FakeGuard	Optical	PDMS-based Haptic Sensor	Haptic Response	Silicone (Dragonskin), Latex, Clay, Gelatin, PlayDoh, Glue and others	**1.4%**	**<$35**

micrometer scale in fingerprint textures and overall finger geometry. The fake finger attack reveals insufficient device security and can breach different types of off-the-shelf AFRS (with anti-spoofing functions) at a success spoof rate of over 93%. Observing that the AFRS market is expected to grow up to 7.1 billion in 2024 [25], an immediate countermeasure is required to overcome the similarity on textural and impedance levels among live and fake fingers.

It is a known fact that the human fingertip does not only comprise of unique fingerprint texture but also a complex multi-layer anatomy containing blood vessels, skin (e.g., epidermis, dermis), finger bone, and tissues. The dynamic interconnectivity among these biological elements contributes to distinct physical measures including fingertip hardness and elasticity during touch interaction. To capture the intrinsic representation of these physical measures in addition to the fingerprint minutiae, we propose a cost-effective and hardware-friendly tactile interface that can be seamlessly integrated with off-the-shelf AFRS. A specialized polydimethylsiloxane (PDMS) layer facilitates a *haptic response* upon interaction with the user's fingertip and the response's magnitude depends on the constitution of interacting surface. Given the difference in anatomy between the human fingertips and spoofing materials, we hypothesize that the haptic response of a live finger and fake finger should be distinguishable through a dedicated recognition model. If our hypothesis holds, the haptic response can become a new dimension of anti-spoofing mechanism against high-precision fake fingers. This new defense offers three distinct advantages:

• **Unprecedented Anti-Spoofing Security:** The proposed technology is the first fingerprint anti-spoofing solution via haptic response in human fingers, and it can defend against sub-micrometer fake finger attacks regardless of spoofing materials.

• **Low-Cost Haptic Technology:** Typically, AFRS supporting multi-dimensional sensing of fingertip's topology costs above $500 [26]. The high sensitivity of the tactile interface makes it possible to measure precise haptic response through low-cost off-the-shelf hardware components (less than $35).

• **Resilience to Alien Fingerprints:** Existing anti-spoofing solutions require prior training with known fake fingers [27] leading to an arms race between attacker (who continuously exploits new materials) and defense mechanism (which needs to retrain with diverse samples). In contrast, the haptic response generated from a live finger is fundamentally different from its fake counterpart, therefore requiring no extensive learning process (further described in Section IX-B).

To this end, we develop a haptic-based anti-spoofing solution, namely *FakeGuard*, for non-invasive and accurate fake finger detection. The foundation of *FakeGuard* rests on biological and behavioral combined traits, called, haptic response effect caused by a fingertip pressing on a PDMS gel surface. During press action, a series of low-cost point LEDs and a circular LED ring uniformly illuminates the gel surface while the haptic response is captured within a sequence of fingerprint samples (less than one second period) by an off-the-shelf camera. The photometric stereo algorithm reconstructs the 3D haptic response from 2D fingerprint samples while ensuring minimum distortion to inherent information about the fingertip's anatomy. Afterward, we utilize grey-level co-occurrences of rotation-invariant local binary patterns for haptic response analysis and build a fingerprint retrieval model to acquire the underlying fingerprint minutiae features. These haptic features are fed to fine-tuned supervised and unsupervised classification models for resilient anti-spoofing in real-world scenarios. Our extensive experiments involve eight types of fake fingers and 12000 spoofing attacks on the haptic response while achieving up to 1.4% average error for fake finger detection. *FakeGuard* is resilient against seven different physical attacks (e.g., brute-force through pressure variations or partial fingerprints, haptic response alteration, and denial-of-service) and maintains a high true positive on live fingers.

Summary: Our contributions in this work are threefold:

- We systematically demonstrate the necessity for improving biometric security by exposing the vulnerability of anti-spoofing functions in latest smart devices against high-precision fake fingers. These fake fingers possess near-identical textural and impedance information as the live fingers of legitimate users.
- We propose a novel anti-spoofing framework that builds upon the multi-dimensional haptic response obtained from fingertip to gel interaction. We develop a haptic-based system, *FakeGuard* that offers high potential for compatibility with traditional optical AFRS on hardware and software levels.
- We conduct a comprehensive study by examining and proving the resilience of *FakeGuard* against fake finger attacks under supervised and unsupervised scenarios. We also explore uncommon physical attacks (e.g., impersonation/alteration, denial of service) to examine its anti-spoofing capability in real-world applications.

II. Related Work

Fingerprint Presentation Attacks: To date, researchers have examined the vulnerability of AFRS through various spoof attacks. For instance, universal 3D fingerprint targets are capable of breaching three different certified optical fingerprint readers [28]. Another study employed high-end 3D printers to fabricate fake fingerprints for spoofing capacitive, contact-optical and contactless-optical fingerprint technologies [29]. Moreover, accessible spoofing materials (e.g., gummy [10], gelatin [30], silicone [31], glue [32], [33], latex [34], clay [17], playdoh [35]) have demonstrated significant threat during presentation attacks. Yet, several of these studies either utilize expensive 3D printers for creating the fake targets or create a surface-level impression (2D) of fake fingerprint rather than the entire 3D finger. *In our work, we expose the vulnerability of state-of-the-art AFRS (enabled with anti-spoofing) via high-precision fake fingers under a cost-effective and low-effort attack model.*

Fake Fingerprint Mitigation: Countermeasures against spoofing attacks involve combined efforts from hardware and software methods. Perspiration and morphological features can be acquired using high-resolution sensors to assist in prevention [36]. Furthermore, physical properties of the fake fingers, e.g., coarseness [17], can be integrated with fingerprint features for anti-spoofing. Table I compares the traditional hardware methods based on their overall economical cost, anti-spoofing performance and sensing mechanism, and shows that proposed *FakeGuard* technology is low-cost, high-resolution and provides higher level of security against presentation attacks. There is a growing trend of utilizing machine learning algorithms such as convolutional neural networks [37], [38], [39], VGG-19 [40], GoogleNet [41], generative adversarial networks [42] and other ensemble approaches [42] as countermeasures; however, these methods are computationally intensive and requires large amount of training samples which is impossible to collect due to the unpredictability of fake fingers. Researchers [43] explore one-class support vector machine (SVM) classifiers to detect spoof targets generated from previously unseen materials, yet the performance is not ideal for real-world deployment. *We propose the first haptic-based anti-spoofing to capture the multi-dimensional fingertip anatomy for defeating high-precision fake fingers.*

III. Case Study on Security of AFRS: Attack Model and Preliminaries

Before describing the spoofing attack, we first introduce the attack target and basic assumptions in our threat model.

A. Adversary Model

We consider a scenario where a victim, hereafter Bob, utilizes common electronic devices with fingerprint anti-spoofing ability (e.g., computer, mobile, smart locks) in daily life. The attacker, namely Alice, aims to compromise the security of target device and acquire the protected sensitive information. Alice uses her innovative skills to manufacture a high-precision fingerprint template of Bob to breach all the security checks across devices and underlying applications. In the past, 2D fingerprint images [44] and low-resolution synthetic fingerprints [45] were deemed sufficient for spoofing, yet the current AFRS (with anti-spoofing) can detect any manufacturing defects on fake fingers. By acknowledging the findings in recent studies [46], [47], Alice carefully controls her manufacturing process to create high-resolution and cost-effective fake fingers. The non-cancelability and high permanence of fingerprint ensure that the attack will be successful irrespective of device or timeline. The high-precision fake finger attack considers three primary assumptions:

A1 *Non-invasiveness: Due to Bob's vigilance, Alice cannot directly or wirelessly access the AFRS's firmware modules.* In smart devices, multiple security checks are integrated during the development process on both hardware and software levels for malicious intrusion detection via tamper-proof packaging [48], [49] or mounting AFRS on encryption circuits [50].

A2 *High-Precision Biometric Traits: Alice is capable of retrieving the precise details of the target's fingerprint patterns.* She can steal Bob's fingerprint from sensitive images on social media, leftover residues or optical cameras [51] and produce the fake fingers via reconstruction techniques [52]. Alice can also create spoof targets from latent fingerprints of non-cooperative subjects by using molds and etching process for printed circuit boards (PCB) [53], [54]. Acquisition and fabrication of 3D fake fingers is an actively explored area [55], [56]. In this paper, we investigate the scenario where fake fingers contain high-precision biometric traits, as well as the proposed countermeasure.

A3 *Manufacturing Ability: Alice does not have to access expensive manufacturing machines.* Although Alice is capable of creating fake fingers from diverse spoofing materials, she is inept in producing biological replicas of the victim's live finger via bionic 3D printers [57] as these machines are economically infeasible in ordinary attack practice.

B. Materials for Advanced Spoofing Attacks

To examine the vulnerability of AFRS unbiased, we need to select a proper spoofing material that can allow the fabrication of high-precision fake fingers. Considering state-of-the-art AFRS rely on texture and impedance information, fake

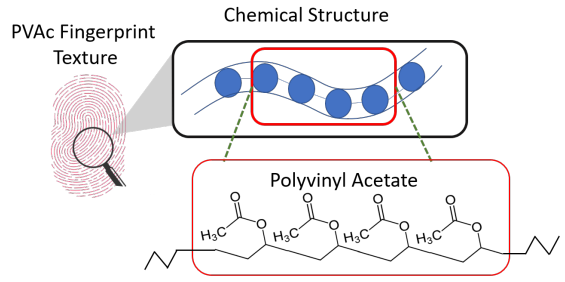

Fig. 2. The chemical structure to constitute high-resolution fake fingers, which are identical to live fingers.

Fig. 3. An array of high-precision fake fingers modeled from index, middle and thumb fingers from 20 subjects.

fingers should also possess identical fingerprint patterns and impedance as human skin. Based on the above requirements, we find that polyvinyl acetate (PVAc) glue [58], [33], [45] is the most suitable spoof material for our attack model. The main ingredient of PVAc glue is polyvinyl acetate [2], an aliphatic rubbery synthetic polymer with the formula $(C_4H_6O_2)_n$. Figure 2 shows its chemical structure within fake fingers.

Chemical attributes: PVAc glue does not possess any strong odor, is non-toxic, and safe to handle by bare hands [59]. It dries quickly at room temperature (20-25°C) with very high bond strength [60]. The pH value is neutral and as an emulsion in water [61], PVAc glue is only soluble in aromatic hydrocarbons, ketons, alcohols, esters, and trichloromethane.

Physical attributes: As a type of macromolecular substance, PVAc glue's particle size belongs in the range from $100nm$ to $1um$ [62]. Its density is 1.191 g/mL at 25°C and dielectric constant is 1.15 [63]. PVAc glue is flexible and texture-stable under normal environments.

Attack Benefits: Due to PVAc glue's particle size from $100nm$ to $1um$, it can support a sub-micrometer scale precision in the fingerprint textures on corresponding fake fingers. Beyond that, we test the impedance from live fingers and PVAc glue fingers. The impedance is measured by ProsKit MT-1280 multimeter (60 $M\Omega$) [64] by placing positive and negative nodes to opposite ends of the fake finger. Our empirical analysis shows the PVAc glue to possess the same order of magnitude impedance (nearly 20 $M\Omega$) with human skin (nearly 10 $M\Omega$). PVAc has a low price of $0.015 per gram, allowing even resource-deficient attackers to obtain the material effortlessly. Given the advantages of PVAc glue, we consider it as a promising material for producing high-precision fake fingers to spoof the commercial AFRS with anti-spoofing functions.

C. High-precision Fake Fingerprint

Attack Requirements: Before introducing the manufacturing process of fake fingers, we need to consider the target requirements as summarized below:

R1 *Target Presentation: Alice will attempt to trick AFRS to perceive the presented input belongs to a legitimate user.* By having a close similarity between Bob's live finger and fake finger and maintaining a continuous vigilance over the victim, Alice will input the fake finger with the same dynamics (i.e., pressure, speed) as Bob during an access attempt.

R2 *Concealment: After the security breach, no traces should remain on smart devices leading to the attacker.* The threat of fake fingers arises from the unpredictability of spoof materials from being recognized by AFRS. However, greasy or viscous materials may leave traces on the device which can be easily identified in forensic analysis.

R3 *Model Precision: Alice will prevent any defects on the input fake finger which can be easily recognized by AFRS.*

Fake Finger Fabrication: The process of generating fake fingers while satisfying Requirement R3 and Assumption A2-A3 is described as follows: ***(i)*** Alice selects a small cubical structure of dimensions 3 cm x 3 cm x 3 cm to store the molding material. ***(ii)*** Due to its accessibility and rheological properties, wax is selected as the base material and poured into the cubical model. ***(iii)*** A subject is asked to place his live finger into the wax material (40°C-45°C). The finger is kept stable to ensure no crease marks on the contact surface. ***(iv)*** Once the material solidifies, the subject's finger is removed to acquire a hollowed mold with the shape of fingertip outlined by fingerprint. ***(v)*** Besides PVAc glue, Alice can also select other advanced spoofing materials and pour them inside the finger-shaped mold. After five hours, the outer wax mold is discarded to acquire a detailed fake finger of the target subject (see Figure 3). Acquisition of 3D fake fingerprints is an explored area [55], [56]; to exploit the highest potential of this attack and extensively evaluate our countermeasures, we choose this method to fabricate the fake finger. After the fabrication of high-precision fake fingers, their spoofing potential is extensively evaluated on the commercial AFRS.

D. A Study on Challenging Anti-Spoofing Functions of Commercial AFRS

Anti-Spoofing Mechanism: To verify the fingerprint liveness, a standard AFRS is coupled with additional hardware or software modules. For hardware-based protection, static features (e.g., capacitance, thermal) are often leveraged to represent the fingerprint. Traditional optical sensing, being prone to 2D presentation attacks, is integrated with software-only methods for anti-spoofing. On the software level, fingerprint liveness is supported by multiresolution [65] or wavelet-based texture analysis [17], convolutional neural networks [19], band-selective Fourier transforms [66] and local phase quantizations [67]. While the AFRS on the consumer market provides a clear distinction of inherent technology, their internal software is often not revealed to the public to prevent threats.

Selected Products in Experiments: For our vulnerability analysis, we select four widely-used smart devices, i.e., ZK-

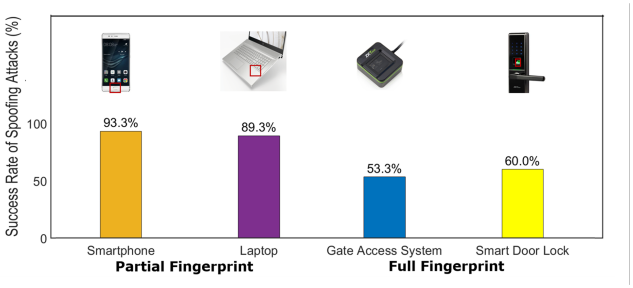

Fig. 4. PVAc high-precision fake fingers can compromise anti-spoofing functions in commercial AFRS. Even partial fake fingerprints offer high spoofing potential considering the textural and impedance similarity between live and fake fingers.

Teco 20R gate access system, ZKTeco TL100 smart door lock, HUAWEI P10 smartphone, and HP envy13 laptop using optical, capacitive, and 3D capacitive AFRS respectively. It is worth mentioning that each of the mentioned AFRS is also enabled with anti-spoofing functions as described in Table II.

TABLE II. DETAILS ABOUT AFRS IN POPULAR SMART DEVICES EMBEDDED WITH POTENTIAL ANTI-SPOOFING FUNCTIONS.

Devices	*Sensing Region*	*Anti-spoofing Mechanism*	*Application Significance*
ZKTeco 20R	Full	Multi-resolution Texture Analysis	Access control
ZKTeco TL100	Full	Local Phase Quantization	Smart lock
HUAWEI P10 Smartphone	Partial	Electrical Conductivity	On-the-go device security
HP Envy13 Laptop	Partial	3D Surface Matching	Intellectual property protection

Attack on Anti-Spoofing Functions: In accordance with assumptions A1-A3, we examine the spoofing potential of high-precision fake fingers. On each device, we first register the target subject as a legitimate user using his live finger. Afterward, we attempt to breach the device's security by presenting the subject's fake finger. The fake fingers, composed of PVAc glue, are pressed 30 times individually while the average result of access attempts is recorded in Figure 4. *It is revealed that the state-of-the-art AFRS have limited security against high-precision fake fingers and there is still sufficient room for improvement.* By having the assistance of victim during the manufacturing process, the superior ridge clarity and strength of fingerprint textures on fake fingers help breach the anti-spoofing functions in optical scanners. The impedance similarity between PVAc glue and human skin allows the fake finger to stimulate a capacitance distribution as a live finger. As a result, even partial fake fingerprints can spoof the capacitive AFRS in smartphone and laptop devices. The 3D surface or texture matching algorithms primarily exploits the ridge strength and clarity information and thus cannot differentiate between our partial fake fingerprints and partial live fingers.

Summary and insights: Our study proves the inefficacy of existing anti-spoofing functions in commercial AFRS to defend against high-precision fake fingers. We propose a cost-effective and practical mitigation solution based on the anatomy characteristics of human fingertip and evaluate its security against *eight* spoofing materials in Sections VIII-X.

IV. FUNDAMENTALS OF LIVENESS DETECTION

Unlike AFRS that focuses on only the exterior of a human fingertip (i.e., fingerprint), we explore new biologic features offered by the entire fingertip with anti-spoofing capabilities. We describe the background of haptic response effect caused when a human fingertip interacts with tactile interfaces.

A. The Principle of Haptic Response

Anti-Spoofing Capability of Fingertip: The human fingertip is a multi-layered structure of different components that interact with each other to allow perception (in form of touch, pressure, vibration and cutaneous tension [68]) of the physical world. Its liveness depends on underlying skeletal elements (e.g., distal phalanx, tendons, and ligamentous structures), fibrous connective tissue networks, vascular network, and skin layers [69]. A fingertip possesses unique physical measures (e.g., hardness, elasticity) whose magnitude depends on the inherent biological network. However, the rigid surface of traditional fingerprint scanners cannot sense these physical measures and restricts to fingertip's outer layer (e.g., sweat, ridges) for anti-spoofing. Although bioimpedance [70] can provide an approximate representation of fingertip composition, it is affected by the skin temperature and body mass while losing the information about the fingerprint.

Tactile Interfaces: Polymers exhibiting viscoelasticity and weak intermolecular forces are increasingly employed in tactile sensors to measure physical characteristics of the interacting medium [71]. In particular, polydimethylsiloxane (PDMS) is a widely-used silicon-based organic polymer possessing multiple features [72] such as nontoxicity, biocompatibility, elasticity, transparency, and durability. When a human fingertip is pressed against the elastomer surface (e.g., PDMS), a deformation occurs in the polymer structure. This deformation is governed by elastostatics partial differential equation (PDE) system [73]:

$$\begin{aligned} \nabla \cdot \boldsymbol{\sigma} + \mathbf{F} &= 0, \\ \boldsymbol{\varepsilon} &= \tfrac{1}{2}\left[\nabla \mathbf{u} + (\nabla \mathbf{u})^{\mathrm{T}}\right], \\ \boldsymbol{\sigma} &= \mathsf{C} : \boldsymbol{\varepsilon}, \end{aligned} \tag{1}$$

where $\boldsymbol{\sigma}$ is the Cauchy stress tensor of the multi-layered structure of human fingertip, $\mathbf{F}$ is the fingertip body force, $\boldsymbol{\varepsilon}$ is the strain tensor related to the PDMS deformation tensor $\mathbf{u}$, and C is the stiffness tensor of a fingertip. The parameters $\boldsymbol{\sigma}$,

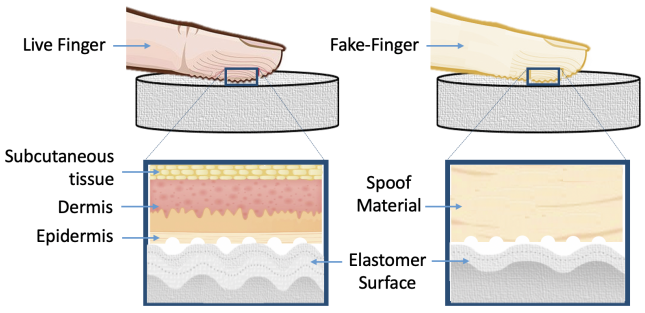

Fig. 5. Haptic response arises when a fingertip is pressed on an elastomer surface and correlates with the anatomy of interacting medium. The high complexity of biological network within a human fingertip makes haptic response challenging to impersonate by attackers.

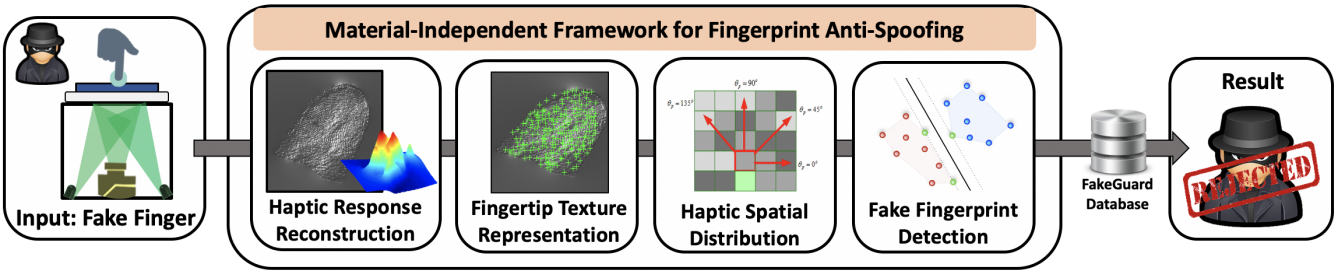

Fig. 6. The overview of *FakeGuard*, a haptic-based fingerprint anti-spoofing with four main processing steps: (1) reconstruction; (2) representation; (3) distribution; (4) detection.

$\mathbf{F}$, ε, and C of a multi-layer fingertip are different from those of single-layered fake fingers, thereby forming a distinctive deformation $\mathbf{u}$. This deformation is visible as haptic response effect whose magnitude correlates to the anatomy of overall fingertip. Specifically, the multi-layered composition of fingertip leads to a non-linear haptic response; single-layered objects (i.e., fake fingers) cause a uniformly distributed haptic response over the contact area. The cross-link networks in polymer structure allow the elastomer to recover its shape within less than one second after the fingertip is removed.

Hypothesis: When a fingertip is pressed against an elastomer surface, the resulting haptic response depends on the finger's anatomy outlined by the fingerprint. Considering the difference between the anatomy of live fingers and spoofing materials in Figure 5, the haptic responses from live and fake fingers should be distinct. In addition, the haptic response cannot be replicated or altered without knowing the intricate anatomy of user's fingertip. The 3D haptic response with inherent fingerprint minutiae textures can be utilized for anti-spoofing.

B. Design Aims

Our resilient anti-spoofing platform, namely *FakeGuard*, should possess the necessary properties as follows:

• **Intrinsic liveness:** An essential requirement for fingerprint anti-spoofing is to detect whether the contact object is a live finger. *FakeGuard* only allows access to legitimate users when the input haptic response is not generated by fake fingers.

• **Privacy-oriented:** It is vital for haptic response to not retain on the tactile surface after the finger is removed. *FakeGuard* utilizes a specially designed PDMS gel that regains its original shape within one second after press action.

• **Cost-effective and ease-of-use:** Although traditional biometrics offer reliable features, the sensing mechanism is often expensive and requires user to follow special instructions. FakeGuard employs a low-cost off-the-shelf smartphone camera to capture the haptic response when a fingertip is naturally pressed on a tactile interface.

• **Robust:** FakeGuard employs a specially designed PDMS gel and reflective acrylic membrane to support lambertian surface while shielding the system from change in surrounding environment.

C. Integration with Commerical AFRS

As an anti-spoofing solution, *FakeGuard* can offer protection against high-precision fake fingers. By design, *FakeGuard* should also have a high potential for integration with existing AFRS and facilitate a smooth transition in access-critical scenarios (e.g., smart locks, home security). We ensure minimum hardware overhead by leveraging ordinal components (e.g., camera, LED) typically present in the optical AFRS technologies, while supporting the acquisition of detailed biometric traits. We also demonstrate software compatibility by utilizing prominent fingerprint techniques to obtain the ridge patterns and textures from the haptic response in Section VII-A.

V. FakeGuard System Overview

We propose *FakeGuard*, which utilizes the anatomy-induced haptic response for fingerprint anti-spoofing. The system, see Figure 6, involves combine efforts from the hardware and software modules. (1) The **hardware** module: a fingertip is pressed on the PDMS gel which is subjected to optical illumination from different directions. The haptic response is recorded within a sequence of images by a smartphone camera. An acrylic reflective membrane is strategically placed to block the ambient light. (2) The **software** module: the measured sequence of images are inputted to the photometric stereo algorithm for 3D reconstruction of haptic response. We employ rotation-invariant local binary patterns (Rot-LBP) and grey-level-co-occurrence matrix (GLCM) to represent the 3D response while utilizing the fingerprint retrieval model for capturing inherent orientation and ridge frequency information. The selected features are fed to a classification model for fake finger detection.

VI. Haptic Response Acquisition Hardware

In this section, we describe our optimized sensor hardware that fulfills the design goals mentioned in Section IV-B.

A. Context-aware PDMS Fabrication

The sensitivity of haptic response depends on the physical characteristics of elastomer surface. To this end, we specially design a PDMS gel with sufficient responsiveness to capture biological features of the contact medium. During material fabrication, we notice that a higher density of PDMS gel restricts the haptic response from fingertip's ridge to a small area, where the singular directional force causes loss in 3D information. Under softer PDMS composition, the fingertip is

subjected to force from multiple directions to make a profound impact on the material. Although the fingerprint textures are precisely captured in the deformation of gel surface, the soft composition of PDMS provides an inferior resilience to drastic variations in ambient temperature and lighting conditions. To satisfy the requirements of sensitivity and robustness, we allow the following design considerations: (1) we integrate dual-layered PDMS gel to act as an interacting medium. The transparent layer is composed of a grade 184 PDMS with polymer to cross-linker mixing ratio of 35:1. A grade 527 PDMS using 1:1 ratio forms the ideal colored layer with sufficient elasticity to capture fingerprint ridges and patterns. The colored composition prevents the ambient light to reach the camera lens. (2) To prevent the effect of specular reflection on the gel surface, we position an acrylic reflective membrane between the PDMS gel and the camera lens. Figure 7 shows the difference between the haptic response of live and fake fingers observed from our specially designed PDMS gel. The proposed sensing layout is resilient to denial-of-service attacks as examined in Section X.

Sensitivity of PDMS to skin color and fingerprint quality: During the development phase, we observed that a transparent PDMS gel surface can retain the fingerprint textures during the press action; however, it is sensitive to the skin tone of users, where a darker tone can reduce the amount of fingerprint information in sensed images. This is a common problem in the biometrics domain [74]. To overcome this, we position a colored and opaque PDMS layer between the user's fingertip and camera lens such that it neutralizes the skin color of the fingertip. In other words, only the deformation of PDMS gel as well as fingerprint reflection on the gel surface (opposite to the side where user presses their fingertip) will be captured in the images. An example is shown in Figure 7, where the color in the sensed images relates to color of PDMS gel and not of the user's skin tone or fake fingers. In the rare scenario when the incoming fingerprint quality is not sufficient, our specially designed dual-layered gel also allows detailed acquisition of haptic response for anti-spoofing or user authentication.

B. Optical Illumination and Response Enhancement

FakeGuard relies on the optical perception of haptic response with inherent anatomy and fingerprint information for anti-spoofing. Figure 8 shows the exterior and interior of *FakeGuard* whose hardware module comprises of:

• *Low-cost LEDs:* Three point LEDs are positioned on the inner shell of sensor to illuminate the PDMS gel from different lighting directions. We employ green point LEDs since the high intensity of red light makes it ineffective for response acquisition. The power consumption of each LED is 0.024W. A white LED circular ring ensures a lambertian surface. It is a surface that appears uniformly bright from all directions of view and reflects the entire incident light.

• *Smartphone Camera:* We consider a low-cost and portable smartphone camera (96 dpi, 3 frames per second) for capturing the haptic response within a sequence of images. The camera is placed at $10cm$ focal length from the gel surface for detailed response acquisition.

• *Raspberry Pi:* The intensity of LEDs and camera parameters are controlled by a Raspberry Pi 4 microcontroller with ARM v8 64-bit SoC.

• *3D Printed Shell:* As the first exploratory study, *FakeGuard* is modeled in a cylindrical structure of height $12cm$ and diameter of $8cm$. A 3D printer is used to manufacture the shell composed of photosensitive resin.

***Cost-effectiveness*:** AFRS with sophisticated anti-spoofing ability costs more than $200 [75]. In contrast, *FakeGuard* comprises low-cost hardware with an overall value of **$31.08**. The cost breakdown is LEDs (3 x $0.03), lighting circle ($0.34), shell ($9.75), acrylic film ($0.12), PDMS gel ($1.46), off-the-shelf camera ($8.95) and Raspberry Pi module ($10.37). Our hardware design demonstrates that *FakeGuard* is practical for real-world deployment in physical access systems.

C. Optometric Stereo Reconstruction

During sensing, the legitimate user presses his fingertip on PDMS gel over 1 second period; every point LED is turned on and off (one at a time) while the images of gel surface are recorded by the camera. Photometric stereo algorithm [76], [77] is a 3D reconstruction solution to estimate the depth and surface orientation from 2D images of the same object under different lighting conditions. It relies on three assumptions: (1) the light sources are far from the object; (2) there are no specular or dark regions on the target object; (3) light is reflected by a surface equally in every direction. We employ photometric stereo to reconstruct the 3D haptic response from a sequence of captured images while ensuring intrinsic information of anatomy and fingerprint patterns. The process of 3D response reconstruction involves determining light direction, surface normal and depth information.

Lighting direction calibration: With appropriate distance between LEDs and gel surface, each of them can be regarded as a point source. We represent every light ray as a vector

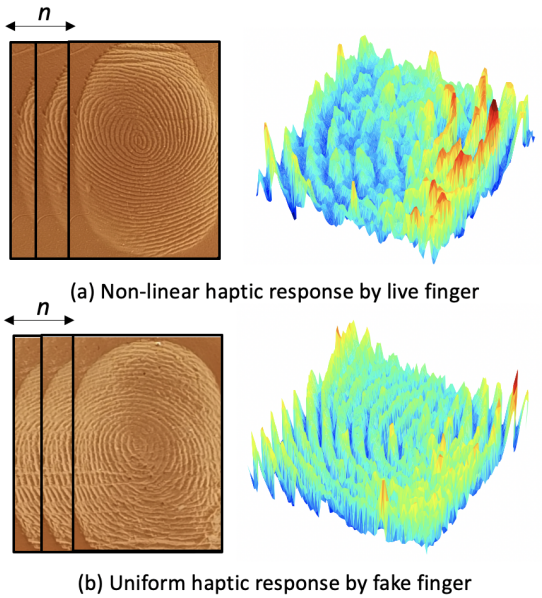

Fig. 7. The PDMS gel offers high sensitivity to capture the intricate haptic response difference between live and fake finger. n is the sequences of captured images.

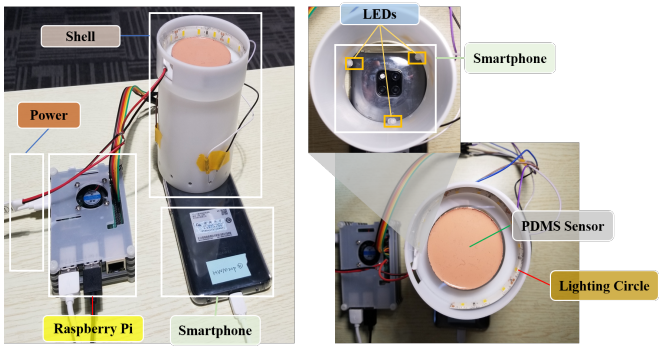

Fig. 8. *FakeGuard* hardware prototype comprising three primary components: (1) optical illuminators (i.e., LEDs, lighting circle); (2) low-cost camera; (3) Raspberry Pi module. Based on optical sensing, the proposed sensing protocol can be inconspicuously integrated into conventional fingerprint scanning without a significant increase in overall cost.

with lighting direction as $\vec{l_m}$=(x_m, y_m, z_m), m$\in$ {1,2,3}. To ensure an ideal sensing platform, the distance between the LED and gel surface is maintained at height $h = 10cm$ and radius $r = 3.7cm$. The pixel-to-centimetre ratio is 102:1 deriving an image size of $M \times N(738 \times 432)$. After expressing the lighting directions in 3D coordinate system, the position of each LED (Lx_m, Ly_m, Lz_m), m$\in$ {1,2,3} is derived by:

$$x_m = x_0 - (M/2) - Lx_m, \tag{2}$$

$$y_m = y_0 - (N/2) - Ly_m, \tag{3}$$

$$z_m = Lz_m \equiv h, \tag{4}$$

where (x_0, y_0) is the center of *FakeGuard* cylindrical shell.

Surface normal: After computing the lighting directions, we can recover the surface normals at each pixel. The lighting directions are represented as a matrix, $\mathbf{L} = \{\vec{l_1}, \vec{l_2}, ..., \vec{l_3}\}$, and the observed pixel intensities $\vec{I}$, from each 2D image can be derived by:

$$\vec{I} = \rho \times \mathbf{L} \times \vec{n}, \tag{5}$$

where ρ represents the albedo. Albedo is the fraction of incident radiation that is reflected by a surface. $\vec{n}$ is the unit surface normal vector. The $\vec{n}$ is pseudo-inverse of $\mathbf{L}$ via:

$$\vec{n} = \frac{(\mathbf{L}^{\mathrm{T}}\mathbf{L})^{-1}\mathbf{L}^{\mathrm{T}}\vec{I}}{\rho}, \tag{6}$$

$$\vec{n} = \{n_x \quad n_y \quad n_z\} = -n_z \{p \quad q \quad -1\}, \tag{7}$$

where p and q are derivatives of original image.

Local depth: Finally, the 3D haptic response is acquired using the algorithm proposed by Frankot and Chellappa [78], which minimizes the least squared error E_F as:

$$E(Z_F) = \iint \left((p - p_{after})^2 + (q - q_{after})^2\right) dxdy, \tag{8}$$

where the p_{after} and q_{after} are the gradient of target surface after reconstruction and Z_F is the result of Fourier transform of 2D image. Figure 9(a) demonstrates the capability of *FakeGuard* in reconstructing high-resolution 3D information from the target finger.

VII. Haptic Response Analysis

When a fingertip is pressed on PDMS gel, the resulting haptic response correlates to the fingertip's anatomy and spreads across three dimensions. We demonstrate the software compatibility of *FakeGuard* with AFRS by extracting multi-level minutiae features from haptic response. Afterwards, we extract the spatial features within the haptic response that relates to the deformation of PDMS gel caused by the user's fingertip.

A. Software Compatibility via Fingerprint Minutiae Retrieval

Fingerprint consists of interleaved ridges and valley patterns which can bifurcate, terminate or run parallel to each other. We introduce a fingerprint retrieval method that integrates level-1 (i.e., local orientation and ridge frequency map) and level-2 (i.e., minutiae position and angle) features as follows:

1) The reconstructed image from photometric stereo algorithm is enhanced via adaptive thresholding, histogram equalization and normalization methods. A gaussian blur (kernel = 5) is applied prior to enhancement for reducing noise.
2) We find the contours in an enhanced fingerprint image to build edges of a graph structure. This aids in creating a convex hull mask for segmenting the background from target object.
3) Gradient-based method [79] estimates the local orientations across a 16x16 pixels averaging window. Given $G_x(i,j)$ and $G_y(i,j)$ are gradient magnitude in horizontal and vertical axes, the dominant direction in a window is:
$$\theta_d = \frac{1}{2} tan^{-1}\left(\frac{\sum_{i=1}^{16}\sum_{j=1}^{16} 2G_x(i,j)G_y(i,j)}{\sum_{i=1}^{16}\sum_{j=1}^{16}(G_x(i,j)^2 - G_y(i,j)^2)}\right), \tag{9}$$
where the orientation direction is 0° or 90° if G_x or G_y = 0. The strength is represented by the length of the segment for every orientation (see Figure 9(c)).
4) After computing the orientation map, the frequencies of ridge and valley patterns are derived for same locations. For each block of size 32x32, ridge frequency is a value $f \in \mathbf{R}$, the inverse of average ridge-line period in neighbourhood [80]. Figure 9(d) shows the ridge frequency map where a lighter block denotes a higher frequency.
5) We employ the NBIS's MINDTCT function from NIST [81] in our work due to its superior performance in minutiae extraction. The MINDTCT involves four primary steps including the generation of image maps, image binarization, detection of initial minutiae set and removal of spurious minutiae to provide a feature set in form of [x, y, θ]. The (x,y) is minutiae location while θ is the angle whose example is shown in Figure 9(e).

Finally, the level-1 (orientation and ridge frequency) and level-2 (minutiae location and angle) features are selected for fingerprint classification. Figure 9 proves the feasibility of fingerprint texture extraction from haptic response; *FakeGuard* offers low-effort integration with traditional AFRS.

B. Haptic Spatial Distribution

The haptic response contains fingerprint information and the spatial distribution of PDMS gel correlated with the

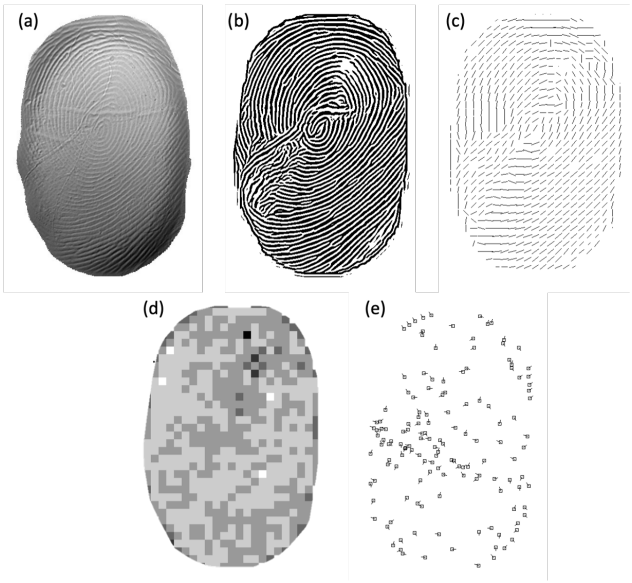

Fig. 9. The fundamental components of fingerprint can be extracted from haptic response: (a) reconstructed; (b) enhanced; (c) orientation; (d) ridge frequency; (e) minutiae.

anatomy of user's fingertip. The response is three-dimensional, i.e., it has a specific depth at a given horizontal and vertical location. Based on our observations, the depth information reflects in a grey-level image through pixel intensity, while the response can be contained in the overall spatial texture distribution.

Rotation-invariant Local Binary Patterns (Rot-LBP): Considering the fingerprint sensing is vulnerable to skin distortion and quality, Rot-LBP is chosen in our work given its robustness to the monotonic transformation of grayscale and rotation invariant through fixed set patterns [82]. Rot-LBP is computed from pixel x and its symmetric neighbor set of P pixels placed on a circle radius of $R = 8$. The difference between the gray value of pixel x from the neighborhood is used for binary patterns of dimension 3.

Grey-Level Co-occurence Matrix (GLCM): To address the large dimensionality of Rot-LBP patterns, we leverage them as an input for GLCM, which quantifies imperceptible changes of gel surface and has demonstrated superior performance in previous anti-spoofing studies [83]. The co-occurrence probability of each grey level pair*(i,j)* appearing in Rot-LBP patterns can be defined as:

$$p(i,j) = \frac{C(i,j)}{\sum_{i=0}^{N-1}\sum_{j=0}^{N-1} C(i,j)}, \tag{10}$$

where *C(i,j)* is the number of occurrences of grey levels i and j within the window $N = 32$. The horizontal and vertical means of the matrix are as follows:

$$u_x = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} i \cdot p(i,j), u_y = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} j \cdot p(i,j). \tag{11}$$

After computing the GLCM in feature angles (0°, 45°, 90° and 135°), we extract 11(x4) haptic-based features from each model. These features, i.e., correlation, contrast, cluster shade, cluster prominence, energy, homogeneity, sum average, sum entropy, sum of squares, sum variance, and information measure of correlation can be grouped into first-order (individual pixel properties) and second-order (relative pixels properties) statistics. The 44 spatial distribution features along with 132 fingerprint features are chosen for fake fingers detection.

C. Anti-Spoof Learning Scheme

As the first exploratory study of haptic response analysis for anti-spoofing, we evaluate the performance of *FakeGuard* via four universal classifiers. Previously, these classifiers have shown promising capability for not only biometrics [84], [85] but also presentation attack detection [86], [87].

• **Weighted K-Nearest Neighbor (KNN):** Given the tradeoff in outlier detection and false positives caused by hyperparameter k in traditional KNN, we employ a weighted KNN ($k = 10$). It relies on a Euclidean distance function with squared inverse distance weight to assign higher values to closest neighbors.

• **Support Vector Machine (SVM):** The goal of SVM is to find an optimal hyperplane in a high-dimensional space with the largest minimum distance to the training samples. We choose a quadratic kernel in our work.

• **Linear Discriminant Analysis (LDA):** LDA aids in transforming the feature vectors in a new subspace to maximize the distance between the classes. A singular value decomposition solver is used.

• **Logistic Regression (LR):** It employs a logistic sigmoid function to generate a probability score for testing samples that is compared against a cutoff to determine the class labels.

• **eXtreme Gradient Boosting (XGBoost):** XGBoost [88] integrates classification and regression trees (CARTs) to search the model of minimum loss against deep-limited level-wise splitting strategy.

• **Light Gradient Boosting Machine (LightGBM):** LightGBM [89] also intrgrates CARTs to determine the class labels. The different is that it use a lightweight splitting strategy i.e., selecting the node that has the maximum gain to split.

• **Convolutional Neural Network (CNN):** It extracts abstracts by convolution kernels. These abstracts are projected into a feature space and the classifier determined labels against such features.

In the following, we identify the suitable classifier for supervised fake finger detection and further examine its performance under unsupervised real-world scenario.

VIII. Evaluation Setup

A. Experimental Preparation

We conduct a pilot study to examine the effectiveness of *FakeGuard* for fake finger detection. *FakeGuard* employs a low-cost smartphone camera to model the haptic response of user's fingertip as it is pressed on the gel surface. Although the ambient environment will comprise of different lighting conditions, the employment of a colored PDMS gel layer and acrylic reflective membrane minimizes the amount of undesirable light rays to reach the camera lens. The experimental

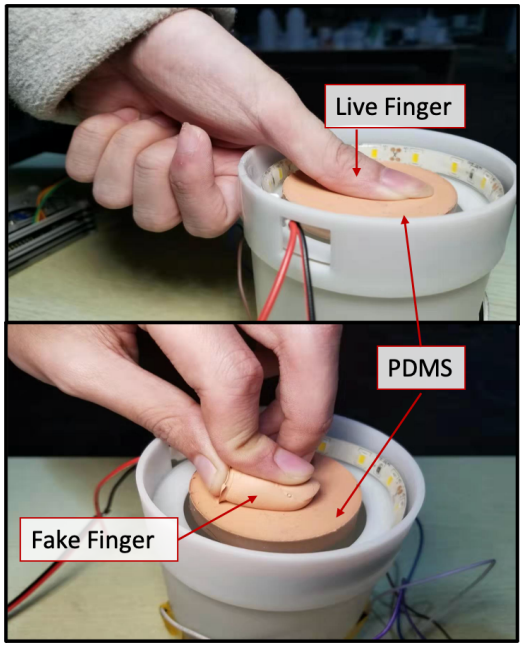

Fig. 10. Experimental setup with a subject performing press actions on a PDMS gel using their live and fake fingers.

setup is shown in Figure 10. The study is performed in a lab environment with room temperature (24°C), moderate ambient light, and no moisture present on the gel surface or the fake finger. *FakeGuard* resilience to template alteration, brute-force, and denial-of-service attacks is discussed in Sections IX-X. To satisfy Requirement R1 in Section III-C, we interact fake fingers with *FakeGuard* in a similar fashion as subjects with their live fingers. During the sensing process, PDMS gel is optically illuminated by three point LEDs and a white circular LED ring while the Raspberry Pi 4 module is leveraged to trigger the activation of LEDs. We employ HUAWEI Mate 20 Pro smartphone with a 96 dpi camera to record the haptic response when a fingertip is pressed on the gel surface. The recorded images are sent to *FakeGuard* for further processing.

B. Experimental Procedure

As the first exploratory study on haptic-based fingerprint anti-spoofing, we recruit 20 subjects (16 males and 4 females) within the age group of 20-40 years. None of the subjects have damage to their fingerprint or suffer from skin-related disorders. During this study, we ensure that all the samples collected from the subjects are de-identified. The subjects are given full disclosure on the nature of our study after which the next steps are conducted based on their willingness to continue. A multi-layer password protection is employed for storing fingerprint data while the physical fake fingers are placed under locked protection. Only the primary researcher is allowed to retrieve the passwords (updated every three weeks) and physical locks. We also hold an active International Review Boards (IRB) approval for collecting physiological data from adult human participants for biometric research. All the evaluations tightly follow the rule of IRB regulation.

Fake Finger Selection: Firstly, we ask every subject to participate in the fabrication process of producing multiple high-precision fake fingers. To date, researchers have analyzed the vulnerability of their proposed system against fake fingers; yet, they do not verify the credibility of generated fake fingers by first testing them against traditional AFRS. If a defective fake finger, being very predictable, is introduced as a testing sample, it might have a significant negative influence on the overall score. Considering that *FakeGuard* does not rely on capacitive-based biometric, we notice that Dragon Skin [90], [24] material possess the most similar haptic response to human fingertip, thereby being an ideal choice for the attacker to spoof *FakeGuard*. In our pilot study, we use Dragon Skin to create a total of six fake fingers (i.e., thumb, index and middle finger of left and right hand) for each subject, making a total of 120 detailed fake fingers. We examine the effectiveness of every fake finger on commercial AFRS (mentioned in Section III-D) and select only those with high spoofing potential. Each subject has at least one ideal fake finger (with a total of 23) to potentially breach the *FakeGuard* security. To prevent any bias, we also evaluate the cross-material performance from different spoofing materials in Section IX-C.

We ask every subject to perform 15 trials. In each trial, the participant first presses their live finger, corresponding to the selected fake finger, on the PDMS gel. This process is repeated 20 times within a single trial. A 10-minutes break separates each trial to ensure that the subject's press action is more natural and similar to a real-world scenario (i.e., non-uniform pressure). For each press action, a one second recording is obtained via smartphone camera. A single recording reveals one 3D image that contains a subject-specific haptic response. Therefore, a total of 6000 3D images (20 subjects * 300 press actions) and 18000 2D images (20 subjects * 300 press action * 3 samples/action) are recorded for live fingers. This experiment is repeated for selected fake fingers (able to spoof the AFRS introduced in Section III) in an identical fashion to generate an overall of 12000 3D images.

Evaluation Metrics: We employ the below metrics which are widely adopted for fingerprint vulnerability analysis [91], [92].

- SpoofRate: percentage of false acceptance of fake finger;
- DenialRate: percentage of false rejection of live finger;
- Average Classification Error (ACE) is defined as:

$$ACE = \frac{SpoofRate + DenialRate}{2}. \quad (12)$$

IX. Anti-spoofing Performance Analysis

For *FakeGuard* to serve as a security mechanism in high-impact applications, it is vital to examine the performance and reliability under real-world conditions. We consider two scenarios: (1) *Supervised Detection (Section IX-A):* classification of live and fake fingers given training samples of both classes; (2) *Unsupervised Presentation Attacks (Section IX-B):* rejecting unknown fake fingers when the model is trained on only samples of live fingers. We also examine advanced attacks on impersonating the haptic response in Section IX-C.

A. Supervised Fake Finger Detection

In the supervised scenario, the classifier is trained on multiple users and used to identify a specific target. This is common

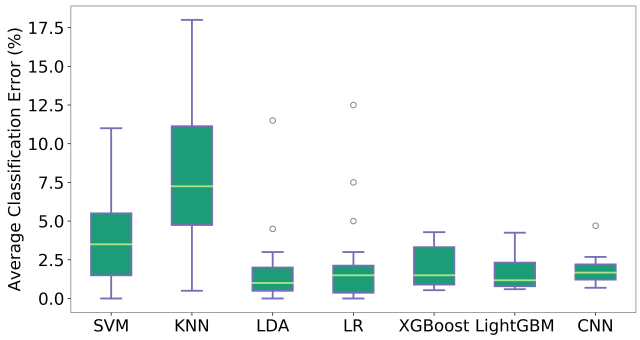

Fig. 11. Evaluation under supervised scenario where *FakeGuard* is trained with samples from both live and fake fingers among different classifiers, i.e., SVM, KNN, LDA, LR, XGBoost, LightGBM and CNN.

in biometric scanners deployed in public environments (e.g., ATM, gate access systems). We perform 10-fold cross validation on 12000 samples (6000 live and 6000 fake) and describe the ACE observed from four universal classifiers in Figure 11. The SVM, KNN, LDA, LR, XGBoost, LightGBM and CNN achieves 3.925%, 8.2%, 1.725%, 2.175%, 2.009%, 1.777% and 1.815% average error respectively while detecting live and fake fingers. The LDA, LR, XGBoost, LightGBM and CNN show promising performance in differentiating the fake and live fingerprint samples due to strength of our haptic response features and 3D reconstructed fingerprint images. To further inspect the trend across subjects, we illustrate the DenialRate and SpoofRate scores in Figure 12. The average DenialRate and SpoofRate are 2.05% and 1.4% respectively. The lower performance of subjects 15 and 16 is due to insufficient haptic response from fingertip sliding, rather than pressing, on the gel surface during the experiments. Our results show the potential of *FakeGuard* over existing anti-spoofing solutions (evaluated in Section III-D) for fake finger detection. In the remainder of paper, we employ a fine-tuned LDA model for classification unless specified.

B. Unsupervised Presentation Attack

During real-world application, a biometric system learns to distinguish between live fingerprints of users but has no knowledge about fake fingers that the adversary might utilize

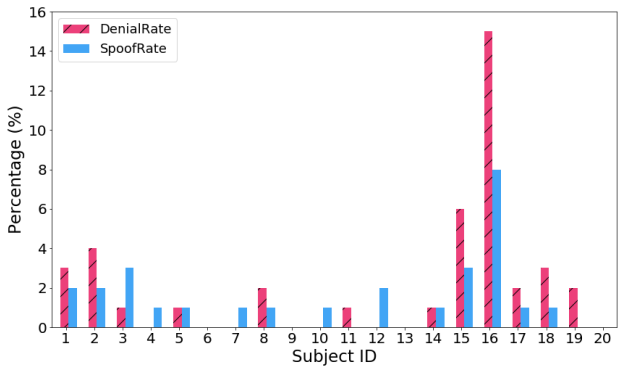

Fig. 12. Detection rate among 20 subjects for supervised fake and live finger detection.

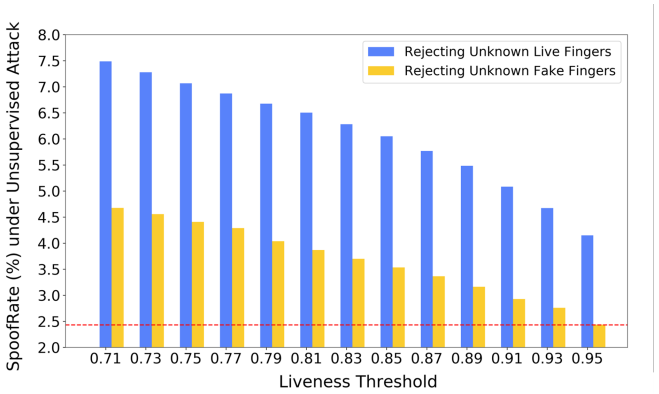

Fig. 13. *FakeGuard* can reject unknown fake fingers when underlying classifier is only trained on live fingers (ideal performance depicted by red line). Despite training with only haptic response features, live fingers from unknown/unauthorized users can still be rejected.

during presentation attacks. An ideal AFRS should be capable of rejecting fake fingers without prior training. However, the existing studies [27] require prior training of their anti-spoofing model on known fake finger samples.

Rejecting Unknown Fake Fingers: We evaluate the performance of *FakeGuard* in rejecting 6,000 unknown fake finger samples when the classifier is only trained on 6,000 live samples with a threshold of liveness. The classifier will accept the input fingerprint as a live subject if and only if the probability of liveness is higher than the threshold. To examine the effectiveness of rejecting fake fingers, the threshold is varied between 0.7 and 0.95 and the percentage of accepted fake fingers is recorded in Figure 13. The average SpoofRate varies from 4.67% to 2.43% depending on the threshold.

Feature Importance: *FakeGuard* utilizes both traditional fingerprint-based features and haptic response; we determine the relevance of both feature subsets to performance under previously considered unsupervised scenario. The classifier is trained and tested on either fingerprint-based features or haptic response and the SpoofRate is described in Figure 14. Even under no extensive learning process, our observations prove that haptic response is a promising anti-spoofing feature that varies significantly between the live finger and fake finger.

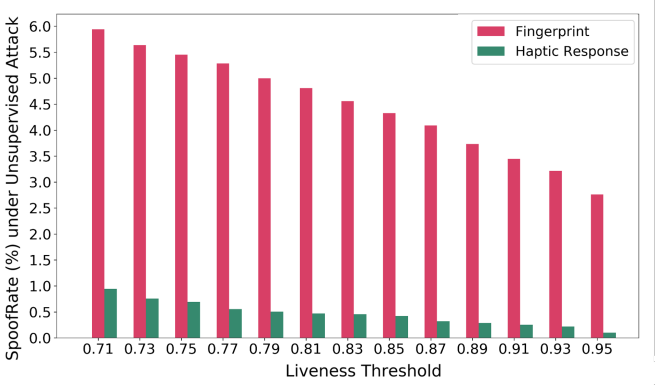

Fig. 14. *FakeGuard* capability to reject unknown fake fingers when trained on fingerprint vs haptic response features.

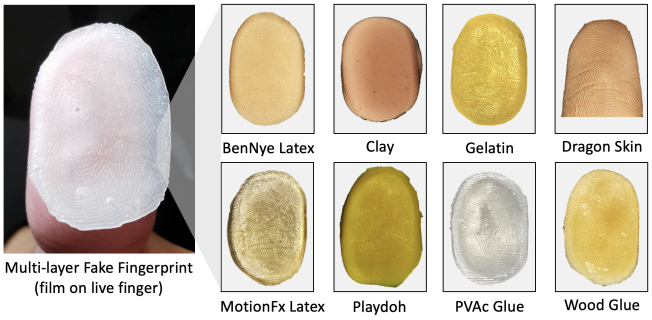

Fig. 15. Fingerprint spoof attacks realized by materials easily accessible in daily life. These materials have been proven to have high spoofing rate against traditional AFRS.

Rejecting Unknown Live Fingers: We examine a real-world scenario where *FakeGuard* is trained on the biometric templates of only legitimate users and needs to reject the untrained live fingers of unknown users. To this end, we train the classifier on 3000 live samples of 10 random subjects and observe the probability of rejecting 3000 samples of another 10 subjects. The results are shown in Figure 13; the average SpoofRate varies from 7.48% to 4.14% depending on the threshold. It is a known fact that fingerprint is unique to every individual, therefore we only utilize the haptic response features to train the classifier in this experiment.

C. An Advanced Attack Study on Impersonating Haptic Response

Upon realizing the relation between haptic response and fingertip's anatomy, the attacker can either overlap his live finger with fake films of different properties or directly manipulate the haptic response generated during the access attempt.

1) Multi-layered Fake Fingerprint: We examine *FakeGuard* potential in rejecting diverse fake films of varying physical and chemical properties (see Figure 15) when they are overlapped on a live finger to resemble the anatomy of victim's fingertip. Fake films (0.6mm width) of 20 subjects, made from seven different spoofing materials, are interacted with *FakeGuard* 50 times individually. Figure

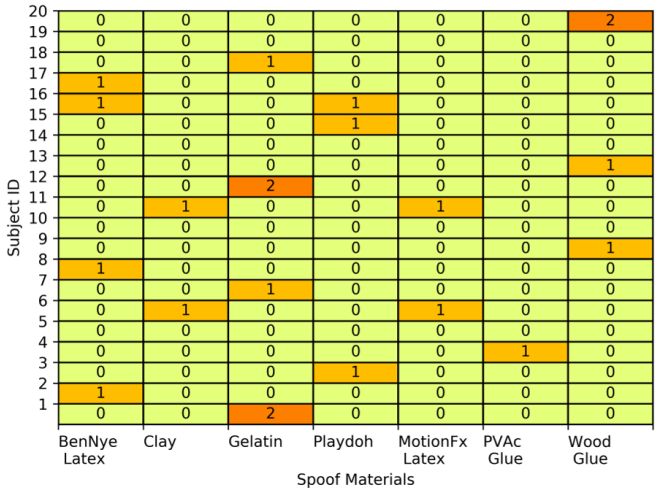

Fig. 17. Number of successful spoofing attempts (out of 45 total attempts) across seven different spoofing materials that the classifier is previously trained on. The performance is consistently low and independent of the spoofing material used to create the fake fingers.

16 illustrates their variations against linear discriminant analysis. Each response yields a point on the graph and the points by real and fake fingers exhibit a clear boundary. The complexity of live fingertips makes them easy to distinguish. The overlap of fake fingerprints is due to their similar structures i.e., overlapping on a live finger. In addition, we test the performance on such fake fingerprints. We consider two scenarios: (1) With-training: all spoofing materials are included in both training and testing. (2) Without-training: *FakeGuard* is trained on selected spoofing materials but tested against fake films made from a different material.

With-training: The haptic response from five press actions (both live and fake finger) of 20 subjects are used for training. Afterward, 45 responses (from fake finger) of each subject are considered for testing. The observed number of successful spoofing attempts in Figure 17 proves that our system is resilient to different types of multi-layered fake fingerprints due to their inherent physiological variations. Although gelatin, Playdoh, PVAc glue are promising materials for spoofing

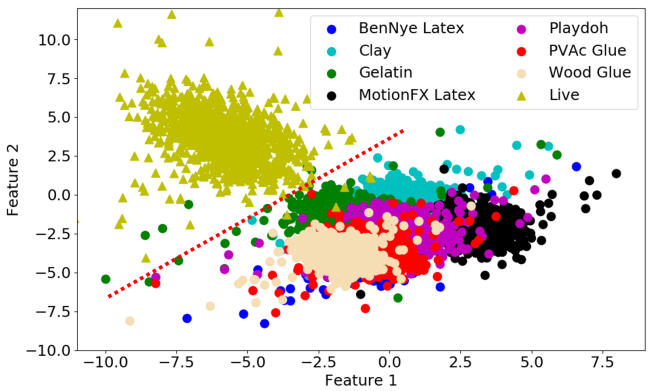

Fig. 16. A two-dimensional representation by LDA of haptic response features to demonstrate the identifiability between live and fake fingertips across various spoof materials. Feature 1 and 2 represent the two dimensions after dimensionality reduction.

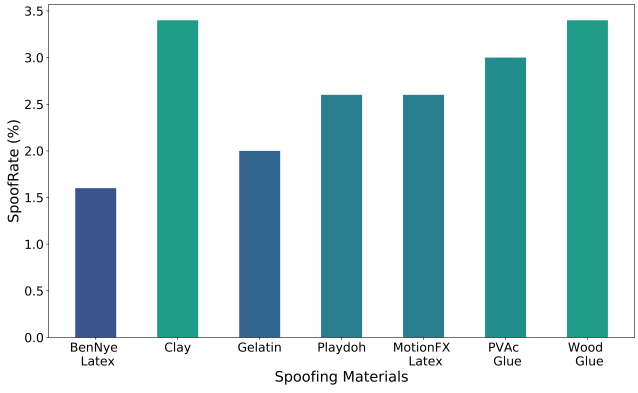

Fig. 18. SpoofRate (%) across seven different spoofing materials that the classifier is not trained on. In contrast to traditional AFRS, *FakeGuard* does not require extensive learning as the haptic response is distinctively different between a live and fake finger.

attacks on state-of-the-art fingerprint anti-spoofing [19], they can still be rejected.

Without-training: Out of seven spoofing materials, the classifier is trained on the haptic response from six materials (50 samples each * 20 subjects) as well as the live fingers (300 samples * 20 subjects), while it is tested against a different spoofing material (50 samples * 20 subjects). This process is repeated such that every spoofing material is included as a part of testing set once. Figure 18 demonstrates a SpoofRate from 1.6-3.4% with an average of 2.7%. A key advantage of *FakeGuard* is that it can be generalized to combat different spoofing materials without prior knowledge.

2) Haptic Response Alteration: Realizing the failure of a high-precision fake finger attack on *FakeGuard*, the attacker aims to alter the haptic response caused by fake fingers to align with legitimate user. However, the haptic response is an intricate feature and difficult to impersonate manually. Therefore, we assume a scenario where the attacker leverages a vibration motor (RB-02S087) to induce dynamic shifts on PDMS gel during the sensing process. These vibration shifts integrate with the haptic response during press action. We examine the SpoofRate under three types of vibration magnitude (light, medium and heavy) for fake fingers of 20 subjects. Our analysis shows that *FakeGuard* is resilient to vibration shifts with SpoofRate as 3%, 3.4% and 4% for light, medium and heavy magnitude respectively. While we utilized the fake finger made with Dragon Skin for this experiment, other spoofing materials would result in similar performance. This is because the vibration introduced by motor causes discrepancies in the Level-2 fingerprint features, allowing *FakeGuard* to reject the input fake fingers.

X. Investigation on Attacking Surfaces

For comprehensiveness of the study, we identify and investigate several attacks affecting the PDMS surface during the sensing process, including brute-force attacks (Section X-A) and denial-of-service attacks (Section X-B). To ensure robustness, we deploy a 10-fold cross-validation scheme to compute the evaluation metrics in the following experiments.

A. Brute-Force Attacks

1) Impact of Partial Fingerprint: Fingerprint sensing has evolved from full fingertip scan to partial regions with the goal of reducing computational costs while providing free-form sensing. However, a small sampling area limits the biometric information and allows the attacker to input different regions of fake fingers to compromise the system. To examine the performance of *FakeGuard* in verifying the partial regions of live and fake fingers, we employ five subjects in our experiment. For each subject, we select four regions (i.e., bottom, left, right and top) of their fake finger and perform an overall of 200 press actions. We also collect live partial fingerprint samples from the same regions. The ACE performance is illustrated in Figure 20. Distinct regions of the fingertip exhibit different haptic responses. For instance, the top region provides a confined response with no significant contribution from fingertip's outer area. In comparison, the bottom region acts similarly to the full fingerprint and promotes a more spatial haptic response. The inability to perform precise press actions using left region of right index finger leads to higher ACE against the right partial fingerprint.

2) Impact of Pressure Variations: During the access attempt, a naive attacker might try to alter the pressure of fake finger to manually align the haptic response of the fake finger as close to a live finger. To examine the resilience against pressure variations, we ask each of the five participants to complete two trials using their live and fake fingers. During each trial, the subject performs 150 press actions under soft, moderate and hard pressure. The results are shown in Figure 20. The current system achieves a satisfactory performance under soft and moderate pressure. Excessive pressure causes a live finger to undergo an instantaneous change in surface. This change is similar to its fake counterpart since the gradual transition in haptic response cannot be captured. Moreover, a typical user is less likely to utilize excessive pressure during access attempt, decreasing the probability of observing high DenialRate. During the experiment, we also observed that a prolonged hard pressure increases the risk of damage to the fake fingers (particularly the fingerprint textures) rendering them unusable after the initial spoof attempt. Thus, this form of trial-and-error attack is less reliable and likely to leave traces (e.g., smudge, scratch) on the PDMS gel which is against the attack requirements (R2 in Section III-C). The detection rate can be improved by adopting a camera with higher sampling rate or extending the sensing period.

B. Denial-of-Service Attacks

Realizing the inefficacy of physical attacks on *FakeGuard*, the attacker aims to manipulate the victim's trust towards our

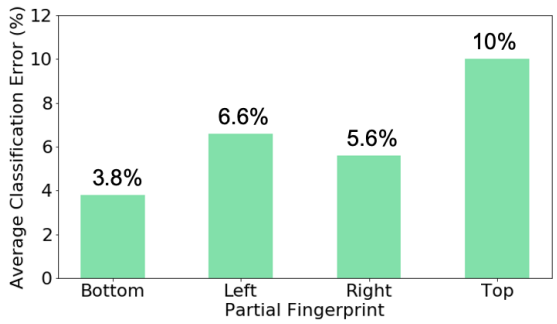

Fig. 19. Evaluation of *FakeGuard* under different regions of partial fingerprints.

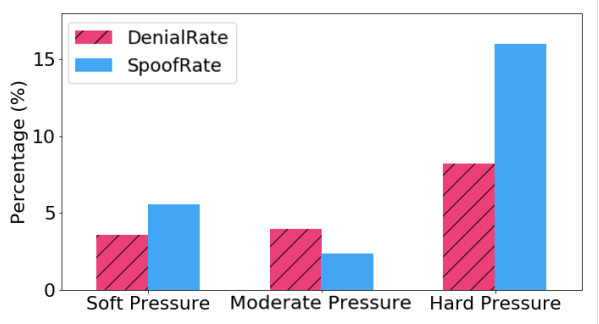

Fig. 20. Evaluation of *FakeGuard* under dynamic pressure during the press action.

system by limiting its capability of fingerprint detection (see DenialRate metric in Section IX-A and X-A). It is a known fact that AFRS have limited robustness to drastic changes in the user's fingertip (i.e., moisture) and ambient environment. By controlling the temperature, lighting or moisture conditions, an attacker can exploit these limitations during the sensing process. For the following experiments, we recruit five subjects to perform 150 press actions under different conditions.

• **Moisture Effect**: In the first trial, the subject's fingertip is in a dry state. During the second trial, the attacker places a humidifier in the immediate vicinity of victim's fingertip to increase its moistness. During the third trial, we ask the subjects to place their finger in water before interacting with *FakeGuard*. The DenialRate is presented in Table III. The results demonstrate a consistent performance regardless of the moisture level on the fingerprint surface.

• **Temperature Effect**: We manipulate the temperature to create three settings, i.e., cold environment ($<0°$C), room temperature (23°C) and warm ambience ($>40°$C) by using a conventional heater/cooler. Table III shows the DenialRate on detecting live fingers of five subjects. The rheological properties of our novel PDMS gel are not influenced by cold or room temperature. However, increasing the temperature above 40°C initiates a structural distortion of PDMS while reducing its capability to regain shape immediately after the press action. DenialRate can be improved by allowing sufficient time (5-10 seconds) in-between trials under warm temperatures.

• **Lightning Effect**: The subjects perform press actions in an ambient environment with three brightness levels, i.e., low optical illumination (<200 Lux), moderate lighting (800 Lux) and very bright light (>1500 Lux) (see Table III). Excessive light rays can cause specular reflection on PDMS and limit photometric stereo reconstruction in deriving haptic response. The effect of ambient light can be effortlessly reduced by optimizing the ocular properties of PDMS and supporting structure in hardware setup as discussed in the next section.

TABLE III. *FakeGuard* RESILIENCE TO NON-IDEAL CHANGES IN THE AMBIENT ENVIRONMENT.

Moisture	*Dry State*	*Moist*	*Wet*
DenialRate	4.2%	3.2%	4.0%
Temperature	*Cold (0°C)*	*Normal (23°C)*	*Warm (40°C)*
DenialRate	4.0%	4.0%	11.4%
Brightness	*Low 200Lux*	*Normal 800Lux*	*High 1500Lux*
DenialRate	4.4%	4.0%	9.6%

XI. DISCUSSION

Aging Effect: In the physical and polymer domain, aging is a conventional process from which the objects can be protected via preservation techniques [93], [94]. To evaluate the effect of aging on PDMS, we re-sample the press actions of three subjects on the *FakeGuard* after six months. The original template of subject's live finger is leveraged for training the model. The performance of new testing samples for live and fake finger detection remains consistent. Our designed PDMS can withstand a temperature up to 65°C before losing the ability to regain its shape after deformation. Under normal usage, the gel is expected to last 3-4 years. PDMS aging is an open problem with room for improvements (PDMS with temperature resilience up to 350°C [95]).

Design Improvements: *FakeGuard* can be improved by addressing three factors: (1) *Pressure Variation: FakeGuard* is primarily aimed to capture the haptic response. Considering pressure variation can also be an important feature for fake finger detection, a continuous 3D model can be employed by leveraging an RGB light source that is simultaneously bright instead of a monochromatic light source that is intermittently bright. Under this condition, the continuous 3D fingerprints will be captured comprising information about pressure variations. (2) *Ambient Light:* our hardware's supporting structure does not facilitate an opaque property, thereby allowing ambient light rays to interfere with the sensing process. In the future, we aim to employ 3D printing to manufacture an opaque supporting structure made from low-cost PLA material. (3) *Energy Consumption:* the white LED ring is utilized to ensure ideal optical illuminance on the gel surface when recording the haptic response. However, its energy consumption of 24W limits the portability of *FakeGuard* to physical-access mechanisms such as smartlocks. A series of low-power point LEDs can replace the white LED ring for sufficient illumination.

Application Scenarios: AFRS has been employed across IoT and physical domain for securing sensitive information or the commodity of users. Considering our work is the first exploration of haptic-based anti-spoofing, *FakeGuard* can ensure complete security in high-impact scenarios, e.g., international-border verification, ATM monetary transactions, smart homes and smart city environments. However, our system's size needs to be reduced for potential deployment in smartphones. Since the photometric stereo will restrict the minimum size of *FakeGuard*, we can leverage other 3D reconstruction methods such as 3D ultrasonic fingerprint [96]. This would allow a drastic reduction in the size of chip to $4.6mm \times 3.2mm$ which is small enough for smartphones. We consider this as a venue of exploration for our future work.

XII. CONCLUSION

The plethora of literature on fingerprint anti-spoofing and development of AFRS provide a false sense of security regarding their capability of fake finger detection. In this paper, we first demonstrate that the current state-of-the-art AFRS can be compromised by high-precision fake fingers. As a mission to identify the fundamental difference between live and fake finger, we consider the biological property of anatomy that is distinct between the human fingertip and the spoofing materials. We develop *FakeGuard* that utilizes the haptic response caused by fingertip to gel surface interaction for fingerprint anti-spoofing. *FakeGuard* is resilient and user-friendly with superior performance against state-of-the-art anti-spoofing. We also show the resilience of *FakeGuard* against template alteration, brute force and denial-of-service attacks.

ACKNOWLEDGEMENT

The authors would like to thank all anonymous reviewers for their insightful comments on this paper. This paper was in part supported by National Key R&D Program of China (Grant No. 2020AAA0107700), National Natural Science Foundation of China (Grant No. 62032021, 61972348, 61772236, and 61872285), and the US National Science Foundation (Grant No. 1822190 and 2050910).

REFERENCES

[1] L. H. Newman, "A cheap 3d printer can trick smartphone fingerprint locks." [Online]. Available: https://www.wired.com/story/cheap-3d-printer-trick-smartphone-fingerprint-locks/

[2] J. Santoemma, "Wood glue," Feb. 25 1992, uS Patent 5,091,458.

[3] I. Goicoechea-Telleria, K. Kiyokawa, J. Liu-Jimenez, and R. Sánchez-Reillo, "Low-cost and efficient hardware solution for presentation attack detection in fingerprint biometrics using special lighting microscopes," *IEEE Access*, vol. 7, pp. 7184–7193, 2019. [Online]. Available: https://doi.org/10.1109/ACCESS.2018.2888905

[4] C. Sousedik, R. Breithaupt, and C. Busch, "Volumetric fingerprint data analysis using optical coherence tomography," in *2013 BIOSIG - Proceedings of the 12th International Conference of Biometrics Special Interest Group, Darmstadt, Germany, September 4-6, 2013*, 2013, pp. 51–62. [Online]. Available: https://dl.gi.de/20.500.12116/17691

[5] D. Baldisserra, A. Franco, D. Maio, and D. Maltoni, "Fake fingerprint detection by odor analysis," in *Advances in Biometrics, International Conference, ICB 2006, Hong Kong, China, January 5-7, 2006, Proceedings*, 2006, pp. 265–272. [Online]. Available: https://doi.org/10.1007/11608288_36

[6] J. Kolberg, D. Gläsner, R. Breithaupt, M. Gomez-Barrero, J. Reinhold, A. von Twickel, and C. Busch, "On the effectiveness of impedance-based fingerprint presentation attack detection," *Sensors*, vol. 21, no. 17, p. 5686, 2021.

[7] S. T. Parthasaradhi, R. Derakhshani, L. A. Hornak, and S. A. Schuckers, "Time-series detection of perspiration as a liveness test in fingerprint devices," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 35, no. 3, pp. 335–343, 2005.

[8] J. Galbally, J. Fierrez, F. Alonso-Fernandez, and M. Martinez-Diaz, "Evaluation of direct attacks to fingerprint verification systems," *Telecommunication Systems*, vol. 47, no. 3, pp. 243–254, 2011.

[9] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of fingerprint recognition*. Springer Science & Business Media, 2009.

[10] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, "Impact of artificial" gummy" fingers on fingerprint systems," in *Optical Security and Counterfeit Deterrence Techniques IV*, vol. 4677. International Society for Optics and Photonics, 2002, pp. 275–289.

[11] S. S. Arora, K. Cao, A. K. Jain, and N. G. Paulter, "3d fingerprint phantoms," in *2014 22nd International Conference on Pattern Recognition*. IEEE, 2014, pp. 684–689.

[12] H. Kang, B. Lee, H. Kim, D. Shin, and J. Kim, "A study on performance evaluation of the liveness detection for various fingerprint sensor modules," in *International Conference on Knowledge-Based and Intelligent Information and Engineering Systems*. Springer, 2003, pp. 1245–1253.

[13] "Hacker fakes german minister's fingerprints using photos of her hands," Dec 2014. [Online]. Available: https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands

[14] D. Winder, "Samsung galaxy s10 fingerprint scanner hacked - here's what you need to know," Apr 2019. [Online]. Available: https://www.forbes.com/sites/daveywinder/2019/04/06/samsung-galaxy-s10-fingerprint-scanner-hacked-heres-what-you-need-to-know/?sh=35fe97ae5d42

[15] K. Singh, "Up: Man learns 'cloning fingerprints' online, 'hacks' 500 bank accounts: Bareilly news - times of india." [Online]. Available: https://timesofindia.indiatimes.com/city/bareilly/man-26-learns-cloning-fingerprints-online-hacks-nearly-500-accounts-with-bank-mitrass-help/articleshow/81158623.cms

[16] A. Ross and A. Jain, "Biometric sensor interoperability: A case study in fingerprints," in *International Workshop on Biometric Authentication*. Springer, 2004, pp. 134–145.

[17] Y. S. Moon, J. Chen, K. Chan, K. So, and K. Woo, "Wavelet based fingerprint liveness detection," *Electronics Letters*, vol. 41, no. 20, pp. 1112–1113, 2005.

[18] T. Chugh, K. Cao, and A. K. Jain, "Fingerprint spoof buster: Use of minutiae-centered patches," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 9, pp. 2190–2202, 2018.

[19] R. F. Nogueira, R. de Alencar Lotufo, and R. C. Machado, "Fingerprint liveness detection using convolutional neural networks," *IEEE transactions on information forensics and security*, vol. 11, no. 6, pp. 1206–1213, 2016.

[20] J. Galbally, F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia, "A high performance fingerprint liveness detection method based on quality related features," *Future Generation Computer Systems*, vol. 28, no. 1, pp. 311–321, 2012.

[21] D. Gragnaniello, G. Poggi, C. Sansone, and L. Verdoliva, "Local contrast phase descriptor for fingerprint liveness detection," *Pattern Recognition*, vol. 48, no. 4, pp. 1050–1058, 2015.

[22] "A cheap 3d printer can trick smartphone fingerprint locks," Jan 2021. [Online]. Available: https://www.wired.com/story/cheap-3d-printer-trick-smartphone-fingerprint-locks/

[23] "Researcher uses 3d-printed fingerprint to spoof biometric authentication," Feb 2021. [Online]. Available: https://www.biometricupdate.com/202008/researcher-uses-3d-printed-fingerprint-to-spoof-biometric-authentication

[24] J. J. Engelsma, S. S. Arora, A. K. Jain, and N. G. Paulter, "Universal 3d wearable fingerprint targets: advancing fingerprint reader evaluations," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 6, pp. 1564–1578, 2018.

[25] S. Singh, "Fingerprint sensor market," 2019. [Online]. Available: https://www.marketsandmarkets.com/PressReleases/fingerprint-sensors.asp

[26] J. Loughran, "3d fingerprint scanner promises accuracy and speed at low cost," Mar 2017. [Online]. Available: https://eandt.theiet.org/content/articles/2017/03/3d-fingerprint-scanner-promises-accuracy-and-speed-at-low-cost/

[27] E. Marasco and A. Ross, "A survey on antispoofing schemes for fingerprint recognition systems," *ACM Computing Surveys (CSUR)*, vol. 47, no. 2, p. 28, 2015.

[28] S. S. Arora, K. Cao, A. K. Jain, and N. G. P. Jr., "Design and fabrication of 3d fingerprint targets," *IEEE Trans. Information Forensics and Security*, vol. 11, no. 10, pp. 2284–2297, 2016. [Online]. Available: https://doi.org/10.1109/TIFS.2016.2581306

[29] J. J. Engelsma, S. S. Arora, A. K. Jain, and N. G. P. Jr., "Universal 3d wearable fingerprint targets: Advancing fingerprint reader evaluations," *CoRR*, vol. abs/1705.07972, 2017. [Online]. Available: http://arxiv.org/abs/1705.07972

[30] C. Barral and A. Tria, "Fake fingers in fingerprint recognition: Glycerin supersedes gelatin," in *Formal to Practical Security*. Springer, 2009, pp. 57–69.

[31] T. Chugh and A. K. Jain, "Fingerprint presentation attack detection: Generalization and efficiency," in *2019 International Conference on Biometrics (ICB)*. IEEE, 2019, pp. 1–8.

[32] Q. Huang, S. Chang, C. Liu, B. Niu, M. Tang, and Z. Zhou, "An evaluation of fake fingerprint databases utilizing svm classification," *Pattern Recognition Letters*, vol. 60, pp. 1–7, 2015.

[33] E. Bowden-Peters, R. C.-W. Phan, J. N. Whitley, and D. J. Parish, "Fooling a liveness-detecting capacitive fingerprint scanner," in *Cryptography and Security: From Theory to Applications*. Springer, 2012, pp. 484–490.

[34] A. Antonelli, R. Cappelli, D. Maio, and D. Maltoni, "Fake finger detection by skin distortion analysis," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 3, pp. 360–373, 2006.

[35] S. A. Schuckers, "Spoofing and anti-spoofing measures," *Information Security technical report*, vol. 7, no. 4, pp. 56–62, 2002.

[36] E. Marasco and C. Sansone, "Combining perspiration- and morphology-based static features for fingerprint liveness detection," *Pattern Recognition Letters*, vol. 33, no. 9, pp. 1148–1156, 2012. [Online]. Available: https://doi.org/10.1016/j.patrec.2012.01.009

[37] R. F. Nogueira, R. de Alencar Lotufo, and R. C. Machado, "Fingerprint liveness detection using convolutional neural networks," *IEEE Trans. Information Forensics and Security*, vol. 11, no. 6, pp. 1206–1213, 2016. [Online]. Available: https://doi.org/10.1109/TIFS.2016.2520880

[38] E. Park, X. Cui, W. Kim, and H. Kim, "End-to-end fingerprints liveness detection using convolutional networks with gram module," *CoRR*, vol. abs/1803.07830, 2018. [Online]. Available: http://arxiv.org/abs/1803.07830

[39] E. Park, X. Cui, T. H. B. Nguyen, and H. Kim, "Presentation attack detection using a tiny fully convolutional network," *IEEE Trans.*

Information Forensics and Security, vol. 14, no. 11, pp. 3016–3025, 2019. [Online]. Available: https://doi.org/10.1109/TIFS.2019.2907184

[40] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," in *3rd International Conference on Learning Representations, ICLR 2015, San Diego, CA, USA, May 7-9, 2015, Conference Track Proceedings*, 2015. [Online]. Available: http://arxiv.org/abs/1409.1556

[41] C. Szegedy, W. Liu, Y. Jia, P. Sermanet, S. E. Reed, D. Anguelov, D. Erhan, V. Vanhoucke, and A. Rabinovich, "Going deeper with convolutions," in *IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2015, Boston, MA, USA, June 7-12, 2015*, 2015, pp. 1–9. [Online]. Available: https://doi.org/10.1109/CVPR.2015.7298594

[42] J. J. Engelsma and A. K. Jain, "Generalizing fingerprint spoof detector: Learning a one-class classifier," *CoRR*, vol. abs/1901.03918, 2019. [Online]. Available: http://arxiv.org/abs/1901.03918

[43] Y. Ding and A. Ross, "An ensemble of one-class svms for fingerprint spoof detection across different fabrication materials," in *IEEE International Workshop on Information Forensics and Security, WIFS 2016, Abu Dhabi, United Arab Emirates, December 4-7, 2016*, 2016, pp. 1–6. [Online]. Available: https://doi.org/10.1109/WIFS.2016.7823572

[44] A. Taneja, A. Tayal, A. Malhorta, A. Sankaran, M. Vatsa, and R. Singh, "Fingerphoto spoofing in mobile devices: a preliminary study," in *2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS)*. IEEE, 2016, pp. 1–7.

[45] E. Marasco and A. Ross, "A survey on antispoofing schemes for fingerprint recognition systems," *ACM Computing Surveys (CSUR)*, vol. 47, no. 2, pp. 1–36, 2014.

[46] C. Kauba, L. Debiasi, and A. Uhl, "Enabling fingerprint presentation attacks: Fake fingerprint fabrication techniques and recognition performance," *arXiv preprint arXiv:2012.00606*, 2020.

[47] R. B. Gonzalo, B. Corsetti, I. Goicoechea-Telleria, A. Husseis, J. Liu-Jimenez, R. Sanchez-Reillo, T. Eglitis, E. Ellavarason, R. Guest, C. Lunerti, *et al.*, "Attacking a smartphone biometric fingerprint system: A novice's approach," in *2018 International Carnahan Conference on Security Technology (ICCST)*. IEEE, 2018, pp. 1–5.

[48] S. Ravi, A. Raghunathan, and S. Chakradhar, "Tamper resistance mechanisms for secure embedded systems," in *17th International Conference on VLSI Design. Proceedings.* IEEE, 2004, pp. 605–611.

[49] O. Kömmerling and M. G. Kuhn, "Design principles for tamper-resistant smartcard processors." *Smartcard*, vol. 99, pp. 9–20, 1999.

[50] K. W. McCalley, S. D. Wilson, D. R. Setlak, N. W. Van Vonno, and C. L. Hewitt, "Enhanced security fingerprint sensor package and related methods," Sept. 21 1999, uS Patent 5,956,415.

[51] S. Swanson and S. Swanson, "Fingerprints go the distance," Oct 2012. [Online]. Available: https://www.technologyreview.com/s/422400/fingerprints-go-the-distance/

[52] F. Liu and D. Zhang, "3d fingerprint reconstruction system using feature correspondences and prior estimated finger model," *Pattern Recognition*, vol. 47, no. 1, pp. 178–193, 2014.

[53] I. Goicoechea-Telleria, A. Garcia-Peral, A. Husseis, and R. Sanchez-Reillo, "Presentation attack detection evaluation on mobile devices: Simplest approach for capturing and lifting a latent fingerprint," in *2018 International Carnahan Conference on Security Technology (ICCST)*. IEEE, 2018, pp. 1–5.

[54] T. Van der Putte and J. Keuning, "Biometrical fingerprint recognition: don't get your fingers burned," in *Smart Card Research and Advanced Applications*. Springer, 2000, pp. 289–303.

[55] "Defcon: Fooling biometric sensors using 3d printed fake fingerprints - 3dprint.com: The voice of 3d printing / additive manufacturing," Aug 2020. [Online]. Available: https://3dprint.com/271540/d-defcon-fooling-biometric-sensors-using-3d-printed-fake-fingerprints/

[56] "Bypassing biometric systems with 3d printing and 'enhanced' grease attacks," June 2020. [Online]. Available: https://dreamlab.net/media/img/news/WP_Biometrics_v5.pdf

[57] C. Schubert, M. C. Van Langeveld, and L. A. Donoso, "Innovations in 3d printing: a 3d overview from optics to organs," *British Journal of Ophthalmology*, vol. 98, no. 2, pp. 159–161, 2014.

[58] F. Klatte, "Manufacture of esters and ethers of ethylidene glycol and of vinyl alcohol." Jan. 13 1914, uS Patent 1,084,581.

[59] "Polymer properties database." [Online]. Available: https://polymerdatabase.com/PolymerBrands/PVA.html

[60] C. Stead, "What is pva glue?" Dec 2020. [Online]. Available: https://www.wood-finishes-direct.com/blog/what-is-pva-glue/

[61] A. Kaboorani and B. Riedl, "Mechanical performance of polyvinyl acetate (pva)-based biocomposites," in *Biocomposites*. Elsevier, 2015, pp. 347–364.

[62] H.-W. Cui and G.-B. Du, "Preparation and characterization of exfoliated nano-composite of polyvinyl acetate and montmorillonite," *Journal of Chemical Engineering and Materials Science*, vol. 2, no. 8, pp. 122–128, 2011.

[63] N. Chemicals, "Nitchen chemicals," http://www.polyvinylacetate.cn/pvac/.

[64] amazon, "amazon," https://www.amazon.com/Eclipse-MT-1280-ProsKit-Multimeter-Digital/dp/B003TYIC9K.

[65] A. Abhyankar and S. Schuckers, "Fingerprint liveness detection using local ridge frequencies and multiresolution texture analysis techniques," in *2006 international conference on image processing*. IEEE, 2006, pp. 321–324.

[66] C. Jin, H. Kim, and S. Elliott, "Liveness detection of fingerprint based on band-selective fourier spectrum," in *International Conference on Information Security and Cryptology*. Springer, 2007, pp. 168–179.

[67] L. Ghiani, G. L. Marcialis, and F. Roli, "Fingerprint liveness detection by local phase quantization," in *Proceedings of the 21st International Conference on Pattern Recognition (ICPR2012)*. IEEE, 2012, pp. 537–540.

[68] A. Abdouni, M. Djaghloul, C. Thieulin, R. Vargiolu, C. Pailler-Mattei, and H. Zahouani, "Biophysical properties of the human finger for touch comprehension: influences of ageing and gender," *Royal Society open science*, vol. 4, no. 8, p. 170321, 2017.

[69] J. T. Shores, "Anatomy and physiology of the fingertip," in *Fingertip Injuries*. Springer, 2015, pp. 1–9.

[70] C. Cornelius, R. Peterson, J. Skinner, R. Halter, and D. Kotz, "A wearable system that knows who wears it," in *Proceedings of the 12th annual international conference on Mobile systems, applications, and services*, 2014, pp. 55–67.

[71] H.-K. Lee, J. Chung, S.-I. Chang, and E. Yoon, "Normal and shear force measurement using a flexible polymer tactile sensor with embedded multiple capacitors," *Journal of Microelectromechanical Systems*, vol. 17, no. 4, pp. 934–942, 2008.

[72] J. C. Lötters, W. Olthuis, P. H. Veltink, and P. Bergveld, "The mechanical properties of the rubber elastic polymer polydimethylsiloxane for sensor applications," *Journal of micromechanics and microengineering*, vol. 7, no. 3, p. 145, 1997.

[73] W. S. Slaughter, *The linearized theory of elasticity*. Springer Science & Business Media, 2012.

[74] P. Drozdowski, C. Rathgeb, A. Dantcheva, N. Damer, and C. Busch, "Demographic bias in biometrics: A survey on an emerging challenge," *IEEE Transactions on Technology and Society*, vol. 1, no. 2, pp. 89–103, 2020.

[75] D. Thakkar, "Biometric devices: Cost, types and comparative analysis," 2019. [Online]. Available: https://www.bayometric.com/biometric-devices-cost/

[76] R. J. Woodham, "Photometric method for determining surface orientation from multiple images," *Optical engineering*, vol. 19, no. 1, p. 191139, 1980.

[77] A. Kumar, *Contactless 3D Fingerprint Identification*. Springer, 2018.

[78] R. T. Frankot and R. Chellappa, "A method for enforcing integrability in shape from shading algorithms," *IEEE Transactions on pattern analysis and machine intelligence*, vol. 10, no. 4, pp. 439–451, 1988.

[79] N. K. Ratha, S. Chen, and A. K. Jain, "Adaptive flow orientation-based feature extraction in fingerprint images," *Pattern Recognition*, vol. 28, no. 11, pp. 1657–1672, 1995.

[80] L. Hong, Y. Wan, and A. Jain, "Fingerprint image enhancement: algorithm and performance evaluation," *IEEE transactions on pattern analysis and machine intelligence*, vol. 20, no. 8, pp. 777–789, 1998.

[81] M. D. Garris, C. I. Watson, R. McCabe, and C. L. Wilson, "User's guide to nist fingerprint image software (nfis)," Tech. Rep., 2001.

[82] L. Nanni and A. Lumini, "Local binary patterns for a hybrid fingerprint matcher," *Pattern recognition*, vol. 41, no. 11, pp. 3461–3466, 2008.

[83] S. B. Nikam and S. Agarwal, "Wavelet energy signature and glcm features-based fingerprint anti-spoofing," in *2008 international conference on wavelet analysis and pattern recognition*, vol. 2. IEEE, 2008, pp. 717–723.

[84] C. Giuffrida, K. Majdanik, M. Conti, and H. Bos, "I sensed it was you: authenticating mobile users with sensor-enhanced keystroke dynamics," in *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*. Springer, 2014, pp. 92–111.

[85] N. V. Boulgouris and Z. X. Chi, "Gait recognition using radon transform and linear discriminant analysis," *IEEE transactions on image processing*, vol. 16, no. 3, pp. 731–740, 2007.

[86] C. Sousedik and C. Busch, "Presentation attack detection methods for fingerprint recognition systems: a survey," *Iet Biometrics*, vol. 3, no. 4, pp. 219–233, 2014.

[87] R. Raghavendra, K. B. Raja, and C. Busch, "Presentation attack detection for face recognition using light field camera," *IEEE Transactions on Image Processing*, vol. 24, no. 3, pp. 1060–1075, 2015.

[88] T. Chen and C. Guestrin, "Xgboost: A scalable tree boosting system," in *Proceedings of the 22nd acm sigkdd international conference on knowledge discovery and data mining*, 2016, pp. 785–794.

[89] G. Ke, Q. Meng, T. Finley, T. Wang, W. Chen, W. Ma, Q. Ye, and T.-Y. Liu, "Lightgbm: A highly efficient gradient boosting decision tree," *Advances in neural information processing systems*, vol. 30, pp. 3146–3154, 2017.

[90] S. E. Harris, "Silicone skin trays: An innovative simulation approach to nurse practitioner skills training," *Clinical Simulation in Nursing*, vol. 49, pp. 28–31, 2020.

[91] G. L. Marcialis, A. Lewicke, B. Tan, P. Coli, D. Grimberg, A. Congiu, A. Tidu, F. Roli, and S. Schuckers, "First international fingerprint liveness detection competition—livdet 2009," in *International Conference on Image Analysis and Processing*. Springer, 2009, pp. 12–23.

[92] E. Marasco and C. Sansone, "Combining perspiration-and morphology-based static features for fingerprint liveness detection," *Pattern Recognition Letters*, vol. 33, no. 9, pp. 1148–1156, 2012.

[93] R. J. Young and P. A. Lovell, *Introduction to polymers*. CRC press, 2011.

[94] X. Cui, G. Zhu, Y. Pan, Q. Shao, M. Dong, Y. Zhang, Z. Guo, *et al.*, "Polydimethylsiloxane-titania nanocomposite coating: fabrication and corrosion resistance," *Polymer*, vol. 138, pp. 203–210, 2018.

[95] K. Ren, Y. Zheng, W. Dai, D. Ryan, C. Fung, and H. Wu, "Soft-lithography-based high temperature molding method to fabricate whole teflon microfluidic chips," in *14th International Conference on Miniaturized Systems for Chemistry and Life Sciences, Groningen, The Netherlands*, 2010, pp. 554–556.

[96] H. Tang, Y. Lu, F. Assaderagh, M. Daneman, X. Jiang, M. Lim, X. Li, E. J. Ng, U. Singhal, J. M. Tsai, D. A. Horsley, and B. E. Boser, "11.2 3d ultrasonic fingerprint sensor-on-a-chip," in *2016 IEEE International Solid-State Circuits Conference, ISSCC 2016, San Francisco, CA, USA, January 31 - February 4, 2016*. IEEE, 2016, pp. 202–203. [Online]. Available: https://doi.org/10.1109/ISSCC.2016.7417977