

# Exploring Reliable PPG Authentication on Smartwatches in Daily Scenarios

JIANKAI TANG\*, Key Laboratory of Pervasive Computing, Ministry of Education, Department of Computer Science and Technology, Tsinghua University; Ant Group, China

JIACHENG LIU\*, Key Laboratory of Pervasive Computing, Ministry of Education, Department of Computer Science and Technology, Tsinghua University, China

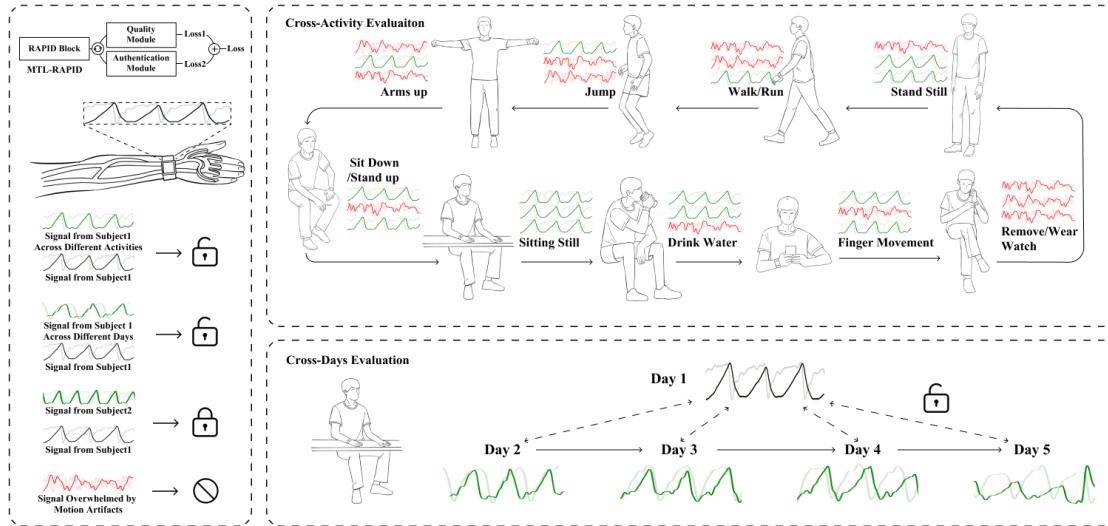
RENLING TONG, KAI ZHU, and ZHE LI, Ant Group, China

XIN YI, Key Laboratory of Pervasive Computing, Ministry of Education, Department of Computer Science and Technology, Tsinghua University, China

JUNLIANG XING, Key Laboratory of Pervasive Computing, Ministry of Education, Department of Computer Science and Technology, Tsinghua University, China

YUANCHUN SHI, Key Laboratory of Pervasive Computing, Ministry of Education, Department of Computer Science and Technology, Tsinghua University, China and Intelligent Computing and Application Laboratory of Qinghai Province, Qinghai University, China

YUNTAO WANG<sup>†</sup>, Key Laboratory of Pervasive Computing, Ministry of Education, Department of Computer Science and Technology, Tsinghua University, China



**Fig. 1. MTL-RAPID makes PPG authentication on smartwatches more reliable.** MTL-RAPID simultaneously assesses signal quality and verifies user identity with only 80k parameters. User studies were conducted to evaluate its performance under cross-activity and cross-day scenarios.

Photoplethysmography (PPG) Sensors, widely deployed in smartwatches, offer a simple and non-invasive authentication approach for daily use. However, PPG authentication faces reliability issues due to motion artifacts from physical activity and physiological variability over time. To address these challenges, we propose MTL-RAPID, an efficient and reliable PPG authentication model, that employs a multitask joint training strategy, simultaneously assessing signal quality and verifying user identity. The joint optimization of these two tasks in MTL-RAPID results in a structure that outperforms models trained on individual tasks separately, achieving stronger performance with fewer parameters. In our comprehensive user studies regarding motion artifacts ( $N = 30$ ), time variations ( $N = 32$ ), and user preferences ( $N = 16$ ), MTL-RAPID achieves a best AUC of 99.2% and an EER of 3.5%, outperforming existing baselines. We open-source our PPG authentication dataset along with the MTL-RAPID model to facilitate future research on GitHub.

CCS Concepts: • Security and privacy → Biometric Authentication; Usability in security and privacy.

Additional Key Words and Phrases: Photoplethysmography, Smartwatch authentication, Multi-task Learning

**ACM Reference Format:**

Jiankai Tang, Jiacheng Liu, Renling Tong, Kai Zhu, Zhe Li, Xin Yi, Junliang Xing, Yuanchun Shi, and Yuntao Wang. 2025. Exploring Reliable PPG Authentication on Smartwatches in Daily Scenarios. 1, 1 (April 2025), 26 pages. <https://doi.org/10.1145/nnnnnnn.nnnnnnn>

## 1 Introduction

As smartwatches become increasingly integrated into daily life, reliable authentication is crucial for safeguarding sensitive data, such as health information, messages, and payment details. Smartwatches frequently store personal data and act as access points for connected devices or services [19, 50], making them attractive targets for unauthorized access. As their functionality expands, implementing reliable authentication methods is imperative to prevent unauthorized access and data breaches.

Traditional PIN-based authentication on smartwatches poses challenges due to small screens, slower input speeds, and usability issues during movement [35]. These factors also lead to security risks, as users often choose simpler PINs, making them vulnerable to shoulder surfing [10, 56]. Similarly, static biometric authentication methods, such as fingerprint and facial recognition, provide user-friendly and secure alternatives but require additional sensors, which

---

<sup>\*</sup>Equal contributions.

<sup>†</sup>Corresponding author.

---

Authors' Contact Information: Jiankai Tang, tjk24@mails.tsinghua.edu.cn, Key Laboratory of Pervasive Computing, Ministry of Education, Department of Computer Science and Technology, Tsinghua University; Ant Group, China; Jiacheng Liu, Key Laboratory of Pervasive Computing, Ministry of Education, Department of Computer Science and Technology, Tsinghua University, China; Renling Tong, Kai Zhu, Zhe Li, Ant Group, China; Xin Yi, Key Laboratory of Pervasive Computing, Ministry of Education, Department of Computer Science and Technology, Tsinghua University, China; Junliang Xing, Key Laboratory of Pervasive Computing, Ministry of Education, Department of Computer Science and Technology, Tsinghua University, China; Yuanchun Shi, Key Laboratory of Pervasive Computing, Ministry of Education, Department of Computer Science and Technology, Tsinghua University, China and Intelligent Computing and Application Laboratory of Qinghai Province, Qinghai University, China, shiyc@tsinghua.edu.cn; Yuntao Wang, yuntaowang@tsinghua.edu.cn, Key Laboratory of Pervasive Computing, Ministry of Education, Department of Computer Science and Technology, Tsinghua University, China.

---

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

© 2025 Copyright held by the owner/author(s). Publication rights licensed to ACM.

Manuscript submitted to ACM

can increase the size and weight of smartwatches, reducing their convenience. Bluetooth-based authentication, though convenient, introduces proximity-based risks such as interception or spoofing [48]. These challenges highlight the need for adaptive, secure, and user-friendly authentication solutions specifically designed for wearable devices.

Photoplethysmography (PPG), a commonly used technique in smartwatches for health monitoring, offers a promising alternative for authentication. PPG measures blood volume changes in the microvascular bed of tissues and can extract physiological signals such as heart rate and blood oxygen levels. More importantly, PPG data reveals distinctive physiological patterns unique to each individual, enabling its use for biometric authentication, commonly referred to as PPG authentication [4]. This method does not require additional hardware, making it highly practical and cost-effective for broad adoption. By analyzing PPG data, a smartwatch can provide non-invasive, efficient authentication, enhancing both security and user convenience [47].

However, despite its potential, the reliability of PPG authentication in real-world scenarios remains a challenge. Daily activities involving significant hand movements or physical exercise can introduce motion artifacts that can affect the accuracy and reliability of the authentication process. Moreover, managing power consumption is critical for smartwatch authentication design. Therefore, efficient PPG authentication algorithms are necessary to allow frequent authentication without frequent recharging [6], ensuring security while maintaining usability and appeal for everyday wear. These issues underscore the need for efficient, reliable authentication methods capable of managing variability and ensuring consistent performance even in dynamic conditions [47, 51].

In this paper, we explore efficient and reliable PPG on smartwatches for daily scenarios. Our approach proactively detects suitable conditions for authentication and performs the authentication task without requiring active unlocking at the moment of use, allowing the user seamless and uninterrupted access. To achieve this, we proposed the **Multi-Task Learning Reliable and Accurate PPG-based model for efficient ID authentication (MTL-RAPID)**, specifically designed to address the challenges of PPG-based authentication for daily scenarios. Our MTL-RAPID model utilizes a multi-task joint architecture to extract and analyze global and local vascular features, heartbeat patterns, and human motion forms from PPG signals, along with their interrelationships. By adjusting the passing rate of the quality assessment task, we can adapt authentication strength to various scenarios. With only 80k parameters, our method offers efficient and accurate quality assessment and identity verification, making it ideal for deployment on smartwatches. Our main contributions are as follows:

- (1) We introduced MTL-RAPID, a lightweight model designed to assess PPG signal quality and perform authentication simultaneously, enabling reliable smartwatch authentication in daily scenarios.
- (2) We conducted three user studies to evaluate the reliability of the MTL-RAPID model on cross-activity ( $N = 30$ ), cross-day ( $N = 32$ ) and user preference ( $N = 16$ ), achieving 99.2% AUC and 3.5% EER at best, with significant user preference over PIN methods.
- (3) We open-sourced a PPG authentication dataset spanning multiple daily activities, along with the MTL-RAPID model, to enhance reproducibility and encourage the widespread adoption of PPG-based authentication (see supplementary materials).

## 2 Related Work

We first reviewed existing authentication methods on smartwatches from traditional unlock patterns to new biometric approaches. We then discuss the reliability of those authentication methods in real-life mobile scenarios. At last, we investigated unsupervised and supervised PPG authentication methods.

## 2.1 Authentication Methods on Smartwatches

Explicit authentication methods, such as PINs and graphical patterns, though widely used, are plagued by significant usability issues due to the small size of smartwatch screens, necessitating precise inputs [35]. These methods also suffer from security vulnerabilities; simplistic and memorable choices by users make these methods prone to attacks, with an attacker potentially cracking 4.6% of 4-digit PINs within 10 online guesses [30]. Pattern authentication is similarly risky, with crack rates varying from 13.33% to 32.55% in different studies [2, 3], influenced by well-documented biases [33]. Levy et al. [23] proposed an authentication method when users write signatures, achieving an EER of 2.36% and an AUC of 98.52% ( $N = 66$ ). These explicit methods have shown promising performance but require additional effort from users.

Implicit biometric authentication presents an alternative by using physiological or behavioral traits, which show promise in improving security without the cumbersome input methods. Cornelius et al. [5] achieved a 13.1% Equal Error Rate (EER) using on-wrist bioimpedance ( $N = 8$ ), highlighting its potential for secure authentication. Low-frequency vibration responses measured by Lee et al. [21] initially showed a promising 1.37% EER ( $N = 19$ ), but a rise to 4.99% FRR over a week suggests issues with long-term stability. Acoustic response with retraining classifiers utilized by Huh et al. [13] achieves 0.79% EER on recall-session study ( $N = 20$ ). While these methods demonstrate effectiveness, they either require additional sensors or have been validated only on small sample sizes.

PPG authentication on smartwatches presents a viable alternative due to its widespread use and low power consumption compared to other biometric methods. Shang and Wu [51] were the first to explore the feasibility of combining PPG with gesture-based authentication, achieving a 91.6% true rejection rate using wrist-worn sensors across 12 subjects. In a separate study, Zhao et al. [61] reported a 90.7% accuracy using a gradient boosting tree method for PPG-based authentication on smartwatches with 20 participants across hours in a single day. Differing from these initial approaches, our research expands the field by conducting user studies with more participants with longer time intervals between sessions to address real-world challenges.

## 2.2 Reliable Authentication in Mobile Scenarios

Reliable authentication, particularly in mobile environments, has become a critical focus in the security domain. Traditional methods such as passwords and explicit biometric verification(e.g., face [28, 36], fingerprint) are known for their high reliability but often interrupt the user's workflow. In contrast, implicit authentication methods aim to enhance user experience by seamlessly integrating into daily activities(e.g., pick-up [22]). These methods analyze subtle behavioral features such as gait patterns [34], touch posture [31, 60], and voice identification [45] to verify a user's identity without their active participation.

Despite the appeal of implicit methods for their unobtrusive nature, they often fall short in reliability when compared to traditional authentication methods. The primary challenge is their unstable performance in uncontrolled environments, leading to redundant and potentially frustrating authentication checks [9, 29, 37, 38]. Addressing these reliability issues is essential for their potential widespread commercial adoption and the overall enhancement of security in mobile scenarios.

### 2.3 Photoplethysmography (PPG) Authentication Methods

Photoplethysmography (PPG) authentication has been extensively explored, though most studies have focused on feasibility studies using fingertip PPG datasets [17, 18, 20, 26, 32, 39, 46]. Only a few have tested methodologies on wrist-worn devices [51, 61] as detailed in section 2.1.

Unsupervised algorithms in PPG authentication typically involve extracting features from both the time domain (e.g., peaks, intervals, slopes) and the frequency domain of the PPG signal. Methods such as peak detection, cross-correlation, Continuous Wavelet Transform (CWT), Principal Component Analysis (PCA), K-Nearest Neighbors (KNN), Linear Discriminant Analysis (LDA), and Naive Bayes classifier (NBC) are employed to cluster and identify patterns without relying on previously labeled data [4, 16, 46, 59].

On the other hand, supervised algorithms use labeled classes to learn discriminative features crucial for authentication. Techniques include convolutional neural networks (CNNs), long short-term memory (LSTM), auto encoder (AE) and others. Luque et al. [26] introduced an end-to-end network, Pu et al. [41] utilized an auto encoder to transform PPG into latent space, and Wan et al. [57] developed a deep CNN model that extracts features from both time-domain and frequency-domain signals. Despite their promising results, these methods exhibit limitations, such as the use of excessively long segments (45-60 seconds) for authentication, which is impractical for everyday use [58]. Unfortunately, some studies lack clarity regarding dataset selection, testing procedures, segment length, the number of segments evaluated, and whether segments span different subjects.

To overcome these limitations, we have organized and open-sourced our code and datasets (see supplementary materials), enhancing transparency and enabling fair comparative analysis with the state-of-the-art algorithms [1, 14, 57]. To the best of our knowledge, we are the first to introduce the multi-task architecture based on the PPG optical principle for authentication, significantly enhancing efficiency and reliability under variable conditions.

## 3 Reliable and Accurate PPG-based model for efficient ID authentication (MTL-RAPID)

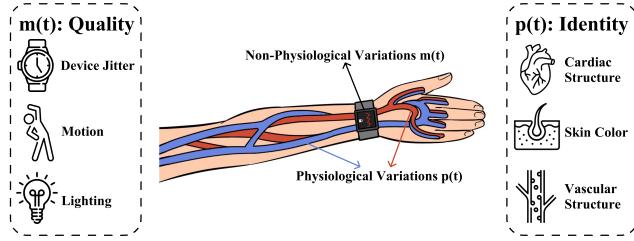
In the methodological section of this paper, we introduce Multi-Task Learning Reliable and Accurate PPG-based model for efficient ID authentication (**MTL-RAPID**). We first present our optical basis in Section 3.1 and describe the architecture of the basic RAPID block in Section 3.2 and MTL-RAPID model in Section 3.3. We justify the algorithmic principles of PPG that guide our model design in Section 3.4. Based on the MTL-RAPID, we introduce the authentication procedure (i.e., registration and authentication) in Section 3.5. We also included the preprocess and evaluation setup in Section 3.6 and Section 3.7.

### 3.1 Optical Principle

Our foundational optical model uses Shafer's Dichromatic Reflection Model [49] to analyze PPG signals. Our goal is to accurately extract vascular features, heartbeat patterns, and human motion forms along with their interrelationships from PPG, thereby enabling identity verification and quality assessment. We consider the PPG values captured by the photodetector sensor represented as follows:

$$\mathcal{C}_k(t) \approx \mathbf{u}_s \cdot I_0 \cdot \Phi(m(t), p(t)) + \mathbf{u}_p \cdot I_0 \cdot p(t) + \mathbf{v}_n(t) + I_{ds} \quad (1)$$

In Eqn. (1),  $I_0$  represents the luminance intensity level, relatively constant in wearable devices.  $\mathbf{u}_d$  denotes the unit color vector of skin tissue, while  $\mathbf{u}_p$  indicates the relative pulsatile strengths influenced by the absorption properties of hemoglobin and melanin.  $p(t)$  captures the physiological changes, including individual-specific arterial characteristics



**Fig. 2. Optical Principle.** PPG signals contain two key components: non-physiological variations  $m(t)$ , influenced by external factors like lighting, body movements, and jitter, and physiological variations  $p(t)$ , driven by heart activity, vascular structure, and skin anatomy.

and heartbeat patterns, which are fundamental to identity verification tasks based on PPG signals. The variable  $m(t)$  encompasses all non-physiological variations, such as fluctuations in lighting, body movements, and the jitter of wearable devices.  $\sigma_n(t)$  accounts for the quantization noise inherent in the sensor, and finally  $I_{ds}$  denotes other components that can be seen as constant.

Due to the entanglement between  $m(t)$  and  $p(t)$ ,  $m(t)$  can interfere with the extraction of  $p(t)$  features. Therefore,  $m(t)$  contains quality information of the PPG signal and can be used to assess whether a specific PPG signal is suitable for identity verification tasks. Thus, it is crucial to use a method that can simultaneously extract features of  $m(t)$  and  $p(t)$ , as well as their interactions, for reliable PPG-based identity verification.

### 3.2 RAPID Block

The RAPID block is a module we designed for PPG identity verification and waveform quality assessment tasks. Inspired by the Gao et al. MTL network NDDR-CNN [8], we designed separate paths within the block to extract features for each task. We then merge the features from both tasks through concatenation, enabling multi-task training.

As illustrated in the RAPID block shown in Figure 3, it consists of two main components: the Quality Path and the Identity Path. The Quality Path is better suited for extracting local quality information from PPG signals. These quality features manifest as signal distortion and waveform chaos, typically due to motion and device jitter, and correspond to the  $m(t)$  component in Eqn. (1). The Identity Path, due to its larger receptive field, is more suitable for extracting temporal features rich in user identity information, reliably learning the  $p(t)$  component in Eqn. (1).

To streamline our model while retaining its architecture, we incorporated a bottleneck layer inspired by the InceptionTime model [14], reducing the input vector's dimension and model complexity. Finally, we integrate SENet [12] to introduce an attention mechanism to help the model choose important features automatically.

### 3.3 MTL-RAPID

In practical applications, noise in the data can significantly impact the accuracy of authentication models. Therefore, it is crucial to first filter the signals using a waveform quality classifier.

Our MTL model comprises a shared-bottom model consisting solely of three identical RAPID blocks. Inspired by the HyperFace architecture [42], we utilize one shared RAPID block to extract various shallow features from PPG waveforms, which apply to both tasks. Additionally, the shared module is responsible for learning the complex interrelationships between waveform quality and physiological features, represented by the function  $\Phi$  in Eqn. (1). However, due to the

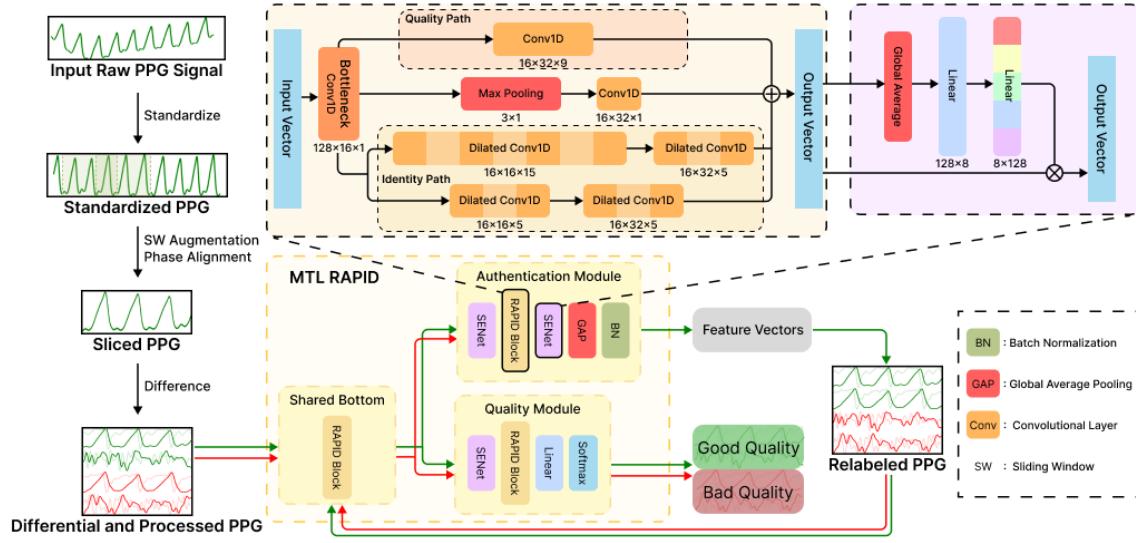


Fig. 3. **MTL-RAPID architecture.** We propose a multi-task RAPID model and switch training procedure to accomplish waveform quality assessment and identity verification tasks simultaneously.

significant differences in the features required for waveform quality assessment and identity verification tasks, our MTL model does not have a large shared module, and simple task-specific sub-networks consist only of a few simple linear layers, like most image recognition MTL models [27, 42]. Consequently, we have configured both task-specific sub-networks to be identical RAPID blocks.

**3.3.1 Mode switch.** The task of PPG waveform quality assessment and identity verification in our system follows a sequential relationship. Specifically, the PPG signal first undergoes waveform inspection to filter out motion samples, after which the remaining samples are subjected to identity verification. This sequential relationship distinguishes itself from the parallel relationship commonly seen in image recognition tasks, where multiple advanced features are extracted simultaneously from the same image [27, 42]. Due to the unidirectional flow of information in serial tasks, which requires altering the flow of information depending on the task being performed, we have implemented a mode switch following the shared module. This switch controls whether the information enters the quality assessment or the identity verification module.

**3.3.2 MTL training approach.** Noise is a common issue in wrist PPG datasets, which can negatively impact the training of identity verification models. Although the participants' movement states are labeled during data collection, different movement states may not necessarily indicate the suitability of the signals for identity verification tasks due to possible physiological changes. Therefore, to address the absence of suitable labels for training quality assessment modules within the dataset, we employ an MTL training approach with a label correction mechanism. This method simultaneously trains both the quality assessment and identity verification modules. We use the identity verification module's ability to authenticate correctly as a standard; during training, we reassign quality labels to signal segments based on this criterion.

### 3.4 Justify MTL RAPID Design for PPG Authentication

In designing of our multi-task learning (MTL) model, we prioritize two crucial factors: reliability and efficiency. Authentication scenarios can range from typical daily interactions to situations demanding high security. To accommodate this variability, our model incorporates an adjustable threshold within the quality assessment module during the authentication process. This adaptability allows us to finely balance authentication strength with usability, tailoring the security measures to fit the context of use.

Efficiency is achieved by integrating multiple tasks within a single model framework, rather than maintaining separate models for each task. This unified approach not only simplifies the system architecture but also reduces the computational overhead involved in running parallel models. By consolidating tasks, our MTL model enhances processing speed and resource utilization, making it significantly more efficient for future deployment in practical applications where both performance and power consumption are critical considerations.

### 3.5 Authentication Procedure

The PPG authentication system facilitates natural user authentication through passive interaction, removing the need for active user operations such as input or touch. The authentication process consists of two essential steps: registration and authentication.

- (1) **Registration:** Users record at least one 6-second PPG segment as their authentication template.
  - *Motion Study (Section 4.1) and Cross-day Study (Section 4.2):* A random 6-second PPG segment is selected from the database as the registered template to evaluate the authentication methods' effectiveness.
  - *Usability Study (Section 5):* Users manually record PPG data, starting with 10 seconds. If no 6-second segment passes the quality check, recording continues until a valid segment is extracted.
- (2) **Authentication:** The system compares the recorded PPG segments with existing templates to determine user identity based on segment similarity.
  - *Motion Study (Section 4.1) and Cross-day Study (Section 4.2):* PPG segments (excluding registered templates) are randomly selected as positive pairs, while segments from other users are randomly selected as negative pairs.
  - *Usability Study (Section 5):* Once worn, the smartwatch automatically collects PPG signals and unlocks if a 6-second segment passes the quality filter and identification process. Segments that fail the filter do not trigger any state change until a static PPG segment is authenticated.

### 3.6 Preprocess

The workflow for data preprocessing and signal analysis is illustrated in Figure 3. We first standardized the signals by resampling them to 60Hz. A 4th-order Butterworth filter with a frequency range of 0.5 Hz to 10 Hz was applied to ensure optimal signal clarity. To improve robustness, we incorporated a sliding window technique for data augmentation. A 6-second window with a 2-second overlap is used, starting at the first trough detected in the PPG signal to ensure phase alignment. Each signal is processed in both differentiated and non-differentiated forms before being input into the system, enhancing the model's ability to capture both transient and steady-state features.

### 3.7 Evaluation Setup

**Setup.** Our system was developed under Python 3.8 and PyTorch 2.1 framework, tested for performance on an NVIDIA GeForce RTX 4090 GPU. All random seeds were set to 2024.

**Train and test split.** In this subject-independent experiment, a five-fold cross-validation approach was used. The dataset was divided such that each fold’s test set contained 20% of the subjects, while the remaining 80% of subjects were used for training and validation. For each fold, 1,000 static pairs and 1,000 motion pairs were randomly selected, with each set consisting of 500 positive pairs and 500 negative pairs. These pairs were evenly sampled from the respective subjects (e.g., 5 subjects  $\times$  200 samples = 1,000 pairs). Positive pairs were generated by randomly selecting segments from the same subject, while negative pairs were created by pairing segments from different subjects. This method ensures a more balanced evaluation of performance across varying data quality and subject independence.

**Evaluation metrics.** We used several metrics to evaluate performance, including Area Under the Curve (AUC) and Equal Error Rate (EER), both of which provide threshold-independent insights. Higher AUC and lower EER values indicate better subject differentiation. Additionally, at a fixed False Rejection Rate (FRR) of 0.10, we measured the False Acceptance Rate (FAR) for each approach. Fixing the FRR allows us to simulate real-world conditions where a specific level of rejection tolerance is acceptable, ensuring a consistent benchmark for comparison. In practice, FAR is often a critical focus, as it indicates the likelihood of mistakenly accepting an unauthorized user, which is particularly important for security-sensitive applications. This fixed-FRR evaluation complements threshold-independent metrics, providing a more comprehensive understanding of the methods’ performance under realistic conditions. Reported metrics are averaged from 5 folds’ results.

### 3.8 Feasibility Study with Open Finger PPG Datasets

Table 1. Detailed information on the datasets used in the experiment

Dataset Name	Subject Number	Sampling Rate	Collection Device	Position	Activity Label
MIMIC-III [15]	~1400	125Hz	-	Fingertip	-
BIDMC [40]	53	125Hz	-	Fingertip	-
MMPD-S [52]	33	30Hz	HKG-07C+	Fingertip	✓
DaLiA [44]	15	64Hz	Empatica E4	Wrist	✓
ANT-Motion	30	250Hz	Maxim	Wrist	✓
	30	250Hz	Goodix	Wrist	✓
ANT-Time	32	250Hz	Maxim	Wrist	✓

**3.8.1 Dataset.** Considering the vast diversity and widespread availability of well-established PPG datasets [15, 25, 40, 52–55], we first evaluated our proposed block architecture, RAPID, using those open-source datasets. In feasibility experiment, we utilized three open-source datasets: MIMIC-III [15], BIDMC [40], and MMPD-S [52], as detailed in Table 1. These datasets primarily feature single-channel green light PPG signals and are collected from fingertip sensors for medical use.

**3.8.2 Baseline Algorithms.** We constructed the RAPID model using two blocks and compared it with existing methods. InceptionTime [14], known for time series processing, performs well but is too large to deploy on wearable devices. CorNET [1], which combines LSTM and CNN architectures, has shown decent results in PPG-based heart rate estimation and identity verification. CNN\_MFFD [57] also demonstrates robust performance using a pure CNN design. We also adapted CNN\_LSTM [7], originally used for fetal heart rate estimation, leveraging its effective frequency domain feature extraction capabilities.

Table 2. Comparison of basic model performance on identity verification task

Model	PARAMS↓	MMPD-S			MIMIC-III			BIDMC		
		AUC↑	EER↓	FAR↓	AUC↑	EER↓	FAR↓	AUC↑	EER↓	FAR↓
RAPID	38752	<b>0.95</b>	<b>0.13</b>	<b>0.15</b>	<b>0.97</b>	<b>0.07</b>	<b>0.03</b>	<b>0.97</b>	0.08	<b>0.05</b>
InceptionTime [14]	471680	0.93	0.15	0.22	<b>0.97</b>	0.08	0.04	<b>0.97</b>	<b>0.07</b>	<b>0.05</b>
CorNET [1]	88896	0.91	0.18	0.29	<b>0.97</b>	0.12	0.16	0.94	0.10	0.11
CNN_MFFD [57]	99456	0.85	0.23	0.44	0.96	0.09	0.07	0.91	0.16	0.26
CNN_LSTM [7]	571264	0.84	0.24	0.44	0.93	0.11	0.15	0.86	0.23	0.50

AUC = Area Under the Curve, EER = Equal Error Rate, FAR = False Accept Rate (When False Reject Rate = 0.10).

**3.8.3 RAPID Performs Best in Feasibility Study.** As outlined in Table 2, our RAPID model, demonstrates strong performance in all dataset tests, achieving AUC scores of 0.95 on the MMPD-S[52], 0.97 on the MIMIC-III [15], and 0.97 on the BIDMC[40] datasets, outperforming all competing baselines. The closest competitor, InceptionTime [14], was substantially larger in model size, highlighting RAPID’s efficiency and capability in extracting meaningful PPG features.

## 4 Reliable PPG Authentication on Wrist-worn Devices

### 4.1 Study 1: Reliable PPG Authentication on Daily Scenarios

To validate the performance of PPG authentication in real-life scenarios, we conducted a user study using wrist-based PPG sensors. The study evaluated the RAPID model without the quality assessment module on datasets containing both static and motion PPG signals, highlighting the challenges posed by daily activities and motion artifacts. Subsequently, we introduced our MTL-RAPID model, enhanced with quality assessment module and identity verification module. This method demonstrated robust performance on our collected ANT dataset, effectively addressing the issues associated with poor-quality PPG signals in real-world applications.

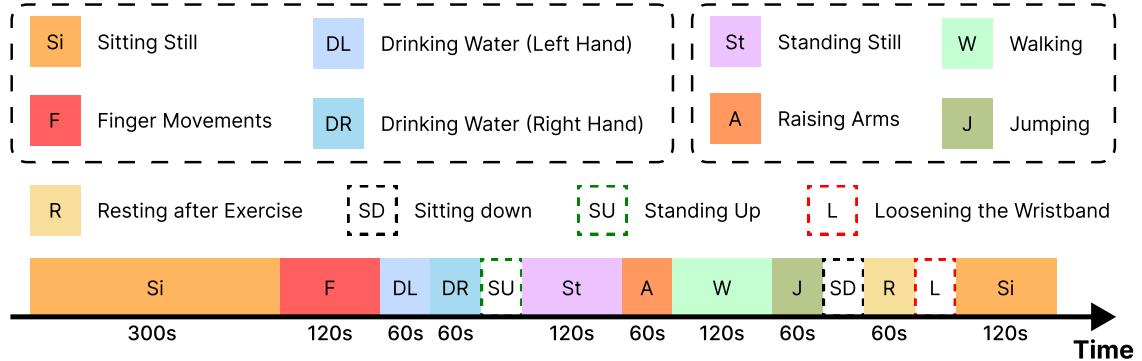


Fig. 4. **Procedure for data collection.** ANT motion dataset features 10 activities (ranging from 60 to 300 seconds) with the re-worn process.

**4.1.1 Participants and Apparatus.** We recruited 30 participants (two of them are not willing to disclose data and are not included in the following experiments) from our research institution. Among the 28 participants, all were right-handed, with an average age of 30.0 years ( $SD = 3.04$ ). The group included 16 males (57.1%) and 12 females (42.9%). Skin tones, classified using the Monk Scale<sup>1</sup>, were primarily type 3 (60.7%), followed by type 4 (21.4%), type 2 (10.7%),

<sup>1</sup>[https://en.wikipedia.org/wiki/Monk\\_Skin\\_Tone\\_Scale](https://en.wikipedia.org/wiki/Monk_Skin_Tone_Scale)

and type 5 (7.1%). Finger conditions included normal (67.9%), moist (14.3%), dry (10.7%), dirty (3.6%), and peeling (3.6%). This diverse sample provides a robust foundation for our study. The study protocols were reviewed and approved by the university's Institutional Review Board (IRB). Each participant wore wristbands equipped with two different PPG sensors: Goodix<sup>2</sup> on the left wrist and Maxim<sup>3</sup> on the right. After obtaining consent, participants were asked to perform 10 daily activities, including sitting, standing, walking, and jumping. These activities, detailed in Figure 4, were designed to simulate typical real-world usage without restricting specific movements, ensuring the data closely reflects daily behavior.



(a) Participants wearing wrist-based sensors.

(b) Goodix and Maxim sensors.

Fig. 5. Devices in the user study.

The data collected from these activities forms the Activity Noise Tracking (ANT) dataset, which addresses the limitations of prior datasets. Unlike other publicly available single-channel fingertip PPG datasets, such as MIMIC-III [15] and BIDMC [40], ANT includes three-channel data (red, green, and infrared) from wrist-worn sensors. This multi-channel approach offers a more comprehensive capture of user signals, as different wavelengths provide complementary information about the user's physiological state. Additionally, wrist-worn sensors are more suitable for everyday use compared to fingertip sensors, making the ANT dataset more relevant for evaluating systems in realistic settings.

**4.1.2 Experiments Setup.** To demonstrate the necessity and reliability of the MTL-RAPID architecture, we conducted experiments on the motion data with the RAPID model and the MTL-RAPID model.

**Experiments on the impact of motion artifacts.** We evaluated the performance of five models—InceptionTime [14], CorNET [1], CNN\_MFFD [57], CNN\_LSTM [7], and our RAPID model using the ANT dataset collected from Maxim and Goodix sensors, along with the DaLiA [44] dataset. In this experiment as Table 3, we first trained all models exclusively on static data to establish baseline performance. We then compared the performance on the complete datasets (static and motion data, denoted as mixed data) to assess how motion noise impacted identity verification accuracy.

**Experiments on MTL-RAPID effectiveness.** To assess the reliability of MTL-RAPID in real-world scenarios, we designed two distinct experimental strategies. Our MTL-RAPID model was trained jointly on diverse activity data to integrate signal quality assessment with identity verification. In comparison, baseline methods (InceptionTime [14],

<sup>2</sup>[https://www.goodix.com/en/product/sensors/health\\_sensors/gh3220t](https://www.goodix.com/en/product/sensors/health_sensors/gh3220t)

<sup>3</sup><https://www.analog.com/en/resources/reference-designs/maxrefdes280.html>

CorNET [1], CNN\_MFFD [57], CNN\_LSTM [7]) used separate training phases: their quality filters were trained on mixed data with activity labels, while verification modules were trained only on stable sitting data.

The evaluation process mirrored real-world usage through a two-stage filtering system. For each test set (2,000 sample pairs), signals were first screened by quality assessment modules with only qualified samples progressing to identity verification. This approach automatically excludes unreliable PPG segments before authentication attempts occur, closely replicating actual smartwatch operating conditions.

**4.1.3 Results. Baselines and RAPID method fail on datasets with motion artifacts.** As shown in Table 3, the RAPID model outperformed baseline methods in most cases, achieving an AUC of 0.98 on the ANT\_Maxim dataset while maintaining the smallest model size.

On mixed datasets, RAPID maintained superior performance due to its noise robustness, while all models declined in performance, reflecting the challenges of real-world applications with motion artifacts. This suggests that in practical scenarios, relying solely on identity verification models may not produce reliable results without addressing signal quality.

Experiments show that PPG signals fluctuate significantly in real-life scenarios due to sensor placement and heart rate variations. These fluctuations significantly degrade the reliability of identity verification. For example, during activities like running or gym workouts, motion noise and temporal changes often lead to incorrect identification.

To address this, we designed the MTL-RAPID model. The model evaluates data quality before proceeding with identity verification, ensuring verification is only conducted when signal quality is adequate. This approach improves system reliability and adaptability in dynamic environments.

Table 3. The Impact of Motion Data on Identity Verification Performance

Model	PARAMS↓	ANT_Maxim_static			DaLiA_static			ANT_Goodix_static		
		AUC↑	EER↓	FAR↓	AUC↑	EER↓	FAR↓	AUC↑	EER↓	FAR↓
RAPID	38752	<b>0.98</b>	<b>0.06</b>	<b>0.03</b>	0.85	0.23	0.51	<b>0.97</b>	<b>0.09</b>	<b>0.09</b>
InceptionTime [14]	471680	0.97	0.09	0.08	<b>0.87</b>	<b>0.20</b>	<b>0.36</b>	0.95	0.12	0.17
CorNET [1]	88896	0.95	0.11	0.12	0.81	0.25	0.61	0.91	0.17	0.28
CNN_MFFD [57]	99456	0.89	0.19	0.33	0.84	0.24	0.47	0.75	0.31	0.67
CNN_LSTM [7]	571264	0.80	0.27	0.54	0.75	0.32	0.66	0.66	0.39	0.76

Model	PARAMS↓	ANT_Maxim_mixed			DaLiA_mixed			ANT_Goodix_mixed		
		AUC↑	EER↓	FAR↓	AUC↑	EER↓	FAR↓	AUC↑	EER↓	FAR↓
RAPID	38752	<b>0.82</b>	<b>0.26</b>	<b>0.55</b>	0.73	0.34	0.76	<b>0.79</b>	<b>0.29</b>	<b>0.64</b>
InceptionTime [14]	471680	0.81	0.27	0.63	<b>0.75</b>	<b>0.30</b>	<b>0.69</b>	0.76	0.30	0.66
CorNET [1]	88896	0.78	0.29	0.64	0.70	0.34	0.83	0.74	0.32	0.72
CNN_MFFD [57]	99456	0.73	0.33	0.72	0.74	0.32	0.66	0.66	0.39	0.80
CNN_LSTM [7]	571264	0.68	0.37	0.75	0.59	0.43	0.87	0.59	0.44	0.85

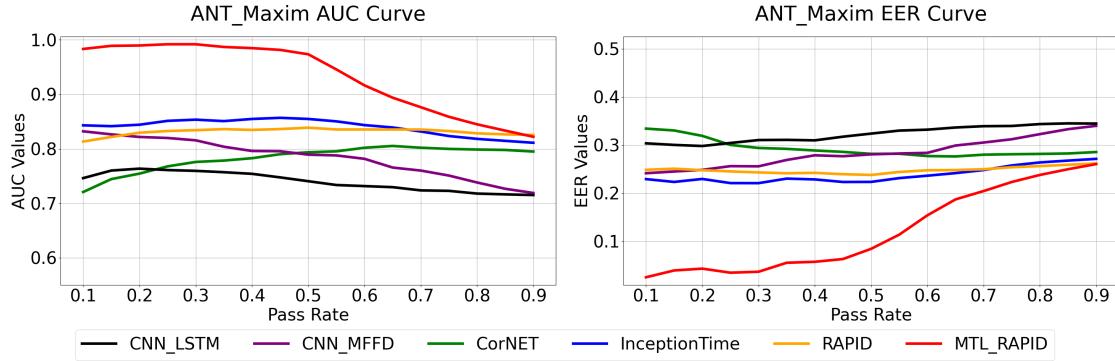
AUC = Area Under the Curve, EER = Equal Error Rate, FAR = False Accept Rate (When False Reject Rate = 0.10).

**MTL-RAPID outperforms sequentially connected models.** We compared MTL-RAPID (Section 3.3) with traditional approaches using separate quality classifiers and identity verification models. By adjusting the final classification threshold, we ensured all models were validated on an equal number of samples. The performances of ANT\_Maxim, DaLiA [44] and ANT\_Goodix are visualized in Figure 6, Figure 7 and Figure 8, where the x-axis represents the pass rate after filtering, and the y-axis displays the AUC and EER of the identity verification task.

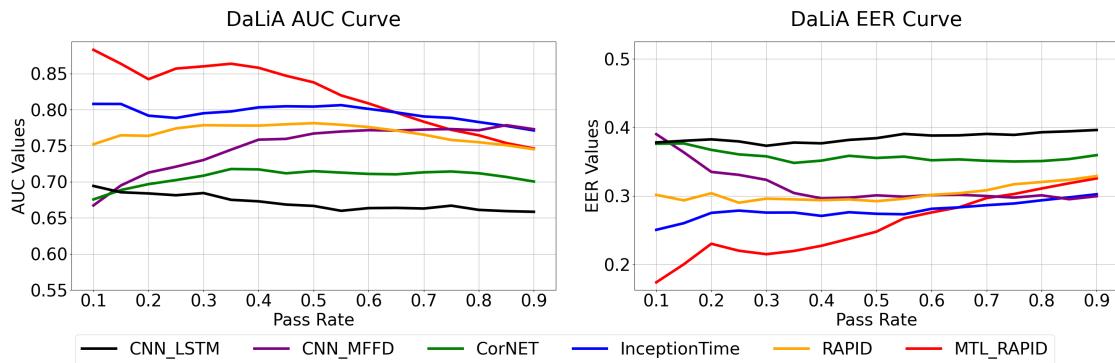
Excluding noisy samples improves AUC and reduces EER for identity verification. Notably, MTL-RAPID consistently outperforms separate RAPID models and other methods, regardless of the number of remaining sample pairs. This advantage stems from the simultaneous training of the quality assessment and authentication modules in MTL-RAPID,

enabling the model to learn inter relationships between these tasks. At a pass rate of approximately 25%, MTL-RAPID achieved an AUC of **99.2%** and an EER of **3.5%** on the ANT\_Maxim dataset, demonstrating its reliability in handling noisy data from daily activities.

Adjusting classification thresholds enables flexible trade-offs between data availability and authentication performance. For instance, in low-risk scenarios like message checks, a higher pass rate enhances convenience. Conversely, in high-security applications like payment authentication, stricter filtering prioritizes accuracy and security, ensuring only high-quality data is used for authentication.



**Fig. 6. The results of cross-activity experiments on ANT\_Maxim dataset.** MTL-RAPID got the best AUC of **99.2%** and an EER of **3.5%**, outperforming all baselines. The x-axis represents the pass rate after filtering, and the y-axis displays the AUC and EER of the identity verification task.



**Fig. 7. The results of cross-activity experiments on DaLiA dataset.** MTL-RAPID got the best AUC of **88.3%** and an EER of **17.4%**, outperforming all baselines. The x-axis represents the pass rate after filtering, and the y-axis displays the AUC and EER of the identity verification task.

#### 4.2 Study 2: Reliable PPG Authentication on Cross-Day Scenarios

Considering the daily wearing patterns of smartwatches, developing a robust cross-day authentication model is crucial. To address this, we conducted a user study focusing primarily on the performance and stability of the system in

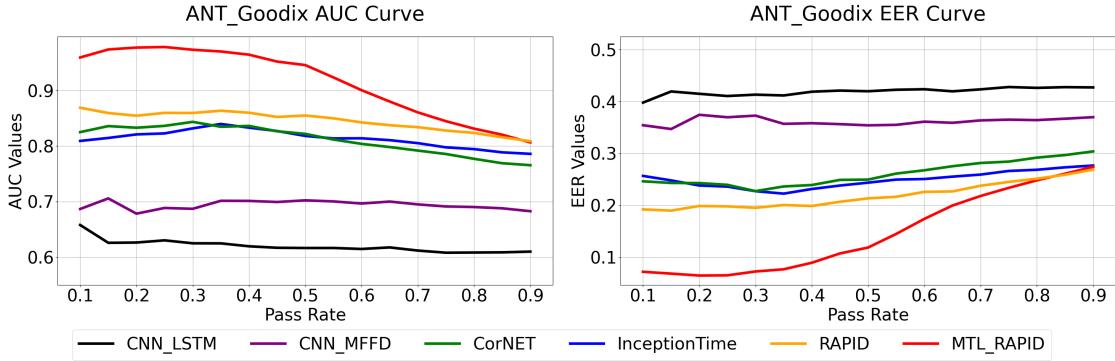


Fig. 8. **The results of cross-activity experiments on ANT\_Goodix dataset.** MTL-RAPID got the best AUC of 97.8% and an EER of 6.5%, outperforming all baselines. The x-axis represents the pass rate after filtering, and the y-axis displays the AUC and EER of the identity verification task.

cross-time verification scenarios. This study aimed to evaluate the models’ ability to maintain reliable authentication across different days, highlighting the challenges in long-term usability.

**4.2.1 Participants and Apparatus.** To evaluate the long-term reliability of PPG-based authentication, we conducted a follow-up user study four months after the movement study. In this study, we recruited 32 participants and collected data over five consecutive days. Among them, 28 were right-handed (87.5%) and 4 were left-handed (12.5%). The average age was 30.97 years ( $SD = 3.55$ ). The group comprised 21 males (65.6%) and 11 females (34.4%). Skin tones were distributed as type 3 (31.3%), type 2 (25.0%), type 4 (21.9%), and type 5 (12.5%). Regarding finger conditions, 28 participants (87.5%) had normal fingers, while 3 (9.4%) had moist fingers, and 1 participant (3.1%) had peeling.

After obtaining consent, participants were fitted with wristbands equipped with Maxim<sup>4</sup> sensors. They were instructed to remain seated or office status(allowing slight hand and body movements while seated). We collected 5 minutes of three-channel PPG signals (red, green, and infrared) for each posture. Over the following four days, participants returned to collect additional data under the same conditions.

**4.2.2 Experiments on Cross-day Authentication Scenario.** To assess the accuracy of identity verification over different time intervals following user registration, we tested the MTL-RAPID and other models at intervals of 1, 2, 3, and 4 days. This evaluation aimed to validate the model’s robustness to physiological variations over time.

We designed a two-phase training strategy to evaluate authentication performance across different days. First, we trained the base MTL-RAPID model using data from 16 subjects in the ANT motion dataset, as described in Section 4.1. Subsequently, we fine-tuned the model using static sitting data from the training set corresponding to the test days, adapting it to temporal variations. The training and test sets were split using a five-fold subject-independent approach, as described in Section 3.7.

**4.2.3 RAPID Series Outperform Baselines on Cross-Day Scenarios.** Our experimental results demonstrate RAPID series got the best performance in cross-day authentication scenarios, while also revealing the inherent challenges of long-term biometric verification. As shown in Figures 9-12, the RAPID series consistently outperformed all baselines

<sup>4</sup><https://www.analog.com/en/resources/reference-designs/maxrefdes280.html>

across all tested intervals. In the one-day scenario (Figure 9), MTL-RAPID achieved an AUC of 82.3% and EER of 26.1%, surpassing InceptionTime by 7% (AUC: 82.3% vs. 75.3%). This lead was maintained in the two-day scenario (Figure 10) with an AUC of 81.4% and EER of 5.3%, outperforming CorNet (AUC: 81.4% vs. 78.4%). While all methods exhibited performance degradation compared to the cross-activity dataset, the RAPID series showed a more stable trend. On the third day, the original RAPID model achieved the best performance with an AUC of 72.9% and EER of 33.2%, slightly outperforming MTL-RAPID (AUC: 70.9%).

The RAPID series' consistent outperformance highlights the effectiveness of its design, with MTL-RAPID excelling in short to medium time frames and the original RAPID model demonstrating strong performance in specific long-term scenarios. Despite the challenges posed by physiological variations, these results underscore the potential of the RAPID series for real-world applications and emphasize the need for future research to address the fundamental limitations of long-term biometric verification.

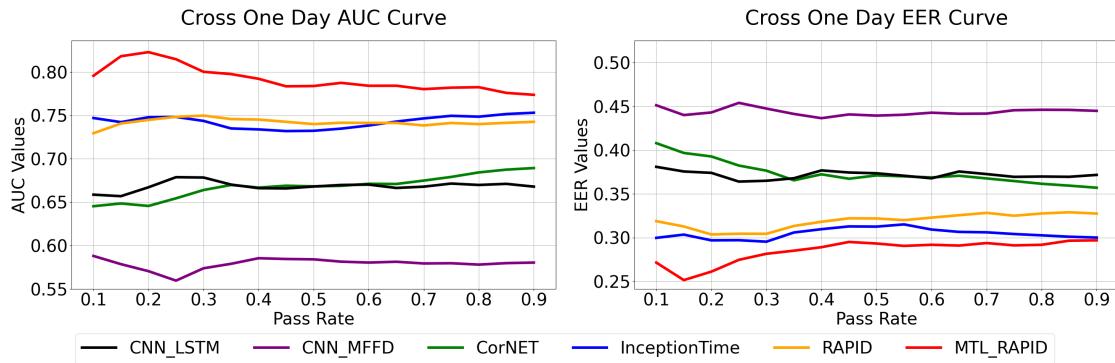


Fig. 9. **The results of cross one day experiments on ANT\_Maxim dataset.** MTL-RAPID got the best AUC of 82.3% and an EER of 26.1%, outperforming all baselines. The x-axis represents the pass rate after filtering, and the y-axis displays the AUC and EER of the identity verification task.

### 4.3 Ablation Study

The ablation study results highlight the importance of selecting optimal parameters for PPG-based identity authentication. By systematically evaluating the impact of window length, sampling rate, and multi-channel signals, we identified configurations that balance performance and practicality. These findings not only validate the robustness of the RAPID model but also provide insights into the trade-offs between accuracy and real-world feasibility.

**4.3.1 Window Length Selection.** When preprocessing signals, segmenting the PPG signals into equal-length PPG fragments is necessary. Different segment lengths can affect the model's performance in identity authentication tasks and influence feasibility in real-world applications. We trained and tested the RAPID model on PPG signals of varying lengths using five datasets: BIDMC[40], ANT\_Maxim, ANT\_Goodix, DaLiA[44], and MMPD[52]. The results are recorded in Table 4. For the BIDMC[40] dataset, which has a sufficient amount of data per subject, we experimented with segment lengths of 25 seconds and 30 seconds. However, due to insufficient data per subject in the other four datasets, these longer segment lengths were tested only on the BIDMC[40] dataset.

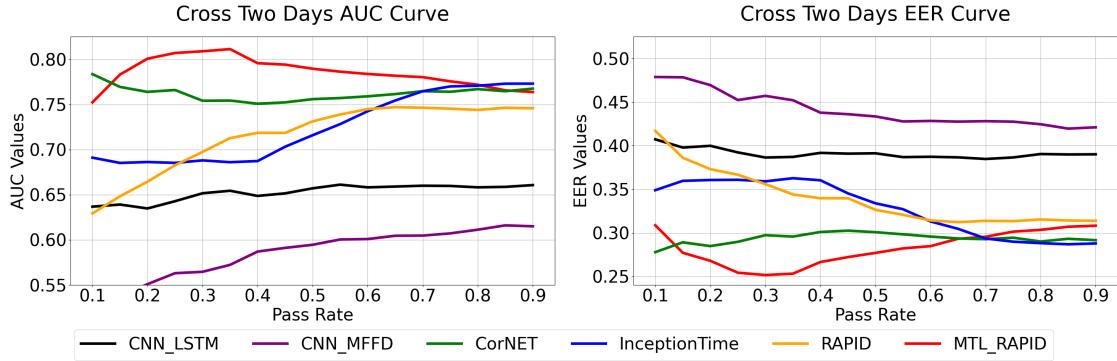


Fig. 10. **The results of cross two days experiments on ANT\_Maxim dataset.** MTL-RAPID got the best AUC of 81.4% and an EER of 5.3%, outperforming all baselines. The x-axis represents the pass rate after filtering, and the y-axis displays the AUC and EER of the identity verification task.

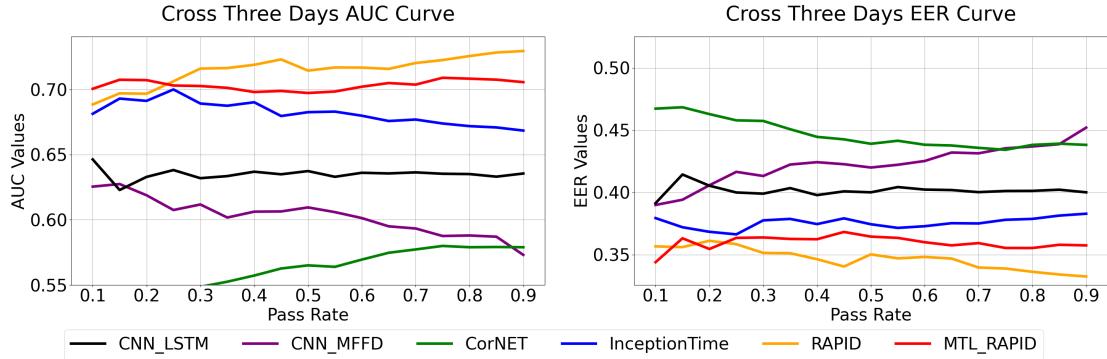


Fig. 11. **The results of cross three days experiments on ANT\_Maxim dataset.** RAPID got the best AUC of 72.9% and an EER of 33.2%, outperforming all baselines. The x-axis represents the pass rate after filtering, and the y-axis displays the AUC and EER of the identity verification task.

Table 4. The impact of PPG signal duration on identity authentication performance

PPG Length	BIDMC		ANT_Maxim		ANT_Goodix		DaLiA		MMPD	
	AUC↑	EER↓	AUC↑	EER↓	AUC↑	EER↓	AUC↑	EER↓	AUC↑	EER↓
3s	0.96	0.10	<b>0.97</b>	0.08	0.96	0.10	<b>0.84</b>	<b>0.24</b>	0.93	0.14
6s	0.97	0.09	<b>0.97</b>	<b>0.07</b>	0.95	0.11	0.82	0.26	0.93	0.14
10s	<b>0.98</b>	<b>0.07</b>	<b>0.97</b>	0.08	<b>0.96</b>	<b>0.10</b>	0.83	0.25	<b>0.94</b>	<b>0.12</b>
15s	0.97	<b>0.07</b>	0.95	0.10	0.94	0.13	0.82	0.26	0.91	0.16
20s	0.96	0.08	0.95	0.12	0.92	0.15	0.79	0.27	0.91	0.17
25s	0.97	0.08								
30s	0.96	0.09								
							Not Applicable			

AUC = Area Under the Curve, EER = Equal Error Rate

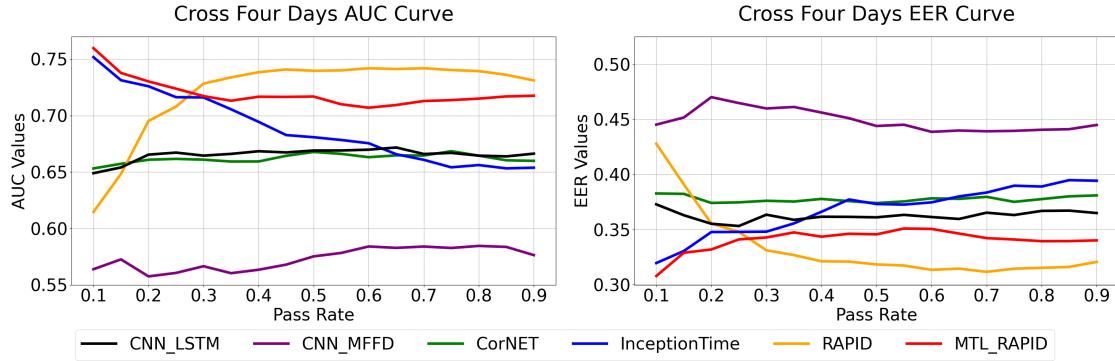


Fig. 12. **The results of cross four days experiments on ANT\_Maxim dataset.** MTL-RAPID got the best AUC of 76.0% and an EER of 30.8%, outperforming all baselines. The x-axis represents the pass rate after filtering, and the y-axis displays the AUC and EER of the identity verification task.

As shown in Table 4, the 6-second and 10-second segments achieve comparable performance across datasets (e.g., BIDMC: AUC=0.97 vs. 0.98; ANT\_Maxim: AUC=0.97 for both). However, shorter segments (3s) exhibit degraded performance on motion-prone datasets like BIDMC (AUC=0.96 vs. 0.97 for 6s), while longer segments ( $\geq 15$ s) reduce practicality without performance gains (MMPD AUC drops to 0.91 at 15s). This balance between robustness and usability justifies the 6-second choice.

**4.3.2 Sampling Rate Selection.** To determine the optimal PPG sampling frequency, we conducted experiments using the RAPID model on four datasets with high original sampling frequencies: ANT\_Maxim, ANT\_Goodix, MIMIC-III[15], and BIDMC[40]. We tested the identity authentication performance at four commonly used sampling frequencies (30Hz, 60Hz, 125Hz, and 250Hz). The results are recorded in Table 5. Since the original sampling frequencies of MIMIC-III[15] and BIDMC[40] are only 125Hz, we did not perform the 250Hz tests on these two datasets.

Table 5. The impact of PPG signal's sampling rate on identity authentication performance

Sampling Rate	ANT_Maxim		ANT_Goodix		MIMIC-III		BIDMC	
	AUC↑	EER↓	AUC↑	EER↓	AUC↑	EER↓	AUC↑	EER↓
30Hz	0.81	0.26	0.79	0.28	0.96	0.09	<b>0.97</b>	<b>0.08</b>
60Hz	<b>0.97</b>	<b>0.08</b>	<b>0.95</b>	<b>0.11</b>	<b>0.97</b>	<b>0.08</b>	<b>0.97</b>	<b>0.08</b>
125Hz	<b>0.98</b>	0.08	0.95	0.12	0.96	0.08	0.96	0.08
250Hz	<b>0.98</b>	0.07	0.96	0.10	Not Applicable			

AUC = Area Under the Curve, EER = Equal Error Rate

While 125Hz and 250Hz marginally improve ANT\_Maxim performance (AUC=0.98 vs. 0.97 at 60Hz), 60Hz achieves optimal or near-optimal results across all datasets (e.g., ANT\_Goodix AUC=0.95 vs. 0.96 at 250Hz) while halving computational requirements compared to higher rates. This makes 60Hz a pragmatic compromise between signal fidelity and efficiency.

**4.3.3 Multi-Channels PPG.** Due to the varying absorption rates of different wavelengths of light by the human body, PPG signals recorded under different wavelengths capture different information. We compared the training performance

of single-channel green light and three-channel PPG on two ANT datasets to assess whether multi-channel signals provide better authentication results. The results are shown in Table 6.

Table 6. The impact of the number of channels in PPG signals on identity authentication performance

Channels	ANT_Maxim			ANT_Goodix		
	AUC↑	EER↓	FAR↓	AUC↑	EER↓	FAR↓
1 Channel	<b>0.97 ± 0.01</b>	<b>0.08 ± 0.02</b>	0.07 ± 0.04	0.86 ± 0.06	0.21 ± 0.06	0.47 ± 0.22
3 Channels	<b>0.97 ± 0.01</b>	<b>0.08 ± 0.02</b>	<b>0.05 ± 0.03</b>	<b>0.95 ± 0.01</b>	<b>0.11 ± 0.01</b>	<b>0.13 ± 0.04</b>

AUC = Area Under the Curve, EER = Equal Error Rate, FAR = False Accept Rate (When False Reject Rate = 0.10).

Three-channel PPG demonstrates critical advantages: it maintains ANT\_Maxim’s performance (AUC=0.97) while dramatically improving ANT\_Goodix’s AUC from 0.86 to 0.95 and reducing FAR by 72% (0.47 to 0.13). This spectral diversity captures complementary biometric features, particularly beneficial for devices with lower baseline performance.

Our ablation studies collectively justify the parameter choices: 6-second segments balance performance (BIDMC AUC=0.97) and usability; 60Hz sampling optimizes computational efficiency without sacrificing accuracy (ANT\_Maxim AUC=0.97 vs. 0.98 at 125Hz); and 3-channel PPG enhances reliability, especially for challenging scenarios (ANT\_Goodix FAR=0.13 vs. 0.47). These selections establish a robust foundation for practical PPG-based authentication systems.

## 5 Usability Study

While we validated reliability in real-world, long-term scenarios, we also recognized usability as a crucial component influencing user preference. We conducted a user study to evaluate the proposed PPG-based authentication method in comparison with PIN-based authentication, which is currently the most widely used commercially implemented authentication method for smartwatches. We aimed to evaluate the time duration required for registration and authentication, the success rates for both legitimate users and potential attackers, and the overall user experience. Feedback from participants and their test results were collected for analysis. The study protocols were reviewed and approved by the university’s IRB. All participants were informed about the protocols and agreed to participate in the study.

### 5.1 Participants and Apparatus

**5.1.1 Demographics.** We recruited 16 participants from the students and faculties at the university. Among the participants, 9 were female, and 7 were male, with an average age of 23.6 years (SD = 2.76). All participants were right-handed and instructed to wear the smartwatch on their left wrist. Regarding smartwatch usage habits, 31.25% of participants reported wearing a smartwatch daily, while 56.25% stated that they seldom or never used smartwatches.

In terms of prior experience with smartwatch authentication, 58.3% of participants had never used any authentication method on a smartwatch, 16.7% had used PIN-based methods, and the remainder relied on mobile phones to activate their smartwatches. This latter approach was excluded from the study as it is not an independent authentication method and requires the use of additional devices. Furthermore, 75% of participants agreed that implementing authentication methods is both meaningful and necessary for protecting privacy on smartwatches.

**5.1.2 Devices.** In the study, we utilized three smartwatches: a custom-built PPG watch designed for PPG-based authentication, and two commercially available smartwatches using PIN-based authentication, including an Apple Watch Series 10<sup>5</sup> and a Xiaomi Smart Band 9<sup>6</sup>, as shown in Figure 13.

The custom PPG watch featured a MAX30101<sup>7</sup> PPG sensor, a 3D-printed casing, and a strap. It was connected to an Arduino Uno board via USB, which interfaced with a MacBook Air and sampled at approximately 100 Hz. The collected signals were preprocessed using the method described in Section 3.6, then transmitted to a pretrained MTL-RAPID model, trained on the ANT\_Maxim dataset illustrated in Figure 4. The MTL-RAPID model ran on the CPU of the MacBook Air.

The Apple Watch, with a larger screen size ( $1.81 \times 1.65$  inches,  $1.53 \text{ in}^2$ ), used a 4-digit PIN for authentication. While this setup provided easier access for users, it also increased the risk of successful attacks. In contrast, the Xiaomi Smart Band, with a smaller and narrower screen ( $1.87 \times 0.43$  inches,  $0.80 \text{ in}^2$ ), employed a 6-digit PIN, offering stronger security but requiring more effort from users.

## 5.2 Evaluation Setup

**5.2.1 Attack Model.** In this study, we aim to compare the vulnerabilities of PIN-based and PPG-based authentication systems against unauthorized user attacks. To achieve this, we first describe the attack models for both methods.

Extensive prior research has examined attack models for PIN-based authentication, focusing primarily on the vulnerability of passwords to being observed or memorized by unauthorized users. Following this approach, we simulate attacks by allowing the experimenter to observe participants entering their PIN and then attempting to unlock the device using the observed PIN.

For PPG-based authentication, previous studies have primarily investigated attack models where remote PPG (rPPG) signals are extracted from facial videos to generate PPG data from other body regions, potentially compromising authentication systems [11, 24]. However, these methods remain theoretical, requiring additional video data, and are not applicable to watch-only scenarios. In this experiment, we simulate attacks on PPG-based authentication by using a different user's wrist PPG signals to gain unauthorized access to the device.



(a) Participants wearing the PPG watch.



(b) PPG watch, Xiaomi Smart Band and Apple Watch.

Fig. 13. Devices in the user study.

<sup>5</sup><https://www.apple.com/apple-watch-series-10/>

<sup>6</sup><https://www.mi.com/global/product/xiaomi-smart-band-9/>

<sup>7</sup><https://www.analog.com/en/products/max30101.html>

**5.2.2 Experiment Procedure.** In this study, the experimenter first provided a brief introduction to the procedure and obtained informed consent from the participants.

During the registration process, the watch first collected PPG templates from the participants, which took at least 10 seconds. Once the templates were collected, the watch attempted authentication three times. Additionally, three random PPG signals, collected from different subjects prior to the experiment, were used to attempt an attack on the watch. A 15-second break was provided before each authentication attempt and attack. During template collection, the signals were sent to the MTL-RAPID model for quality assessment and were filtered based on a confidence threshold of 0.8. If no valid signal met the threshold, the template collection procedure was extended until at least one valid template was collected. If multiple templates were qualified, all of them were stored.

In the authentication stage, 10 seconds of PPG signals prior to authentication were used, assuming they belonged to the same person attempting to authenticate. If no valid signal was collected, the stage was extended until a valid signal was found. Multiple qualified signals were compared using an all-to-all comparison, with the final result determined by a majority vote.

After the PPG-based authentication session, participants wore the Apple Watch and registered a password. They then attempted authentication three times, while the experimenter stood approximately 50 centimeters away, trying to observe and memorize the password. The experimenter then attempted an attack by entering the memorized password. If either the participant or the experimenter entered the wrong password, the attempt was considered a failure. Participants were then asked to wear the Xiaomi Smart Band and perform the same task. These steps were repeated three times, with participants registering a different password for both the Apple Watch and Xiaomi Smart Band each time.

Next, an experiment was included to evaluate the cognitive load of participants. During a 5-minute video-based learning session session, participants were prompted to unlock the watch or band five times while watching. After the video, participants completed a questionnaire to rate their experience with the user study and express their preferences for the different authentication methods.

### 5.3 Results

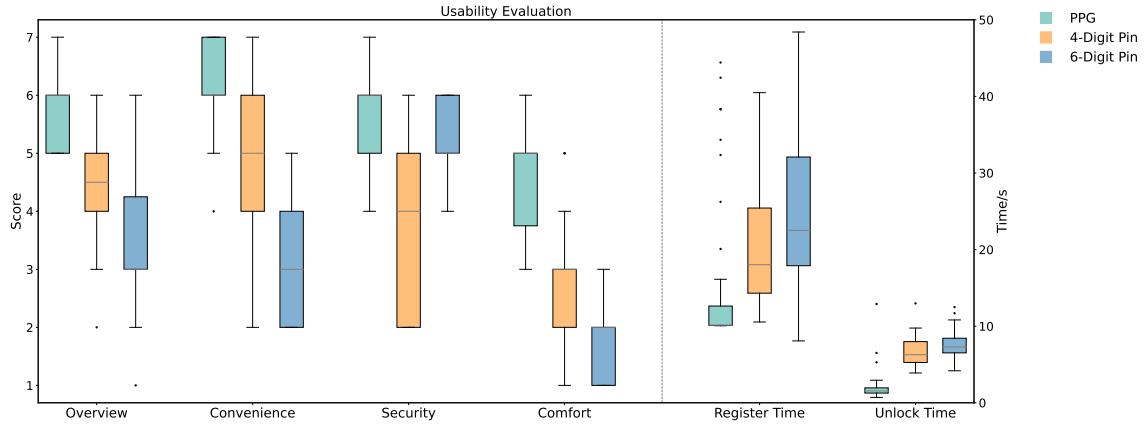


Fig. 14. **Usability Evaluation.** The user preference regarding convenience, security, comfort and time consumption.

**5.3.1 Authentication Performance.** In the experiment, we recorded several metrics for each participant, including the number of successful and failed authentication attempts, the number of successful and failed attacks by unauthorized users, and the time taken for each phase. For PPG-based smartwatches, the recorded authentication time excludes the pre-collected 10 seconds, as it is not part of the user's intentional unlocking action. Figure 14 presents the experimental results, showing the distribution of registration and unlock time.

The average registration time for PPG-based smartwatches was 14.7 seconds ( $SD=9.52s$ ), significantly faster than that of the Apple Watch (24.8 seconds,  $SD=23.0s$ ) and the Xiaomi Smart Band (28.8 seconds,  $SD=18.7s$ ). The longer registration times for the Apple Watch and Xiaomi Smart Band stem from several factors.

First, their registration processes were unintuitive, with many participants failing to notice that they needed to unlock the device with an existing password before setting a new one. This led to confusion and, in some cases, device lockouts. Second, the small screen of the devices worsened usability challenges. This was particularly evident for the Xiaomi Smart Band, which featured a compact screen with 11 densely packed keys, resulting in a high likelihood of accidental touches.

The average authentication time for the PPG-based smartwatch was 1.98 seconds ( $SD=3.15s$ ), significantly faster than that of the Apple Watch (6.68 seconds,  $SD=2.44s$ ) and the Xiaomi Smart Band (7.55 seconds,  $SD=2.27s$ ). It is worth noting that as participants became more familiar with the experimental procedures, they registered and entered PINs faster. Consequently, the first time required for PIN-based registration and authentication in real-world scenarios is likely longer than the average times reported in this study.

Regarding accuracy, the PPG-based smartwatch achieved an average authentication success rate of 98.6% and an average attack success rate of 1.4%, outperforming both the Apple Watch (authentication success rate = 95.8%, attack success rate = 71.5%) and the Xiaomi Smart Band (authentication success rate = 88.2%, attack success rate = 16.0%).

The Apple Watch has a high authentication success rate but suffers from a high attack success rate, likely due to its 4-digit PIN and larger screen, which reduce input errors but increase the risk of PIN observation. In contrast, the Xiaomi Smart Band, with a 6-digit PIN and smaller screen, is less prone to PIN observation from a distance but has a higher chance of input errors, explaining its lower authentication success rate and much lower attack success rate. Our PPG watch strikes a good balance between high authentication success and resistance to attacks.

**5.3.2 User Preference.** At the end of the experiment, we collected user experience data from all participants through a survey. The survey used a 7-point Likert scale to assess the overall experience with the three smartwatches and user experiences during key stages of the experiment. The user experience data from the 16 participants were analyzed using the Friedman test (non-parametric test), as the data distribution's normality was uncertain. Pairwise comparisons were conducted using the Wilcoxon signed-rank test, with Bonferroni correction applied to control for Type I errors.

- (1) **Overall experience:** The survey results showed the following overall experience ratings: PPG watch ( $M = 5.75$ ,  $SD = 0.577$ ), Apple Watch ( $M = 4.38$ ,  $SD = 1.09$ ), and Xiaomi Smart Band ( $M = 3.56$ ,  $SD = 1.26$ ). The Friedman test revealed a significant difference in the overall user experience across the three smartwatches ( $X^2(2, N = 16) = 18.73, p < 0.001$ ). Further Wilcoxon pairwise comparisons indicated significant differences between the PPG watch and both the Apple Watch ( $p = 0.027$ ) and the Xiaomi Smart Band ( $p < 0.001$ ). These results suggest that the PPG watch provided a significantly better overall user experience compared to the PIN-based devices.
- (2) **Convenience of authentication:** The survey results indicated the following convenience ratings: PPG watch ( $M = 6.13$ ,  $SD = 0.885$ ), Apple Watch ( $M = 4.94$ ,  $SD = 1.18$ ), and Xiaomi Smart Band ( $M = 3.25$ ,  $SD = 1.13$ ). The

Friedman test showed a significant difference in authentication convenience between the devices ( $X^2(2, N = 16) = 23.41, p < 0.001$ ). Wilcoxon pairwise comparisons showed significant differences between the PPG watch and both the Apple Watch ( $p = 0.042$ ) and the Xiaomi Smart Band ( $p < 0.001$ ). These results suggest that PPG-based authentication is significantly more convenient than PIN-based methods.

- (3) **Security of authentication:** The survey results on perceived security were as follows: PPG watch ( $M = 5.62, SD = 0.957$ ), Xiaomi Smart Band ( $M = 5.13, SD = 0.719$ ), and Apple Watch ( $M = 3.69, SD = 1.44$ ). The Friedman test revealed a significant difference in perceived security across the devices ( $X^2(2, N = 16) = 14.37, p < 0.001$ ). Wilcoxon pairwise comparisons showed significant differences between the PPG watch and the Apple Watch ( $p = 0.002$ ). However, there was no significant difference between the PPG watch and the Xiaomi Smart Band ( $p = 1.00$ ). These results indicate that users perceive 4-digit PIN (Apple Watch) as less secure than PPG and 6-digit PIN (Xiaomi Smart Band), while PPG and 6-digit PIN are considered equally secure.
- (4) **Cognitive comfort:** The survey results showed that the cognitive comfort perceived by users during the video-based learning task was as follows: PPG watch ( $M = 4.38, SD = 0.957$ ), Apple Watch ( $M = 2.88, SD = 1.088$ ), and Xiaomi Smart Band ( $M = 1.81, SD = 0.75$ ). The Friedman test showed a significant difference in cognitive load across the three devices ( $X^2(2, N = 16) = 23.72, p < 0.001$ ). Further Wilcoxon pairwise comparisons revealed a significant difference between the PPG watch and the Xiaomi Smart Band ( $p = 0.000$ ), but no significant difference between the PPG watch and the Apple Watch ( $p = 0.065$ ). These results suggest that users felt more comfortable using the PPG watch and Apple Watch.

## 6 Discussion and Future Work

This paper explores efficient and reliable PPG authentication on smartwatches for daily scenarios. In this section, we discuss the major results, findings, limitations and future work.

### 6.1 Reliable PPG Authentication on Smartwatches

In this paper, we demonstrated that PPG authentication faces reliability challenges due to motion artifacts and physiological variability over time. The proposed foundational RAPID block is designed based on optical physiological principles, enabling robust handling of external noise. In the static scenario with ANT\_Maxim, the RAPID block achieves a high AUC of 0.98, outperforming all baseline models. MTL-RAPID demonstrated strong performance against motion artifacts, as shown in Table 3. It is the state-of-the-art model compared to sequentially connected baseline models, as depicted in Figure 6-8, achieving an AUC of 99.2% and an EER of 3.5% on the ANT motion dataset.

However, addressing physiological variability over time remains a key challenge for PPG-based authentication, with significant potential for improvement. To our knowledge, we are the first to explore physiological variability in the context of long-term PPG authentication. This paper presents our exploration of the MTL-RAPID model over time, which achieved a 7% improvement in AUC on cross-day tasks compared to the best baseline. The RAPID series' consistent superiority highlights the effectiveness of its design, particularly the multi-task learning strategy.

### 6.2 Efficient PPG Authentication on Smartwatches

Authentication is a frequently used function on smartwatches, making edge-efficient methods essential for practical deployment. MTL-RAPID demonstrates significant efficiency advantages over previous methods in terms of model size, inference time, and memory usage. With only 80k parameters, MTL-RAPID is smaller than any of the models in related

work. Its architecture leverages an efficient multi-task learning (MTL) design, which further reduces the parameter count.

Additionally, MTL-RAPID offers highly efficient inference times, averaging just **1.58 ms** per operation—less than half the time of the next best-performing model, InceptionTime [14], which averages 3.08 ms. This substantial reduction in processing time makes MTL-RAPID a suitable solution for real-time applications, where quick response times are critical. In terms of memory usage, MTL-RAPID excels with a peak memory usage of 3.40 MB, which is only 1/10 of InceptionTime's[14] 34.35 MB. This substantial reduction in memory usage makes MTL-RAPID particularly well-suited for resource-constrained devices like smartwatches or other wearables.

### 6.3 Opensource Efforts for PPG authentication

We opensource the largest wrist PPG authentication dataset ANT alongside our MTL-RAPID model to advance research in PPG-based authentication and foster collaboration. The former largest wrist PPG dataset DaLiA [44] only has a single channel signal from only 15 participants. Our ANT dataset has 30 subjects covering 3-channel PPG signals and 10 daily activities. By sharing this data, we aim to provide researchers with valuable resources to further explore the challenges in real-world PPG authentication, such as motion artifacts and physiological variability over time.

### 6.4 Limits and Future Work

We acknowledge that the size and diversity of our participant pool may not fully represent real-world demographics, and the 4-day interval may not capture the full complexity of physiological signal variability. In future work, we plan to expand the dataset to include a broader demographic and conduct longitudinal studies over longer periods. These efforts are essential for understanding PPG signal dynamics and improving the reliability of authentication systems.

As shown in Figure 9- 12, all methods exhibit a significant decline in performance over time. This decline highlights the influence of physiological changes, such as heart rate, skin temperature, and vascular characteristics, on PPG signal consistency. Future research is needed to develop reliable solutions for addressing physiological variability. Potential directions include adaptive learning techniques to continuously fine-tune the model based on evolving physiological patterns, as well as multi-modal authentication systems combining PPG with other biometric signals, such as accelerometer data.

We recommend adopting an updated template strategy [43] to better accommodate daily variations in PPG signals. We argue that temporal changes in PPG signals could enhance theft prevention, albeit posing challenges for algorithmic performance. Additionally, developing advanced algorithms to compensate for physiological variability could maintain high authentication accuracy over extended periods, improving the viability of PPG-based authentication in real-world applications.

## 7 Conclusion

In this paper, we present MTL-RAPID, the first model to seamlessly integrate signal quality assessment with PPG-based identity verification. Designed as a motion-robust solution, MTL-RAPID demonstrates superior performance in handling real-world daily activities compared to existing methods. By leveraging a multi-task learning strategy, our model significantly enhances authentication accuracy, achieving remarkable results with a 99.2% AUC and a 3.5% EER on the challenging noisy ANT dataset, outperforming all existing baselines. Additionally, this study pioneers the evaluation of PPG authentication reliability across multiple days, effectively addressing the critical challenge of time-varying PPG signal characteristics. Our user study further validates the practicality of MTL-RAPID, revealing

a statistically significant user preference ( $p < 0.05$ ) for our PPG authentication method over traditional PIN-based approaches. To foster further research and innovation in PPG authentication on smartwatches, we will open-source the MTL-RAPID model along with the ANT dataset.

## References

- [1] Dwaipayan Biswas, Luke Everson, Muqing Liu, Madhuri Panwar, Bram-Ernst Verhoef, Shrishail Patki, Chris H. Kim, Amit Acharyya, Chris Van Hoof, Mario Konijnenburg, and Nick Van Helleputte. 2019. CorNET: Deep Learning Framework for PPG-Based Heart Rate Estimation and Biometric Identification in Ambulant Environment. *IEEE Transactions on Biomedical Circuits and Systems* 13, 2 (2019), 282–291. <https://doi.org/10.1109/TBCAS.2019.2892297>
- [2] Seunghun Cha, Sungsu Kwag, Hyoungshick Kim, and Jun Ho Huh. 2017. Boosting the guessing attack performance on android lock patterns with smudge attacks. In *Proceedings of the 2017 ACM on Asia conference on computer and communications security*. 313–326.
- [3] Geumhwan Cho, Jun Ho Huh, Junsung Cho, Seongyeol Oh, Youngbae Song, and Hyoungshick Kim. 2017. Syspal: System-guided pattern locks for android. In *2017 IEEE Symposium on security and privacy (SP)*. IEEE, 338–356.
- [4] Tilendra Choudhary and M Sabarimalai Manikandan. 2016. Robust photoplethysmographic (PPG) based biometric authentication for wireless body area networks and m-health applications. In *2016 Twenty Second National Conference on Communication (NCC)*. IEEE, 1–6.
- [5] Cory Cornelius, Ronald Peterson, Joseph Skinner, Ryan Halter, and David Kotz. 2014. A wearable system that knows who wears it. In *Proceedings of the 12th annual international conference on Mobile systems, applications, and services*. 55–67.
- [6] Ashok Kumar Das, Mohammad Wazid, Neeraj Kumar, Muhammad Khurram Khan, Kim-Kwang Raymond Choo, and YoungHo Park. 2018. Design of Secure and Lightweight Authentication Protocol for Wearable Devices Environment. *IEEE Journal of Biomedical and Health Informatics* 22, 4 (2018), 1310–1322. <https://doi.org/10.1109/JBHI.2017.2753464>
- [7] Eleni Fotiadou, Ruud JG van Sloun, Judith OEH van Laar, and Rik Vullings. 2021. A dilated inception CNN-LSTM network for fetal heart rate estimation. *Physiological Measurement* 42, 4 (2021), 045007.
- [8] Yuan Gao, Jiayi Ma, Mingbo Zhao, Wei Liu, and Alan L Yuille. 2019. Nddr-cnn: Layerwise feature fusing in multi-task cnns by neural discriminative dimensionality reduction. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*. 3205–3214.
- [9] Lorena Gonzalez-Manzano, Jose M. De Fuentes, and Arturo Ribagorda. 2019. Leveraging User-Related Internet of Things for Continuous Authentication: A Survey. *ACM Comput. Surv.* 52, 3, Article 53 (June 2019), 38 pages. <https://doi.org/10.1145/3314023>
- [10] Marian Harbach, Alexander De Luca, and Serge Egelman. 2016. The Anatomy of Smartphone Unlocking: A Field Study of Android Lock Screens. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (San Jose, California, USA) (CHI ’16). ACM, New York, NY, USA, 4806–4817. <https://doi.org/10.1145/2858036.2858267>
- [11] Shun Hinatsu, Daisuke Suzuki, Hiroki Ishizuka, Sei Ikeda, and Osamu Oshiro. 2022. Evaluation of PPG feature values toward biometric authentication against presentation attacks. *IEEE Access* 10 (2022), 41352–41361.
- [12] Jie Hu, Li Shen, and Gang Sun. 2018. Squeeze-and-excitation networks. In *Proceedings of the IEEE conference on computer vision and pattern recognition*. 7132–7141.
- [13] Jun Ho Huh, Hyejin Shin, HongMin Kim, Eunyong Cheon, Youngeun Song, Choong-Hoon Lee, and Ian Oakley. 2023. Wristacoustic: through-wrist acoustic response based authentication for smartwatches. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 6, 4 (2023), 1–34.
- [14] Hassan Ismail Fawaz, Benjamin Lucas, Germain Forestier, Charlotte Pelletier, Daniel F Schmidt, Jonathan Weber, Geoffrey I Webb, Lhassane Idoumghar, Pierre-Alain Muller, and François Petitjean. 2020. Inceptiontime: Finding alexnet for time series classification. *Data Mining and Knowledge Discovery* 34, 6 (2020), 1936–1962.
- [15] Alistair EW Johnson, Tom J Pollard, Lu Shen, Li-wei H Lehman, Mengling Feng, Mohammad Ghassemi, Benjamin Moody, Peter Szolovits, Leo Anthony Celi, and Roger G Mark. 2016. MIMIC-III, a freely accessible critical care database. *Scientific data* 3, 1 (2016), 1–9.
- [16] Nima Karimian, Mark Tehranipoor, and Domenic Forte. 2017. Non-fiducial ppg-based authentication for healthcare application. In *2017 IEEE EMBS international conference on biomedical & health informatics (BHI)*. IEEE, 429–432.
- [17] Walter Karlen, M Turner, Erin Cooke, Guy Dumont, and J Mark Ansermino. 2010. CapnoBase: Signal database and tools to collect, share and annotate respiratory signals. In *2010 Annual meeting of the society for technology in anesthesia*. Society for Technology in Anesthesia, 27.
- [18] Sander Koelstra, Christian Muhl, Mohammad Soleymani, Jong-Seok Lee, Ashkan Yazdani, Touradj Ebrahimi, Thierry Pun, Anton Nijholt, and Ioannis Patras. 2011. Deap: A database for emotion analysis; using physiological signals. *IEEE transactions on affective computing* 3, 1 (2011), 18–31.
- [19] Masoud Mehrabi Koushki, Borke Obada-Obiech, Jun Ho Huh, and Konstantin Beznosov. 2021. On smartphone users' difficulty with understanding implicit authentication. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–14.
- [20] Joon Lee, Daniel J Scott, Mauricio Villarroel, Gari D Clifford, Mohammed Saeed, and Roger G Mark. 2011. Open-access MIMIC-II database for intensive care research. In *2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*. IEEE, 8315–8318.
- [21] Sunwoo Lee, Wonsuk Choi, and Dong Hoon Lee. 2021. Usable user authentication on a smartwatch using vibration. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*. 304–319.

- [22] Wei-Han Lee, Xiaochen Liu, Yilin Shen, Hongxia Jin, and Ruby B. Lee. 2017. Secure Pick Up. *Proceedings of the 22nd ACM on Symposium on Access Control Models and Technologies - SACMAT '17 Abstracts* (2017). <https://doi.org/10.1145/3078861.3078870>
- [23] Alona Levy, Ben Nassi, Yuval Elovici, and Erez Shmueli. 2018. Handwritten Signature Verification Using Wrist-Worn Devices. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2, 3, Article 119 (Sept. 2018), 26 pages. <https://doi.org/10.1145/3264929>
- [24] Ke Liu, Jiankai Tang, Zhang Jiang, Yuntao Wang, Xiaojing Liu, Dong Li, and Yuanchun Shi. 2024. Summit Vitals: Multi-Camera and Multi-Signal Biosensing at High Altitudes. *arXiv preprint arXiv:2409.19223* (2024).
- [25] Mingxuan Liu, Jiankai Tang, Yongli Chen, Haoxiang Li, Jiahao Qi, Siwei Li, Kegang Wang, Jie Gan, Yuntao Wang, and Hong Chen. 2024. Spiking-PhysFormer: Camera-Based Remote Photoplethysmography with Parallel Spike-driven Transformer. *arXiv:2402.04798 [cs.CV]*
- [26] Jordi Luque, Guillem Cortes, Carlos Segura, Alexandre Maravilla, Javier Esteban, and Joan Fabregat. 2018. End-to-end photoplethysmographY (PPG) based biometric authentication by using convolutional neural networks. In *2018 26th European Signal Processing Conference (EUSIPCO)*. IEEE, 538–542.
- [27] Jiaqi Ma, Zhe Zhao, Xinyang Yi, Jiliu Chen, Lichan Hong, and Ed H Chi. 2018. Modeling task relationships in multi-task learning with multi-gate mixture-of-experts. In *Proceedings of the 24th ACM SIGKDD international conference on knowledge discovery & data mining*. 1930–1939.
- [28] U. Mahbub, S. Sarkar, V. M. Patel, and R. Chellappa. 2016. Active user authentication for smartphones: A challenge data set and benchmark results. In *2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS)*. IEEE, Piscataway, NJ, USA, 1–8. <https://doi.org/10.1109/BTAS.2016.7791155>
- [29] Ahmed Mahfouz, Tarek M. Mahmoud, and Ahmed Sharaf Eldin. 2017. A survey on behavioral biometric authentication on smartphones. *Journal of Information Security and Applications* 37 (2017), 28 – 37. <https://doi.org/10.1016/j.jisa.2017.10.002>
- [30] Philipp Markert, Daniel V Bailey, Maximilian Golla, Markus Dürmuth, and Adam J Aviv. 2020. This pin can be easily guessed: Analyzing the security of smartphone unlock pins. In *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 286–303.
- [31] Liam M. Mayron. 2015. Behavioral Biometrics for Universal Access and Authentication. In *Universal Access in Human-Computer Interaction. Access to Today's Technologies*, Margherita Antona and Constantine Stephanidis (Eds.). Springer International Publishing, Cham, 330–339.
- [32] George B Moody and Roger G Mark. 2001. The impact of the MIT-BIH arrhythmia database. *IEEE engineering in medicine and biology magazine* 20, 3 (2001), 45–50.
- [33] Collins W. Munyendo, Miles Grant, Philipp Markert, Timothy J. Forman, and Adam J. Aviv. 2021. Using a blocklist to improve the security of user selection of android patterns. In *Proceedings of the Seventeenth USENIX Conference on Usable Privacy and Security (SOUPS'21)*. USENIX Association, USA, Article 3, 19 pages.
- [34] K. Niinuma, U. Park, and A. K. Jain. 2010. Soft Biometric Traits for Continuous User Authentication. *IEEE Transactions on Information Forensics and Security* 5, 4 (2010), 771–780. <https://doi.org/10.1109/TIFS.2010.2075927>
- [35] Ian Oakley, Jun Ho Huh, Junsung Cho, Geumhwan Cho, Rasel Islam, and Hyoungshick Kim. 2018. The personal identification chord: A four buttonauthentication system for smartwatches. In *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*. 75–87.
- [36] Ioannis Papavasileiou, Savanna Smith, Jinbo Bi, and Song Han. 2017. Gait-based Continuous Authentication Using Multimodal Learning. In *Proceedings of the Second IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies* (Philadelphia, Pennsylvania) (CHASE '17). IEEE Press, Piscataway, NJ, USA, 290–291. <https://doi.org/10.1109/CHASE.2017.107>
- [37] V. M. Patel, R. Chellappa, D. Chandra, and B. Barbello. 2016. Continuous User Authentication on Mobile Devices: Recent progress and remaining challenges. *IEEE Signal Processing Magazine* 33, 4 (2016), 49–61. <https://doi.org/10.1109/MSP.2016.2555335>
- [38] Vishal M Patel, Rama Chellappa, Deepak Chandra, and Brandon Barbello. 2016. Continuous user authentication on mobile devices: Recent progress and remaining challenges. *IEEE Signal Processing Magazine* 33, 4 (2016), 49–61.
- [39] Marco AF Pimentel, Alistair EW Johnson, Peter H Charlton, Drew Birrenkott, Peter J Watkinson, Lionel Tarassenko, and David A Clifton. 2016. Toward a robust estimation of respiratory rate from pulse oximeters. *IEEE Transactions on Biomedical Engineering* 64, 8 (2016), 1914–1923.
- [40] Marco A. F. Pimentel, Alistair E. W. Johnson, Peter H. Charlton, Drew Birrenkott, Peter J. Watkinson, Lionel Tarassenko, and David A. Clifton. 2017. Toward a Robust Estimation of Respiratory Rate From Pulse Oximeters. *IEEE Transactions on Biomedical Engineering* 64, 8 (2017), 1914–1923. <https://doi.org/10.1109/TBME.2016.2613124>
- [41] Limeng Pu, Pedro J Chacon, Hsiao-Chun Wu, and Jin-Woo Choi. 2022. Novel robust photoplethysmogram-based authentication. *IEEE Sensors Journal* 22, 5 (2022), 4675–4686.
- [42] Rajeev Ranjan, Vishal M Patel, and Rama Chellappa. 2017. Hyperface: A deep multi-task learning framework for face detection, landmark localization, pose estimation, and gender recognition. *IEEE transactions on pattern analysis and machine intelligence* 41, 1 (2017), 121–135.
- [43] Ajita Rattani, Biagio Freni, Gian Luca Marcialis, and Fabio Roli. 2009. Template update methods in adaptive biometric systems: A critical review. In *Advances in Biometrics: Third International Conference, ICB 2009, Alghero, Italy, June 2-5, 2009. Proceedings* 3. Springer, 847–856.
- [44] Attila Reiss, Ina Indlekofer, Philip Schmidt, and Kristof Van Laerhoven. 2019. Deep PPG: Large-Scale Heart Rate Estimation with Convolutional Neural Networks. *Sensors* 19, 14 (2019). <https://doi.org/10.3390/s19143079>
- [45] P. Samangouei, V. M. Patel, and R. Chellappa. 2015. Attribute-based continuous user authentication on mobile devices. In *2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS)*. IEEE, Piscataway, NJ, USA, 1–8. <https://doi.org/10.1109/BTAS.2015.7358748>
- [46] Jorge Sancho, Álvaro Alesanco, and José García. 2018. Biometric authentication using the PPG: A long-term feasibility study. *Sensors* 18, 5 (2018), 1525.

- [47] Abhijit Sarkar, A Lynn Abbott, and Zachary Doerzaph. 2016. Biometric authentication using photoplethysmography signals. In *2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS)*. IEEE, 1–7.
- [48] Suranga Seneviratne, Yining Hu, Tham Nguyen, Guohao Lan, Sara Khalifa, Kanchana Thilakarathna, Mahbub Hassan, and Aruna Seneviratne. 2017. A Survey of Wearable Devices and Challenges. *IEEE Communications Surveys & Tutorials* 19, 4 (2017), 2573–2620. <https://doi.org/10.1109/COMST.2017.2731979>
- [49] Steven A Shafer. 1985. Using color to separate reflection components. *Color Research & Application* 10, 4 (1985), 210–218.
- [50] Muhammad Shahzad and Munindar P Singh. 2017. Continuous authentication and authorization for the internet of things. *IEEE Internet Computing* 21, 2 (2017), 86–90.
- [51] Jiacheng Shang and Jie Wu. 2019. A usable authentication system using wrist-worn photoplethysmography sensors on smartwatches. In *2019 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 1–9.
- [52] Jiankai Tang, Kequan Chen, Yuntao Wang, Yuanchun Shi, Shwetak Patel, Daniel McDuff, and Xin Liu. 2023. Mmpd: multi-domain mobile video physiology dataset. In *2023 45th Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC)*. IEEE, 1–5.
- [53] Jiankai Tang, Xinyi Li, Jiacheng Liu, Xiyuxing Zhang, Zeyu Wang, and Yuntao Wang. 2024. Camera-Based Remote Physiology Sensing for Hundreds of Subjects Across Skin Tones. arXiv:2404.05003 [cs.CV]
- [54] Jiankai Tang, Kegang Wang, Hongming Hu, Xiyuxing Zhang, Peiyu Wang, Xin Liu, and Yuntao Wang. 2023. ALPHA: AnomaLous Physiological Health Assessment Using Large Language Models. arXiv:2311.12524 [cs.LG]
- [55] Pieter-Jan Toye. 2023. Vital Videos: A dataset of face videos with PPG and blood pressure ground truths. arXiv:2306.11891 [cs.CV]
- [56] Emanuel von Zezschwitz, Alexander De Luca, and Heinrich Hussmann. 2014. Honey, I Shrunk the Keys: Influences of Mobile Devices on Password Composition and Authentication Performance. In *Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational (Helsinki, Finland) (NordiCHI '14)*. ACM, New York, NY, USA, 461–470. <https://doi.org/10.1145/2639189.2639218>
- [57] Li Wan, Kechen Liu, Hanan Abdullah Mengash, Nuha Alruwais, Mesfer Al Duhayyim, and K Venkatachalam. 2024. Deep learning-based photoplethysmography biometric authentication for continuous user verification. *Applied Soft Computing* 156 (2024), 111461.
- [58] Umang Yadav, Sherif N Abbas, and Dimitrios Hatzinakos. 2018. Evaluation of PPG biometrics for authentication in different states. In *2018 International Conference on Biometrics (ICB)*. IEEE, 277–282.
- [59] Junfeng Yang, Yuwen Huang, Ruili Zhang, Fuxian Huang, Qinggang Meng, and Shixin Feng. 2021. Study on ppg biometric recognition based on multifeature extraction and naive bayes classifier. *Scientific Programming* 2021 (2021), 1–12.
- [60] H. Zhang, V. M. Patel, M. Fathy, and R. Chellappa. 2015. Touch Gesture-Based Active User Authentication Using Dictionaries. In *2015 IEEE Winter Conference on Applications of Computer Vision*. IEEE, Piscataway, NJ, USA, 207–214. <https://doi.org/10.1109/WACV.2015.35>
- [61] Tianming Zhao, Yan Wang, Jian Liu, Yingying Chen, Jerry Cheng, and Jiadi Yu. 2020. Trueheart: Continuous authentication on wrist-worn wearables using ppg-based biometrics. In *IEEE INFOCOM 2020-IEEE Conference on Computer Communications*. IEEE, 30–39.