applied sciences

MDPI

Article

A Behavioral-Based Fingerprint Liveness and Willingness Detection System

Abdulaziz Almehmadi

Department of IT, Faculty of Computing and IT, SNCS Research Center, University of Tabuk, Tabuk 47512, Saudi Arabia; aalmehmadi@ut.edu.sa

Abstract: Fingerprints have been used for decades to verify the identity of an individual for various security reasons. Attackers have developed many approaches to deceive a fingerprint verification system, ranging from the sensor level, where gummy fingers are created, to gaining access to the decision-maker level, where the decision is made based on low matching criteria. Even though fingerprint sensor-level countermeasures have developed advanced metrics to detect any attempt to dupe the system, attackers still manage to outwit a fingerprint verification system. In this paper, we present the Micro-behavioral Fingerprint Analysis System (MFAS), a system that records the micro-behavior of the user's fingertips over time as they are placing their fingerprint on the sensor. The system captures the stream of ridges as they are formed while placed on a sensor to combat the attacks that deceive the sensor. An experiment on 24 people was conducted, wherein the fingerprints and the behavior of the fingertip as it is placed were collected. Subsequently, a gummy finger was created to try to fool the system. Further, a legitimate user was chosen to participate in an experiment that mimicked an attempt to use their fingertip unwillingly to detect coerced fingerprint placement. After applying the micro-behavior, the system reported 100% true positives and 0% false-negatives when providing legitimate vs. gummy-based fingerprints to authenticate a malicious user. The system also reported a 100% accuracy in differentiating between a voluntary and a coerced fingerprint placement. The results improve the fingerprint robustness against attacks on a fingerprint sensor by factoring in micro-behavior, thus helping to overcome fake and coerced fingerprint attacks.

Keywords: fingerprint verification; micro-behavioral; system design; fingerprint sensor; coercion detection; behavioral biometrics

Citation: Almehmadi, A. A Behavioral-Based Fingerprint Liveness and Willingness Detection System. *Appl. Sci.* **2022**, *12*, 11460. https://doi.org/10.3390/app122211460

Academic Editors: Juan A. Gómez-Pulido and Javier Hernando

Received: 17 September 2022
Accepted: 9 November 2022
Published: 11 November 2022

1. Introduction

Authenticating identity is a major step in most security systems because access levels and privileges are based on that identity. As authentication measures, including knowledge-based, possession-based, and biometric-based systems, are advancing to offer more robust, accurate, and user-friendly capabilities, attacks on authentication systems have been advancing as well, resulting in the development of the ability to trick an authentication system so that an imposter gains access to resources as a legitimate user. As a result, research has advanced to mitigate such threats and vulnerabilities that an authentication system may experience. Some measures are policy-based, and others are technical. Among all of the authentication systems, biometrics has shown an advantage over other authentication systems, including knowledge- or possession-based systems. For example, biometric-based technologies cannot be forgotten or lost, as opposed to other authentication-based systems. Further, biometric-based systems reveal the identity of a user overtly or covertly, making identity authentication an automated process. Further, biometric systems show a greater robustness against attacks when compared to knowledge- or possession-based systems. Biometric-based technologies include physiological-based measures such as the fingerprint, iris, retina, and face recognition, as well as behavior-based measures such as the signature and gait.

Since fingerprint technology is the most used and accepted among users, as opposed to iris- or retina-based technologies, and is more accurate when compared with behavior-based biometric systems [1], it has been adopted by the latest smartphones to authenticate a user and provide them access. This has resulted in attacks focusing on fooling fingerprint-based biometric systems and mainly circumventing the fingerprint sensor.

Fingerprint technologies inherit the general known vulnerabilities to attacks on any biometric system, as shown in Figure 1. The first vulnerability is attacking and fooling the sensor, where an attacker provides a fake fingerprint. Numerous approaches tackle fake fingerprint attacks using liveness detection, where a system determines if a provided fingerprint is alive or fake. Some examples of fingerprint liveness detection include pulse rate, pore changes over time, and oxygen-level detection. Further, the sensor level attacks include forcing and coercing a user to place their fingerprint to authenticate and gain access. A few solutions were proposed, such as using a specific finger to authenticate, which provides limited access or access to a fake interface while reporting the incident. The second inherited vulnerability in biometric systems is attacking the channel between the sensor and the feature extractor, where an attacker records the signals that are sent from the sensor and then replays the signals to fool the biometric system. A few solutions were provided such as implementing a challenge-response metric where a sensor sends a unique seed number each time it is used, and a feature extractor validates the seed number before accepting and analyzing the signal that is sent to the feature extractor. The third vulnerability is attacking the feature extractor component with an override attack, where a feature extractor does not extract any features but limited ones from the fingerprint where any fingerprint may match a stored template. The fourth vulnerability is attacking the channel between the feature extractor and the matcher, where a synthesized feature vector is embedded into the channel, and the matcher will always report a high matching score for the attacker to gain access. The fifth vulnerability is in attacking the channel between the feature extractor and the template database with a channel interception, where a template is modified or altered prior to storage. The sixth vulnerability is in attacking the template database itself by replacing templates with the attacker's template. The seventh vulnerability is in attacking the matcher, where a matcher always returns a high matching score despite the true matching score. Finally, the eighth vulnerability is in overriding the final decision, where a decision is always to allow access despite any of the previous steps in a biometric system. A typical solution to attacks 3–8 is applying the challenge-response method to ensure that the data being received are from a trusted unaltered component of the biometric system. All oval shapes in Figure 1 represent the possible attack, and all rectangular shapes represent a typical biometric component to authenticate a user.

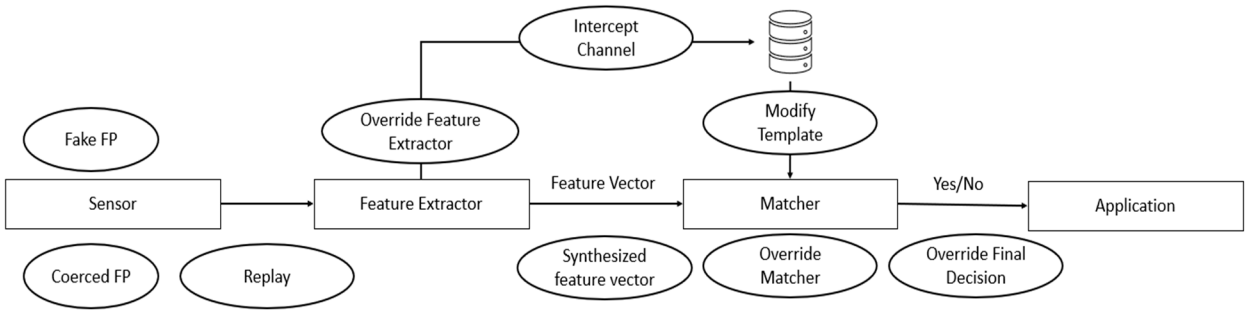

Figure 1. Biometric-based system attacks.

All inherited vulnerabilities create the potential for successful attacks on any fingerprint-based biometric system to fool the authentication system and provide an impostor access. Since most of the attacks (2–7), except for the sensor-level attacks, are similar to those used against any biometric system and can include solutions such as encryption, the cancellation of biometrics [1], and challenge-response mechanisms [2], we find that the research community has carried out substantial work to strengthen this form of security control.

However, the sensor-level attacks on fingerprint technologies weaken the technology and require further advancements.

Two of the most successful attacks on the sensor level are fake fingerprints, where a fingerprint is fake in its origin, e.g., a gummy finger, a reconstruction of a fingerprint from a stored template [3], and coerced fingerprints, where a legitimate user's willingness to provide a fingerprint is not detected and where a user is forced to provide the fingerprint. Although there is no willingness detection component in fingerprint-based biometric systems, there are Liveliness Detection (LD) measures that have been proposed to combat the threat and to ensure that the fingerprint comes from the real user and not from a reconstructed latent impression left on the sensor. Various techniques for liveness detection (LD) have been proposed; some are physiological, detecting the heartbeat or oxygen level from the finger, and others are image-based analyses detecting the changes in pores over time [4–7].

Even though the current literature shows a great capability of detecting a fake fingerprint, attackers can still develop ways to deceive the liveness detection components. Simulating a heartbeat and including changes in pores have become easily executed processes that have shown success in fooling the fingerprint-based biometric systems at the sensor level. However, none of the previous approaches took into consideration the micro-behavioral aspects of the fingerprint impression while it is being placed on the sensor over time. None of the previous work evaluated the possibility of evaluating the fingerprint impression shape construction over time as a behavioral measurement to detect a fake fingerprint, where a micro-behavior is an involuntary movement measured in micro-seconds.

In this paper, we propose a behavioral measurement of a fingerprint while it is placed on the sensor to improve the liveness detection component and propose a willingness detection component with the behavioral measurement. An attacker may simulate a heartbeat but will not be able to provide the genuine behavior of the user's finger when placed on the sensor to verify the fingerprint. Additionally, the behavior of a user, willing or forced, is expected to differ when analyzing the behavior to detect willingness. Not only do the characteristics of the fingerprint matter, but the behavior of the user's finger while leaving the print and while being placed on the sensor also matter. The proposed components take into account the spread of the fingerprint, the formation of the ridges and valleys, as well as the duration and angle.

1.1. Contributions

The main contributions of this article are:

1. a novel micro-behavioral-based measurement component in fingerprint-based biometric systems to improve their resistance to sensor-level fingerprint attacks such as constructed and coerced fingerprints.
2. a behavior-based fingerprint liveness detection.
3. a behavior-based fingerprint willingness detection.
4. a classification model that determines if a fingerprint is legitimate.
5. a classification model that determines the willingness level of a user.
6. a placement of the proposed components in fingerprint-based biometric systems.
7. evaluating the potential of the proposed micro-behavioral component in detecting attacks on sensor-level fingerprint systems.

1.2. Scope

The scope of this paper covers providing fingerprint-based biometric systems with two micro-behavioral components that enhance the results of the liveness detection and detect if a user is willing to provide the fingerprint to ensure that the provided fingerprint does not just match in terms of shape with the stored template but also passes the behavioral characteristics of the temporal micro-behavioral measurement while placing the fingerprint on the sensor surface.

The remainder of this paper is organized as follows: the literature review is provided in Section 2. In Section 3, the hypotheses and objectives are proposed. In Section 4, the system design is proposed and detailed. In Section 5, the methodology, experiment design, and data analysis are given. In Section 6, the results are provided. In Section 7, the results are discussed, and the limitations are given. Finally, the conclusion and future work are provided in Section 8.

2. Literature Review

Fingerprint-based authentication systems are robust against various biometric-based attacks due to the various features that can be detected in a single fingerprint, as well as the research conducted to strengthen biometric technologies. Fingerprints, in particular, have seen worldwide acceptance due to the advancements in technology that make them one of the best choices for human authentication. Currently, smartphones include fingerprint technology to unlock the smartphone, because biometric-based technology does not require information to be remembered or even typed. The broad adoption of the technology has made it subject to numerous attacks intending to gain access to the sensitive information stored on smartphones and to impersonate an individual by fooling the biometric system. Fingerprint-based technologies cannot be forgotten or lost, as contrasted with other authentication systems, but introduce a new realm of vulnerabilities that need to be addressed. Fingerprint technologies have shown a great deal of strength against various attacks, but according to [8–10], they can still be deceived at the sensor level, where an attacker presents a sample that might be fake or forces a user to provide their biometric trait. Various approaches have been proposed to combat the two sensor-level attacks, fake samples and coercion, as detailed in the next two subsections.

2.1. Liveness Detection as Sensor-Level Attack Mitigation in Fingerprint-Based Systems

Liveness Detection (LD) technologies have been proposed to combat the use of fake or decapitated fingerprints to ensure that the presented fingerprint is alive and authentic. The authors in [11] used digitized statistical image features with sampling from Gaussian distribution to detect fake fingerprints as a method for liveness detection. They concluded that the points from the center of the fingerprint present more information to help detect a fake fingerprint than the pixels from the edge. As a result, they were able to improve the traditional digitized statistical image feature from 85% to 91% accuracy.

The authors in [12] used joint time frequency analysis to detect a fake fingerprint. They tested a profiling approach that reached 90% accuracy, a wavelet-based approach using a Daubechies wave that reached 81% accuracy, and a cascaded system reaching 100% accuracy in differentiating between a live fingerprint and a silicon one.

Other researchers used convolutional neural networks (CNN) to detect fake fingerprints. In [13], the authors used CNN to evaluate the LivDet 2019 database, which is a liveness detection competition that includes 2000 live and fake fingerprints, reaching 95% accuracy. The authors in [14] also used CNN with an enhancement, reaching 98% in terms of accuracy in differentiating between fake and real fingerprints. Further, the authors in [15] used Slim-ResCNN applied to the LivDet 2017 database and reached 95.25%.

An evaluation of liveness detection-based software was carried out by [16] using CNN and local binary patterns, reaching 95.2% accuracy. Moreover, a density-connected CNN was used and optimized using a genetic algorithm to achieve a liveness detection rate reaching a 98.22% accuracy [17]. The authors in [18] also used CNN on the LivDet 2015 database and reached 95.5% accuracy based on 50,000 fake and real fingerprints. Finally, the authors in [19] used a template-probe CNN on the LivDet 2015 database, reaching 97.24% accuracy in differentiating between real and fake fingerprints.

Various other approaches have been proposed to detect liveness in a fingerprint, including using a score-level fusion [20], reaching 96.88% accuracy, using automatic template updating using the fusion of ECG and Fingerprint [21], reaching 97.4% accuracy, using

a two-layer parallel SVM network based on aggregated local descriptors [22], reaching 95.32% accuracy, and using SVM [23], reaching 100% accuracy.

Table 1 summarizes the methods described in the literature and the accuracy reached in differentiating between fake and real fingerprints.

Table 1. Summary of methods described in the literature and the accuracy achieved for Liveness Detection.

Method	Accuracy	Ref.
Binarized statistical image feature with sampling from Gaussian distribution	91%	[11]
Joint time frequency analysis	100%	[12]
CNN	95%	[13]
CNN-Enhanced	98%	[14]
Slim-ResCNN	95.25%	[15]
CNN	95.2%	[16]
Density-connected CNN	98.22%	[17]
CNN	95.5%	[18]
Template-probe CNN	97.24%	[19]
Score-level fusion	96.88%	[20]
ECG Fusion	97.4%	[21]
2-Layer Parallel SVM	95.32%	[22]
SVM	100%	[23]

The literature documents a high accuracy in differentiating between fake and real fingerprints using various approaches. However, none of the previous approaches examined the analysis of the micro-behavior during fingerprint placement to detect if a fingerprint is fake or real.

2.2. Approaches for Fingerprint-Based Coerced User Attacks Detection on the Sensor Level

Although biometric systems provide convenience and a high level of security, and because the presentation of the biometric features is not always subject to a user's acceptance or denial when compared to knowledge- or possession-based authentication mechanisms, users are subject to coercion, wherein a user, at gunpoint, is forced to present their fingerprint to provide an attacker access. The research community provided various solutions to address this specific sensor-level attack.

The authors in [10] provide a general overview of coercion detection in biometric systems and indicate that there are three techniques that can be used to detect coercion: involuntary, where a system automatically detects coercion based on analyzing the user's behavior, a voluntary technique where a user provides indications of coercion, and environmental techniques, where cameras or proximity sensors detect multiple individuals close to an authentication system. The authors further detail several considerations when designing a coercion detection system, such as performance implications, where systems require more than 15 min of gathered data to determine coercion. The authors state that lying, stress, and fear are the primary emotions that accompany coercion. However, the accuracy of detecting a lie, or stress and fear, has a low accuracy of 71% and 82%, respectively. Other research has reached 90% accuracy in detecting these emotions [24]. The other consideration is the diversity of operating devices and their configurations that impact the accuracy of a coercion detection system, as well as cultural, medical, and user acceptance for gathering data to detect coercion.

One of the novel techniques for detecting coercion is the tangible key technique (TKT), where a user can trigger a coercion detection by pressing a button. The other techniques involve skin conductivity responses to detect a user's emotions, such as stress and fear. The third technique is the intentional false authentication (IFA), which is widely adopted by banks, where a user clicks or writes their password reversed or authenticates using another fingerprint to trigger the coercion detection system. Finally, there is the facial micro-movement (FMM) method, where micro-movements caused by facial micro-expressions are observed to detect fear.

Further, the authors in [25] provided an analysis of coercion resistance in a wiretapping coercer by analyzing changes in skin conductance while authenticating to detect the change in the user's emotion as a sign of coercion.

Although numerous valid countermeasures were proposed to safeguard a system from sensor-level attacks, such as developing liveness detection, coercion, where a legitimate user is forced to place their fingerprint on the sensor, has not been widely covered. The convenience of current fingerprint technology, by authenticating a legitimate user in less than a second, has led to the possibility of placing the sensor on the legitimate user's finger to gain illegitimate access.

Even though the literature shows a tremendous effort to provide a reliable LD and coercion detection metrics especially with the new approach of detecting fingerprints in a touchless way [26] that was proposed by Priesnitz et al., none of the previous works used the micro-behavior characteristics that are unique to the user and which differ from a fake fingerprint and are different when a user is forced vs. willing to provide their fingerprint. DeutschmannNeil et al. [27] and Marc et al. [28] were issued US patents that allow for creating a behavioral profile of a user by collecting their acceleration, gryo, and gps data for the first and facial cues and the user voice to create a user profile to determine if a legitimate user is the one placing their fingerprint; however, the micro-behavior of the fingerprint itself has not been tested.

The next section details the hypotheses and objectives to provide a behavioral-based liveness detection and a metric for coercion detection from the sensor level for testing and evaluation.

3. Hypotheses and Objectives

Attacks on the sensor-level of a fingerprint-based biometric system have been addressed by introducing Liveness Detection (LD); however, attackers have developed measurements to fool and bypass the LD component [29]. Therefore, there is a demand to introduce a new metric that strengthens the LD component to reduce the success of sensor-based attacks. Further, the detection of a user's willingness in order to prevent coerced fingerprints as an attack on sensor-level fingerprint systems has not been addressed. Because a behavior-based measurement on the micro-level, where an attack on the sensor becomes harder to achieve, may serve that purpose, we developed the following hypotheses to combat the threat and make the sensor level of a fingerprint-based biometric system more robust.

3.1. Hypotheses

The main hypothesis is that "the micro-behavioral measurement of the fingertip as it is placed on the touch-based sensor surface over time until a fingerprint is fully formed is a valid mechanism to verify whether the fingerprint is fake or real and if a user is coerced".

The rationale of the main hypothesis is that fingertips, when placed on the surface of the touch-based sensor, possess skin characteristics and fingertip formations that are different from gummy fingers made from different materials such as gelatin, Play-Doh, 3D materials such as nylon, polypropylene, thermoplastic elastomers (TPE) or thermoplastic polyurethane (TPU), or simply silicone. The spread of the fingerprint on the sensor surface over time, the contour shape changes, the angle, the speed, the contact locations, and the size are expected to differ when compared with other materials, when placed by someone other than the legitimate user, or when a legitimate user is coerced to place their fingerprint in the sensor.

To support the main hypothesis, we developed a supporting hypothesis that states that "skin and known fake fingerprint material show a difference when compared with each other at different times". Additionally, we developed a second supporting hypothesis that states that "a fingertip, when placed by the legitimate user, shows a difference when compared with a fingertip placed by an attacker, whether using a fake fingerprint or forcing the legitimate user to place their fingertip on the sensor".

3.2. Objectives

To test the hypotheses, we developed the following objectives

1. To design the micro-behavioral fingerprint analysis system
2. To test the first supporting hypothesis of whether the micro-behavior of fingertips, when placed on the sensor surface over time, shows a difference between skin and other materials
3. To test the second supporting hypothesis of whether the micro-behavior of a fingertip, when placed on the sensor surface over time, shows a difference between the legitimate user placing their fingertip and an attacker using a constructed fingerprint
4. To test the second supporting hypothesis of whether the micro-behavior of fingertips, when placed on the sensor surface over time, shows a difference between the legitimate user placing their fingertip and a coerced but legitimate user
5. To evaluate the micro-behavioral fingertip analysis system in terms of its capability to improve liveness detection and the detection of the willingness of fingerprint placement
6. To test the main hypothesis of whether a micro-behavioral fingertip analysis system in a fingerprint-based biometric system can mitigate attacks on the sensor level with a fake fingerprint or coerced user

4. Micro-Behavioral Fingerprint Analysis System (MFAS) Design

Advancements in sensing technology have made it possible to detect micro-movements, multiple movements measured at the micro-level, and, therefore, micro-behavior, that is, unintentional and uncontrolled movements [30,31]. This capability allows for designing a micro-behavior fingerprint analysis system (MFAS) to strengthen the sensor level of a fingerprint-based biometric technology by detecting fake or coerced fingerprints and to support the hypotheses of this research work.

The micro-behavioral fingerprint analysis system (MFAS) consists of seven components and six features, as depicted in Figure 2:

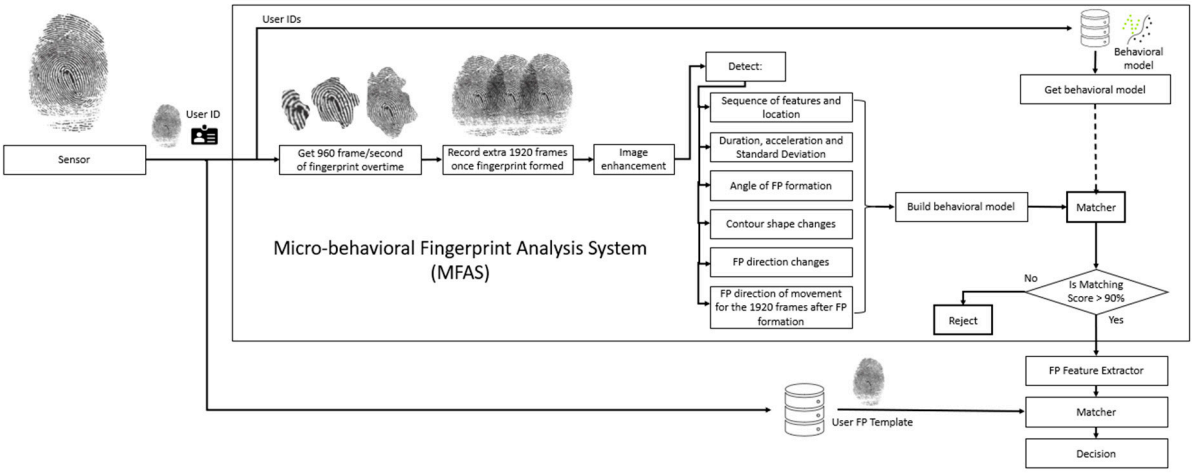

Figure 2. The MFAS steps to detect a fake vs. a real and a willing vs. a coerced fingerprint.

1. Sensor: The MFAS system is composed of a Samsung Note 20 smartphone camera placed under a clear thin glass surface with 330 dots per inch (dpi) resolution and 960 images per second.
2. Fingerprint capture: The capture component is an automated trigger to capture a print once a fingertip is in the scan frame, prior to touching the glass surface. It captures 960 images per second for 6 s. It captures the first touch of the fingertip on the sensor until the fingerprint is fully formed, with no changes, and then keeps on capturing for another 2 s while the fingerprint is stationary.

3. Image enhancement: The component enhances all captured images by applying smoothing, segmentation, enhancement, digitization, and then thinning to allow the system to detect the minutiae on the fingerprint. This step is important in capturing and analyzing the formation of the ridges over time.
4. Micro-behavioral-based Fingerprint Feature Extraction component: It detects six features from the captured images while a fingerprint is being formed on the surface of the sensor:
    a. The sequence of features appearing over time and the location of each feature
    b. Duration of fingerprint formation, acceleration between each captured image, and standard deviation
    c. The angle of the fingerprint formation
    d. Contour shape changes detection
    e. Fingerprint direction of changes
    f. Fingerprint micro-movement while stationary

Each of the features will be detailed in the data analysis section of this article and a list of abbreviations is provided in Abbreviations.

5. Micro-behavior model creation: The MFAS then captures the feature vector and creates a one-to-one behavioral matching model for the user.
6. Matcher: The matcher component is fed the stored behavioral model and the newly created behavioral model and returns a matching score.
7. Decision maker: The decision-maker component allows the user to pass to the next checkpoint on the fingerprint-based biometric system if the matching score of micro-behavior is above a specific threshold or rejects the sample on a non-matched behavior basis, which could be due to a fake fingerprint or a coerced submission of a fingerprint.

The seven components in Figure 2 depict the micro-behavioral fingerprint analysis system (MFAS), as well as the detected features, to build the fingerprint behavioral model for matching. Figure 3 depicts a typical fingerprint-based biometric system equipped with a liveness detection system, where the liveness detection system stands between the sensor and the feature extractor and can reject a fingerprint if it is fake prior to sending the data from the sensor to the feature extractor. Figure 4 depicts the placement of the proposed micro-behavioral fingerprint analysis system (MFAS), where it stands between the sensor component and the typical liveness detection system and can reject a coerced fingerprint placement prior to forwarding the fingerprint details to the feature extractor.

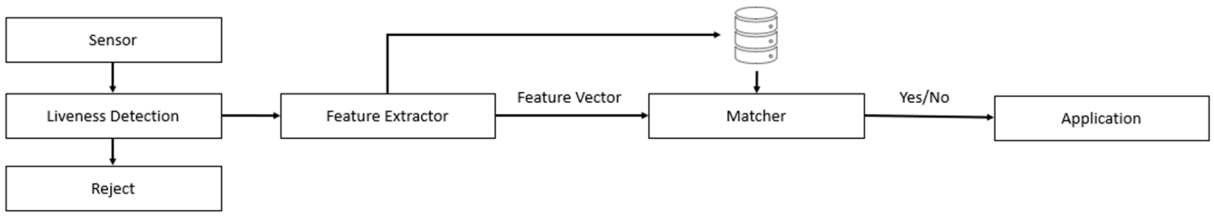

Figure 3. A typical fingerprint-based biometric system equipped with a liveness detection system.

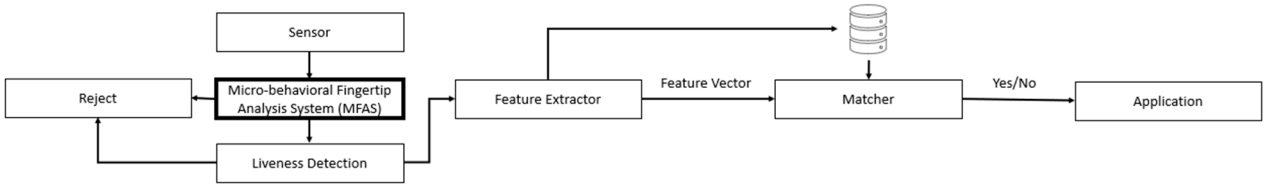

Figure 4. The placement of the proposed micro-behavioral fingerprint analysis system.

Objective 1 of the process of designing the MFAC system states that "the goal to design the micro-behavioral fingerprint analysis system" has been achieved. The next step is to

evaluate the potential of the system to detect fake or coerced fingerprints after building a dataset of fake vs. real fingerprints and willingness vs. coerced datasets.

5. Methodology, Experiment Design, and Data Analysis

5.1. Methodology

To achieve Objectives 2 through 6, test the hypotheses, and provide a quantitative analysis and evaluation of the proposed MFAS system and its capability in detecting if a fingerprint possesses the behavioral characteristics of a legitimate user while providing the fingerprint and that the fingerprint is provided voluntarily and willingly and is not coerced, we elected to use human-based experimentation to collect the behavioral characteristics, analyze them in accordance with the MFAS system, and then report the results.

5.2. Experiment

The experiment follows a between-subject design, where subjects are divided into two groups: legitimate users and attackers, where legitimate users provide their fingerprints and attackers create a gummy finger using play-dough to try and deceive the system. Then, a within-subject design is used by requesting legitimate users to provide their fingerprints with less of a willingness to evaluate the users' willingness using the MFAS system. All behavioral data, as well as the fingerprints, are collected and then fed into the MFAS system for analysis, identifying each group in the process.

5.2.1. Experiment Goal

The main goal of the experiment is to provide reliable data that enable the evaluation of the proposed MFAS system, achieve the objectives, and test the hypotheses. It is designed so that legitimate users' behavioral characteristics and fingerprints can be collected, and then attackers who have access to the fingerprint try to attack the system by exploring two cases, with and without the MFAS system, and report the results. Further, the willingness of the legitimate users is evaluated using the MFAS system to detect if a user is coerced or willing to provide their fingerprint.

5.2.2. Subjects

In a controlled environment, 24 female and male subjects aged between 20 and 47 years old participated in the experiment. All subjects were right-handed and had no fingerprint concerns, such as scars or not having a clear fingerprint, which might have impacted the reliability of their fingerprint acquisition. The subjects were informed that a fingerprint system was being evaluated, and the one who can trick the system will get a gift card. The rationale of the award was to motivate participants to try their best to fool the system and to create motivation when participating, which is important to compare willingness to provide a fingerprint vs. unwillingness.

5.2.3. Procedure and Discussion

Subjects began by signing a consent form that stated that they were asked to enroll in a fingerprint-based biometric system and then verified their identity by providing their fingerprint. This step was important in testing the capability of the system in matching fingerprints correctly. Participants were then requested to create a fake fingerprint for themselves and to try to dupe the system. Some Play-Doh was given to each participant, and they were taught how to reconstruct their fingerprint from a latent image remaining on a glass surface obtained when they enrolled. Each participant was then asked to place the fake fingerprint on the sensor. The fake fingerprints were then randomly assigned to other participants to try and fool the system. In this case, a participant enrolls, creates a fake fingerprint, and tests it. If it is successful in deceiving a traditional fingerprint-based biometric system, we assign the fake fingerprint to an attacker to try to fool the system by using the assigned fake fingerprint. This is important in evaluating the MFAS functioning between subjects, even when using the same fake fingerprint.

We then informed each participant of the privacy implications if one's fingerprint details are revealed, since anyone can then reconstruct a fake fingerprint based on theirs and then impersonate them using the fake fingerprint. Then, we told the participants that they now needed to allow us to publish their fingerprint in our research paper; if permission was denied, their participation would not be approved. This step was important in creating the unwillingness of providing a fingerprint and then comparing it with the first fingerprint they provided when enrolling and hoping to win the gift card. After the participants provided their fingerprints again, we informed them that no fingerprint would actually be published but that this was done to create the state of unwillingness and compare it with the opposite state of willingness which was needed to build a system that prevents coerced fingerprints in the MFAS.

By the end of the experiment, we obtained the necessary fingerprints and the micro-movement characteristics of the following conditions:

1. Enrollment with willingness behavior
2. Fake fingerprint used by the legitimate user
3. Fake fingerprint used by an attacker
4. Unwillingness fingerprint behavior

In each of the four cases, participants participated once with a dry fingerprint and then with a wet fingerprint to detect if the skin condition would affect the results of the MFAS. They then participated again after we placed a drop of water on the glass surface, in dry skin and wet skin conditions, to see if the surface condition affected the results of the MFAS. A total of four trials were performed per participant. To ensure that the sequence of the conditions did not affect the results of evaluating the MFAS, we randomized the sequence of the conditions per each participant. Some started with dry skin and a dry surface, while others started with wet skin and a wet surface.

The participation in each of the conditions collected the overall shape of the fingerprint and the six features listed in the MFAS design, including the following:

1. The sequence and location of the features appearing over time
2. The duration of fingerprint formation, the acceleration between each captured image, and the standard deviation
3. The angle of the fingerprint formation
4. Contour shape changes detection
5. Fingerprint direction of changes
6. Fingerprint micro-movement while stationary

Figure 5 depicts the smartphone and glass surface setup and the fingerprint capture over time. Table 2 summarizes the trials per participant in each of the conditions where, during the unwillingness trials, 17 out of 24 participants participated hesitantly.

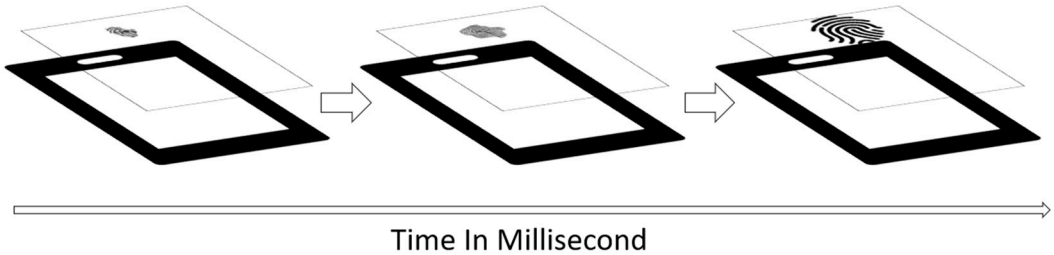

Figure 5. The setup of the experiment with the smartphone camera pointed toward a glass surface for capturing the fingerprint over time.

Table 2. Trials per participant in each of the conditions.

Trial	Condition			
	Dry Skin Dry Surface	Dry Skin Wet Surface	Wet Skin Dry Surface	Wet Skin Wet Surface
Enrollment with willingness behavior	24	24	24	24
Fake fingerprint used by the legitimate user	24	24	24	24
Fake fingerprint used by an attacker	24	24	24	24
Unwillingness fingerprint behavior	17	17	17	17
Total trials	89	89	89	89

5.3. Data Analysis

5.3.1. Data Analysis for a Traditional Fingerprint-Based Biometric System Using the Experimental Data

After collecting the behavioral data from the 24 participants in all four trials, enrollment occurred, which involves a willing fingerprint placement, testing their fake fingerprint, an attacker trying to fool the system with another's fake fingerprint, and, finally, the unwillingness of providing a legitimate fingerprint. All of the trials were performed under four conditions using different skin and surface conditions. The dataset was then set and ready for analysis to test how a traditional fingerprint-based biometric system, with and without the MFAS, behaved. We then reported the results.

A traditional fingerprint-based biometric system only needs the full images of the fingerprints, fully formed, without the behavioral measurements. It works by enhancing the fingerprint images by applying smoothing, segmentation, enhancement, and digitization and then thinning and extracting the fingerprint features, such as bifurcation and termination. The more features are used, the more accurate the system is and the more resources and time it needs to match a single fingerprint. Therefore, we only trained a neural network on bifurcation and termination with the directions and locations in each fingerprint. The template was then stored in a database, taking advantage of the first trial for all participants. All fingerprints were enrolled into the database successfully with 100% accuracy.

Next, we used the fake fingerprint images that were created by legitimate users and placed on the sensor. Only fully formed fingerprints were extracted and enhanced and then matched against the enrolled fingerprint. The same was carried out with the fake fingerprints that were used by the attackers, and the same analysis was performed on the unwilling fingerprint activity carried out at the end of the experiment, which was matched against the stored fingerprint template.

The analysis was conducted to test whether the dataset is good enough for a traditional fingerprint-based biometric system and to see if any of the fake fingerprints could gain access for the attackers.

The results show that all 24 participants' fingerprints were enrolled successfully into the system and were verified when providing unwilling fingerprints. This meant that, regardless of whether a user is willing to provide their fingerprint or is forced to do so, the system still provides access, as the fingerprint is the same in each condition. Rolling out in overly wet and overly dry conditions, the system still gives 100% accuracy in matching the fingerprints. In the case of fake fingerprints, an average of 93.5% were able to authenticate using their fake fingerprints, and an average of 95.5% were able to authenticate using another's fake fingerprints in optimal wet conditions. Only when the skin or the fingerprinting surface is wet do the fingerprint features become visible, since overly dry or overly wet conditions make the ridges of a fingerprint nonvisible. Figure 6 depicts the impact on the skin and surface conditions for the visibility of a fingerprint. These results show how important it is to incorporate liveness detection to safeguard a fingerprint-based biometric system that can be attacked even with simple Play-Doh. Table 3 shows the results per condition.

Figure 6. Fingerprint visibility in mid-wet, wet, and dry conditions.

Table 3. Results of a traditional fingerprint-based biometric system with no MFAS.

Trial	Condition				Average	
	Dry Skin Dry Surface	Dry Skin Wet Surface	Wet Skin Dry Surface	Wet Skin Wet Surface	All	Optimal (One Wet)
Enrollment with willingness behavior	79%	100%	100%	83%	90%	100%
Fake fingerprint used by the legitimate user	61%	96%	91%	64%	78%	93.5%
Fake fingerprint used by an attacker	64%	94%	97%	65%	80%	95.5%
Unwillingness fingerprint behavior	77%	100%	100%	81%	89%	100%

The above results show how a traditional system can behave against the fake and coercion-based attacks on the sensor of a fingerprint-based biometric system and show that the system authenticates an attacker as being legitimate. It also authenticates a legitimate user, whether they are willing or coerced to provide a fingerprint. The next step is to provide the micro-behavioral data using the MFAS to test its capability to protect the users in the case of fake fingerprints or coerced conditions.

5.3.2. Data Analysis for a Traditional Fingerprint-Based Biometric System Using the Experiment Data with MFAS

Each of the four conditions of the experiment for the four skin conditions is analyzed according to the MFAS algorithm in this section. First, touch is detected once a border of a fingerprint is present on the glass surface as an initial touch. In all, 960 images per second for 5 s for each of the fingerprints and 1920 images were collected per participant per condition in the four conditions of enrollment. These included fake fingerprints tested by a legitimate user, fake fingerprints tested by an attacker, and coerced fingerprint placement in the four skin and surface conditions. We then applied smoothing, enhancement, digitization, and thinning for every collected image. Each of the steps is performed in sequence to enhance the quality of the images for extracting fingerprint features such as bifurcation and termination and their angles and locations. Figures 7–9 depict the enhancement of the fingerprint images. Although this may seem resource-consuming, it was necessary to have as much information as possible and then test the system with less data and evaluate the impact on the system's accuracy and acceptability.

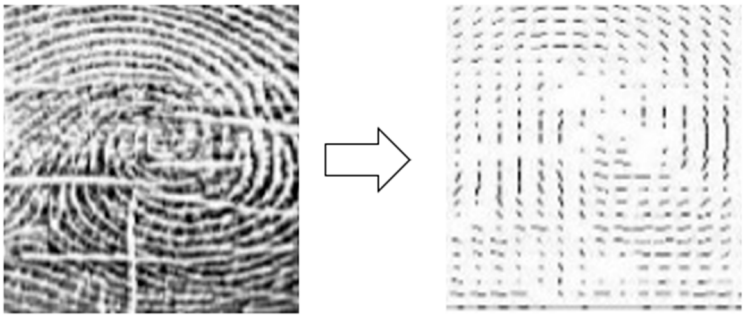

Figure 7. Fingerprint smoothing.

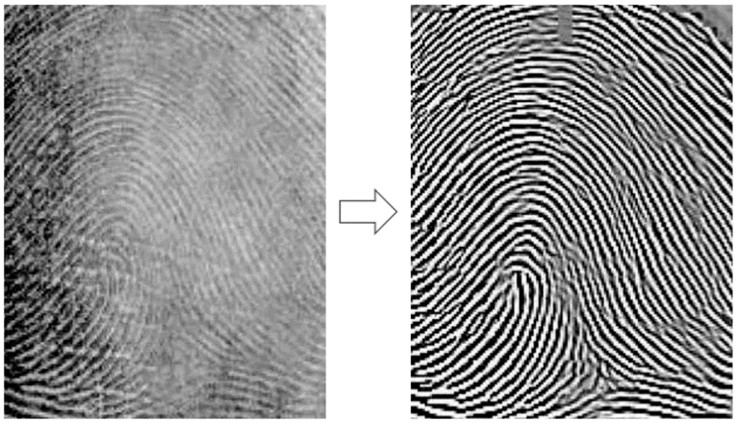

Figure 8. Enhancement after applying the Gabor filter on the fingerprints.

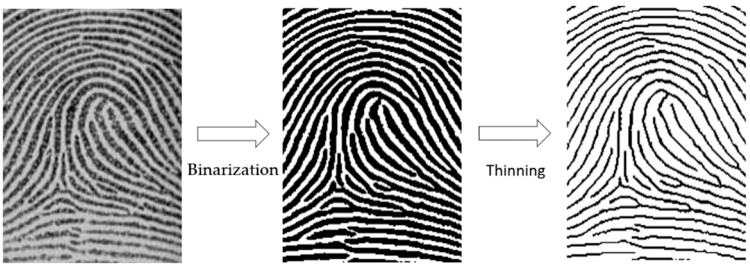

Figure 9. Digitization and thinning.

Smoothing was carried out to remove any scars or dirt so the visibility of ridges is clear, as depicted in Figure 7.

Further enhancement includes filling gaps in ridges, separating parallel ridges, and removing noise using adaptive contextual filters. We used a frequency and orientation-selective Gabor filter, as depicted in Figure 8.

Digitization was used to remove gray scale pixels using an adaptive threshold where an eight-pixel representation is reduced to one pixel. Then, thinning was applied to facilitate the work for minutia detection, where the width of a ridge is reduced to one pixel, as depicted in Figure 9.

All of the bifurcation and termination features of a fingerprint are extracted, along with their locations and directions. After the features extraction was carried out, the system reported the sequence of detected features as they appeared. This shows the usual points in a fingerprint that a user starts with and the sequence of those features while being placed on the glass surface when providing their fingerprint. It is hypothesized to be unique when compared to an attacker and serves as a behavioral feature to differentiate when a user is coerced or willing to provide their fingerprint. Figure 10 depicts the detected features at first touch, mid-touch, and final complete fingertip touch on the glass surface,

and it clearly shows the gradual appearance of fingerprint features over time. However, instead of capturing only three instances, all 960 images per second for 5 s were analyzed to provide a detailed appearance of the sequence of fingerprint features and the location and orientation of each feature, bifurcation, and termination of ridges, where each shape, circle triangle or square, depicts the an instance of the fingerprint where new fingerprint features were detected.

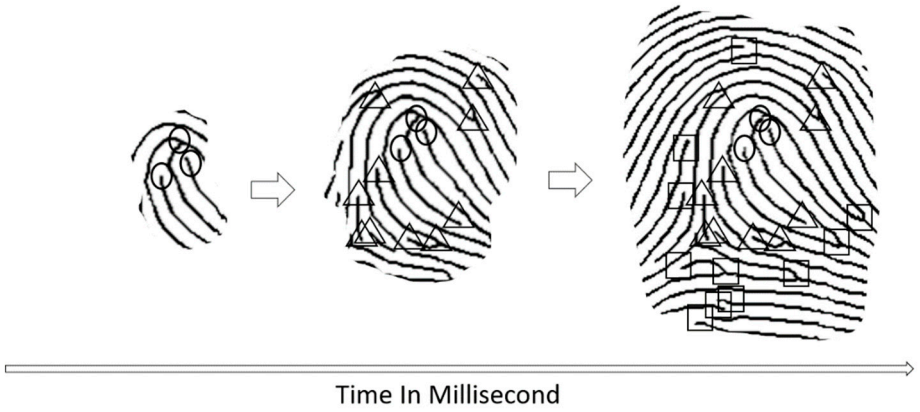

Figure 10. Sequence of fingerprint features detected over time.

Subsequently, the duration between each feature appearing and the newly discovered other features are computed. This allows for computing the acceleration of the fingerprint as it is placed on the glass surface and allows for detecting the first touch-point and the spread of the fingerprint over time, along with at what speed and acceleration. Then, the standard deviation of time between each feature discovered is computed to determine how the deviation changes as the fingerprints are placed on the sensor. Is it placed smoothly with no deviation, indicating comfort or the robotic, automated placement of a fingerprint, or does it fluctuate? The answer may assist in detecting whether a fingerprint is being placed by a legitimate user or an attacker, or whether it is placed with willingness or coercion.

This allows for detecting whether the angle of fingerprint formation is from top to bottom or from left to right, noting the specific degree with a predefined threshold that can be adjusted to improve the system's accuracy so that it is not so specific that it denies a legitimate user access and not so general that it allows an attacker access. The angle of formation is detected by comparing the flow of discovered new features as a fingerprint is being placed on the glass surface. Changes in the angle of formation indicate if a fingerprint starts from top to bottom but then slides to the right and left.

These detected data points are essential in forming the micro-behavioral model for each user to then compare it with fake fingerprints by the same user or an attacker, or when comparing the willingness-based fingerprint placement against coerced fingerprint placement.

The contour of the fingerprint as it is being placed on the glass surface is then computed over time, and the changes in the shape of the contour per frame are computed. This provides the detail of the fingerprint surface shape as well as the detailed micro-behavior of the user. Figure 11 depicts the fingerprint contour detection over time.

Finally, the system analyzes the final 1920 frames after a fingerprint is completely placed on the glass surface and reports the micro-movements' directional changes. A fingerprint that is completely still, with no changes at all, may be considered a sign of a fake fingerprint.

If this is the first time a user is using the system, the system creates a new template of the overall fingerprint ridge features and creates the micro-behavioral model. It then stores them in the database with the user's ID. If the user is authenticating their identity, the system pulls the two templates—the fingerprint ridge features and the behavioral model—and compares them with the newly submitted fingerprint shape and behavioral model.

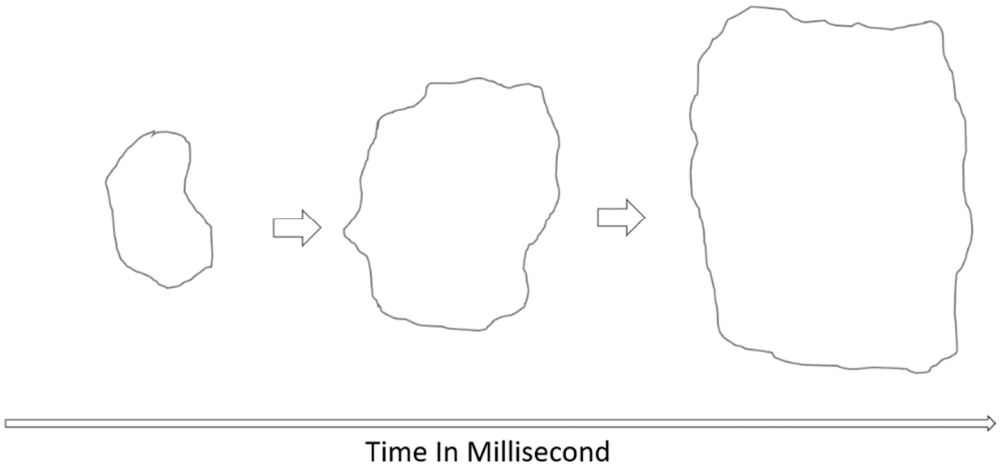

Figure 11. Fingerprint contour detection over time.

For the creation of the ridge-based features template, we stored the ridge type, bifurcation or termination, and the x, y coordinates of the ridges, as well as the angle of the tangent line on the x-axis ridge following a typical fingerprint template, as per the FBI. The type is given 1 bit and the location is given 18 bits of x and y values. The direction of the ending is given 8 bits, for a total of 27 bits, following the Automated Fingerprint Identification System (AFIS). A typical number of 10–100 features is usually detected in each fingerprint, which is sufficient to differentiate individuals. For matching the ridge-based features, we used correlation-based matching, where the alignment of the stored template and the new fingerprint are fed into the system and the correlation is computed. For the creation of the micro-movement behavior template, all micro-movement behavior, during and after a fingerprint is provided, is fed into a One Class Support Vector Machine (OCSVM) to create the class. For matching the micro-movement behavior, we used the OCSVM to evaluate if the new behavior matches the class of the stored behavior template.

If the ridge-based features match the submitted fingerprint, the matching of the micro-movement behavior of the fingerprint is accomplished if it passes a pre-defined threshold, thus authenticating the user's identity and providing access.

We concluded with four datasets:

1. A legitimate user providing their fingerprint.
2. A legitimate user providing their Play-Doh fingerprint.
3. An attacker providing the legitimate user's Play-Doh fingerprint.
4. A legitimate user unwillingly providing their fingerprint.

All of the datasets are in four different conditions:

1. Dry surface, dry skin.
2. Dry surface, wet skin.
3. Wet surface, dry skin.
4. Wet surface, wet skin.

A total of 16 datasets were created, after being analyzed by the MFAS, to achieve the objectives of this research work and support the hypotheses. The next section provides the results obtained.

In summary, the MFAS system enhances all temporal images as they are collected and then extracts the six features in all images. The MFAS then matches the newly acquired micro-behavioral features with those already stored and returns the results. Figure 12 depicts the overall MFAS data analysis as a fully automated fingerprint-based biometric system from the start of fingerprint placement until a decision of access is granted or denied.

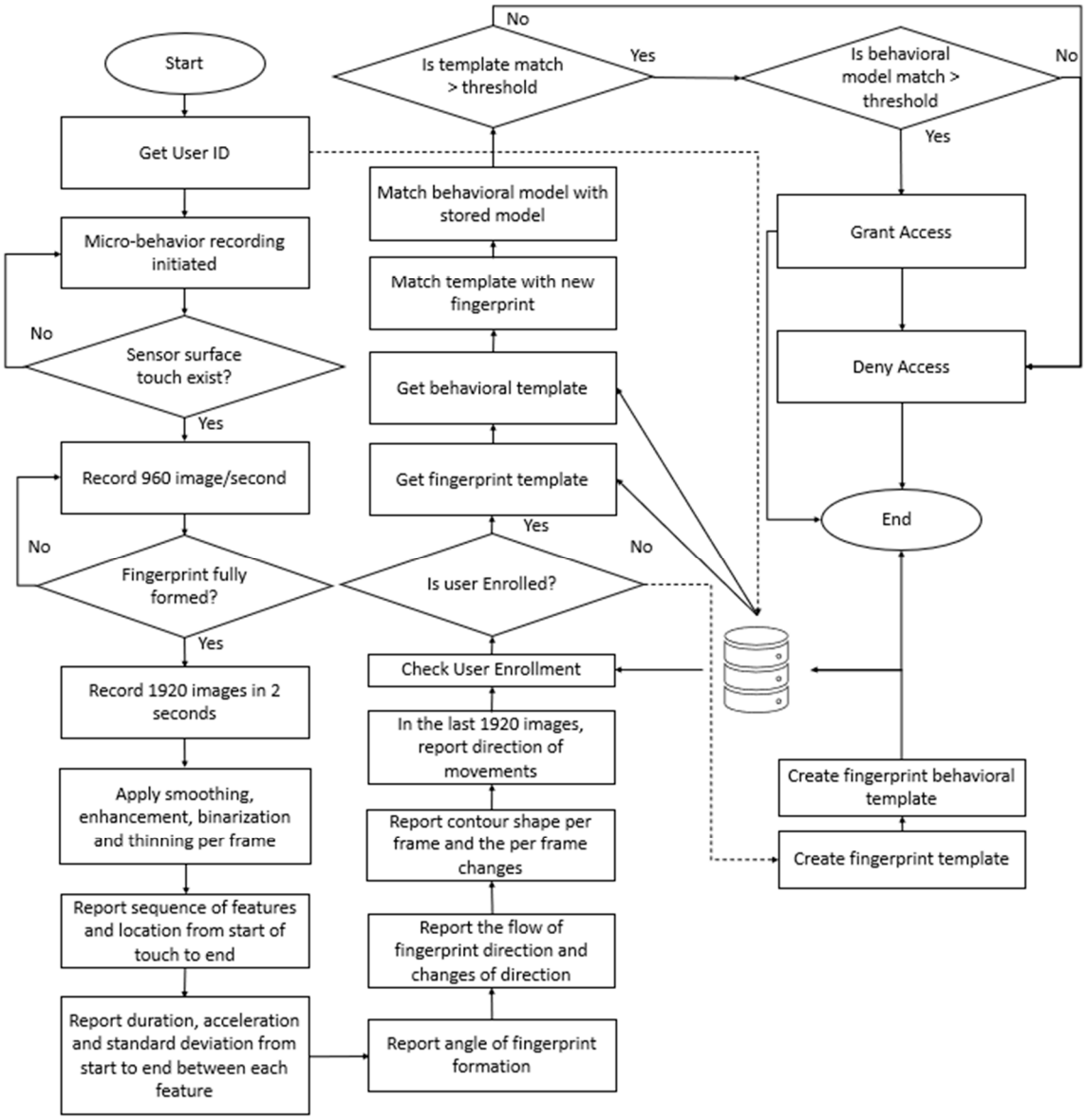

Figure 12. MFAS Data Analysis Algorithm.

6. Results

In this section, the experiment results are reported using all 16 datasets created after applying the MFAS data analysis component. Objectives 2 through 6 are achieved, and the hypotheses' results are provided, showing that the MFAS system is capable of detecting a fake fingerprint and a coerced fingerprint placement using the proposed micro-movement behavioral characteristics. A discussion on the findings is then provided.

MFAS Results

The results reported on the traditional fingerprint system, using ridge-based matching, show that traditional systems are not capable of detecting fake fingerprint placement by an attacker, where 95.5% of all fake data in optimal sensor and finger wet conditions are authenticated as being legitimate. Neither does it provide the capability of detecting coerced fingerprint placement given that 100% of these fingerprints are authenticated as being legitimate, as shown in Table 3, where a legitimate user at gun-point is forced to provide their fingerprint to authenticate and provide access to an attacker.

After analyzing the data using the MFAS, where the micro-movement behavior is captured while a fingerprint is being placed on the glass surface, the system shows a reduction in fake fingerprints being categorized as legitimate and a reduction in the percentage of matching when a user is willing to or coerced into provide their fingerprint. Table 4 shows the results of the 16 datasets while using the OCSVM classifier.

Table 4. Results of a traditional fingerprint-based biometric system using MFAS with OCSVM micro-movement behavior matching.

Trial	Condition				Average	
	Dry Skin Dry Surface	Dry Skin Wet Surface	Wet Skin Dry Surface	Wet Skin Wet Surface	All	Optimal (One Wet)
Enrollment with willingness behavior	88%	96%	94%	91%	92.25%	95%
Fake fingerprint used by a legitimate user	68%	72%	71%	62%	68.25%	71.5%
Fake fingerprint used by an attacker	52%	57%	61%	55%	56.25%	59%
Unwillingness fingerprint behavior	59%	64%	67%	56%	61.5%	65.5%

The results show that the MFAS can differentiate between real skin and Play-Doh, even if it is used by a legitimate user, since the spread of the skin has different micro-behavioral characteristics when compared to the user's skin. This has been shown in all 4 skin and surface dry and wet conditions, which achieves the second objective, which states "To test the first supporting hypothesis: if micro-behavioral fingertips, when placed on the sensor surface, over time show a difference between skin and other material", and supports the first supporting hypothesis, which states "Skin and other known fake fingerprint material show a difference when compared with each other", with a difference of 20% in dry skin–dry surface, 24% in dry skin–wet surface, 23% in wet skin–dry surface, and 29% in wet skin–wet surface, an overall average of 24%, and an optimal condition average of 23.5% between real fingerprints and Play-Doh-based fingerprints used by the legitimate user.

The results also show that the MFAS is capable of differentiating between the legitimate user placing their fingerprint vs. an attacker using a Play-Doh-based fingerprint, with a difference of 36% in dry skin–dry surface, 39% in dry skin–wet surface, 33% in wet skin–dry surface, and 36% in wet skin–wet surface, an average difference of 36%, and an average optimal condition of 36%. The results achieve the third objective, which states "To test the second supporting hypothesis of whether a micro-behavioral fingertip, when placed on the sensor surface, over time shows a difference between the legitimate user placing their fingertip vs. an attacker using a constructed fingerprint".

Further, the results show that the MFAS can differentiate between when a user provides their fingerprint willingly or unwillingly, with a difference of 29% in dry skin–dry surface, 32% in dry skin–wet surface, 27% in wet skin–dry surface, and 35% in wet skin–wet surface, an average difference of 30.75%, and an optimal condition average of 29.5%. The results support the fourth objective, which states "To test the second supporting hypothesis of whether micro-behavioral fingertips, when placed on the sensor surface, over time show a difference between a legitimate user placing their fingertip and a coerced legitimate user". Together, the third and fourth objectives' results support the second supporting hypothesis, which states that "A fingertip, when placed by the legitimate user, shows a difference when compared with a fingertip placed by an attacker, regardless of whether the attacker is using a fake fingerprint or forcing the legitimate user to place their fingertip on the sensor".

The overall results suggest that the MFAS is capable of detecting the liveness factor of the fingerprint or if a user is coerced to submit their fingerprint by using the micro-movement behavior while a fingerprint is placed on the sensor. This achieves the fifth objective, which states "To evaluate the micro-behavioral fingertip analysis system in terms of its capability to improve liveness detection and detect the willingness of fingerprint placement". Further, the results show that the MFAS is capable of mitigating attacks on the sensor level with a fake fingerprint or a user being coerced to submit their fingerprint and archives the sixth objective, which states "To test the main hypothesis of whether a micro-

behavioral fingertip analysis system in a fingerprint-based biometric system can mitigate attacks on the sensor level with a fake fingerprint or coerced use". Finally, the results show promise in terms of the capability of the MFAS in supporting the main hypothesis, which states that "Micro-behavior measurement of the fingertip as it is placed on the touch-based sensor surface over time until a fingerprint is fully formed is a valid mechanism to verify if the fingerprint is fake or real and if a user is coerced".

Figure 13 depicts the overall results, with and without the MFAS, in the four scenarios. It clearly shows a decrease in the matching score between an attacker using a fake fingerprint and a legitimate user and between a legitimate user when willing to provide their fingerprint and when being forced to do so.

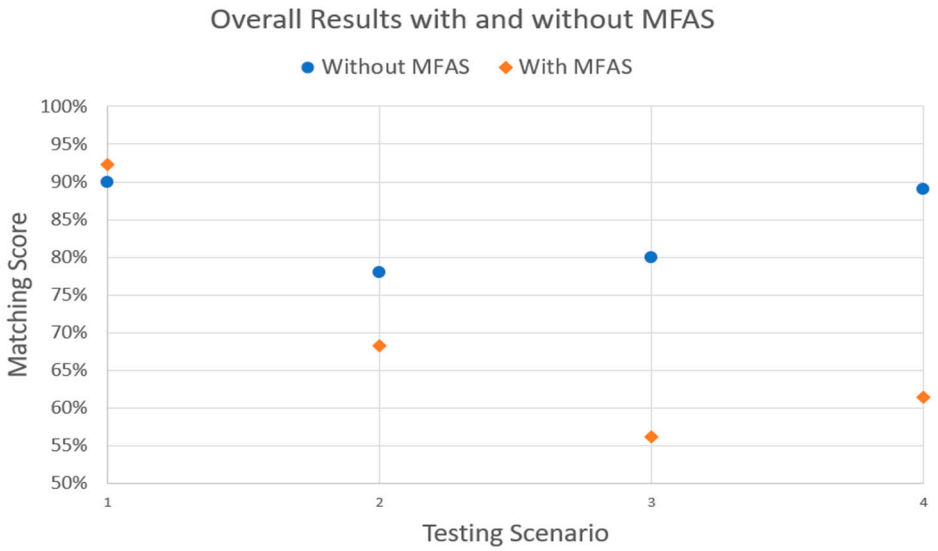

Figure 13. The overall results, with and without the MFAS, in the four scenarios, where 1 is a legitimate enrollment, 2 is for a fake fingerprint used by the legitimate user, 3 is for a fake fingerprint used by an attacker, and 4 is for an unwilling submission of a legitimate user's fingerprint.

The results show that, if the predefined threshold of the micro-behavior matching component is set to 72%, none of the attacks, whether using a fake fingerprint or forcing a user to submit their fingerprint, would be successful, thus providing traditional fingerprint-based biometric systems with a component that can mitigate such attacks.

The MFAS system provides a novel micro-behavioral-based measurement component in fingerprint-based biometric systems to improve their resistance to sensor-level fingerprint attacks such as constructed and coerced fingerprints. The micro-behavioral measurement differentiates between a live fingerprint and a fake fingerprint and differentiates between a willing and a coerced fingerprint placement, where an OCSVM is used to create a match between a legitimate fingerprint and a fake fingerprint and a willingly placed fingerprint and a coerced one. Finally, the micro-behavioral proposed component is placed in a traditional fingerprint-based biometric system and shows promising results in terms of improving the liveness detection of a fingerprint using the behavioral measurement and a promising result in terms of determining if a user is willing to or coerced into providing their fingerprint.

7. Discussions and Limitations

Although the MFAS shows promising results in differentiating between a legitimate fingerprint and a fake fingerprint when placed by an attacker and shows a capability in differentiating between a fingerprint being placed willingly and one coerced into being placed, the system takes an unacceptable amount of time to authenticate a user. The average data analysis is over 23 s, 7 s of which are required for the behavior capture and an average of 16 s of which are required for the data analysis. Therefore, we re-analyzed the data at

three intervals: the beginning, middle, and last part of a fingerprint placement, which is equivalent to 1.5 s, on average. This was carried out without the analysis of the 2 s after a fingerprint is stationary, which reduced the computational time for the analysis to under 5 s, on average. Although this improves the functionality in terms of the time of the MFAS, it impacts the accuracy of the detection. Table 5 shows the MFAS results after reducing the number of samples used when analyzing the micro-movement behavior of a fingerprint, and Figure 14 depicts the overall results after the reduction.

Table 5. Results of a traditional fingerprint-based biometric system using MFAS OCSVM at a reduced sample size for improving the acceptability of the system.

Trial	Condition				Average	
	Dry Skin Dry Surface	Dry Skin Wet Surface	Wet Skin Dry Surface	Wet Skin Wet Surface	All	Optimal (One Wet)
Enrollment with willingness behavior	83%	90%	92%	87%	88%	91%
Fake fingerprint used by the legitimate user	73%	78%	77%	69%	74.25%	77.5%
Fake fingerprint used by an attacker	59%	62%	68%	57%	61.5%	65%
Unwillingness fingerprint behavior	64%	72%	76%	62%	68.5%	74%

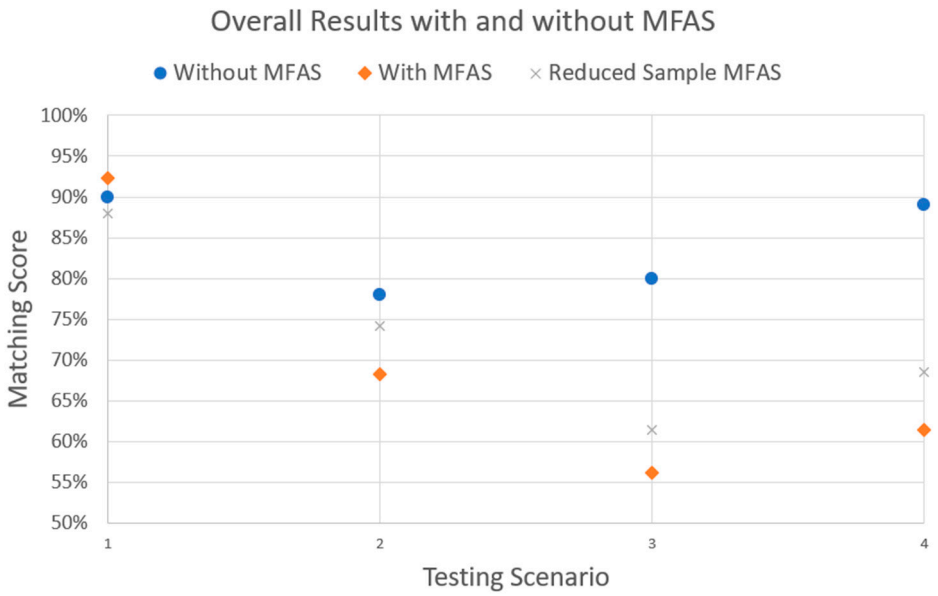

Figure 14. Overall results with and without MFAS, including the reduction in samples and its impact on the results of the MFAS.

The results show a reduction in the accuracy of the MFAS; yet, it is still capable of detecting a fake fingerprint and a coerced user. With a requirement to increase the threshold to a minimum of 78% instead of 72%, a difference of 6% is required. The trade-off between security and convenience allows for a faster system that is still capable of detecting the attacks.

It is important to note that the data were not acquired over a long period of time or with a change in the user's sitting or standing position, and these factors may have an impact on the accuracy of the MFAS. However, this research work is meant to show that the proposed technology shows potential for detecting fake fingerprints and coerced user attacks using micro-behavior analysis. The system has been tested in a controlled environment to test and report its capabilities. The MFAS shows promising results, but it has not been tested in real-life scenarios. Future work is required to strengthen the technology, as discussed in the future work section.

Although the authors in [32] proposed a method for detecting the liveness of a fingerprint by analyzing the skin elasticity, which is the closest to our approach among the other research studies in the literature, our approach shows a greater depth, a higher accuracy, and the ability to use the system to detect not just fake fingerprints but also unwilling and coerced placements of a fingerprint. The proposed method by the authors shows good accuracy in differentiating between skin elasticity and other materials used for constructing a fake fingerprint, such as Play-Doh. The correlation coefficient and the signal intensity are computed, as well as the standard deviation of the fingerprint. The authors used the Fisher Linear Discriminate to differentiate skin from other materials. They reached an EER of 4.78% when compared with methods using odor analysis [33] and skin distortion [34,35], which reached EERs of 7.48% and 4.90% respectively, while in MFAS, we reached an EER of 0% for both sensor-level attacks and fake or coerced fingerprint placements in the controlled environment. While the results are very promising, further research in real-life settings is required.

8. Conclusions and Future Work

In this paper, a micro-behavioral component has been proposed to combat fake fingerprint attacks as a liveness detection method. Further, willing vs. coerced users providing their fingerprints have been studied to investigate the proposed system's capability of detecting such attacks in comparison with the traditional fingerprint-based biometric systems.

The results support the main hypothesis, which states that "Micro-behavior measurement of the fingertip as it is placed on the touch-based sensor surface over time, until a fingerprint is fully formed, is a valid mechanism for verifying if the fingerprint is fake or real and if a user is coerced". This method has a threshold of 72% accuracy that is required to match the fingerprint behavior to differentiate between the attacks and the legitimate user. Further, a reduction in the sample size for evaluation was tested to improve the system's acceptability in terms of the amount of time needed for each assessment, reaching a reduction in MFAS accuracy of 6%; however, it was still enough to differentiate between the attacks and the legitimate user, with the threshold required to be at least 78% with an EER of 0% in the controlled environment and created dataset.

Future work includes testing the system over time, with various scenarios, including sitting and standing, at a specific urgency level, and at a specific stress level, to study the impact on the behavior model. Further, the system may be tested with a hill-based attack where a robotic arm-based system mimics the behavior of a user and retries until it reaches an acceptable level. Solutions to such problems are on limiting the number of trials and not reporting the matching score; however, studying if a robotic arm may still mimic a user's micro-behavior is of interest in attacking and strengthening the MFAS. Further, since the smartphone used in the experiment was to utilize the slow-motion capability, it is interesting to explore how one can connect smartphones with traditional fingerprint scanners to detect coerced fingerprint placement or use smartphones to authenticate individuals utilizing the slow-motion feature to detect if a user is being coerced to authenticate their identity using their fingerprint. Finally, a hybrid approach between the current technologies that provide fingerprint-based coercion detection and MFAS may limit the vulnerabilities in each system and make it robust. Future work is important in order to strengthen the technology and further help in understanding its advantages and disadvantages.

Funding: Funded by the Deanship of Scientific Research at the University of Tabuk, Grant: S-1443-0033.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

Acknowledgments: The author would like to thank the Deanship of Scientific Research at the University of Tabuk for funding the research. Grant: S-1443-0033 and thank the Sensor Networks and Cellular Systems (SNCS) research center for the support.

Conflicts of Interest: The author declares no conflict of interest.

Abbreviations

MFAS	Micro-behavioral Fingerprint Analysis System
LD	Liveliness Detection
CNN	Convolutional Neural Networks
TKT	Tangible Key Technique
IFA	Intentional False Authentication
FMM	Facial Micro-movement
TPE	Thermoplastic Elastomers
TPU	Thermoplastic Polyurethane
DPI	Dots Per Inch
AFIS	Automated Fingerprint Identification System
OCSVM	One Class Support Vector Machine

References

1. Kim, J.; Teoh, A.B.J. One-factor Cancellable Biometrics based on Indexing-First-Order Hashing for Fingerprint Authentication. In Proceedings of the 24th International Conference on Pattern Recognition (ICPR), Beijing, China, 20–24 August 2018; pp. 3108–3113. [CrossRef]
2. Syarif, M.A.; Nen, L.M.; Goh, A.; Win, L.K.; Ng, K.S.; Tiong, L.C.O. Challenge response interaction for biometric liveness establishment and template protection. In Proceedings of the 2016 14th Annual Conference on Privacy, Security and Trust (PST), Auckland, New Zealand, 12–14 December 2016; pp. 698–701. [CrossRef]
3. Cappelli, R.; Maio, D.; Lumini, A.; Maltoni, D. Fingerprint Image Reconstruction from Standard Templates. *IEEE Trans. Pattern Anal. Mach. Intell.* **2007**, *29*, 1489–1503. [CrossRef] [PubMed]
4. Memon, S.; Manivannan, N.; Balachandran, W. Active pore detection for liveness in fingerprint identification system. In Proceedings of the 2011 19th Telecommunications Forum (TELFOR), Belgrade, Serbia, 22–24 November 2011; pp. 619–622. [CrossRef]
5. Johnson, P.; Schuckers, S. Fingerprint pore characteristics for liveness detection. In Proceedings of the 2014 International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, Germany, 10–12 September 2014; pp. 1–8.
6. Lu, M.; Chen, Z.; Sheng, W. A Pore-Based Method for Fingerprint Liveness Detection. In Proceedings of the 2015 International Conference on Computer Science and Applications (CSA), Wuhan, China, 20–22 November 2015; pp. 77–81. [CrossRef]
7. Marcialis, G.L.; Roli, F.; Tidu, A. Analysis of Fingerprint Pores for Vitality Detection. In Proceedings of the 2010 20th International Conference on Pattern Recognition, Istanbul, Turkey, 23–26 August 2010; pp. 1289–1292. [CrossRef]
8. Nuraisha, S.; Shidik, G.F. Evaluation of Normalization in Fake Fingerprint Detection with Heterogeneous Sensor. In Proceedings of the 2018 International Seminar on Application for Technology of Information and Communication, Semarang, Indonesia, 21–22 September 2018; pp. 83–86. [CrossRef]
9. Baek, Y. The fake fingerprint detection system using a novel color distribution. In Proceedings of the 2016 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Korea, 19–21 October 2016; pp. 1111–1113. [CrossRef]
10. Matthew, P.; Anderson, M. Developing coercion detection solutions for biometrie security. In Proceedings of the 2016 SAI Computing Conference (SAI), London, UK, 13–15 July 2016; pp. 1123–1130. [CrossRef]
11. Li, Q.; Chan, P.P.K. Fingerprint liveness detection based on binarized statistical image feature with sampling from Gaussian distribution. In Proceedings of the 2014 International Conference on Wavelet Analysis and Pattern Recognition, Lanzhou, China, 13–16 July 2014; pp. 13–17. [CrossRef]
12. Bhanarkar, A.; Doshi, P.; Abhyankar, A.; Bang, A. Joint time frequency analysis based liveness fingerprint detection. In Proceedings of the 2013 IEEE Second International Conference on Image Information Processing (ICIIP-2013), Shimla, India, 9–11 December 2013; pp. 166–169. [CrossRef]
13. Kumar, A.K.T.; Vinayakumar, R.; Variyar, S.V.V.; Sowmya, V.; Soman, K.P. Convolutional Neural Networks for Fingerprint Liveness Detection System. In Proceedings of the 2019 International Conference on Intelligent Computing and Control Systems (ICCS), Madurai, India, 15–17 May 2019; pp. 243–246. [CrossRef]
14. Lazimul, L.T.P.; Binoy, D.L. Fingerprint liveness detection using convolutional neural network and fingerprint image enhancement. In Proceedings of the 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), Chennai, India, 1–2 August 2017; pp. 731–735. [CrossRef]
15. Zhang, Y.; Shi, D.; Zhan, X.; Cao, D.; Zhu, K.; Li, Z. Slim-ResCNN: A Deep Residual Convolutional Neural Network for Fingerprint Liveness Detection. *IEEE Access* **2019**, *7*, 91476–91487. [CrossRef]
16. Nogueira, R.F.; Lotufo, R.D.; Machado, R.C. Evaluating software-based fingerprint liveness detection using Convolutional Networks and Local Binary Patterns. In Proceedings of the 2014 IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications (BIOMS), Rome, Italy, 17 October 2014; pp. 22–29. [CrossRef]
17. Jian, W.; Zhou, Y.; Liu, H. Densely Connected Convolutional Network Optimized by Genetic Algorithm for Fingerprint Liveness Detection. *IEEE Access* **2021**, *9*, 2229–2243. [CrossRef]

18. Nogueira, R.F.; Lotufo, R.D.; Machado, R.C. Fingerprint Liveness Detection Using Convolutional Neural Networks. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 1206–1213. [CrossRef]
19. Jung, H.Y.; Heo, Y.S.; Lee, S. Fingerprint Liveness Detection by a Template-Probe Convolutional Neural Network. *IEEE Access* **2019**, *7*, 118986–118993. [CrossRef]
20. Zhang, Y.; Gao, C.; Pan, S.; Li, Z.; Xu, Y.; Qiu, H. A Score-Level Fusion of Fingerprint Matching with Fingerprint Liveness Detection. *IEEE Access* **2020**, *8*, 183391–183400. [CrossRef]
21. Komeili, M.; Armanfard, N.; Hatzinakos, D. Liveness Detection and Automatic Template Updating Using Fusion of ECG and Fingerprint. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 1810–1822. [CrossRef]
22. Jian, W.; Zhou, Y.; Liu, H. 2-layer Parallel SVM Network Based on Aggregated Local Descriptors for Fingerprint Liveness Detection. In Proceedings of the 2021 13th International Conference on Communication Software and Networks (ICCSN), Chongqing, China, 4–7 June 2021; pp. 296–304. [CrossRef]
23. Ibrahim, Y.; Mu'Azu, M.B.; Adedokun, A.E.; Sha'Aban, Y.A. A performance analysis of logistic regression and support vector machine classifiers for spoof fingerprint detection. In Proceedings of the 2017 IEEE 3rd International Conference on Electro-Technology for National Development (NIGERCON), Owerri, Nigeria, 7–10 November 2017; pp. 1–5. [CrossRef]
24. Sayette, M.A.; Cohn, J.F.; Wertz, J.M.; Perrott, M.a.; Parrott, D.J. A psychometric evaluation of the facial action coding system for assessing spontaneous expression. *J. Nonverbal Behav.* **2001**, *25*, 167–185. [CrossRef]
25. Küsters, R.; Truderung, T.; Vogt, A. Verifiability, Privacy, and Coercion-Resistance: New Insights from a Case Study. In Proceedings of the 2011 IEEE Symposium on Security and Privacy, Oakland, CA, USA, 22–25 May 2011; pp. 538–553. [CrossRef]
26. Priesnitz, J.; Rathgeb, C.; Buchmann, N.; Busch, C.; Margraf, M. An overview of touchless 2D fingerprint recognition. *J. Image Video Proc.* **2021**, *2021*, 8. [CrossRef]
27. Davis, M.E.; Dyor, M.G.; Gerrity, D.A.; Huang, X.; Hyde, R.A.; Levien, R.A.; Lord, R.T.; Lord, R.W.; Malamud, M.A.; Myhrvold, N.P.; et al. Tegreene. RPX Corp. U.S. Patent 8,713,704, 19 April 2014.
28. Deutschmann, I.; Costigan, N.; Libell, T.; Nordström, P. Behaviometrics AB. U.S. Patent 9,531,710, 27 December 2016.
29. Fei, J.; Xia, Z.; Yu, P.; Xiao, F. Adversarial attacks on fingerprint liveness detection. *J. Image Video Proc.* **2020**, *2020*, 1. [CrossRef]
30. Borza, D.; Itu, R.; Danescu, R. Real-time micro-expression detection from high speed cameras. In Proceedings of the 2017 13th IEEE International Conference on Intelligent Computer Communication and Processing (ICCP), Cluj-Napoca, Romania, 7–9 September 2017; pp. 357–361. [CrossRef]
31. D'Angelo, L.T.; Neuhaeuser, J.; Zhao, Y.; Lueth, T.C. SIMPLE-Use—Sensor Set for Wearable Movement and Interaction Research. *IEEE Sens. J.* **2014**, *14*, 1207–1215. [CrossRef]
32. Jia, J.; Cai, L.; Zhang, K.; Chen, D. A new approach to fake finger detection based on skin elasticity analysis. In *International Conference on Biometrics*; Springer: Berlin/Heidelberg, Germany, 2007; pp. 309–318.
33. Baldisserra, D.; Franco, A.; Maio, D.; Maltoni, D. Fake Fingerprint Detection by Odor Analysis. In *Advances in Biometrics*; Zhang, D., Jain, A.K., Eds.; Springer: Berlin/Heidelberg, Germany, 2005; Volume 3832, pp. 265–272.
34. Antonelli, A.; Cappelli, R.; Maio, D.; Maltoni, D. A New Approach to Fake Finger Detection Based on Skin Distortion. In *Advances in Biometrics*; Zhang, D., Jain, A.K., Eds.; Springer: Berlin/Heidelberg, Germany, 2005; Volume 3832, pp. 221–228.
35. Cappelli, R.; Maio, D.; Maltoni, D. Modeling Plastic Distortion in Fingerprint Images. In *Lecture Notes in Computer Science*; Singh, S., Murshed, N., Kropatsch, W.G., Eds.; Springer: Berlin/Heidelberg, Germany, 2001; Volume 2013, pp. 369–376.