mmPalm: Unlocking Ubiquitous User Authentication through Palm Recognition with mmWave Signals

Yucheng Xie*, Xiaonan Guo†, Yan Wang‡, Jerry Q. Cheng§,
Tianfang Zhang¶, Yingying Chen¶, Yi Wei†, Yuan Ge†
*Yeshiva University, †George Mason University, ‡Temple University, §New York Institute of Technology, ¶Rutgers University
Email: *yucheng.xie@yu.edu, †{xguo8, ywei8, yge3}@gmu.edu, ‡y.wang@temple.edu, §jcheng18@nyit.edu
¶{tz203, yingche}@scarletmail.rutgers.edu

2024 IEEE Conference on Communications and Network Security (CNS) | 979-8-3503-7596-1/24/$31.00 ©2024 IEEE | DOI: 10.1109/CNS62487.2024.10735583

Abstract*—Biometric authentication systems are increasingly needed across a broad range of applications including in smart city environments (e.g., entering hotels), and in smart home environments (e.g., controlling smart devices). Traditional methods, such as face-based and fingerprint-based authentication, usually incur high costs to be installed in all this kind of environments. In this paper, we develop a ubiquitous low-effort user authentication approach, *mmPalm*, based on palm recognition using millimeter wave (mmWave) signals. mmWave technology has been adopted by WiGig and 5G, making *mmPalm* a low-cost solution that can be widely adopted in public places. In addition, the high resolution of mmWave signals allows *mmPalm* to extract detailed palm characteristics (e.g., palm geometry, skin thickness, and texture) that can assemble distinctive palmprints for user authentication. Our innovative virtual antennas design further increases the spatial resolution of a commercial mmWave device, enabling it to fully capture the comprehensive palmprint features. Moreover, to address the challenge of small-scale environmental changes (e.g., variations in palm-device distances and palm orientations), we design a novel palm profile augmentation method, utilizing a Conditional Generative Adversarial Network (cGAN) to generate synthetic palm profiles for mitigating palm instability. Furthermore, we design a cross-environment adaptation framework based on transfer learning to address the challenge of large-scale environmental changes, including multipath variations introduced by human bodies and nearby furniture. Extensive experiments with 30 participants through 6 months demonstrate that *mmPalm* achieves 99% authentication accuracy with resilience against different types of attacks, including random, impersonation, and counterfeit.

I. Introduction

Biometric authentication methods have gained immense popularity due to their enhanced security features and user-friendliness. Existing biometric authentication methods typically utilize fingerprints, faces, or palms to differentiate users [1, 2, 3]. While these systems are generally accurate, their high costs can hinder widespread implementation, particularly in smart cities (e.g., accessing high-rise apartments, hotels, hospitals, and customizing vehicle functions) and in smart homes (e.g., managing smart devices and enhancing AR/VR experiences). Consequently, there is a pressing need for a cost-effective, ubiquitous user authentication method to provide secure and convenient access in these scenarios. Millimeter wave (mmWave) technology offers high sensing resolution due to its high-frequency and short wavelength. It has the potential to assist user authentication. Furthermore, mmWave has been integrated into current and next-generation wireless protocols, such as WiGig (IEEE 802.11ad and 802.11ay) [4] and 5G [5], making it a suitable candidate for cost-effective and ubiquitous

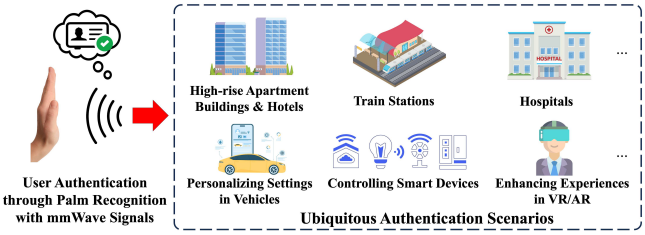


Fig. 1. Application scenarios of mmWave-based user authentication via palm information.

user authentication in daily applications. This inspired us to explore a new biometric that extracts people's palm information through fine-grained mmWave signals for the access control of smart city, and smart home environments.

Toward this end, we focus on two crucial elements: 1) the distinctive characteristics of human palms for user authentication, and 2) the low-cost mmWave sensing technology to accurately capture these fine-grained features of the palm. Research in biomedical fields has confirmed that the features of human palms, such as geometry, thickness, and skin distribution, differ significantly across individuals [6, 7]. Moreover, the texture of each person's palm, including principal lines, wrinkles, minutiae, and delta points, is uniquely identifiable [8]. Initial researchers have proposed a prototype to capture palm biometric information via cameras for customers verification, which has been tested in a restaurant [3]. Due to the need for installing cameras, the high costs may impede the widespread deployment of this system in daily life. Recently, researchers have shown that when users hold their smart devices, the palm biometric information can be captured by acoustic signals for user authentication [9, 10]. These systems require the mobile devices to actively generate dedicated acoustic signals during user authentication process. This may limit the application of these systems in other scenarios (e.g., smart cities). In this work, we propose to extract these palm characteristics from mmWave signals reflected by human palms to form distinctive palmprints, including palm geometry, skin thickness, and texture, for user authentication. Different from existing palm biometric-based approaches, our approach uses mmWave, which is low-cost, low-effort, and can be ubiquitously deployed in many smart applications, as depicted in Figure 1. For instance, a low-cost mmWave-enabled WiFi device can be installed in a high-rise apartment building entrance, where a user just needs to raise a palm to verify his/her identity and get through the secured entrance. In the automotive domain,

mmWave radars are frequently integrated to provide assisted driving and collision avoidance mechanisms. These devices can be leveraged for palm biometric-based user authentication, automatically enabling personalized vehicle settings.

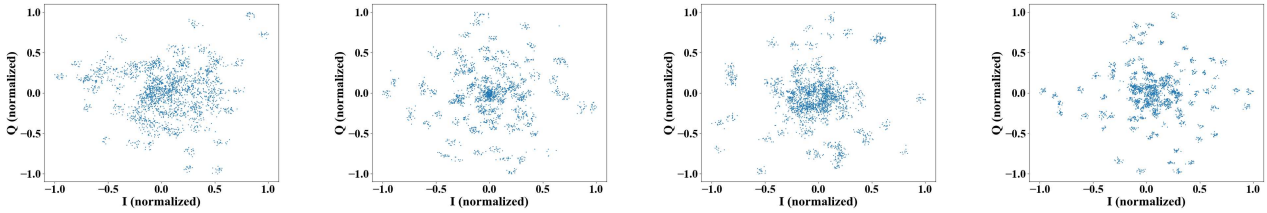
The unique characteristics of mmWave technology (i.e., high frequencies, short wavelengths, and broad bandwidth) make it more suitable for fine-grained sensing tasks, such as vital sign monitoring [11], than lower-frequency RF technologies (e.g., traditional WiFi at 2.4 or 5 GHz). Researchers have demonstrated that mmWave technology can be utilized for users identification by capturing distinct gait patterns [12] or signature movements [13]. Moreover, mmWave has shown potential for voice authentication by capturing throat vibration during communication [14]. Additionally, researchers have proposed using mmWave signals to capture detailed facial information for user authentication. Xu et al. [15] develop an mmWave-based face authentication system that relies on virtual registration signals generated from facial photos. Its complex hardware design make it less practical in real-life scenarios. In contrast, our approach explores palm biometrics, requiring users only to raise their hand for authentication. Our work only employs a low-cost commercial mmWave device to extract palm biometrics without additional devices. Furthermore, we envision our approach can complement existing authentication systems (e.g., face-based authentication) by offering a secondary factor for enhanced security.

In this paper, we propose *mmPalm*, which utilizes a commercial mmWave device to capture distinctive palmprint embedded in the reflected signals from human palms for user authentication. Particularly, *mmPalm* emits Frequency-Modulated Continuous Waves (FMCW) that vary in frequency over time and capture the reflection of these signals from a user's palm. We find that the differences between the transmitted and reflected signals, resulting from their interaction with the palm, directly correlate with the user's palmprint, including palm geometry, skin thickness, and palm texture. *(1)* The palm geometry (e.g., contour and size) can influence the interaction surface area and angle with the mmWave signals, altering their reflection and refraction. *(2)* Skin thickness modulates the mmWave energy absorption or reflection, and variations of the skin layers can cause non-uniformities in local electromagnetic fields within the skin, impacting the intensity and phase of the signals. *(3)* The palm texture, characterized by unique patterns of ridges and valleys, exhibits variations in density and dielectric properties, which influence the reflection and absorption characteristics of the mmWave signals. These palmprint features are unique to individuals, enabling *mmPalm* to effectively authenticate users by analyzing the reflected mmWave signals. The core of *mmPalm*'s authentication process is utilizing these unique palmprint features to establish and verify user palm profiles. During the enrollment stage, *mmPalm* allows users to establish unique palm profiles by facing their palms to the mmWave device. This distinctive palm profile is then utilized for identity verification during authentication sessions.

However, realizing *mmPalm* using a commercial mmWave device faces several challenges. First, the limited number of antennas on a commercial mmWave device makes it hard to capture comprehensive palmprint features. This restriction hinders the ability to produce high-dimensional measurements from independent antennas and effectively differentiate a large number of individuals for user authentication. Second, involuntary variations in palm orientation and distance during the authentication phase can result in misalignments between palm profiles captured during enrollment and those used in authentication, reducing the authentication accuracy in practical usage. Third, the presence of environmental reflectors, including arms, human bodies, furniture, and walls, can cause unpredictable changes in received multipath signals [16]. Traditional methods to handle these problems require collecting a huge amount of training data, which is impractical in real deployment.

To address the aforementioned challenges, we develop *mmPalm* with three main components. *(1)* To capture comprehensive palmprint features from a commercial mmWave device, our system exploits multiple virtual antennas to gather reflected mmWave signals from various angles, allowing for a collection of more complete and detailed palmprint data. We also design palm detection and segmentation algorithms to determine mmWave signals predominately from palm reflections, ensuring effective extraction of fine-grained palm biometrics. *(2)* To handle the challenge of different palm-device distances and variations in palm orientation, we develop a systematic data collection method for efficiently collecting palm profiles with designated positions and orientations. Moreover, to diminish the efforts required for palm data collection and labeling, we design a conditional generative-based method to synthesize virtual palm profiles. *(3)* To mitigate the influence of multipath signal reflections in practical scenarios, we develop a robust feature extractor trained on existing datasets that isolates palm features impervious to environmental variations. This ensures that users only need to register their palm profiles once in one environment, and the system can continue to function effectively in different environmental conditions. Our contribution can be summarized as follows:

- We develop a low-cost, user-friendly, and ubiquitous palm-based user authentication approach leveraging a commercial mmWave device, requiring users only to raise their hand for authentication.
- We exploit virtual antennas to capture detailed spatial information of palmprint, including palm geometry, skin thickness, and texture. We also develop methodologies for accurate palm detection and segmentation based on Range-Elevation heatmap to facilitate effective palm biometric extraction.
- We develop a palm profile augmentation module using a systematic data collection method and a Conditional Generative Adversarial Network to enhance the system's resilience against variations in palm positions and orientations.
- Our cross-environment adaptation module utilizes an Adversarial Autoencoder with Maximum Mean Discrepancy regularization to mitigate the multipath impact in dynamic



(a) Palm-reflected signal of User1 (b) Palm-reflected signal of User2 (c) Palm-reflected signal of User3 (d) Palm-reflected signal of User4

Fig. 2. In-phase and Quadrature (IQ) distributions of the reflected mmWave signals from 4 different users.

environments, making our approach to achieve consistent performance regardless of environmental changes.

- We conduct extensive experiments with 30 users, studying palm-device distance, palm orientations, and environment changes to verify the effectiveness and robustness of our system. Results show that *mmPalm* recognizes users consistently with around 99% accuracy. We also evaluate our system under different attacks, which demonstrate that our system can achieve accurate and robust user authentication and resistance to spoofing attacks.

II. Background and Feasibility Study

A. Sensing User Palm via mmWave Signals

In this work, our basic idea is to use palm-reflected signals for user authentication. To determine whether the reflected signals include reflections from the palm, we measure and analyze the frequency and phase of the reflected signals, allowing us to detect the presence and further determine the location of the palm within the sensing area. In particular, the mmWave device transmits FMCW signals, generating Intermediate Frequency (IF) signals upon receiving reflections. We use IF signals to detect the distance of the palm because its frequency shift is linearly correlated with the distance between the mmWave device and the palm. The IF signal can also be used to detect the angle of the palm by analyzing the phase shifts between multiple antennas in the same mmWave device [17].

B. Modeling the Impact of Palm Biometric Features on mmWave Signal Propagation

After detecting the palm, we proceed to establish a relationship between the reflected signal and the palm's biometric features. The mmWave signal forms a channel between the device and the user's palm as it reflects off the palm and back to the device. This interaction results in a distinctive channel response that captures the palm's biometric features. Specifically, the palm's geometry impacts the channel by affecting the reflected signal's pattern, introducing specific phase shifts and amplitude variations in the IF signal. Furthermore, variations in palm skin thickness and texture can alter the dielectric and electromagnetic properties of the reflected signal, resulting both amplitude and phase changes. The combination measurements of amplitude and phase alterations enable *mmPalm* to capture detailed palm biometric features that are embedded in the channel response.

In particular, we model the impact of palm biometric features on the palm reflected mmWave signal by establishing a function that relates the amplitude and phase shifts in the IF signal to the palm's biometrics. This function can be described as $(A_{\text{IF}}, \phi_{\text{IF}}) = f(G, S, T)$, where A_{IF} and ϕ_{IF} represent the amplitude and phase shifts of the IF signal. G, S, and T represent the geometry, skin thickness, and texture of the palm, respectively. By connecting these palm characteristics to the measured amplitude and phase shifts, the function f depicts how palm biometrics impact the mmWave signal propagation. We train deep neural networks on collected palm reflected signals to effectively learn this function f.

C. Feasibility of Using Palm-reflected mmWave Signals for User Differentiation

To demonstrate the feasibility of user differentiation using mmWave signals, we conducted preliminary experiments to examine palm-reflected signals from different users. We employ a $77 \sim 81$GHz mmWave device (i.e., TI AWR1642). Specifically, we collect palm-reflected signals from 4 users and the In-phase and Quadrature (IQ) data collected in 0.1 seconds are visualized in Figure 2. The results indicate that different users exhibit various distributions of reflection phase and amplitude. Given the experiments are conducted in the same environment with the same palm-device distance and orientation, the differences of the received signals are dominated by the differences in users' palms. This observation inspires us to establish a relationship between the original transmitted and palm-reflected signals to derive users' palm biometrics.

III. Attack Models

The goal of an adversary is to gain unauthorized access to specific devices (e.g., smart vehicles, VR/AR devices) or locations (e.g., hotels, banks, and government agencies) that are restricted to legitimate users and equipped with palm-based user authentication system using mmWave signals. Based on different prior knowledge and techniques that are available to the adversary, we categorize potential threats into three distinct attack types, including *random attack*, *impersonation attack*, and *counterfeit attack*.

Random Attack. The adversary attempts to gain unauthorized access without any prior knowledge of the palm biometrics from legitimate users. During random attack, the adversary attack can try different random palm positions (e.g., distances, postures, orientations), with the expectation that the palm biometrics embedded in the reflected mmWave signals will be similar with legitimate users and bypassing the user authentication provided by *mmPalm*.

Impersonation Attack. Different from the random attack without any prior knowledge of user palm information, the adversary is able to know how the legitimate users place their

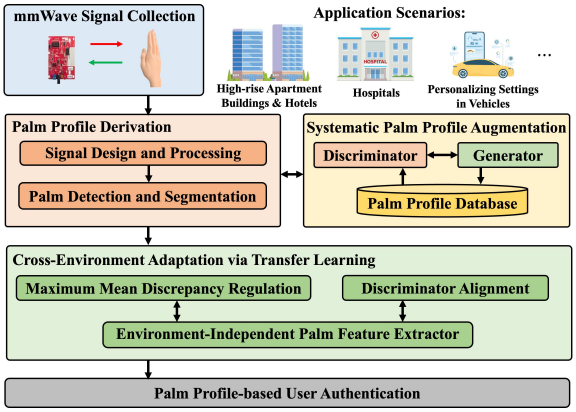


Fig. 3. System overview of *mmPalm*.

palms and their palm biometrics (e.g., palm size). This information can be obtained through video surveillance, social engineering, or even observations during user enrollments. During impersonation attack, the adversary can try by himself/herself or recruit other users with similar palm and instruct them to replicate the palm placements of the legitimate users, thus attempting to bypass the authentication provided by *mmPalm*.

Counterfeit Attack. In counterfeit attack, the adversary might further access to the user's detailed 3D palm contour. This fine-grained information might be obtained in medical institutions, where 3D model of the patient's body part is built for medical diagnosis, surgical planning, and other purposes. Based on the captured palm biometrics, the adversary could utilize a 3D printing to replicate physical palm models, which share similar geometry with the legitimate users. Then the adversary attempts to bypass the user authentication scheme provided by *mmPalm* with the palm replica.

IV. mmPalm System Implementation

The system has been designed with four modules, including *palm profile derivation*, *palm profile augmentation*, *cross-environment adaptation via transfer learning*, and *palm profile-based user authentication*, as illustrated in Figure 3.

A. Palm Profile Derivation

Software-defined TDM-MIMO System Implementation. To determine reliable mmWave signals for extracting palmprints, *mmPalm* first initiates a transceiving channel between the user's palm and mmWave device to collect IF signals. Then we enhance the spatial capabilities of a commercial mmWave device by constructing multiple virtual antennas. Specifically, we implement this virtual antenna design on TI AWR1642 [18] equipped with 2 transmitter antennas (TXs) and 4 receiver antennas (RXs). We synthesize a 1×8 virtual antenna array by alternating mmWave chirp signals from TX1 and TX2 in a Time-Division Multiplexing manner [19]. The signal collected from each pair (8 pairs in total) of transceivers provides a unique dimension of the palm profile that facilitates capturing spatial details of the palmprints.

Palm-reflected Signal Detection and Segmentation. Alongside the enhanced spatial capability, we develop both a palm detection algorithm and a dynamic segmentation algorithm to detect the presence and further determine the palm-reflected

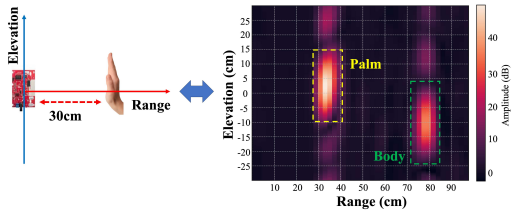


Fig. 4. The Range-Elevation heatmap helps determine the segment of the palm-reflected signals.

signals. In particular, we leverage range-FFT and angle-FFT to generate the range-response profile and Range-Elevation heatmap. As shown in Figure 4, when a human palm is positioned at 30 cm from the mmWave device, it exhibits an elliptical high amplitude on the Range-Elevation heatmap. Our detection algorithm determines the palm position by analysing the reflection energy in the heatmap, as the palm exhibits the strongest energy due to its proximity to the mmWave device. Furthermore, based on the detected palm position, we develop a dynamic segmentation algorithm to capture the signals predominately from palm reflections in the range-response profile. We use a one-dimensional sliding window to extract signals within its range. The window size is established through empirical studies. Each antenna's palm profile is then constructed based on the segmented signals, incorporating both the corresponding phase and amplitude information.

B. Palm Profile Augmentation

Systematic Palm Profile Enrollment. To overcome the performance degradation due to uncertain palm placements and reduce the data collection cost for enrolling users, we realize a palm profile augmentation scheme. Inspired by Apple's FaceID [20] on capturing different angles of users' faces, we instruct the users to slightly move their palms to build comprehensive palm profiles for each user. Figure 5(a) and (c) present a dual-coordinate system framework. The device axes are oriented as follows: x_m is the vertical axis perpendicular to the wavefront emission plane and y_m is the horizontal axis. z_m is the depth axis aligned with the direction of wave propagation. The palm coordinate system is initially aligned with the mmWave device. Then the users could move their palm in a predefined way. The movements include rotating their palms along different directions (x-, y-, and z-axis) and then moving their palms at varying distances away from the device as demonstrated in Figure 5(b) and (d). Through collecting users' palm-reflected signals from different angles and distances, more palm profiles are efficiently created for each individual user, which simulates the authentication scenarios with uncertain palm placements.

Palm Profile Augmentation Based on cGAN. Although collecting diverse palm-reflected signals from slightly different angles and distances is possible, the variability in users' palm placements in practical scenarios complicates this process. It is unrealistic to expect users to provide palm-reflected signals for every possible palm placement during the enrollment phase. To address this challenge, we develop a Conditional Generative Adversarial Network (cGAN) [21] to synthesize virtual palm

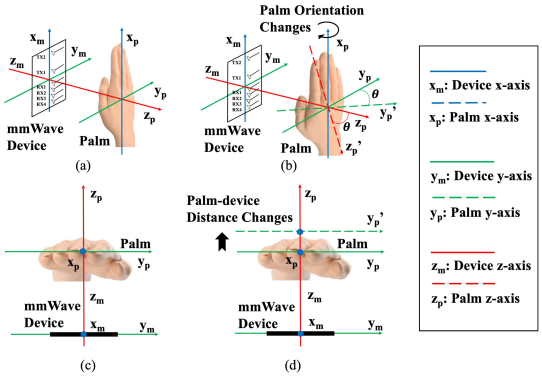


Fig. 5. (a) User authentication via palm without palm orientation changes; (b) Palm orientation changes caused by palm rotation along x-axis; (c) User authentication via palm without palm-device distance changes; (d) Palm-device distance changes caused by palm movement along z-axis.

profiles from the limited real ones collected from users. As demonstrated in Figure 6, the real palm profiles are first categorized into 10 classes along each axis using an unsupervised classification method (i.e., the K-means++ [22]). Each profile can be classified as a one-hot label with 7 attributes that correspond to the specific classes for distance and orientation along each of the three axes (x, y, and z), as well as user ID.

cGAN Training Procedure. During the training phase of the cGAN, the generator $G(\cdot)$ takes a random noise vector and the conditional labels (predicted via K-means++) as inputs and generate virtual palm profiles that share similar distributions with the real palm profiles satisfying the specific conditions, which is realized by minimizing the generation loss L_G. The discriminator $D(\cdot)$ is trained to distinguish between real and synthesized palm profiles, which is achieved by maximizing the discrimination loss L_D. We train cGAN by optimizing the trainable parameters θ_G and θ_D. The generator loss L_G and the discriminator loss L_D are calculated as:

$$L_G = \frac{1}{N}\sum_{i=1}^{N}\log\big(1 - D(G(n_i|c_i))\big),$$
$$L_D = \frac{1}{N}\sum_{i=1}^{N}\big(\log(D(p_i|c_i)) + \log(1 - D(G(n_i|c_i)))\big), \quad (1)$$
$$\arg\min_{\theta_G} L_G, \quad \arg\max_{\theta_D} L_D.$$

where $G(n_i|c_i)$ represents the synthesized profiles with random noise n_i and conditional labels c_i as inputs. $D(p_i|c_i)$ denotes the prediction results (e.g., real or synthesized) of the input profile p_i with the conditional label c_i. N refers the total number of training profiles, and i denotes the index of each profile. During the generating phase, the generator synthesizes virtual palm profiles associated with target labels of palm-device distances and palm orientations.

C. Cross-Environment Adaptation via Transfer Learning

To mitigate environmental factors in the palm profiles, we develop a deep learning framework based on Adversarial Autoencoder (AAE) with Maximum Mean Discrepancy (MMD) regularization [23]. As illustrated in Figure 7, we optimize parameters of the Autoencoder and extract hidden representations as latent palm features. Meanwhile, we minimize the

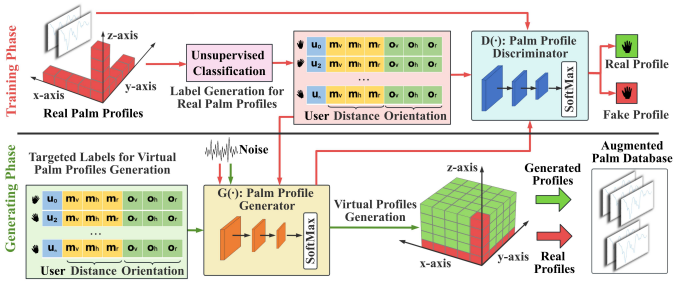


Fig. 6. The process of palm profile augmentation based on cGAN.

MMD among the latent palm features extracted from different environments to reduce the environmental variance. We also develop a discriminator that encourage the latent palm features whose distribution is aligned with a Laplace prior distribution without favoring any particular environment's characteristics [24]. During the authentication phase, the trained feature extractor (encoder) can achieve environmental independence and enable *mmPalm* to be deployed in new environment without any training efforts. In addition, *mmPalm* utilizes the palm profiles collected by the developer to complete the training process, ensuring that users are required to register their palms in only one environment.

Model Training Procedure. We develop a reconstruction loss L_r for the Autoencoder to ensure that the reconstructed palm profiles $\hat{p}$ share similar distributions with the original input p. To minimize the distribution discrepancies among palm profiles collected from different environments, we apply MMD regularization. Specifically, MMD measures the differences of latent palm features between two training environments. During the training process, we minimize the environment alignment loss L_m to optimize the trainable parameters of the encoder $E(\cdot)$ until it generate environment-independent latent palm features. To make the latent palm feature h aligning with the Laplace prior distribution l, we involve adversarial loss L_a while optimizing the parameters of the adversarial discriminator. The optimization process can be described as:

$$L_m = max\Big(\sum_{u,v}\Big|\Big|\frac{1}{N_u}\sum_{i=1}^{N_u}E(p_{u,i}) - \frac{1}{N_v}\sum_{i=1}^{N_v}E(p_{v,i})\Big|\Big|, 0\Big),$$
$$L_r = \frac{1}{N}\sum_{i=1}^{N}MSE(p_i, \hat{p}_i), \quad L_a = \frac{1}{N}\sum_{i=1}^{N}MSE(h_i, l_i),$$
$$\arg\min_{\theta_E,\theta_Z,\theta_{AD}} \lambda_m L_m + \lambda_r L_r + \lambda_a L_a, \quad (2)$$

where N and i denotes the total number and index of palm profiles. u and v denote two training environments. $MSE(\cdot,\cdot)$ refers the mean squared error. θ_E, θ_Z, and θ_{AD} represents the trainable parameters of the encoder, decoder, and adversarial discriminator. λ_m, λ_r, and λ_a denotes the weights of each loss function for balancing the total loss and accelerating convergence.

D. Palm Profile-based User Authentication

After the cross-environment adaptation, we develop a deep-learning-based user classifier to authenticate each individual. It

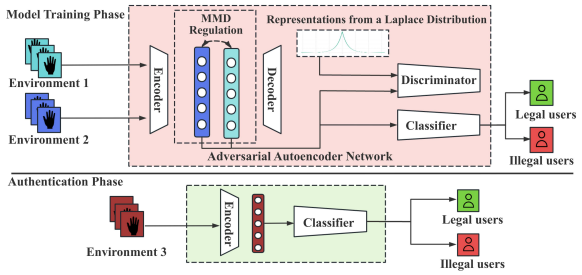


Fig. 7. The cross-environment adaptation module with user classifier.

takes the latent palm feature h as input and output user identity. This output is then compared with the ground truth user identity g, to either authenticate or reject the current user. The training process requires two classes of data: labeled legitimate users and labeled unauthorized adversaries. Both classes' palm profiles are initially enhanced with the proposed palm profile augmentation and processed through the encoder to mitigate environmental factors. For each registered user, a specific pair consisting of an encoder and a classifier is created. During the authentication phase, the testing palm profile needs to pass through all pairs of encoder and classifier. The probability that the palm profile belongs to each user is then computed and used to make an authentication decision. To grant access, the highest probability among all registered users must exceed 0.5.

V. Performance Evaluation

A. Evaluation Methodology

Device Configuration. We implement *mmPalm* using a commercial mmWave device, i.e., TI AWR1642 with a DCA1000EVM data capture and streaming card. The antennas provide a field of view (FOV) of 120° in elevation and 30° in azimuth, with an angular resolution of 15°.

Data Collection. We recruit 30 volunteers including 23 males and 7 females with ages ranging from 21 to 38. We do not set any restrictions on specific palm sizes or any other demographic characteristics that may influence the palm patterns. Necessary consent and IRB approvals are sought for all experiments. When conducting experiments, we position the mmWave device on a table with the antennas pointing towards the ceiling. During the enrollment stage, each participant places the palms directly above the device at a specific distance (e.g., 30 cm). Then, the palm profile is collected by using the developed palm profile augmentation approach. Specifically, each participant places the palm with different distances (e.g., move around $\pm$ 5 cm along each axis with mmWave device as the coordinate origin), and then different orientations (e.g., rotate around $\pm$ 30° along each axis with device plane as 0°). This process can be done within one minute.

Environmental Setup. To evaluate the user authentication performance of *mmPalm* in the presence of large scale changes between the enrollment and authentication environment, we conduct experiments at five different rooms: two offices, two lounges, and one corridor (as shown in Figure 8). The sizes of office 1 and office 2 are 5 m × 3 m and 3 m × 3 m. The size of lounge 1 and lounge 2 are 3 m × 4 m and 4 m × 4 m, and the corridor is 5 m × 9 m. The heights of all rooms are 2.8 m. In

Fig. 8. Illustration of 5 different environments for performance evaluation.

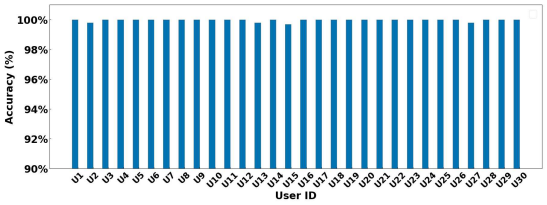


Fig. 9. Overall user authentication performance.

these varying environments, users could wear different clothes, and the placement of the mmWave device varies. In addition, multipath effects arise from both the user's body and the varied placements of devices and furniture.

Evaluation Metrics. To evaluate the effectiveness and robustness of *mmPalm*, we utilize two metrics. *(1) Authentication Accuracy (ACC)* represents the percentage that user i is correctly identified as i among all users. *(2) Attack Success Rate (ASR)* measures the percentage of instances where *mmPalm* incorrectly authenticates an adversary as a legitimate user.

B. Overall User Authentication Performance

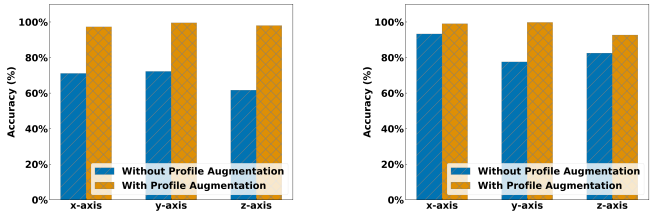
In this part, we first evaluate *mmPalm*'s overall performance in distinguishing multiple users based on unique palmprints.

Experimental Setup. In our experiments, 30 participants are involved in collecting the palm-reflected signals in five environments. During the enrollment phase, we instruct the participants to place their palms above the device with several practical distances (i.e., 15 cm, 30 cm, 45 cm, 60 cm). In the authentication phase, participants are asked to place their palms in the same position and environment. Each participant is alternately considered the legitimate user with the others as unauthorized adversaries to evaluate the authentication performance. The average ACC associated for each user is summarized to demonstrate the authentication performance of *mmPalm*.

Evaluation Results. The average ACC across various distance (i.e., 15 cm, 30 cm, 45 cm, 60 cm) are 99.96%, 99.97%, 99.83%, and 99.75%, receptively. We observe that the system achieve optimal performance when the users position their palm 30 cm from the device. This distance allows the mmWave device to effectively capture the reflected signals from the user's palm while maintaining robust signal amplitude. The ACC at 30 cm for each participant (denoted as U1, U2, ..., U30) is detailed in Figure 9. Notably, *mmPalm* achieves ACCs of 100.00% for most participants. The high authentication accuracy demonstrates that *mmPalm* can precisely authenticate legitimate users through palm-reflected mmWave signals and effectively distinguish them from unauthorized individuals.

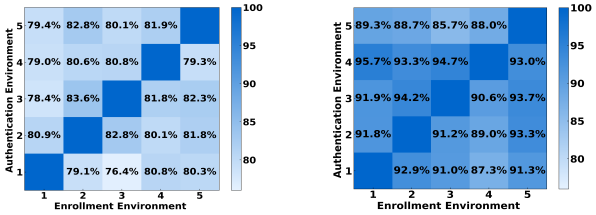
C. Impact of Palm-Device Distance and Palm Orientation

To explore the *mmPalm*'s robustness against variations in palm-device distance and palm orientation, we evaluate it's performance when enrollment and authentication signals are collected under different distances and orientations.



(a) With distance discrepancy (b) With orientation discrepancy

Fig. 10. Authentication accuracy before and after involving palm profile augmentation on different palm-device distances and orientations between the enrollment and authentication data.



(a) Without adaptation (b) With adaptation

Fig. 11. Performance without and with cross-environment adaptation.

Experimental Setup. We collect palm-reflected signals from 10 participants at the same environment. During the enrollment phase, we construct palm profile by collecting palm-reflected signals with the user's palm approximately 30 cm from the mmWave device. In the authentication phase, participants are allowed to place their palms at random distances (within 5 cm) from the original palm location along the x-, y-, and z-axis to collect signals. We further evaluate *mmPalm*'s robustness against variations in palm orientation. In the authentication phase, the palm is rotated within 30° clockwise along the x-, y-, and z-axis relative to the enrollment phase palm position. The average ACC of 10 participants are measured to evaluate the system robustness. We show the average ACC before and after applying palm profile augmentation to demonstrate that our proposed augmentation approach effectively creates robust palm profiles for each user.

Evaluation Results. We present the average ACC with different palm-device distance during enrollment and authentication phase in Figure 10(a). Without palm profile augmentation, *mmPalm* achieves an ACC of 61.64% (z-axis). After palm profiles augmentation, the ACC improves to 97.98%. We also illustrate the average ACC with palm orientation discrepancy in Figure 10(b). Specifically, *mmPalm* achieves an ACC of 77.54% (y-axis) without palm profile augmentation. After applying palm profile augmentation, the ACC significantly improves to 99.76%. This high authentication accuracy after augmenting palm profiles indicates that *mmPalm* can effectively authenticate users in practical scenarios.

D. Impact of Environment Changes

To evaluate *mmPalm* under unpredictable multipath arising from different environments, we conduct experiments in the aforementioned five different environments.

Experimental Setup. During the enrollment phase, we randomly select 2 environments as enrollment settings. 5 volunteers (nonusers) are recruited to provide their palm profiles in both environments, which helps mitigate the impact of environmental factors. 10 users are asked to provide palm profiles in only one of the environments to train the user classifier. In the authentication phase, we validate *mmPalm* by leveraging users' palm-reflected signals collected from an environment completely different from those used in the enrollment phase. We sequentially select each environment as the authentication setting and summarize the accuracy (ACC) associated with different environments, evaluating the impact of multipath effects caused by environmental changes.

Evaluation Results. We summarize the evaluation results of the impact of environmental changes on authentication accuracy in Figures 11(a) and 11(b). We define each environment as a authentication scenario where the users provide the palm data for authentication. And randomly select another environment as the enrollment scenario, where the legitimate users provide their palm profile. When the cross-environment adaptation module is not included in the system, it achieves authentication accuracy ranging from 76.4% to 83.6%, as shown in Figure 11(a). This demonstrates that further removal of environmental factors is necessary to enhance authentication accuracy. Incorporating the cross-environment adaptation module results in improved system performance, with accuracy between 85.7% and 95.7%, and an average accuracy improvement of 10.21%, as illustrated in Figure 11(b). The consistent and significant improvements in authentication accuracy across various settings highlight *mmPalm*'s ability to extract environment-independent features from palmprint, emphasizing the system's adaptability to dynamic environments with low training effort.

VI. Performance under Different Spoofing Attack

A. Performance Under Random Attack

We first evaluate our system against random attacks, where the attackers attempt to bypass *mmPalm* without any prior knowledge of the palm-related biometrics of legitimate users.

Experimental Setup. We recruit 10 participants as legitimate users. These users are asked to register their palms around 30 cm away from the *mmPalm* system. We then recruit another 10 participants, who have no prior knowledge of our system, to act as attackers. These individuals are selected without consideration of palm size. Each attacker is instructed to simply place their palm in front of the mmWave device to initiate the authentication session and simulate an attack on each legitimate user. Data from both the legitimate users and attackers are collected under identical environmental conditions.

Evaluation Results. The attack success rate of random attack is 0%, which supports *mmPalm*'s capability of rejecting unauthorized users during authentication. The resilience of *mmPalm* against random attacks further validates that the palm profiles are distinct among different users and hard be replicated by attackers.

B. Performance Under Impersonation Attack

We then evaluate *mmPalm* performance under impersonation attacks, where the attackers attempt to gain unauthorized access by mimicking the observed palm of legitimate users.

Experimental Setup. To simulate this impersonation attack, we involve 24 participants, selecting one at a time as the

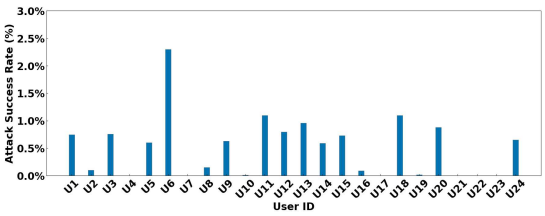


Fig. 12. Attack success rate under impersonation attacks.

legitimate user. Five participants with similar palm sizes to the legitimate user are chosen to act as attackers, attempting to mimic the legitimate user's palm placements. The remaining participants acted as unauthorized adversaries. The average ASR of 5 attackers is calculated to evaluate *mmPalm*'s robustness against impersonation attacks.

Evaluation Results. The average attack success rate of 24 users under impersonation attack is 0.52%. In Figure 12, we notice that the majority of impersonation attackers achieve an attack success rate below 1%. This demonstrates our system's efficacy in preventing in-person biometric forgeries and confirming the robustness of palm biometrics against such attempts due to the challenge in imitating palm geometry, skin thickness, and palm texture.

C. Performance Under Counterfeit Attack

An attacker may attempt an intrusion by using a 2D counterfeit palm approximating the target user's palm dimensions. A sophisticated adversary could leverage 3D scanning and printing technologies to create a replica with precise palm measurements.

Experimental Setup. We designate a volunteer as the victim and fabricated a 2D imitation palm from cardboard and a 3D imitation from plaster. These attack scenarios are depicted in Figure 13. During each authentication attempt, the adversary positions the faux palm before the mmWave device, maintaining consistent placement and orientation to initial verification.

Evaluation Results. Both the 2D decoy palm and the 3D counterfeit palm achieve 0% attack success rate. These findings indicate that replicating palm size and contour alone is insufficient to compromise our system. This observation confirm that the palmprint characteristics extracted by *mmPalm* are sufficiently distinctive, thereby enhancing the system's resistance to counterfeit attacks.

VII. Related Work

Authentication via Human Biometrics. Existing authentication scheme via user biometrics usually rely on users' physiological traits, including faces [2], fingerprints [1], voices [25], retina or iris [26], and behaviour-associated features [27]. Although these unique user biometrics enhance the authentication effectiveness and convenience over traditional approaches (e.g., PIN, token), their high implementation costs (e.g., cameras, sensors, or microphones) limit widespread adoptions in ubiquitous scenarios such as smart cities and smart homes.

Sensing User Palm Characteristics. Recent works have explored measuring users' palm geometry via cameras [28, 3] and acoustic signals [9, 10]. For instance, PalmID [28] employs cameras to capture palm images, extracts distinct line and ridge

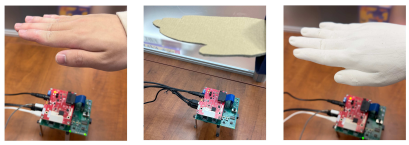


Fig. 13. Physically reproducing palm biometrics using a 2D imitation palm from cardboard and a 3D imitation palm from plaster.

features, and generates a palm profile for each user. Acoustic-based methods focus on extracting the response patterns of acoustic signals that propagate through users' palms to authenticate users. EchoLock [9] senses hand geometry via emitted acoustic signals on smartphones and differentiates users via the unique sound reflection patterns. These methods typically require access to cameras or mobile devices, which may hinder their widespread implementation.

User Authentication Using mmWave. Previous work demonstrate the feasibility of mmWave-based user authentication based on unique human behavior characteristics [13, 12, 29]. For instance, Han et al. develop a signature verification system by capturing hand movements during the user's signature execution process using mmWave [13]. VocalPrint exploits unique disturbances of the reflected mmWave signals caused by vocal vibrations for user authentication [14]. Existing works have also explored authenticating users via fine-grained vital sign monitoring based on mmWave signals [11, 30]. For example, HeartPrint authenticates users using a mmWave radar by sensing their distinctive heartbeat motions [11]. In addition, the mmWave signals bounced off the human face carry the facial biometric features, which allow researchers to develop face-based authentication. For example, mmFace authenticates users by matching facial structure features from mmWave signals with templates created from virtual mmWave signals, which are generated using facial photos [15]. Hof et al. utilize a dedicated mmWave radar sensor equipped with a total of 1024 unique antenna element pairs to collect extensive facial biometric data, which is then used for facial verification [31]. In contrast to these approaches, *mmPalm* only requires the users to raise their hands for authentication, which is user-friendly in practical use. Moreover, *mmPalm* is not significantly impacted by users' physiological status (e.g., stress level), ensuring consistent and robust user authentication. In addition, we use a commercial mmWave device to capture distinctive palmprint embedded in the reflected signals from human palms without external devices. Our approach is low-cost, low-effort, and can be ubiquitously deployed in many smart applications.

VIII. Conclusion

In this paper, we develop *mmPalm*, a low-cost and ubiquitous palm-based user authentication system using a commercial mmWave device, marking a significant step in contactless authentication. The core idea of our work is to harness high-resolution mmWave signals to extract detailed palm characteristics that can assemble distinctive palmprints for user authentication. To accurately capture these palmprints, we construct multiple virtual antennas on a commercial mmWave device to capture detailed palmprint features from various angles.

We also develop palm detection and segmentation algorithms to isolate mmWave signals primarily reflected from palms, ensuring the precise extraction of fine-grained palm biometrics. To accommodate variations in palm-device distances and orientations, we develop a systematic data collection strategy and a conditional generative method to synthesize virtual palm profiles, reducing the need for extensive manual data collection and labeling. Furthermore, we develop a robust feature extractor, which effectively ensures that palm features are resistant to environmental variations. This allows the system to operate efficiently across various settings with a single registration of palm profiles. Extensive experiments show that *mmPalm* achieves high authentication accuracy with resilience against different types of attacks.

IX. Acknowledgment

This work was partially supported by the National Science Foundation Grants CNS2120396, CCF2211163, IIS2311596, CNS2329278, CCF1909963, CNS2120350, III2311598, CNS2120276, CNS2145389, IIS2311597, CNS2304766, and CNS2329280.

References

[1] K. K. Shreyas, S. Rajeev, K. Panetta, and S. S. Agaian, "Fingerprint authentication using geometric features," in *2017 IEEE International Symposium on Technologies for Homeland Security (HST)*. IEEE, 2017, pp. 1–7.

[2] S. Sawhney, K. Kacker, S. Jain, S. N. Singh, and R. Garg, "Real-time smart attendance system using face recognition techniques," in *2019 9th international conference on cloud computing, data science & engineering (Confluence)*. IEEE, 2019, pp. 522–525.

[3] C. Burt, "Popid adds palm for multimodal payments with redrock partnership: Biometric update," Apr 2023, https://www.biometricupdate.com/202304/popid-adds-palm-for-multimodal-payments-with-redrock-partnership.

[4] A. N. Uwaechia and N. M. Mahyuddin, "A comprehensive survey on millimeter wave communications for fifth-generation wireless networks: Feasibility and challenges," *IEEE Access*, vol. 8, pp. 62 367–62 414, 2020.

[5] Qualcomm, "High throughput and ultra-low latency: Benefits of 5g mmwave technology," https://www.qualcomm.com/research/5g/5g-nr/mmwave, 2023, accessed: 2024-04-16.

[6] R. Sanchez-Reillo, C. Sanchez-Avila, and A. Gonzalez-Marcos, "Biometric identification through hand geometry measurements," *IEEE Transactions on pattern analysis and machine intelligence*, vol. 22, no. 10, pp. 1168–1171, 2000.

[7] S. Alekseev, A. Radzievsky, M. Logani, and M. Ziskin, "Millimeter wave dosimetry of human skin," *Bioelectromagnetics: Journal of the Bioelectromagnetics Society, The Society for Physical Regulation in Biology and Medicine, The European Bioelectromagnetics Association*, vol. 29, no. 1, pp. 65–70, 2008.

[8] A. Kumar, D. C. Wong, H. C. Shen, and A. K. Jain, "Personal verification using palmprint and hand geometry biometric," in *Audio-and Video-Based Biometric Person Authentication: 4th International Conference, AVBPA 2003 Guildford, UK, June 9–11, 2003 Proceedings 4*. Springer, 2003, pp. 668–678.

[9] Y. Yang, Y. Wang, Y. Chen, and C. Wang, "Echolock: Towards low-effort mobile user identification leveraging structure-borne echos," in *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*, 2020, pp. 772–783.

[10] C. Wu, J. Chen, K. He, Z. Zhao, R. Du, and C. Zhang, "Echohand: High accuracy and presentation attack resistant hand authentication on commodity mobile devices," in *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, 2022, pp. 2931–2945.

[11] Y. Wang, T. Gu, T. H. Luan, M. Lyu, and Y. Li, "Heartprint: Exploring a heartbeat-based multiuser authentication with single mmwave radar," *IEEE Internet of Things Journal*, vol. 9, pp. 25 324–25 336, 2022. [Online]. Available: https://api.semanticscholar.org/CorpusID:251337908

[12] X. Yang, J. Liu, Y. Chen, X. Guo, and Y. Xie, "Mu-id: Multi-user identification through gaits using millimeter wave radios," in *IEEE INFOCOM 2020-IEEE Conference on Computer Communications*. IEEE, 2020, pp. 2589–2598.

[13] M. Han, H. Yang, T. Ni, D. Duan, M. Ruan, Y. Chen, J. Zhang, and W. Xu, "mmsign: mmwave-based few-shot online handwritten signature verification," *ACM Transactions on Sensor Networks*, 2023.

[14] H. Li, C. Xu, A. S. Rathore, Z. Li, H. Zhang, C. Song, K. Wang, L. Su, F. Lin, K. Ren, and W. Xu, "Vocalprint: exploring a resilient and secure voice authentication via mmwave biometric interrogation," *Proceedings of the 18th Conference on Embedded Networked Sensor Systems*, 2020. [Online]. Available: https://api.semanticscholar.org/CorpusID:227154551

[15] W. Xu, W. Song, J. Liu, Y. Liu, X. Cui, Y. Zheng, J. Han, X. Wang, and K. Ren, "Mask does not matter: Anti-spoofing face authentication using mmwave without on-site registration," in *Proceedings of the 28th Annual International Conference on Mobile Computing and Networking*, 2022, pp. 310–323.

[16] H. Liu, K. Cui, K. Hu, Y. Wang, A. Zhou, L. Liu, and H. Ma, "mtranssee: Enabling environment-independent mmwave sensing based gesture recognition via transfer learning," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 6, no. 1, pp. 1–28, 2022.

[17] T. Instruments, "Radar academy - explore node," https://dev.ti.com/tirex/explore/node?node=A__AXNV8Pc8F7j2TwsB7QnTDw__RADAR-ACADEMY__GwxShWe__LATEST, 2024.

[18] Texas Instruments, "Awr1642 single-chip 77-ghz to 79-ghz automotive radar sensor," https://www.ti.com/product/AWR1642, 2024.

[19] X. Li, X. Wang, Q. Yang, and S. Fu, "Signal processing for tdm mimo fmcw millimeter-wave radar sensors," *IEEE Access*, vol. 9, pp. 167 959–167 971, 2021.

[20] A. Inc. (2024) Apple support: Official support. https://support.apple.com/en-us/108411. Accessed: 2024-06-23.

[21] M. Mirza and S. Osindero, "Conditional generative adversarial nets," *arXiv preprint arXiv:1411.1784*, 2014.

[22] D. Arthur and S. Vassilvitskii, "k-means++: the advantages of careful seeding," in *Proceedings of the Eighteenth Annual ACM-SIAM Symposium on Discrete Algorithms*, ser. SODA '07. USA: Society for Industrial and Applied Mathematics, 2007, p. 1027–1035.

[23] H. Li, S. J. Pan, S. Wang, and A. C. Kot, "Domain generalization with adversarial feature learning," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2018, pp. 5400–5409.

[24] J. Mairal, F. Bach, J. Ponce, and G. Sapiro, "Online learning for matrix factorization and sparse coding." *Journal of Machine Learning Research*, vol. 11, no. 1, 2010.

[25] N. Singh, A. Agrawal, and R. Khan, "Voice biometric: A technology for voice based authentication," *Advanced Science, Engineering and Medicine*, vol. 10, no. 7-8, pp. 754–759, 2018.

[26] A. Kumar and A. Passi, "Comparison and combination of iris matchers for reliable personal authentication," *Pattern recognition*, vol. 43, no. 3, pp. 1016–1026, 2010.

[27] M. Shahzad, A. X. Liu, and A. Samuel, "Behavior based human authentication on touch screen devices using gestures and signatures," *IEEE Transactions on Mobile Computing*, vol. 16, pp. 2726–2741, 2017. [Online]. Available: https://api.semanticscholar.org/CorpusID:38908203

[28] "Palmid," https://www.redrockbiometrics.com/, 2018.

[29] Y. Xie, R. Jiang, X. Guo, Y. Wang, J. Cheng, and Y. Chen, "mmfit: Low-effort personalized fitness monitoring using millimeter wave," in *2022 International Conference on Computer Communications and Networks (ICCCN)*. IEEE, 2022, pp. 1–10.

[30] Y. Wang, T. Gu, T. H. Luan, and Y. Yu, "Your breath doesn't lie: Multi-user authentication by sensing respiration using mmwave radar," *2022 19th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, pp. 64–72, 2022. [Online]. Available: https://api.semanticscholar.org/CorpusID:253123244

[31] E. Hof, A. Sanderovich, M. Salama, and E. Hemo, "Face verification using mmwave radar sensor," in *2020 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*. IEEE, 2020, pp. 320–324.