



From Seaweed to Security: Harnessing Alginate to Challenge IoT Fingerprint Authentication

Pouria Rad
Augusta University
Augusta, Georgia, USA
peslamirad@augusta.edu

Gokila Dorai
Augusta University
Augusta, Georgia, USA
gdorai@augusta.edu

Mohsen Jozani
Augusta University
Augusta, Georgia, USA
mjozani@augusta.edu

ABSTRACT

The increasing integration of capacitive fingerprint recognition sensors in IoT devices presents new challenges in digital forensics, particularly in the context of advanced fingerprint spoofing. Previous research has highlighted the effectiveness of materials such as latex and silicone in deceiving biometric systems. In this study, we introduce Alginate, a biopolymer derived from brown seaweed, as a novel material with the potential for spoofing IoT-specific capacitive fingerprint sensors. Our research uses Alginate and cutting-edge image recognition techniques to unveil a nuanced IoT vulnerability that raises significant security and privacy concerns. Our proof-of-concept experiments employed authentic fingerprint molds to create Alginate replicas, which exhibited remarkable visual and tactile similarities to real fingerprints. The conductivity and resistivity properties of Alginate, closely resembling human skin, make it a subject of interest in the digital forensics field, especially regarding its ability to spoof IoT device sensors. This study calls upon the digital forensics community to develop advanced anti-spoofing strategies to protect the evolving IoT infrastructure against such sophisticated threats.

KEYWORDS

Alginate, Fingerprint spoofing, Capacitive sensors, IoT security, Biometric security, Biometric deception

ACM Reference Format:

Pouria Rad, Gokila Dorai, and Mohsen Jozani. 2024. From Seaweed to Security: Harnessing Alginate to Challenge IoT Fingerprint Authentication. In *The 19th International Conference on Availability, Reliability and Security (ARES 2024)*, July 30–August 02, 2024, Vienna, Austria. ACM, New York, NY, USA, 10 pages. <https://doi.org/10.1145/3664476.3670924>

1 INTRODUCTION

The Internet of Things (IoT) represents a significant evolution in interconnected, intelligent devices, revolutionizing industries from healthcare to transportation. However, ensuring their security becomes paramount as these devices become more integrated into our daily lives. Biometric authentication, particularly fingerprint recognition, is a standard security method in IoT devices. Fingerprint recognition, especially capacitive fingerprint recognition, offers

a unique and personalized method of authentication, leveraging the distinct patterns found on every individual's fingertips. Yet, studies by [3, 17] and [14] highlight the vulnerabilities of such authentication systems against fingerprint spoofing and at the same time their wide usage for biometric-based security solutions in IoT systems.

Historically, various materials have been explored for fingerprint spoofing attacks, including latex, silicone, and gelatin, however, a new competitor has emerged. Alginate, a naturally occurring biopolymer derived from seaweed, has gained prominence in bioprinting or skin mimicry due to its unique properties. It closely mimics the texture and elasticity of human skin, making it an ideal material for creating fingerprint replicas [28]. Moreover, its wide availability and ease of use further accentuate its potential as a spoofing material. Studies have shown that Alginate-based hydrogels present properties suitable for bioprinting of skin models [29], and its combination with other materials can produce skin-like hydrogels with high elasticity and sensitivity [5]. Using Alginate molds, we can cast fingerprints to form a skin-like cast that needs no further post-process to be recognized by the fingerprint sensors. This amplifies a vulnerability challenge for security of fingerprint sensors which needs to be addressed.

While these materials have been used to deceive biometric systems of even advanced authentication mechanisms, the digital age has further complicated this scenario. Former Studies explored the Etsy Platform, where users often share high-resolution images of their hands, which can inadvertently become sources for biometric data extraction using AI and machine learning tools [15]. In their study, they highlighted the risks of posting biometric information online and the lack of adequate protective measures by social media and marketplace companies. With advanced image processing, these fingerprints can be extracted from such photographs, presenting a substantial security concern [18], permanently compromising biometric security for social media users. This exposure is particularly concerning because, unlike passwords, compromised biometric data, such as fingerprints, remains permanently vulnerable [1, 23]. Past breaches highlight this enduring risk [6] and the combination of high-definition camera technology and AI-driven tools magnifies this vulnerability, allowing automated extraction from vast datasets [9]. This underscores the pressing need to address these new age vulnerabilities, especially within forensics contexts.

Therefore, to guide our exploration, we pose the following research question: "How effective is Alginate in spoofing capacitive fingerprint sensors in IoT devices, and what implications does this have for the security of biometric data and the integrity of digital



This work is licensed under a Creative Commons Attribution International 4.0 License.

ARES 2024, July 30–August 02, 2024, Vienna, Austria
© 2024 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-1718-5/24/07
<https://doi.org/10.1145/3664476.3670924>

Table 1: Summary of Related Works

Aspect	Description	Reference
Biometrics Aspects		
Uniqueness	Utilizes individual patterns in fingerprints for secure authentication methods.	[14]
Integration	Non-intrusive integration into smartphones, smart locks, etc.	[17]
Challenges	Faces standardization challenges in IoT; requires active user interaction, poses data breach risks.	[8]
Vulnerabilities	Includes risks from partial systems and smudges on screens that can reconstruct fingerprints.	[26], [17]
Solutions	Introduction of lightweight fuzzy extractors and multimodal authentication for better security.	[8], [27]
Data Protection	Methods to ensure biometric data protection during transmission and storage.	[12]
Material/Method		
Materials	Describes materials like latex, silicone, gelatin, and alginate for creating replicas.	[19], [10], [4], [28]
3D Printing	Advanced techniques for creating detailed fingerprint replicas; also high-resolution image threats.	[21], [15]
Vulnerability Aspects		
Spoofing	Discusses sensors being deceived by material replicas; challenges in liveness detection.	[18], [11]
Residual Finger-prints	Risks from smudges left on sensors; high-resolution sensors increase sensitivity to spoofing.	[17], [2]
IoT Integration	Highlights the resource constraints and security standardization challenges in IoT.	[14]
Concerns		
Digital Exposure	Risks from high-resolution images on social platforms; digital forensics and machine learning techniques extracting fingerprint details.	[15], [18], [25], [9]
Preventative Measures	Emphasizes the need for stricter privacy policies and user education on sharing biometric data.	[23]
Data Compromise	Discusses the lasting threat of biometric data breaches and database vulnerabilities.	[23], [6]
Forensics Solutions	Advocates for biometric template protection and fusion of multiple biometrics to enhance security.	[22], [24]

forensic investigations?" This inquiry not only directs our experimental approach but also frames our discussion on the evolving landscape of IoT security and digital forensic practices.

In this study, we explore the efficacy of Alginate in fingerprint spoofing. While our experiments primarily utilize consensually obtained real-life samples of fingerprint molds, the broader implications of our findings resonate with the digital forensics community. The potential for using publicly available images for fingerprint data extraction to fabricate fingerprint replicas using easily accessible technologies like 3D printing introduces novel challenges that must be addressed to maintain the integrity of forensic investigations and biometric security, particularly in IoT devices. Our research underscores the need for forensic experts to adapt to these emerging threats by understanding the nuances of this vulnerability, pushing stakeholders in the IoT industry to develop more robust security measures, ensuring that devices remain secure even in the face of sophisticated attacks.

The remainder of this paper is structured as follows. Section 2 provides a detailed review of the related work, highlighting the findings of previous studies and identifying gaps. Section 3 describes the methodology employed in our research, detailing the experiments conducted and the rationale behind them. Section 4 presents our findings, followed by a discussion in Section 5. Limitations of this work are presented in Section 6. Finally, Section 7 concludes the paper, offering recommendations for future research and potential solutions to the identified vulnerability.

2 RELATED WORK

The domain of biometric authentication in IoT has garnered significant attention due to its potential to offer secure and user-friendly

mechanisms for device access. This section provides a comprehensive review of the existing literature, focusing on the evolution, strengths, vulnerabilities, and potential threats associated with biometric authentication in IoT. We have summarized related works in Table 1.

The IoT ecosystem is characterized by a vast array of devices, each with its unique functionalities and purposes. As these devices become more integrated into our daily lives, the need for secure and reliable authentication mechanisms becomes paramount. Among the various authentication methods, biometric authentication, particularly fingerprint recognition, has emerged as a preferred choice for many IoT devices.

Fingerprint recognition offers several advantages. Firstly, it leverages the uniqueness of an individual's fingerprint patterns, ensuring that the authentication process is personalized and secure [14]. This uniqueness is a cornerstone of biometric security, making it less vulnerable to breaches in IoT systems or infrastructure. Secondly, fingerprint sensors are compact and can be seamlessly integrated into a wide range of devices, from smartphones to smart door locks. This integration ensures that the user experience remains intuitive and non-intrusive [17].

However, the adoption of fingerprint sensors in IoT devices is not without challenges. The diverse range of IoT devices, each with its computational and sensing capabilities, poses a challenge in standardizing biometric solutions. Moreover, while fingerprints offer stability, they demand active user interaction, which might not always be feasible for continuous authentication. Additionally, the risk of fingerprint data being compromised, either through physical means or digital extraction, remains a significant concern [8].

Several vulnerabilities have been identified in fingerprint-based authentication systems. For instance, partial fingerprint-based authentication systems have been found to be potentially vulnerable, especially when multiple impressions are enrolled per finger [26]. Furthermore, the risk posed by smudges left on device touch screens, which can be used to reconstruct an image of the enrolled fingerprint, has been highlighted in the literature by [17].

To address these challenges and vulnerabilities, researchers have been exploring innovative solutions. The introduction of lightweight fuzzy extractors, which offer a more error-tolerant biometric solution suitable for resource-constrained IoT devices, is one such advancement [8]. Additionally, the concept of multimodal biometric authentication, which combines multiple biometric traits, has been proposed to enhance the reliability and security of authentication systems [27]. With the increasing concerns about the security of biometric data, new methods have been introduced to ensure the protection of biometric data during transmission and storage [12]. As the IoT landscape continues to evolve, so does the need for adaptable and resilient biometric solutions. The dynamic nature of this ecosystem necessitates continuous research and innovation. As devices become more sophisticated and threats evolve, the focus will inevitably shift towards developing more advanced and secure fingerprint authentication mechanisms.

While the advancements in biometric authentication for IoT devices, particularly fingerprint recognition, have brought about enhanced security, they are not without vulnerabilities. The very uniqueness of fingerprints, which makes them a reliable authentication method, also makes them a prime target for attackers. If an attacker can replicate a fingerprint with high fidelity, they can potentially gain unauthorized access to a device or system. Over the years, various materials and methods have been employed to spoof fingerprints, each with its own set of challenges and successes. As we delve deeper into the realm of fingerprint spoofing, it becomes imperative to understand the materials traditionally used, their effectiveness, and the innovative methods attackers might employ. Fingerprint spoofing is the art and science of deceiving a biometric system by presenting a fabricated fingerprint that matches a legitimate user's fingerprint. The success of such an attack is contingent upon the quality and accuracy of the fabricated fingerprint, which is largely determined by the materials and methods employed for its creation. Historically, a variety of materials have been employed to create fake fingerprints. Latex, for instance, is a flexible material that can be molded easily to replicate the fine ridges and valleys of a fingerprint. Its elasticity allows it to adapt to the pressure applied during the authentication process, making it a popular choice for spoofing attacks [19]. Silicone, known for its durability and malleability, can be used to create highly detailed fingerprint replicas. Its texture closely resembles human skin, making it harder for sensors to distinguish between a real finger and a silicone spoof [10]. Gelatin, often used in theatrical makeup, can be molded to create lifelike fingerprint replicas. Its soft texture and moisture content make it a suitable material for spoofing attacks, especially against sensors that rely on moisture detection [4].

The evolution of fingerprint sensors and their increasing sophistication have necessitated the exploration of new materials and methods. Alginate, a biopolymer derived from seaweed, has emerged as a promising material in this context. Its properties, such

as its texture and elasticity that closely mimic human skin, make it a promising material for fingerprint spoofing [28]. Its ability to capture fine details and its inherent conductivity further enhance its potential as a spoofing material.

In terms of methods, the process of fingerprint spoofing typically involves capturing a latent fingerprint, creating a mold, and then using the chosen material to cast a fake fingerprint. Advanced techniques, such as 3D printing, have been explored to create more accurate and detailed fingerprint replicas [21]. The digital age has further complicated the landscape. Platforms where users often share high-resolution images can inadvertently become sources for biometric data extraction, leading to potential spoofing attacks [15]. It's worth noting that while the materials and methods for fingerprint spoofing have evolved, so have the countermeasures. Modern fingerprint sensors incorporate a range of anti-spoofing techniques, from analyzing the electrical properties of the skin to detecting blood flow and moisture content. However, as spoofing methods become more sophisticated, the challenge lies in staying a step ahead of potential attackers.

While understanding the materials and methods used in fingerprint spoofing is crucial, it's equally important to delve into the specific vulnerabilities of capacitive fingerprint recognition systems. These systems, commonly found in IoT devices, present their own set of challenges and vulnerabilities. Capacitive fingerprint recognition systems operate by gauging the capacitance differences between the ridges and valleys of a fingerprint [17]. The ridges, being proximate to the sensor, exhibit a different capacitance than the valleys, and this differential is employed to generate a unique fingerprint pattern. While these sensors are celebrated for their precision and resilience against external environmental factors, they are not impervious to vulnerabilities.

As mentioned before the primary vulnerability of capacitive fingerprint sensors is their susceptibility to spoofing attacks. These vulnerabilities accentuates the importance of integrating supplementary security measures, such as liveness detection. Liveness detection, which ascertains if the presented fingerprint originates from a living individual, has been proposed as a countermeasure against spoofing attacks. However, advanced spoofing materials and techniques can sometimes elude even these liveness detection mechanisms. As explained before, some materials can mimic the sweat pores and intricate details of a real finger, making it a challenge for liveness detection algorithms to distinguish between genuine and fake fingerprints [11].

Furthermore, the escalating resolution of fingerprint sensors, although enhancing accuracy, can also introduce vulnerabilities. High-resolution sensors can capture intricate details of a fingerprint, but they also become more sensitive to minute variations, which can be exploited by adversaries. For instance, an attacker might craft a spoof with exaggerated minute details, potentially increasing the likelihood of a successful attack [2].

On the other hand, the integration of fingerprint sensors in IoT devices introduces additional challenges. Given the resource constraints of many IoT devices, implementing robust security measures becomes a challenge. Additionally, the diverse range of IoT devices, each with its unique hardware and software configurations, makes standardizing security solutions difficult. This diversity can

lead to inconsistencies in security implementations, providing potential loopholes for attackers [14]. While capacitive fingerprint recognition systems offer a reliable and efficient means of biometric authentication, they come with their set of vulnerabilities. Biometric authentication issues and vulnerabilities will evolve with the IoT, and to secure and maintain biometric systems, researchers and industry professionals must keep current and innovate.

3 METHODOLOGY

The widespread integration of capacitive fingerprint identification technology in IoT devices has presented significant security challenges for the digital forensics sector. The objective of our study is twofold: (1) investigate the potential of Alginate in deceiving fingerprint sensors that are often seen in IoT devices; and, (2) explore the feasibility of extracting reproducible fingerprint data from digital photographs available on the internet. Our research delves into two primary areas: firstly, the effectiveness of Alginate in creating deceptive fingerprint impressions, and secondly, the innovative methodology of processing high-resolution photographs to replicate fingerprint data. This approach involves transforming detailed fingerprint patterns extracted from digital images into three-dimensional models, which then serve as molds for Alginate-based fingerprint replicas. By focusing on these specific areas, our study aims to highlight potential vulnerabilities in biometric authentication systems, particularly in IoT devices.

3.1 Material Selection and Preparation

The success of fingerprint spoofing relies heavily on the quality of the material used. A substance’s ability to mimic the tactile and electrical features of human skin may be a determining factor in its ability to fool fingerprint sensors. Many potential candidates were considered in the process of identifying suitable materials, each with its own set of advantages and disadvantages; however, Alginate stood out as particularly promising.

The unique qualities of Alginate were largely responsible for its selection. When mixed with water, it changes into a gelatinous material, having remarkable similarities to the feel and pliability of human skin. Alginate’s intrinsic conductivity and resistivity qualities are very similar to those of human skin, extending the similarities beyond superficial features. Therefore, Alginate presents itself as an excellent option for our experimental efforts.

In this phase of our set of experiments, we aimed to confirm Alginate’s qualities regarding fingerprint spoofing. To achieve this, we used actual fingerprints collected from our lab members and staff to create castings. To get the desired consistency, Alginate powder was mixed with water at a 1:1.5 ratio according to a formula proposed by its manufacturer. After that the mixture was stirred continuously for three minutes to achieve a homogeneous consistency and to ensure alginate mix is smooth and free of clumps, and after that it was poured into molds to capture the intricate patterns that are signatures of genuine fingerprints. The Alginate cast was carefully removed after it had been prepped for use in testing fingerprint sensors in Internet-of-Things gadgets. Figure 1 shows an example of the Alginate molds and casts used in our study.



Figure 1: Example of fingerprint molds and casts made with Alginate

The use of Alginate was also substantiated due to its extensive accessibility and straightforward application. The substance’s non-toxic properties guarantee safety during manipulation, while its rapid curing time expedites the testing procedure. In addition, the biodegradable properties of Alginate are in line with the increasing focus on sustainable research methodologies.

Our first investigations focused on the use of authentic fingerprint molds, but we acknowledge the broader ramifications and potential risks associated with our study. In the following sections, we will explore the proposed idea of extracting fingerprint patterns from photos, transforming them into molds using 3D printing, and utilizing Alginate for casting. This analysis will emphasize the various vulnerabilities that may arise from this process.

3.2 Fingerprint Extraction and 3D Printing

In the contemporary era of widespread digital dissemination, it is possible for even an informal photograph to disclose biometric information unintentionally. This phenomenon is particularly true for visual representations that depict human hands or fingers since they might be susceptible to exploitation for the purpose of extracting fingerprint patterns. The procedure involved in collecting fingerprints from photographs and subsequently reproducing them through 3D printing is a complex and intricate operation.

The theoretical feasibility of utilizing publicly available images for fingerprint spoofing presents a unique and speculative challenge. One potential scenario involves the use of high-resolution images commonly shared on social media platforms, personal blogs, or public forums. These images, particularly those where individuals’ hands are prominently displayed, might inadvertently reveal fingerprint details. The effectiveness of these images in spoofing attacks hinges on the camera’s resolution and the clarity with which

fingerprints are captured. Modern digital cameras and smartphones often possess the capability to take photographs with sufficient detail to disclose fingerprint patterns potentially.

Another significant consideration is the abundance of high-quality images of public figures or individuals frequently captured by high-definition media. These images, stemming from interviews, events, or photo shoots, could serve as potential sources for detailed fingerprint data due to the professional quality of media coverage. Moreover, in forensic investigations or journalistic contexts, where high-resolution images are analyzed for detailed information, there is a risk of such images becoming public, further exacerbating the potential for unauthorized fingerprint data extraction.

For fingerprint extraction, algorithms are the backbone. The YOLO (You Only Look Once) algorithm, known for its efficiency in object detection, was utilized in an earlier study by [15] to swiftly identify and crop hands and fingers from images on platforms like Etsy. However, the extraction is just the beginning. The quality of the fingerprint image often needs enhancement. Techniques such as histogram equalization and Fourier transform have been proposed to improve the clarity and contrast of these images [13]. Another study highlighted the use of deep learning for fingerprint minutiae extraction, demonstrating the potential of neural networks in this domain [7].

Once the fingerprint images are enhanced, the next step is replication. 3D printing offers a solution. While FDM (Fused Deposition Modeling) printers build objects layer by layer, they might not offer the precision required for fingerprints. DLP (Digital Light Processing) printers, on the other hand, use light to solidify a liquid resin, providing a higher resolution suitable for our needs [20].

With the enhanced fingerprint images and a DLP 3D printer, we proposed creating molds that could emulate the fingerprint patterns. The ultimate goal was to determine if these 3D-printed molds, when used with Alginate, could deceive fingerprint sensors.

3.3 IoT Device Selection

Our investigation was limited to fingerprint-sensing house locks and padlocks, sometimes known as “smart locks” among IoT gadgets and devices. The prevalence of these devices is on the rise, providing homeowners with a combination of convenience and a sense of enhanced protection. The combination of keyless entry, apps, and customizable access restrictions, together with the added security provided by fingerprint verification, has contributed to the widespread adoption of these devices.

However, as with many technological advancements, there’s a spectrum of quality and security. Not all fingerprint-enabled home locks are created equal. Research indicates that the affordability of IoT devices often correlates with their vulnerability to security attacks. This is primarily due to the use of lower-quality fingerprint sensors in less expensive models. For instance, a study by [16] revealed that more economical biometric devices tend to compromise on sensor quality, rendering them more susceptible to spoofing attacks. Additionally, their study highlighted that budget constraints in manufacturing low-end IoT devices often lead to a trade-off where functionality is prioritized over security, thus creating exploitable vulnerabilities.

Given this backdrop, our selection criteria for IoT devices was twofold. First, we aimed to choose devices that are commonly available and widely used by consumers. This ensures that our findings have broad relevance. Second, we sought a mix of devices across different price points, allowing us to understand the impact of our proposed vulnerability better. Our methodology’s objective was to provide a comprehensive understanding of the vulnerabilities present in commonly used IoT home locks. By focusing on these devices, we hoped to shed light on potential security risks that millions of homeowners might unknowingly be exposed to.

3.4 Attack Implementation

In our study, we sought to address the potential vulnerabilities in biometric security, specifically focusing on capacitive fingerprint recognition. Our approach combined both our actual experimental procedures and a proposed attack scenario that could be realized in a broader context.

In our experimental setup, we initially focused on collecting real-life fingerprint samples from our research team and lab members, ensuring a variety of unique fingerprint patterns. Once the molds were set and ready, we poured fresh Alginate into them to create fingerprint replicas. These replicas were then used to attempt unauthorized access on a variety of IoT devices equipped with capacitive fingerprint sensors. Our objective was to assess the success rate of these replicas in deceiving the sensors and granting unauthorized access.

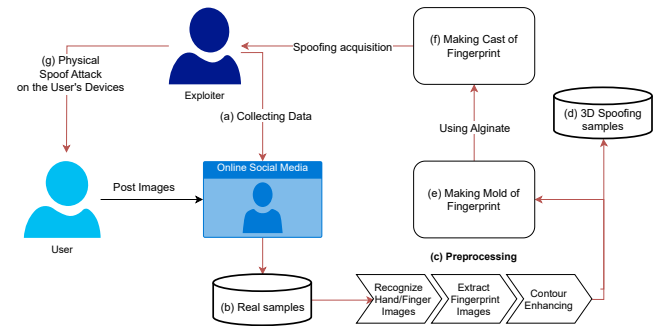


Figure 2: A potential scenario for spoofing attacks.

Parallel to our hands-on experiment, we envisioned a more expansive attack scenario demonstrated in Figure 2 to provide a clearer understanding of our conceptualized approach. In this proposed scenario, adversaries would (a) collect high-resolution fingerprint images from online platforms, where users might inadvertently share their biometric data, and (b) store it. (c) Advanced image processing algorithms would then enhance these images, capturing every minute detail. The enhanced images would be transformed into (d) 3D models, which are stored as ready samples for spoof attacks and would then serve as blueprints for 3D printing. (e) The resultant 3D prints would act as molds for (f) creating fingerprint replicas, potentially using materials like Alginate. Finally, (g) exploiter will use the Alginate cast to conduct a physical spoof attack on the user’s IoT device. This scenario functions as a detailed narrative of the fictitious attack process, providing readers with a

comprehensive overview of the planned techniques and step which biometric security can be compromised in today’s digital age. It is essential to stress that the scenario outlined here is merely a conceptual framework outlining the kinds of threats and attack techniques that an exploiter could use.

Together, our actual experiments and the proposed attack scenario highlight the pressing need for robust biometric security measures, especially as IoT devices become more integrated into our daily lives.

3.5 Adversarial Model

Understanding the potential adversary is paramount, and by modeling the capabilities, intentions, and methods of a potential attacker, we can better anticipate vulnerabilities and design systems to counteract these threats. In the context of our study, the adversarial model focuses on individuals or entities aiming to exploit the vulnerabilities in biometric authentication systems, particularly those using capacitive fingerprint recognition in IoT devices.

The adversary’s operation can be broken down into distinct stages. Initially, they focus on data collection and processing. The adversary scours online platforms, such as social media sites and online marketplaces, to gather high-resolution images that might inadvertently display users’ fingerprints. Once collected, these images undergo enhancement using advanced image processing algorithms, ensuring that even the minutest details of the fingerprint patterns are discernible. The enhanced images are then converted into 3D models.

Following this, the adversary shifts to physical replication and attack. With the 3D models at hand, the adversary employs precision 3D printing techniques, like DLP, to create molds of the fingerprints. Materials like Alginate, which closely mimics the texture and elasticity of human skin, are used to cast replicas from these molds. Armed with these replicas, the adversary attempts to deceive capacitive fingerprint sensors on IoT devices, seeking unauthorized access. It’s crucial to note that while our actual experiments were confined to using real-life fingerprint samples, the adversarial model we propose is broader, encompassing potential real-world scenarios. To validate our conceptual approach, future research should follow a structured methodology. Initially, this would involve the collection and analysis of high-resolution images from online platforms, focusing on those that might inadvertently display users’ fingerprints. Advanced image processing techniques would be employed to enhance these images, ensuring that even the minutest details of the fingerprint patterns are discernible.

For the realization of our study, both in its actual implementation and the proposed concept, a combination of hardware and software tools was envisioned. In the actual experiments we conducted, our toolkit was straightforward yet effective. We utilized Petri dishes and mixing containers, which are essential for preparing and setting the Alginate. These simple tools allowed us to create molds and casts of real-life fingerprints, which were then tested on a specific fingerprint door lock available to our team.

In the broader concept we’re proposing, a more extensive array of tools would be required. High-resolution images, whether from cameras, either professional-grade or advanced smartphone variants, or from images shared over platforms, would be pivotal for

capturing detailed images of fingerprints from various surfaces and lighting. Transitioning from 2D to 3D, a Digital Light Processing (DLP) 3D printer would be recommended. Recognized for their precision, DLP printers can produce detailed prints, capturing the intricacies of fingerprints. Alginate, with its skin-like properties, is suggested as the primary casting material.

On the software spectrum, libraries like OpenCV would be essential for image processing, ensuring the fingerprint patterns retain their clarity and detail. After processing, 3D modeling tools such as Blender or Tinkercad would extrude these enhanced 2D images into 3D models. The YOLO system, known for its real-time object detection capabilities, would be instrumental in swiftly identifying hand and finger images from extensive datasets. Depending on the 3D printer in use, specialized software like Cura or PrusaSlicer might be needed to translate the 3D models into print-ready G-code formats.

Together, these tools, both from our actual experiments and the proposed concept, provide a comprehensive framework. This combination ensures a rigorous examination of biometric security measures under potential real-world attack scenarios. The outcomes of this line of research would have significant implications for both biometric security and the field of digital forensics. By understanding the vulnerabilities in current fingerprint recognition technologies and assessing the potential of new spoofing methods, we can pave the way for enhancing the security and reliability of biometric systems.

3.6 Experiment Setup

We carefully planned our experiment to ensure the accuracy, repeatability, and validity of the results. To simulate real-life situations where an exploiter might attempt unauthorized access using spoofed fingerprints, we conducted our experiments in a controlled laboratory environment. Particular attention was given to maintaining consistent temperature (Exactly 66°F) and humidity levels (Exactly 68% relative humidity (RH)), as these factors significantly influence the setting time and consistency of Alginate.

For the actual experiments, we diverged from traditional fingerprint collection methods. Instead, we directly created molds from the fingers of three willing participants within our research team and lab members. This approach was chosen to ensure a direct and accurate impression of the fingerprints. Participants dipped their right thumb fingers into a specially prepared Alginate mixture, carefully formulated to ensure uniform texture and consistency. The meticulous submersion process for each participant’s finger aimed to capture detailed imprints and avoid any distortions or air bubbles.

Quality control was paramount throughout the process. We established strict protocols for regularly checking and adjusting the Alginate mixture to maintain its optimal ratio and consistency. Each mold was thoroughly inspected for accuracy and completeness before being used to create Alginate casts. Using these direct molds, we then prepared Alginate casts to serve as the spoofed fingerprints. The casts were tested on three different IoT smart door locks equipped with capacitive fingerprint sensors, chosen for their widespread use in modern homes and offices. The selection of devices represented a range of price points and were popular

Table 2: Summary of Spoofing Attempts with Alginate

Device Type	Device Price	Average Success Rate	Average Attempts of First successful outcome	Average global rating to number of reviews
IoT Smart Entry Door Lock 1	\$140	3/20	7/20	0.0057
IoT Smart Entry Door Lock 2	\$250	20/20	1/20	0.0657
IoT Smart Entry Door Lock 3	\$90	0/20	N/A	0.0005

consumer and marketplace choices, each manufactured within the past three years.

During the testing phase, each attempt to unlock the devices using the Alginate casts was meticulously recorded. In total, 180 separate tests were performed (20 attempts per device, across 3 devices, with 3 participants), providing a robust dataset for analysis. We noted the number of attempts made, the time taken for each attempt, and the outcomes (success or failure) of each trial. This data was then used to assess the success rate of the Alginate casts in spoofing the fingerprint sensors.

While valuable insights were gained into the efficacy of Alginate for spoofing attacks, our study did not directly compare the performance of these Alginate casts, other spoofing materials, and the actual subjects’ fingerprints on the IoT devices. Such a comparison could have provided additional insights into the relative effectiveness of Alginate in mimicking actual fingerprints under practical conditions. For that, we will address our roadmap for future research later in the paper to benefit from incorporating this comparative analysis, offering a more holistic understanding of Alginate’s potential to circumvent biometric security measures.

4 RESULTS

As previously discussed, our primary objective was to assess the efficacy of Alginate as a spoofing material for capacitive fingerprint sensors commonly found in IoT devices. Our experiments using Alginate casts to spoof fingerprint sensors were successful on various Home Lock IoT devices and have yielded noteworthy findings. The results indicated in the Table 2 show Fascinating observations.

IoT Smart Entry Door Lock 1, situated at a mid-range price point, demonstrated a moderate vulnerability to Alginate-based spoofing with a success rate of 15%. The variability in success rates across different fingerprint molds suggests that the effectiveness of the spoofing technique might be influenced by the quality of the molds or the inherent characteristics of the device’s sensor.

Surprisingly, IoT Smart Entry Door Lock 2, despite being a higher-priced model, exhibited the highest vulnerability with a 100% success rate in spoofing attacks. This was evident from the fact that, on average, it took fewer attempts to achieve the first successful spoof. While it’s tempting to correlate higher prices with better security, our findings challenge this notion.

The IoT Smart Entry Door Lock 3, the most affordable device tested, resisted all spoofing attempts, further emphasizing that price does not solely dictate the robustness of biometric security.

Furthermore, we determined two other variables to understand the penetrability and trustability of these IoT smart lock devices. The “Average Attempts of First successful outcome” metric is particularly interesting. A lower number in this metric indicates higher vulnerability, as it means fewer attempts were needed to deceive

the sensor. Conversely, a higher number suggests better resilience against spoofing. This metric underscores the importance of rigorous testing and validation to ensure the security and reliability of biometric systems as they become more prevalent in everyday devices.

Our study’s success in spoofing various home lock IoT devices using Alginate casts has crucial implications for biometric security. The ability of Alginate, a natural and easily moldable material, to replicate fingerprints and deceive sensors underscores a significant vulnerability in widely-used biometric systems. This finding suggests that even basic materials can pose a threat to sophisticated security measures.

Furthermore, our experiments contribute to a broader understanding of biometric security’s current limitations and call for continuous innovation in biometric technology, especially in developing anti-spoofing measures. The need for more robust authentication methods is highlighted by the effectiveness of Alginate in spoofing fingerprint sensors.

Additionally, the implications of our study extend into the domain of digital forensics. The ability to create fingerprint replicas challenges traditional forensic methods that rely heavily on fingerprint evidence. This necessitates new forensic techniques to differentiate between authentic and fabricated biometric data, ensuring the integrity of forensic investigations in an era where digital and biometric spoofing is increasingly plausible.

Our preliminary findings validate the hypothesis that Alginate can serve as an effective material for spoofing fingerprint sensors. The results not only underscore the potential vulnerabilities in current biometric security systems but also pave the way for a deeper exploration into the domain of digital forensics. The proposed concept of a novel attack vector targeting Smart Lock devices equipped with fingerprint sensors emphasizes the pressing need for robust countermeasures.

5 DISCUSSIONS

The results of our study highlights the potential vulnerabilities inherent in capacitive fingerprint sensors, especially when confronted with sophisticated spoofing techniques using materials like Alginate. Our findings not only highlight the efficacy of Alginate as a spoofing material but also raise pertinent questions about the broader implications for IoT security.

One of the primary takeaways from our research is the realization that even as technology advances, the fundamental challenges associated with biometric authentication remain. While fingerprint sensors have become more sophisticated over the years, they are not infallible. The fact that a natural material like Alginate, which is readily available and easy to work with, can deceive these sensors

is a testament to the persistent challenges in the realm of biometric security.

In the age of social media, where influencers frequently share personal moments online, a potential risk emerges with the advanced biometric security breach method using Alginate-based fingerprint replicas. Envision a scenario where a malicious actor, through meticulous analysis of an influencer’s Instagram feed, discovers their residence and gathers high-resolution images showcasing their fingerprints. Utilizing these images, the adversary employs 3D printing technology to create precise fingerprint replicas from Alginate. This technique could allow unauthorized access to the influencer’s home, exploiting biometric security measures to protect their privacy and safety. Implementing stricter privacy settings and advocating for social media platforms to develop algorithms that alert users to potential biometric data exposures can significantly mitigate risks. This speculative situation underscores the urgent need for reinforced security protocols in an increasingly interconnected and publicly exposed society.

The connection of our research to digital forensics and incident response is significant. Our findings necessitate a reconsideration of digital forensic practices, particularly in scenarios where spoofed fingerprints could be used to gain unauthorized access to devices containing critical evidence. The need for advanced detection techniques and new forensic methodologies to distinguish genuine from fabricated fingerprints is more crucial than ever. This research not only demonstrates a security vulnerability but also calls for collaborative efforts between cybersecurity and digital forensics communities to devise effective strategies for preventing, detecting, and responding to advanced spoofing attacks.

Our investigation into IoT device biometric security reveals a complex landscape where device price does not directly correlate with security efficacy. Intriguingly, the most budget-friendly device tested, the IoT Smart Entry Door Lock 3, was impervious to all spoofing attempts, challenging the assumption that higher cost ensures better protection. This finding underscores the importance of implementing the underlying technology and security features over price. Policymakers and regulatory bodies must conduct comprehensive evaluations of these devices and sensors, establishing institutions dedicated to testing and disseminating reliability scores for each sensor prior to getting released to the market and industry. Establishing a comprehensive framework for regular, updated assessments of security measures, facilitated by a coalition of manufacturers, cybersecurity experts, and policymakers, can ensure that security standards evolve alongside technological advancements. This public-private partnership model would encourage sharing best practices and contribute to developing universally robust biometric security protocols, reinforcing the importance of technology and implementation over price. Additionally, our analysis highlighted a nuanced relationship between device price, the average attempts required for a successful spoofing outcome, and the devices’ global ratings concerning the number of reviews. These correlations that relate to the vulnerability and trustability of these capacitive sensors further emphasize the need for a detailed examination of biometric security measures, advocating for a shift in focus towards the efficacy of security implementations rather than mere cost. Future research should include a detailed comparative analysis to benchmark Alginate against other materials, providing a

more comprehensive understanding of its effectiveness in biometric security contexts.

Our research is meant to prompt a rethinking of how biometric security is implemented in IoT security devices while introducing a threat concept that we set to explore more around it in the future. As we progress toward a more interdependent global community, the stakes have never been higher. It’s crucial that we keep ahead of would-be exploiters by constantly developing and improving our security protocols, especially with the emerging and rapid growth of artificial intelligence tools and image enhancement algorithms. Our findings point to potential weak spots, suggest new potential dangers, and pave the way for improved defenses on the road.

6 CHALLENGES AND LIMITATIONS

While our research provides significant insights into the use of Alginate for fingerprint spoofing, it is not without limitations. Achieving a consistent mixture of Alginate was pivotal for the reliability of our tests. Even slight variations in the consistency could affect the sensor’s ability to read the spoofed fingerprint accurately. Ensuring this uniformity in the Alginate mixture for every cast posed a significant challenge.

Another factor that introduced variability was the fingerprint sensors themselves. Different IoT devices, sometimes even those produced by the same manufacturer, might have sensors with distinct sensitivities and recognition algorithms. This inherent variability could lead to inconsistent results when testing across multiple devices. We focused our study on capacitive fingerprint sensors because our initial tests with optical and ultrasonic sensors, including those on mobile phones and laptops, showed a high failure rate. In contrast, a significant number of IoT devices with capacitive sensors were successfully spoofed. This focus allows us to address vulnerabilities that have a broader impact on everyday users.

While our research provides useful information about the security of fingerprint sensors in IoT devices, readers should proceed with care. While the IoT Lock Device 2 we utilized in our experiments did not display any glaring flaws, we cannot rule out the possibility of device-specific vulnerabilities. To get a full picture of the device’s security, it would be helpful to do research on numerous devices of the same model to find whether it was this specific device that was weak towards our spoofing attack or if it is the same with all devices by this specific manufacturer.

In addition, the sample size of our study was small. This study only looked at the possibility of employing Alginate as a spoofing material; future research on the threat we proposed would explore a wider range of devices and materials to strengthen our findings and establish more certain conclusions. As a result, not only would our current findings be confirmed, but perhaps more nuances relating to biometric security in IoT devices would be uncovered as well.

Our controlled lab environment, while meticulously set up, might not mirror all real-world conditions. External factors such as ambient temperature, humidity, and the natural wear-and-tear of the sensor can influence the success rate of a spoofing attack. Additionally, the study did not include a direct comparison with other spoofing materials. These limitations highlight the need for future research with larger sample sizes, more diverse devices, and comparative analyses to validate and expand upon our findings.

For the proposed concept attack, the quality of the sourced fingerprint images is of utmost importance. Low-resolution images or those with obscured fingerprints can diminish the accuracy of the 3D-printed molds, thereby affecting the overall success rate of the attack.

Finally, while 3D printing is advanced, it has its own set of limits. The precision required to capture the minute minutiae of a fingerprint pattern is immense, and even little differences in printer accuracy or the printing material (e.g. resin or filaments) might result in recognition failures.

7 CONCLUSIONS AND FUTURE WORK

The use of capacitive fingerprint recognition technology within the rapidly expanding domain of IoT devices has introduced a range of advantages and complexities. Although the authentication procedures mentioned above provide convenient access, our research has revealed their vulnerability to sophisticated spoofing techniques, specifically through the use of Alginate. The potential of Alginate to circumvent the biometric security of IoT devices is underscored by its deceiving qualities, as well as its inherent features that closely resemble the conductivity and resistance of human skin.

Our proof-of-concept, which involved crafting molds directly from genuine fingerprints and subsequently replicating them using Alginate, showcased the material's remarkable ability to mimic real fingerprints both visually and tactically. This study raises concerns about potential breaches of individual privacy, especially in light of the novel image identification algorithms and attack scenarios we provided. The concept of extracting fingerprint images from publicly available sources, enhancing them, and then creating 3D models for spoofing purposes remains a significant area of concern and future exploration.

While our experiments provide foundational insights, they do not encompass the full scope of the proposed novel vulnerability involving public image sources. The exploration of these scenarios underscores the necessity for increased awareness and the development of preventive measures. This includes educating the public about the risks associated with sharing high-resolution images and urging social media platforms to implement technologies that obscure fingerprint details. Additionally, it highlights the imperative for more advanced anti-spoofing technologies in biometric systems to counteract these potential threats. This speculative examination provides a foundation for future research, emphasizing the need for ongoing innovation in the field of biometric security and digital forensics to safeguard against the evolving methods of biometric data exploitation. Further research is required to explore this aspect comprehensively.

Our future research efforts will focus on these aspects, aiming to validate the theoretical model we have proposed. By addressing these challenges, we intend to provide a more comprehensive understanding of the risks associated with fingerprint data exploitation, particularly in the context of IoT device security. This exploration will not only contribute to the technological understanding of biometric spoofing but also emphasize the critical need for enhanced security measures in the rapidly evolving digital landscape. As we look to the future, the structured hypotheses we formulated—both

device-specific and material-specific will serve as foundational pillars for subsequent investigations. These hypotheses not only encapsulate our current understanding but also set the stage for a series of controlled experiments. Specifically, we aim to rigorously evaluate the interplay between different materials and device models in the context of spoofing attacks, with a keen focus on validating or refuting our initial postulations about Alginate's efficacy and the vulnerabilities of specific IoT devices.

Our research makes it evident that the digital forensics community needs to step up its efforts to develop effective anti-spoofing solutions. As IoT Smart locks become more commonplace, protecting our private information becomes more than simply a technological difficulty; it's a social necessity. Our findings reveal new information and sound the alarm for increased attention and new approaches to security as the IoT infrastructure continues to develop at an exponential rate.

ACKNOWLEDGMENTS

The authors would like to thank Bradley Boswell, Rajon Bardhan and Seth Barrett, Ph.D. Students in the School of Computer & Cyber Sciences, Augusta University, for assisting in conducting the experiments. The authors would like to acknowledge the National Science Foundation (NSF) (Award number: 2131509) for supporting this project.

REFERENCES

- [1] Asma.Aounallah, Hakim.Bendjenna, and Abdallah.Meraoumia. 2022. Privacy Preservation of Biometrics Used for IoT Systems Security: Brief Review. (2022).
- [2] Denis Baldisserra, Annalisa Franco, Dario Maio, and Davide Maltoni. 2005. Fake fingerprint detection by odor analysis. (2005), 265–272.
- [3] Edwin Bowden-Peters, Raphael C W Phan, John N Whitley, and David J Parish. 2012. Fooling a liveness-detecting capacitive fingerprint scanner. *Cryptography and Security: From Theory to Applications: Essays Dedicated to Jean-Jacques Quisquater on the Occasion of His 65th Birthday* (2012), 484–490.
- [4] Raffaele Cappelli, Dario Maio, and Davide Maltoni. 2007. Fake finger detection by skin distortion analysis. *IEEE Transactions on Information Forensics and Security* 1, 3 (2007), 360–373. <https://doi.org/10.1109/TIFS.2006.884585>
- [5] Aida Cavallo, T. Al Kayal, A. Mero, A. Mezzetta, A. Pisani, I. Foffa, C. Vecoli, M. Buscemi, L. Guazzelli, and G. Soldani. 2023. Marine Collagen-Based Bioink for 3D Bioprinting of a Bilayered Skin Model. *Pharmaceutics* (2023). <https://doi.org/10.3390/pharmaceutics15051331>
- [6] Ann Cavoukian and Alex Stoianov. 2012. Biometric encryption: A positive-sum technology that achieves strong authentication, security AND privacy. *Commissioner, Ontario* (2012).
- [7] Luke Nicholas Darlow and Benjamin Rosman. 2017. Fingerprint minutiae extraction using deep learning. (2017), 22–30.
- [8] Shahriar Ebrahimi and S. Bayat-Sarmadi. 2021. Lightweight Fuzzy Extractor Based on LPN for Device and Biometric Authentication in IoT. *IEEE Internet of Things Journal* (2021). <https://doi.org/10.1109/JIOT.2021.3050555>
- [9] Uwe Engelmann, Matthias Quasthoff, Marco Lünich, and Martin Döring. 2018. Media forensics and deep learning: An overview. In *2018 IEEE International Workshop on Information Forensics and Security (WIFS)*. IEEE, 1–7.
- [10] Javier Galbally, Julian Fierrez, and Javier Ortega-Garcia. 2010. Evaluation of direct attacks to fingerprint verification systems. *Telecommunication Systems* 47, 3-4 (2010), 243–254. <https://doi.org/10.1007/s11235-010-9294-4>
- [11] Luca Ghiani, Abdenour Hadid, Gian Luca Marcialis, and Fabio Roli. 2013. Fingerprint Liveness Detection using Binarized Statistical Image Features. (2013).
- [12] Muhammed Golec, Sukhpal Singh Gill, Rami Bakhoun, and Omer Rana. 2020. BioSec: A biometric authentication framework for secure and private communication among edge devices in IoT and industry 4.0. *IEEE Consumer Electronics Magazine* 11, 2 (2020), 51–56.
- [13] Rafael C Gonzalez. 2009. *Digital image processing*. Pearson education india.
- [14] M. S. Hossain, M. Ghulam, S. Rahman, W. Abdul, A. Alelaiwi, and A. Alamri. 2016. Toward end-to-end biometrics-based security for IoT infrastructure. *IEEE Wireless Communications* 23 (2016), 44–51. <https://doi.org/10.1109/MWC.2016.7721741>
- [15] Mohsen Jozani, Gianluca Zanella, Maxium Khanov, Gokila Dorai, and Esra Akbas. 2022. The Need for Biometric Anti-spoofing Policies: The Case of Etsy. In *International Conference on Digital Forensics and Cyber Crime*. Springer, 295–306.

- [16] Santosh Kumar, Mohd Dilshad Ansari, Midde Venkateswarlu Naik, Vijender Kumar Solanki, and Vinit Kumar Gunjan. 2020. A comparative case study on machine learning based multi-biometric systems. *Advances in Cybernetics, Cognition, and Machine Learning for Communication Technologies* (2020), 353–365.
- [17] Hoyeon Lee, Seongyeol Kim, and Taekyoung Kwon. 2017. Here Is Your Fingerprint!: Actual Risk versus User Perception of Latent Fingerprints and Smudges Remaining on Smartphones. In *Proceedings of the 33rd Annual Computer Security Applications Conference*. <https://doi.org/10.1145/3134600.3134643>
- [18] C. Busch M. Gomez-Barrero, Jascha Kolberg. 2018. Towards Fingerprint Presentation Attack Detection Based on Short Wave Infrared Imaging and Spectral Signatures. (2018).
- [19] Tsutomu Matsumoto, Hiroyuki Matsumoto, Koji Yamada, and Satoshi Hoshino. 2002. Impact of artificial gummy fingers on fingerprint systems. In *Proceedings of SPIE Vol.*, Vol. 4677. International Society for Optics and Photonics, 275–289. <https://doi.org/10.1117/12.462666>
- [20] Bernhard Mueller. 2012. *Additive manufacturing technologies–Rapid prototyping to direct digital manufacturing*. Vol. 32. Emerald Group Publishing Limited.
- [21] Thomas Neubauer and Johannes Kolb. 2016. A survey on biometric sensorial spoofing. *Journal of Computer Security* 24, 2 (2016), 143–157. <https://doi.org/10.3233/JCS-150543>
- [22] Vaishali Patel and Devesh C Jinwala. 2015. Secure and efficient fingerprint verification based on image processing and cryptographic techniques. *Procedia Computer Science* 45 (2015), 554–561.
- [23] Nalini K Ratha, Jonathan H Connell, and Ruud M Bolle. 2001. Enhancing security and privacy in biometrics-based authentication systems. *IBM systems Journal* 40, 3 (2001), 614–634.
- [24] Arun Ross and Anil Jain. 2003. Information fusion in biometrics. *Pattern recognition letters* 24, 13 (2003), 2115–2125.
- [25] Arun A Ross, Karthik Nandakumar, and Anil K Jain. 2016. *Handbook of Biometrics*. Springer.
- [26] A. Roy, N. Memon, and A. Ross. 2017. MasterPrint: Exploring the Vulnerability of Partial Fingerprint-Based Authentication Systems. *IEEE Transactions on Information Forensics and Security* 12 (2017), 2013–2025. <https://doi.org/10.1109/TIFS.2017.2691658>
- [27] E. Sujatha and A. Chilambuchelvan. 2018. Multimodal Biometric Authentication Algorithm Using Iris, Palm Print, Face and Signature with Encoded DWT. *Wireless Personal Communications* (2018). <https://doi.org/10.1007/s11277-017-5034-1>
- [28] Jie Xu, Shuangshuang Zheng, Xueyan Hu, Liying Li, Wenfang Li, Roxanne J Parungao, Yiwei Wang, Yi Nie, Tianqing Liu, and Kedong Song. 2020. Advances in the Research of Bioinks Based on Natural Collagen, Polysaccharide and Their Derivatives for Skin 3D Bioprinting. *Polymers* (2020). <https://doi.org/10.3390/polym12061237>
- [29] Tanja Zidarič, Marko Milojević, L. Gradišnik, Karin Stana Kleinschek, U. Maver, and T. Maver. 2020. Polysaccharide-Based Bioink Formulation for 3D Bioprinting of an In Vitro Model of the Human Dermis. *Nanomaterials* (2020). <https://doi.org/10.3390/nano10040733>