Towards Nonintrusive and Secure Mobile Two-Factor Authentication on Wearables

Yetong Cao, *Student Member, IEEE,* Fan Li, *Member, IEEE,* Qian Zhang, Song Yang, *Member, IEEE,* and Yu Wang, *Fellow, IEEE*

Abstract—Mobile devices are promising to apply two-factor authentication to improve system security. Existing solutions have certain limits of requiring extra user effort, which might seriously affect user experience and delay authentication time. In this paper, we propose PPGPass, a novel mobile two-factor authentication system, which leverages Photoplethysmography (PPG) sensors available in most wrist-worn wearables. PPGPass simultaneously performs a password/pattern/signature authentication and a physiological-based authentication. To realize both nonintrusive and secure, we design a two-stage algorithm to separate clean heartbeat signals from PPG signals contaminated by motion artifacts so that users do not have to deliberately keep their bodies still. In addition, to deal with noncancelable issues when biometrics are compromised, we design a repeatable and non-invertible method to generate cancelable feature templates as alternative credentials. We leverage the great power of *Random Forest* and *Support Vector Data Description* to detect adversaries and verify a user's identity. To the best of our knowledge, PPGPass is the first nonintrusive and secure mobile two-factor authentication based on PPG sensors. Extensive experiments demonstrate that PPGPass can achieve the false acceptance rate of 3.11% and the false recognition rate of 3.71%, which confirms its high effectiveness, security, and usability.

Index Terms—Mobile/wearable computing, two-factor authentication, biometrics

1 Introduction

In recent years, two-factor authentication is widely deployed by mobile devices to further improve system security and enhance user privacy-preservation. It provides an additional line of defense besides traditional commonly used authentication approaches. For example, when a user wants to log in to a system, the user enters a password as usual. Synchronously, the system will apply two-factor authentication to verify whether the current user matches the pre-registered user profile. As mobile devices have increasing relations with personally and financially sensitive information during people's daily behaviors like messaging, health caring, and payment, current mobile two-factor authentication is taking over more importance.

Given the need for mobile two-factor authentication, many authentication techniques can be combined to provide promising solutions. Existing studies are broadly organized into two categories: *Knowledge-based* and *Biometrics-based*. *Knowledge-based studies* assume that a secret is shared between an owner and a device, which will be provided every time when the device is used [1]. Most commonly used passwords/PINs/patterns inputs are inherently vulnerable to shoulder surfing attacks and smudge attacks [2], [3]. In terms of two-factor authentication, existing systems mainly require user extra involvement, such as Duo [4], Encap Security [5], and Google 2-step verification [6]. They need users to type in verification codes received by text messages or automated phone calls from trusted phone numbers or trusted devices, which seriously affect user experience and delay authentication time. *Biometrics-based studies* include physiological-based and behavioral-based techniques. Physiological-based techniques can reach high identification accuracy. However, iris scan and voiceprint are inconvenient for users to authenticate frequently and continuously. Fingerprints are prone to be hacked in social media (e.g., stealing raw fingerprint from a photograph) [7]. Face recognition, could be hacked via images or videos of a user [8]. Furthermore, they are suffering from replay attacks [9]. Behavioral-based techniques also need user extra involvement, such as writing signatures [10], speaking lips [11], and breathing gestures [12]. Screen touch gestures can verify users nonintrusively [13]–[15], but it has proven ineffective against advanced statistical attacks [16]. To deal with such issues, Photoplethysmography (PPG) sensors in the increasing popularity of wrist-worn wearables provide a unique opportunity for realizing nonintrusive and secure mobile two-factor authentication.

In this paper, we propose PPGPass, which takes the first step to develop a nonintrusive and secure mobile two-factor user authentication system using PPG sensors in wrist-worn wearables. It enables two-factor authentication by combining conventional mobile authentication schemes and physiological-based authentication. Particularly, PPGPass effectively adds the unique PPG features as the second factor of authentication, which can enhance the security of existing mobile authentication solutions. Fig. 1 shows the working paradigm of PPGPass. The first factor is obtained by the mobile device, which can be password, PIN, pattern,

- *Y. Cao, F. Li and S. Yang are with School of Computer Science, Beijing Institute of Technology, Beijing, 100081, R.P.China. E-mail: {yetongcao,fli,S.Yang}@bit.edu.cn*
- *Q. Zhang is with School of Software, Tsinghua University, China, 100084, R.P. China. E-mail: qzhang2019@mail.tsinghua.edu.cn*
- *Y. Wang is with Department of Computer and Information Sciences, Temple University, Philadelphia, Pennsylvania 19122, USA. E-mail: wangyu@temple.edu*
- *F. Li is the corresponding author.*

Manuscript received MONTH DAY, YEAR; revised MONTH DAY, YEAR.

signature, etc. And, the second factor is cancelable cardiac features obtained from the PPG sensor available in most wrist-worn devices. When a user wants to access, he/she submits the passcode and cancelable features. Then, the enrolled devices add time-stamp to the submitted messages and transmit them to the system. The system examines the time-stamped identifier to ascertain that the submitted credentials are originally collected, and the server establishes trust when the user provides both the correct passcode and the cardiac features.

Specifically, PPGPass focuses on three goals. 1) **Non-intrusive authentication**: PPG signals are easy to be disturbed by hand motions. The user is usually required to remain stationary while acquiring PPG data. This affects the user experience and makes PPG-based authentication incompatible with common authentication approaches (e.g., signatures writing and passwords/patterns inputs). We propose a two-stage Motion Artifacts (MAs) removal algorithm to efficiently obtain clean heartbeat signals, which enables to nonintrusively authenticate users without extra user involvement. 2) **High accuracy authentication**: We first align derived PPG signals in the angle-domain. Afterward, we select 40 geometric features from single and multiple cardiac cycles, which reflect consistent and intrinsic individual characteristics to support high accuracy authentication. We design an authentication model consists of a user differentiator and multiple adversary detectors, which defenses random attacks. Furthermore, we perform data augmentation on the collected training data set so that the pre-trained classifier can cope with various issues. 3) **Secure authentication when biometrics are compromised**: Cardiac biometrics are permanently associated with a user and cannot be revoked or replaced. Once such biometrics are intercepted, the victim users have to manage the impact for the rest of their lives. To address this, we design a repeatable and non-invertible method to generate cancelable feature templates as alternative credentials, which provides solutions to re-instate the account and protect privacy information.

The advantages of PPGPass are three-fold. First, it could be easily applied to existing wrist-worn wearables without extra hardware and cost, which enables every device to authenticate users via PPG sensors. Second, it is compatible with current commonly used techniques of mobile authentication, especially offering simultaneous authentication with users' signatures writing or passwords/PINs/patterns inputs. Third, collecting PPG signals requires physical contact with the skin, which is secure and intractable to steal or duplicate. Our extensive evaluations with multiple participants demonstrate that PPGPass is efficient and robust to verify users for mobile two-factor authentication.

The main contributions are listed in the following:

- We propose a novel mobile two-factor authentication system leveraging PPG sensors in wrist-worn wearables. To the best of our knowledge, PPGPass is the first work using PPG sensors to enable nonintrusive and secure user authentication in which users need no extra involvement and cancelable feature templates can be generated as new credentials when biometrics are compromised.
- We design a two-stage MAs removal algorithm to precisely separate clean heartbeat signals from original PPG signals with intensive noise, which enables the simultaneous verification of users with commonly used authentication approaches (e.g., signatures writing, passwords/PIN/patterns inputs), rather than requiring users to stay still.
- We explore 40 geometric features in the angle-domain from single cardiac cycle and multiple cardiac cycles. To further improve authentication accuracy, we perform data reshaping to align PPG signals in the angle-domain and develop two mechanisms to enrich the training dataset. We design an authentication model which consists of a Random Forest (RF) based user differentiator, and multiple Support Vector Data Description (SVDD) based adversary detectors. By combining them together, the model can detect adversaries and recognize a user in multi-user systems.
- We design a repeatable and non-invertible transform method to generate cancelable feature templates for classification, which support highly secure authentication and allow users to re-register alternative credentials against attacks.
- We conduct extensive experiments with multiple participants using our prototype. The results show that PPGPass can achieve the false acceptance rate of 3.11% and the false recognition rate of 3.71%, which confirms its efficiency and robustness.

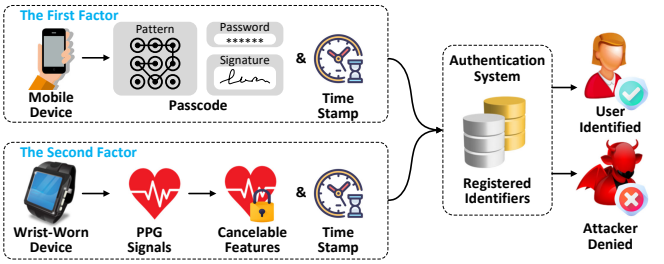


Fig. 1. Working paradigm of PPGPass.

The rest of this paper is organized as follows. Section 2 surveys related work. Section 3 introduces PPG sensors, design challenges, overview, and workflow. Section 4 presents details of data preprocessing. Section 5 describes data reshaping mechanism, geometric feature extraction and classification. Section 6 gives how to re-register new credentials when biometrics are compromised. Section 7 shows evaluation results. Finally, Section 8 concludes the paper. A preliminary of this paper appeared in [17].

2 Related Work

Heart-based Authentication: Electrocardiogram (ECG) has a long history in biometric authentication. For example, ECG features are extracted by Welch spectral analysis and principal component analysis, and then a k-nearest neighbors method is applied to verify users [18]. Cardiac Scan [19] uses geometric and non-volitional features of cardiac motion for continuous authentication. It uses a DC-coupled continuous-wave radar to collect heartbeat information for identity classification. In terms of PPG signals, authentication schemes have been explored from various perspectives. Fourier series analysis and semi-discrete decomposition

methods are applied to extract discriminable features [20]. CardioCam [21] collects pulse signals at fingertips to extract unique cardiac biometrics and achieve effective and reliable user verification. However, these methods require users to keep still during authentication, which fails in the moving hand scenarios. Zhao et.al [22], [23] propose a PPG-based continuous authentication system that mitigates mild and sparse MAs caused by far-wrist activities (e.g., moving forearm) using a special moving average filter. When near-wrist activities (e.g., grabbing a cup) occur and cause severe MAs, they discard the data contaminated by MAs, which greatly restricts the system usage scenarios. Moreover, they focus on one-factor authentication and can not be applied with conventional methods (i.e., writing signatures, input password/pattern) since they can not handle the MAs caused by near-wrist activities. In addition, independent component analysis, singular value decomposition, and adaptive filters have provided the opportunity to reduce MAs while preserving the morphological features of the original PPG [24]–[26]. These methods rely on additional hardware to obtain motion information to reduce MAs. Since the impact of movement on the MAs is rather vague, these approaches usually produce unreliable results. Therefore, there is a need to overcome the severe MAs and obtain accurate heartbeat signal without rely on additional hardware.

Cancelable Authentication: When biometrics are compromised, a hacker could be verified successfully to the systems by presenting biometrics. Unlike passwords that can be changed or reset, biometrics are permanently associated with a user and cannot be revoked or replaced, which results in the biometric credentials divulged forever. To address this, one view is to encrypt data at local devices and decrypt data at the system server. However, this creates a possible attack point to get access to the decrypted templates [27]. Brain Password [28] uses head-mounted devices to capture event-related brainwaves under visual stimuli and generates cancelable brainwaves by replacing different visual stimuli. For iris, fingerprint, and face-based authentication, many methods have been proposed to transform data in the signal domain or the frequency domain, which aim to morph original biometric templates [29]–[31]. Our work focuses on designing a PPG-based cancelable method for mobile two-factor authentication systems.

Mobile Two-factor Authentication: Bluetooth-based approaches execute cryptographic challenge-response protocols over a Bluetooth channel between an enrolled phone and a login device [32], [33]. While they may not easy to be compatible with standard web browsers. Proximity-Proof [34] verifies users by automatically transmitting a two-factor authentication response via inaudible OFDM-modulated acoustic signals to the system. Other RF signals, such as Wi-Fi [35], [36], are also leveraged to recognize and verify users. Acoustic sensing has been widely applied in many mobile applications (e.g., relative positioning [37], [38], driving motion detection [39]). In addition, EchoPrint [40] focuses on leveraging facial features obtained from both acoustic signals and vision for authentication. However, it uses a one-time login process, which is not secure enough to authenticate users in the duration of certain applications. Moreover, it relies on user's involvement in specific activities , which is inconvenient and degrade user experience.

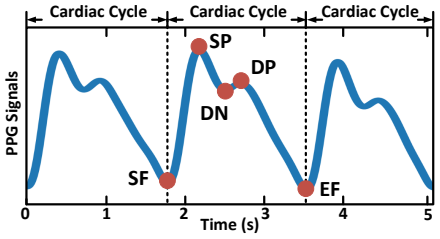


Fig. 2. Fiducial points in PPG signals.

Compared with existing works, PPGPass adds the cardiac feature extracted from PPG data as the second factor for authentication, which can handle intense MAs caused by near-wrist hand movements. Particularly, PPGPass proposes to generate cancelable features to avoid the security issue for biometrics. When applied to a two-factor authentication system, PPGPass is more suitable since it can verify the user's identity synchronously with the major authentication methods. Furthermore, the PPG-based authentication can be conducted secretly and requires no extra user effort.

3 Preliminaries

3.1 PPG Sensor

PPG signals reflect characteristics of human heartbeats, which can be easily obtained via PPG sensors in most commodity wrist-worn wearables. Specifically, a typical PPG sensor employs green, red, and infrared light sources and photodiode chips that are highly sensitive to light changes.

The basic principle of PPG sensors is to detect blood volume by measuring changes in light absorption. Cardiac motions contain successive human heart relaxation (diastole) and contraction (systole). As shown in Fig. 2, during one cardiac cycle, atria relax to fill with 70% blood of the total volume from atria through open mitral valve [19], which results in a sharp increase in PPG signals because blood absorbs more light than surrounding tissue [41]. The start of atria relaxation is the point of starting foot (SF) in PPG signals. Then, ventricles start to contract and pump blood, which is corresponding to a systolic peak (SP). Atria continue to relax and fill the remaining 20% blood (ventricles, at least, free up 10% of the volume for the contraction [19]), which results in a slower increase in PPG signals, then ventricles contract again. This process is corresponding to points from dicrotic notch (DN) to diastolic peak (DP) in PPG signals. To denote ending foot (EF), we set SF in the next cardiac cycle as the EF in the current cycle. Such five points in one cardiac cycle are denoted as fiducial points in PPG signals and play an important role in user authentication.

3.2 Challenges

In order to realize a nonintrusive and secure mobile two-factor user authentication using PPG sensors in wrist-worn wearables, the following challenges need to be addressed.

The first challenge is to separate clean heartbeats from PPG signals contaminated by MAs. MAs are caused by irregular distance changes between PPG sensors and the

wrist. A slight movement will lead to inaccurate heartbeat signals. Such noise has overlapping frequency with heartbeats component and especially exists in a mobile two-factor authentication system along with users' signatures writing or passwords/PINs/patterns inputs. The removal of these continuous and intense MAs remains a challenge that needs to be further studied. In this work, we propose a two-stage MAs removal algorithm to continuously separate clean heartbeat signals.

The second challenge is to characterize intrinsic and consistent features from PPG signals. In order to realize a highly secure authentication system, determining what kinds of features to extract is critical. Commonly used heartbeat features, such as HRV, are strongly influenced by specific states (e.g., emotions) [42]. Thus, they suffer from insufficient authentication accuracy, especially in the presence of MAs. In this work, we extract geometric features based on fiducial points that reflect the consistent characteristics of individual heartbeats. To further improve authentication accuracy, we perform data reshaping to align PPG signals in the angle-domain and use data augmentation methods to enrich the training dataset.

The third challenge is to generate alternative credentials when biometrics are compromised. Cardiac biometric information is permanently associated with a user, which leads to an issue that when compromised it cannot be revoked or replaced. Moreover, if the biometrics are compromised in one application, it can be used to compromise other applications that apply the same biometrics [27]. In this work, we design a repeatable and non-invertible transform method to generate cancelable feature templates, which allows users to re-register alternative credentials when biometrics are compromised.

3.3 System Model

We consider a two-factor user authentication system, which utilizes cardiac traits extracted from PPG sensor of wrist-worn device and passcode collected by a mobile device (e.g., smartphones, smartwatches, tablets, or multi-touch laptops). To a user, he/she only needs to unlock the mobile device with the passcode and does not need to cooperate explicitly to extract cardiac traits. To better understand the authentication scheme, it is necessary to describe the communication model and adversary model.

3.3.1 Communication Model

We design the two-factor authentication that involves two participants: a set of users and a single remote server. The mobile device and wrist-worn device obtain the passcode and cardiac traits of each user and send them to the server. The server verifies the user and warns the presence of user spoofing. Furthermore, the authentication process typically consists of four phases: user enrollment, login, user authentication, and identifier change phase. In the user enroll phase, the user submits his/her passcode and the cardiac trait. Then the server issues a unique identifier, which consists of the passcode and the cardiac features. In the login phase, the user sends a login request to the server. In the user authentication phase, the user first verifies the legitimacy of the server, then the user sends his/her passcode and the cardiac trait to the server. To prevent replay attacks, we adopt a well-established encrypted time-stamped identifier. The server examines the time-stamped identifier to ascertain that the submitted credentials are originally collected, and the server establishes trust only when the user provides both the correct passcode and the cardiac features. When user spoofing is detected or the user requests to change the stored credential, the user submits a new passcode and new cardiac features. Specifically, we design a novel method to transfer cardiac features to a features vector because cardiac features are permanent and can not be changed manually.

3.3.2 Adversary Model

What a truly two-factor scheme can ensure is that, only the user who possesses both a correct passcode and a valid cardiac trait can be successfully verified by the server. We consider user spoofing in such two-factor authentication system:

1) Random attack: the adversary can randomly guess the passcode and provide his/her cardiac trait for authentication. Though such assumption is reasonable, it is inadequate to pose a practical threat because it is hard for the adversary to guess the correct passcode and cheat on the cardiac trait-based verification at the same time. Moreover, a determined adversary can eavesdrop the passcode through compromising databases, shoulder surfing, etc. In this case, the two-factor authentication is degraded to single-factor authentication. The adversary launches attacks by wearing user's wearable devices and providing his/her own cardiac trait for authentication, which is similar to the brute-force attack. We have study the performance of our system when defending against the random attack in Section 7.4.
2) Replay attack: the PPG duplication technology experience a sluggish development. PPG signal collection requires skin contact with sensors, which is inconvenient to duplicate, and nearly impossible to replay and fool the sensor. However, a replay attack could be conducted by an adversary user who eavesdrops between the communicating parties, e,g., in full control of the communication channel. In this case, the adversary can intercept the passcode and the cardiac traits then retransmit them to launch attacks. Nevertheless, the times-tamp discrepancy [43] can be used to limit the impact of replay attacks.

Moreover, some adversaries eavesdrop on the communication between two targets through man-in-the-middle-attack to steal private information. For example, health conditions or cardiac diseases might be inferred from cardiac features. An adversary user can analyze the cardiac features and sell information of users with heart disease to medical providers. Furthermore, an adversary user can use the data of users with specific cardiac diseases to fool a healthcare system that allocates health benefits to certain patients. The healthcare system may mistakenly classify this adversarial user as someone who has a certain illness and hence this adversarial user can be qualified to enjoy certain healthcare treatments or benefits.

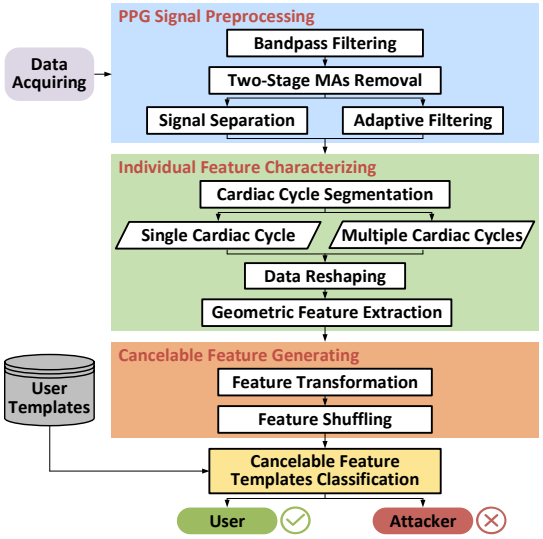


Fig. 3. Overview of PPGPass.

3.4 Overview & Workflow

We consider the two factors for authentication separately. The first factor can be commonly used mobile authentication methods such as password verification, pattern verification, and signature verification. Typically, such authentication schemes consist of three basic phases, register a unique passcode, the user inputs the passcode on the mobile device, and then the passcode is sent to the server for verification.

In this paper, we focus on the study of the second factor for authentication, which explores using PPG features to identify the user. The overview of PPGPass is shown in Fig. 3, which consists of three parts: *PPG Signal Preprocessing*, *Individual Feature Characterizing*, and *Cancelable Feature Generating*. PPG signals are continuously acquired via wrist-worn devices. In *PPG Signal Preprocessing*, the original signals firstly go through a bandpass filter. Secondly, the signals are further cleaned by a two-stage MAs removal algorithm (including signal separation and adaptive filtering), which results in noise-free heartbeat signals. In *Individual Feature Characterizing*, PPGPass firstly segments the obtained clean heartbeat signals by cardiac cycles. Then, in order to reduce the effect of the dynamic nature of biometrics (presenting nonstationary over time), PPGPass reshapes signals from the time-domain to the angle-domain and extracts critical and consistent geometric features from both single and multiple cardiac cycles. In *Cancelable Feature Generating*, PPGPass transforms the extracted features to generate cancelable feature templates and shuffles the features, which can be used for re-registering as alternative credentials. Lastly, the cancelable feature templates are sent to the server, where PPGPass constructs an authenticator based on the Random Forest (RF) classifier and multiple Support Vector Data Description (SVDD) classifiers. Moreover, to prevent an adversary from launching replay attacks using the intercepted features, similar to [43], an encrypted time-stamped identifier is generated for each cancelable feature template.

As shown in Fig. 4, the workflow of PPGPass mainly includes two phases: *User Enrollment Phase* and *User Authentication Phase*. In *User Enrollment Phase*, PPGPass acquires

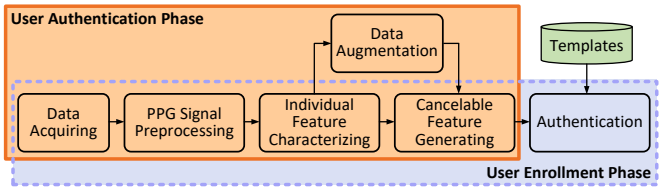


Fig. 4. Workflow of PPGPass.

PPG signals from every new user via wrist-worn wearables. The signals are then processed by *PPG Signal Preprocessing*, and *Individual Feature Characterizing*. Before *Cancelable Feature Generating*, we perform *Data Augmentation* to enrich the training data. Note that this phase is conducted on personal wrist-worn wearables at the user-end locally. Then, the generated cancelable features are sent from the user-end to the server-end. At the server end, an SVDD-based adversary detector is trained for each new user, and the RF-based user differentiator is updated. In *User Authentication Phase*, like in the user enrollment phase, PPGPass noninstrusively acquires PPG signals from a user and performs *PPG Signal Preprocessing*, *Individual Feature Characterizing*, and *Cancelable Feature Generating*. Then, at the server end, the user differentiator examines the extracted features and outputs a predicted user ID. After that, an adversary detector validates the user. After each authentication, we update the recognition model to improve system performance. When biometrics are compromised, PPGPass enables to generate cancelable feature templates as alternative credentials for re-registering. This process is similar to reassign a new bank account to the user whose account is compromised.

4 PPG Signal Preprocessing

4.1 Data Filtering

Synchronized with individual heartbeats, PPG signals can be leveraged as intrinsic biometrics to authenticate users. However, users' behaviors in other common authentication techniques (e.g., writing signatures, passwords/PINs/patterns inputs) and surrounding environmental changes cause inevitable noise on PPG signals obtained via wrist-worn wearables. In order to realize noninstrusive user authentication (not require users to stay still during authentication), the acquisition of clean PPG signals (heartbeat signals) is necessary.

Since the human heart rate is generally 50-100 beats per minute, we apply a fourth-order Butterworth filter with a bandwidth of 0.25-$10Hz$ on original PPG signals. After this process, noises caused by baseband drift (due to breathing) and power-line are filtered, remaining heartbeat signals and MAs. Because the frequency spectrum of MAs ($0.1Hz$ or more) has every chance of overlapping with that of heartbeat signals (0.5-$4Hz$) [26], we continue to process PPG signals by the designed algorithm in the following, which aims to further effectively remove MAs in PPG signals.

4.2 Two-Stage MAs Removal Algorithm

Fig. 5 shows the interference of MAs on PPG signals collected via a wrist-worn wearable. Before T_1, a user remains

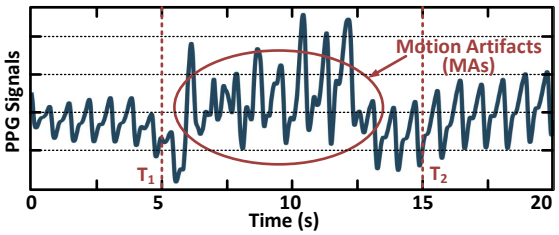


Fig. 5. PPG signals contaminated by MAs.

stationary and the signals are relatively periodic. Then, the user is asked to write sentences about 10 seconds from T_1 to T_2. We observe that the signals are dramatically changed in random patterns.

Previous MAs removal methods can only be applied to sudden, short-lived, and slight MAs. While, PPGPass aims to provide a nonintrusive two-factor user authentication with existing approaches, such as writing signatures or entering passwords. Under such scenarios, PPG signals are mixed with continuous and intense MAs, which cannot be directly used to extract characteristics for user authentication.

To tackle this problem, inspired by semi-blind source separation (S-BSS) and adaptive filtering methods, we design a two-stage MAs removal algorithm to separate clean heartbeat signals from original PPG signals. In the first stage, we use a modified S-BSS algorithm [25] to estimate heartbeat signals and MAs. In the second stage, the estimated signals from the first stage are invoked as reference signals, and then we apply adaptive filtering to obtain clean heartbeat signals.

4.2.1 The First Stage

The basic task of S-BSS is estimating parts of source signals that are linearly combined in observations. The process is formulated as extracting one or more signals in time t, denoted as an n-dimensional vector $S(t) = [S_1(t), ..., S_n(t)]^{\mathrm{T}}$, from an observed m-dimensional signals mixed vector $X(t) = [X_1(t), ..., X_m(t)]^{\mathrm{T}}$ by estimating an unknown matrix W: $S(t) = W^T X(t)$.

Generally, S-BSS assumes that the dimension of $S(t)$ is the same as that of $X(t)$: $n = m$. After data filtering, PPG signals are two-dimensional composed of heartbeat signals and MAs: $S(t) = [S_{heart}(t), S_{ma}(t)]^{\mathrm{T}}$. In order to obtain the same dimensional vector $X(t)$, we collect both green and infrared light data from a PPG sensor at the same time: $X(t) = [X_{green}(t), X_{infrared}(t)]^{\mathrm{T}}$.

Heartbeat signals are quasi-periodic and MAs signals are non-periodic. So, given a heartbeat period τ, the following conditions are satisfied in $S(t)$:

$$\begin{aligned} &\mathbb{E}\{S_{heart}(k)S_{heart}(k+\tau)\} > 0, \\ &\mathbb{E}\{S_{ma}(k)S_{ma}(k+\tau)\} = 0, \end{aligned} \tag{1}$$

where k is a time in t and $\mathbb{E}\{*\}$ is an expectation operator. Under the condition $\|W\| = 1$, the objective function in S-BSS algorithm to solve W is:

$$\begin{aligned} maximize \quad J(W) &= \mathbb{E}\{S(k)S(k+\tau)\} \\ &= W\mathbb{E}\left\{X(k)X(k+\tau)^{\mathrm{T}}\right\}W^{\mathrm{T}}. \end{aligned} \tag{2}$$

According to Equ. (1), for the desired source signals $S_{heart}(t)$, $J(W)$ will reach a high value, while other signals $S_{ma}(t)$ will make $J(W)$ reach a low value. So we can estimate $S_{heart}(t)$ by maximizing $J(W)$. According to Equ. (2), the objective function can be written as:

$$\begin{aligned} J(W) &= \frac{1}{2}J(W) + \frac{1}{2}J(W)^{\mathrm{T}} \\ &= \frac{1}{2}W(H_X(\tau) + H_X(\tau)^{\mathrm{T}})W^{\mathrm{T}}, \end{aligned} \tag{3}$$

where $H_X(\tau) = \mathbb{E}\{X(k)X(k+\tau)^{\mathrm{T}}\}$. Then, the maximization of Equ. (2) is equivalent to finding the eigenvector corresponding to the maximum eigenvalue (denoted as an operator $\mathbb{EIG}(*)$) of $H_X(\tau) + H_X(\tau)^{\mathrm{T}}$:

$$W = \mathbb{EIG}(H_X(\tau) + H_X(\tau)^{\mathrm{T}}). \tag{4}$$

In practice, due to finite signal samples, cross-correlation values in Equ. (1) of $X(k)$ are calculated nonzero. Thus, we replace to solve W by:

$$W = \mathbb{EIG}(\sum_{i=1}^{P}(H_X(i\tau) + H_X(i\tau)^{\mathrm{T}})), \tag{5}$$

where P is a positive integer. The increase of P will make the converged solution W closer to the ideal result and ensure the successful extraction of the next stage.

4.2.2 The Second Stage

Heartbeat signals and MAs are assumed to be linearly mixed in PPG signals in the first stage. In fact, they are not ideally linear mixed. In order to further remove MAs, we apply an adaptive filter to continue to clean MAs in PPG signals.

We use the output data $S_{ma}(t)$ from the first stage as reference signals, which is the key to achieve the effective performance of adaptive filtering. Then, we apply adaptive step-size least mean squares (AS-LMS) [26] adaptive filtering for removing MAs. The effectiveness of the two-stage MAs removal algorithm is investigated in Section 7.8, which lays the foundation for PPGPass to authenticate users using PPG sensors in wrist-worn wearables.

4.2.3 Signal Period Estimation

We estimate the period τ of PPG signals by autocorrelation function, which provides potential periods. Since the MA removal algorithm in the first stage does not strictly require an optimal τ, we adopt two shortest periods τ_1 and τ_2 as a set of candidate periods: $\{i\tau_1, i\tau_2, i = 1, 2, 3, 4\}$. Because signals with lower skewness and kurtosis are regarded with less noise [26], we choose the best output data as clean heartbeat signals by comparing their skewness and kurtosis.

5 Individual Feature Characterizing

5.1 Segmentation

After signal preprocessing, we obtain clean heartbeat signals from the original PPG signals. Thus, heartbeat cycles can be segmented by finding local minimums and maximums. We use the first derivative and the second derivative to find the five fiducial points (SF, SP, DN, DP, and EF) in each cycle.

TABLE 1
Geometric Features based on Fiducial Points

Category	Feature	Description
Point-Based	$S(sp)$, $S(dn)$, $S(dp)$	Peak values of fiducial points.
	$L(sp,dp)$, $\sum \boldsymbol{L(dp_i, dp_{i+1})}$	Differences between X-axis of points.
	$\frac{S(sp)-S(sf)}{L(sf,sp)}$	Combination of the above two cases.
	$\frac{L(sf,sp)}{L(sf,ef)}$, $\frac{L(sf,dn)}{L(sf,ef)}$, $\frac{L(sf,dp)}{L(sf,ef)}$, $\frac{L(dp,ef)}{L(sf,dp)}$, $\sum \frac{\boldsymbol{L(sp_i,dn_i)}}{\boldsymbol{L(sp_i,sf_{i+1})}}$	Ratios of differences between X-axis of points.
	$\lvert S(dn) - y_{sfdn}\rvert$, $\boldsymbol{\lvert S(sf) - y_{spsf}\rvert}$, $\sum \frac{\boldsymbol{\lvert S(sp)-y_{spsp}\rvert}}{\boldsymbol{\lvert S(sf)-y_{spsp}\rvert}}$	Points of tangency.
Area-Based	$A(sf,dn)$, $A(sf,dp)$, $A(dn,ef)$, $A(dp,ef)$	Areas enclosed by X-axis and S between points.
Statistic-Based	$\sum_{dp}^{ef} \lvert V\rvert$, $\sum_{sf}^{ef} \lvert V\rvert$, $\frac{\sum \lvert V>0\rvert}{\sum \lvert V<0\rvert}$, $\frac{\sum_{sp}^{ef} \lvert V\rvert}{\sum_{sp}^{ef} \lvert S\rvert}$, $\frac{\sum_{sf}^{sp} \lvert V\rvert}{\sum_{sf}^{ef} \lvert S\rvert}$	Sums of S and V and their combinations.
	$\frac{\sum \lvert V>0\rvert}{C(V>0)} * \frac{\sum \lvert V<0\rvert}{C(V<0)}$	Sums and counts of V.
	$\frac{\sum_{sf}^{sp} \lvert V\rvert}{L(sf,sp)}$, $\frac{\sum_{sp}^{ef} \lvert V\rvert}{L(sp,ef)}$, $\frac{\sum_{sf}^{sp} \lvert V\rvert}{L(sf,sp)} * \frac{\sum_{sp}^{ef} \lvert V\rvert}{L(sp,ef)}$, $\frac{\sum_{sp}^{ef} \lvert V\rvert}{\sum_{sf}^{ef} \lvert V\rvert} * \frac{L(sp,ef)}{L(sf,ef)}$	Combination of sums of V and $L(*)$.
	$\boldsymbol{\sum_{sp}^{sf} \lvert S - y_{sfsp}\rvert}$, $\boldsymbol{\sum_{sf}^{sp} \lvert S - y_{sfsp}\rvert}$, $\boldsymbol{\sum_{sf}^{sp} \lvert S - y_{sfsp}\rvert}$	Sum of differences between S and y_{sfsp}.
	$\boldsymbol{\sum_{sp}^{ef} \lvert S - y_{sfsf}\rvert}$, $\boldsymbol{\sum_{dp}^{ef} \lvert S - y_{sfsf}\rvert}$, $\frac{\boldsymbol{\sum_{sf}^{sp} \lvert S-y_{sfsf}\rvert}}{\boldsymbol{\sum_{sp}^{ef} \lvert S-y_{sfsf}\rvert}}$, $\frac{\boldsymbol{\sum_{sf}^{sp} \lvert S-y_{sfsf}\rvert}}{\boldsymbol{\sum_{sf}^{ef} \lvert S-y_{sfsf}\rvert}}$	Sum of differences between S and y_{sfsf}.
	$\boldsymbol{\sum_{sp}^{dp} \lvert S - y_{spsp}\rvert}$, $\boldsymbol{\sum_{dn}^{dp} \lvert S - y_{spsp}\rvert}$, $\frac{\boldsymbol{\sum_{sp}^{dn} \lvert S-y_{spsp}\rvert}}{\boldsymbol{\sum_{sp}^{sf} \lvert S-y_{spsp}\rvert}}$, $\frac{\boldsymbol{\sum_{sp}^{dn} \lvert S-y_{spsp}\rvert}}{\boldsymbol{\sum_{sp}^{sf} \lvert S-y_{spsp}\rvert}}$	Sum of differences between S and y_{spsp}.
	$\frac{\boldsymbol{\sum_{sf}^{sp} \lvert S-y_{sfsf}\rvert}}{\boldsymbol{\sum_{sp}^{sp} \lvert S-y_{spsp}\rvert}}$	Combination of the above two cases.

i and $i+1$ present the current cycle and the next cycle, respectively.
Multiple cycles features are in **bold**.

5.2 Feature Extraction

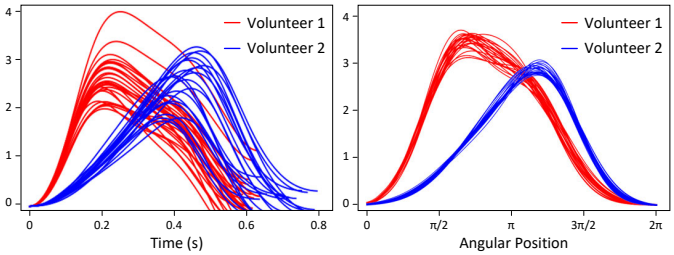
In heart-based authentication systems with minimal security requirements, instantaneous and average heart rate are used as authentication features. However, two people with different patterns of heartbeat signals can share the same heart rate. In addition, heart rate can be artificially accelerated or decelerated through exercise or meditation. Commonly used HRV features are also used for authentication. However, they vary with different emotions, postures, and signal acquisition locations.

Fig. 6(a) shows the derived clean PPG signals from two volunteers. It can be observed that PPG signals exhibit a significant difference in the shape of heartbeat signals between two volunteers. Also, we can easily observe that PPG signals from a volunteer have unique patterns such as the near positions of peak and trough. These demonstrate the potential that geometric features based on signal shapes can be used in verifying users.

To capture the characteristics of individual heartbeat signals, particularly as shown in Table. 1, we explore 40 geometric features based on the five fiducial points from a single cardiac cycle and multiple cardiac cycles.

The features can be categorized into three types: *Point-Based*, *Area-Based*, and *Statistic-Based*. We use S to represent values of heartbeat signals and use V to represent the first derivative of S. *Point-Based* features contain peak values and differences between X-axis of points such as $S(sp)$, $L(sp,dp)$, and $\sum L(dp_i, dp_{i+1})$, where $L(*)$ is an operator calculating differences between X-axis of points. Additionally, it also includes points of tangency, such as $|S(dn) - y_{sfdn}|$, $|S(sf) - y_{spsf}|$, and $\sum \frac{|S(sp)-y_{spsp}|}{|S(sf)-y_{spsp}|}$, where y_{sfdn} is a line connection SF and DN in one cycle, y_{spsf} and y_{spsp} are lines connection SP in the current cycle and SF and SP respectively in the next cycle. *Area-Based* features contain areas enclosed by X-axis and S including $A(sf,dn)$, $A(sf,dp)$, $A(dn,ef)$, and $A(dp,ef)$, where $A(*)$ is an operator calculating definite integral for S. To obtain statistic features, we define $C(*)$ as a counting operator. We also define y_{sfsp} as the line connecting SF and SP in one cycle. For multiple cycles, we define y_{sfsf} as the line connecting point SF in the current cycle and the next cycle. *Statistic-Based* features contain sums and counts of V, and sum differences between S and the defined lines.

5.3 Data Reshaping



(a) Time-domain PPG signals (b) Angle-domain PPG signals

Fig. 6. Illustration of PPG signals.

Due to the dynamic nature of biometrics, signal lengths and amplitudes between cycles of PPG signals present non-stationary over time. If geometric features are extracted directly from the time-domain, such differences will influence the uniqueness of features. So, we align the PPG signals by transforming them from time-domain $S(t)$ to angle-domain $S(\theta)$ using the following formula [44]:

$$S(\theta) = \sum_{i \in \{sf,sp,dn,dp,ef\}} a_i \Delta\theta_i exp\left(-\frac{\Delta\theta_i^2}{2b_i^2}\right). \quad (6)$$

The variable θ represents instantaneous angular position, where $\theta = tan^{-1}(S(t)/t)$. The variables $\{sf, sp, dn, dp, ef\}$ represent five fiducial points, and θ_i represents their angular potions with $i \in \{sf, sp, dn, dp, ef\}$. $\Delta\theta_i = (\theta - \theta_i) \, mod \, 2\pi$ for each fiducial point position θ_i. Each

component $a_i \Delta\theta_i exp\left(-\frac{\Delta\theta_i^2}{2b_i^2}\right)$ can be described in the form of Gaussian distribution, and a_i and b_i are estimated by Expectation Maximization (EM) algorithm.

Fig. 6 (a) shows the time-domain PPG signals, and Fig. 6 (b) shows the reshaped PPG signal in the angle-domain, respectively. We can observe that the angle-domain signals of the same user show smaller variances in the positions of the fiducial points. At the same time, angle-domain signals of different users remain distinct. Therefore, the derived features of the same user can be more unique in the angle-domain, thus helps to overcome variances in features and improves authentication accuracy.

5.4 Cancelable Feature Temples Classification

5.4.1 Data Augmentation

In *User Enrollment Phase*, the classifier requires sufficient training data to accommodate variations of heartbeat under various practical scenarios. However, it is inconvenient and usually takes a lot of effort to collect sufficient training data from users. To relieve the pain of data collection, we collect a small amount of data from users and enrich the training data using data augmentation techniques.

Data augmentation aims to regenerate data sets from the existed data sets, expand the limited training data sets and achieve accurate authentication. Conventional data augmentation techniques is usually used in the field of computer image recognition, such as flip, rotation, cropping, and scale scaling. Several research studies have investigated data augmentation for sensor data. Thickstun *et al.* [45] augment music by stretching or shrinking the data with linear interpolation. McFee *et al.* [46] use an audio degradation toolbox to generate addition training data. The toolbox is originally designed to test the robustness of audio analysis methods against degradations of the audio quality, which might lead to domain-specific augmentation problems. Li *et al.* [47] exploit to create additional accelerometer and gyroscope data by perturbing the location of the sensor data (permutation and cropping), distorting the timestamps between elements (sampling), and increasing noise (scaling and jittering). Kiyasseh *et al.* [48] focus on the augmentation of time-series PPG by masking randomly-chosen time and/or frequency bands in a spectrogram representation. Though these methods show promising results, these could be detrimental in our design. The time-warping and addition noise might change the underlying data distribution and degrade authentication. The mask of frequency bands might affect the subsequent feature extraction.

To design a data augmentation method suitable for our application, we ask seven participants to collect PPG signals in different situations, such as different emotions and psychological pressures. We observe that the PPG waveforms exhibit complex morphological changes, which are hard to study quantitatively due the natural variability of PPG waveforms. Therefore, we turn to study the features extracted from PPG signals. Based on our experiments, we observe that the heartbeat features are different in values under different emotions, pressures, and circadian rhythms. In addition, the denoised heartbeat signals might diverse in feature values due to the different intensities of MAs. Therefore, we expand the training data set by enriching the heartbeat feature values.

We carefully compare the feature values collected by the same user in different scenarios and find that features vary in a small range. Also, we observe that some features are related, e.g., $S(sp)$ and $\frac{S(sp)-S(sf)}{L(sf,sp)}$ increase or decrease synchronously. By reasonably enriching the value of the features based on their relations, we can estimate the feature collected in different situations.

Therefore, we perform the following operations to enrich features value:

1) **Change feature values based on their relations**. To model the relations between the heartbeat features, we build a feature graph. We start from building trees, and each tree starts from a root node that represents a point-based feature such as $S(sp)$. Then, we construct its child nodes, which include all the features directly related to it (e.g., features that are linearly related to the current feature). If a feature is directly related to multiple features, we join these nodes by edges. We keep adding features directly related to each node as child nodes until all features are included. Considering that some features are positive related, some are negative related, we save the graph in the form of matrix G:

$$G = \begin{bmatrix} 0 & 1 & ... & 2 \\ 1 & 0 & ... & 1/4 \\ \vdots & \vdots & \ddots & \vdots \\ 1/2 & 4 & ... & 0 \end{bmatrix}$$

Each row and each column represents heartbeat features. The i^{th} row and j^{th} column entry of the matrix describes the detailed relationship between the i^{th} feature and j^{th} feature. If the element is 0, it means that the two features are unrelated.
After obtaining the feature graph, we change feature values based on the feature graph. The relations of features (nodes in the graph) are preserved. This can be regarded as scaling the features to certain classes of fluctuation. We first change the value of the root node to its $\varpi\%$, and then change their related features accordingly (positive or negative). If a node is not adjacent to any other node, it is scaled to its $\varpi\%$. In our case, $varpi$ is experimentally set to be within $[95, 105]$. By preserving the labels and change the feature values, we obtain new feature sequences and enrich the training data.
2) **All features add or subtract a random value**. This is a primitive approach to change feature values. Given a feature sequence $F = \{f_1, f_2, ..., f_{40}\}$, we preserve its label and add or subtract a random value ζ to the features as: $F = \{f_1 + \zeta, f_2 + \zeta, ..., f_{40} + \zeta\}$ or $F = \{f_1 - \zeta, f_2 - \zeta, ..., f_{40} - \zeta\}$. Finally, a new feature sequence can be obtained. To better accommodate variations in features and ensure security, we set the random value ζ no more than 5% of the maximum value of the feature series.

5.4.2 Authentication Model

As PPGPass aims to allow users to re-register new credentials when biometrics (PPG signals or feature templates)

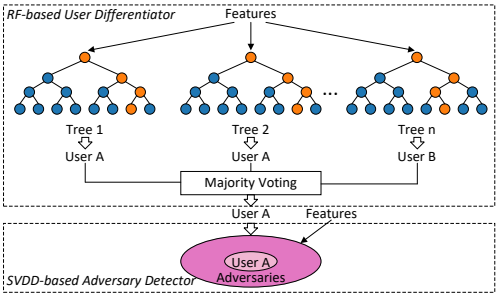


Fig. 7. Authentication model of PPGPass.

are compromised, instead of the original augmented features, the input features for a random forest classifier are cancelable features, which will be described in detail in Section 6. Therefore, when biometrics are compromised, PPGPass enables to generate new sets of cancelable features, which will be used as alternative credentials for users to re-register in the system.

We make the following considerations when designing the authentication model.

1) The classifier should distinguish adversaries and verify legitimate users accurately. This is essential for authentication systems.
2) The heart-based biometrics may change over time. The classifier should be able to overcome the inconsistency of heartbeat features.
3) The overall computing cost and storage cost should be minimized.

Based on the above discussions, our basic idea is to build an adversary detector for each user to validate a legitimate user, and also build a user differentiator to recognize a user for multi-user systems.

Since the adversaries will never provide their data from training, we apply a one-class classifier to overcome the imbalanced training data. Popular approaches such as similarity/distance-based classifiers only provide *hard classification*, and a reasonable threshold takes a lot of effort to establish. Therefore, we adopt *SVDD*, which determines the boundary of a specific user class and assigns a sample to that class according to whether it falls within or outside the boundary.

As for multi-user systems, we adopt the RF classifier to recognize users. RF is an ensemble of decision trees, which avoids overfitting when building enough trees. Previous works have demonstrated that RF receives high accuracy in user verification. In addition, RF requires little computation cost when training and updating. Combined with SVDD, the authentication model can distinguish the specific user from other users and adversaries. We compare RF and SVDD with several commonly used classifier in Section 7.6.1.

Although several classifiers such as decision tree, support vector machine, and k-nearest neighbor perform well in related works, we choose RF because it has the best performance in our experimentally study, which is presented in Section 5.5

5.4.3 Model Training and Classification

Fig. 7 shows the architecture of the proposed authentication model, which consists of an RF-based user differentiator and an SVDD-based adversary detector. During the *User Enrollment Phase*, users provide their heartbeat signals to the system. Afterward, PPGPass performs *PPG Signal Preprocessing*, *Individual Feature Characterizing*, *Data Augmentation*, and *Cancelable Feature Generating* to the collected PPG signals and obtains the augmented, transferred features. In the server end, we first train an adversary detector for each user. Specifically, we feed the features of a specific user to an SVDD classifier, which determines the boundary of the legitimate user class and adversaries class. Meanwhile, the features from different users are mixed together to train RF. We first use bagging to randomly draw feature samples and then grow a decision tree for each set of feature samples.

During the *User Authentication Phase*, when an anonymous user wearing a wrist-worn wearable wants to access the system via two-factor authentication with existing approaches, such as writing signatures or entering passwords, PPGPass launches PPG sensors of the wearable. The collected PPG signals are processed through *PPG signal preprocessing*, *individual feature characterizing*, and *cancelable feature generating*, resulting in cancelable feature templates. During classification, the transformed features are submitted to the server. The system examines the time-stamped identifiers to ascertain that the measurements are originally collected. Then we verify the submitted passcode (e.g., password, pattern, signature) by implementing existing schemes. As for the transformed PPG features, we analyze them with the pre-trained decision trees and generate the final classification result by majority vote. Then, we use the adversary detector of the predicted user to determine whether this access is legitimate.

5.4.4 Detection of Adversaries

If a user provides the wrong passcode and invalid identity features, we consider him/her an adversary, and we warn the user who he/she claims to be. When an anonymous user provides a valid passcode and an invalid PPG feature template, he/she might be an adversary who somehow eavesdrops on the first factor. Therefore, we check the number of attempts of the user, and we determine an adversary as he/she reached maximum attempts. In contrast, when an anonymous user provides a valid PPG feature template and an invalid passcode, he/she is more likely to be a legitimate user who has forgotten the passcode, because in our context, *who you are* is harder to attack than *what your know*. For those users, we set a higher threshold for the maximum attempts. If the user exceeds the maximum number of attempts, he/she will be considered an attacker. The limit of login attempts effectively prevents random attacks, which adds an extra layer of security.

5.4.5 Model Updating

To overcome the dynamic nature of heartbeat features, we update the classification model after successful recognitions. For single-user systems, we expand the training data to include the newly collected data and retrain the SVDD classifier regularly. For multi-user systems, we first retrain

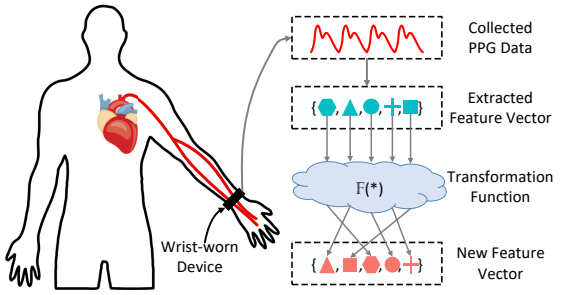


Fig. 8. The transformation function changes the extracted feature vector to a new feature vector.

the SVDD classifier for the specific user. Then each decision threshold is updated from leaf nodes to root nodes.

6 Cancelable Feature Generating

6.1 Security Issues

Biometrics, such as fingerprints, iris, face, and cardiac motion, present unique individual characteristics, which have been leveraged for user authentication with high accuracy. However, the use of biometrics raises three main security issues as follows.

Noncancelable: When biometrics are compromised, a hacker could be verified successfully to systems by presenting biometrics via replay attacks. Unlike passwords that can be changed or reset, biometrics are permanently associated with a user and cannot be revoked or replaced, which results in the biometric credentials divulged forever.

Application Cross-matching: Biometrics probably are used to register in multiple applications. If biometrics are compromised, a hacker could use the same method to get access to all these applications.

Privacy Leakage: Biometrics themselves imply some kinds of private information. For example, health conditions or cardiac diseases might be inferred from cardiac features. When using biometrics as inputs for authentication, users have a concern about invasion of privacy.

6.2 Feature Transformation

To solve the above issues, we propose to convert the extracted geometric features by a transform function $\mathbb{F}(*)$. As shown in Fig. 8, the original feature vector is transformed by the transformation function, which changes the order and value of the elements in the feature vector. In other words, our system modifies the PPG features to avoid any potential risk. In practice, when a user needs to change his/her PPG-based credential, the system will update the user's identity profile in the database through a new transformation function. Furthermore, users can register different applications through different transformation functions. Once the worst happens and data breach occurs in the database, the adversary cannot reverse the users' privacy information (i.e., physical condition) from the stored features because the real order and value of the elements in the feature vector are unknown to them.

Such a transforming process has two design guidelines as follows.

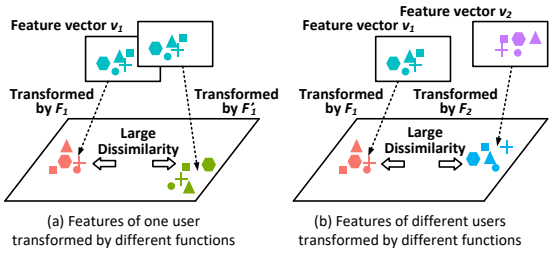


Fig. 9. Illustration of feature transformation strategies.

Repeatable: For regular user enrollment and every authentication phase, for one person the transform function fuses the extracted features in the same fashion. Once features are compromised, the transform function should generate a new variant (a new set of fused features) that will be used for re-registering a new credential. This process is similar to a bank giving a new credit card to a user when the card is stolen. In addition, the transform function should also generate different sets of fused features for different applications. Therefore, a repeatable transform function can solve the noncancelable issue and render cross-matching impossible.

Non-invertible: Even if the transform function is compromised, the original features or PPG signals (have been non-invertible reshaped and presented as features) should not be recovered. Therefore, a non-invertible transform function can avoid privacy leakage (recovery of secret heartbeat signals).

The strategies of transform function $\mathbb{F}(*)$ are in the following, which are also demonstrated in Fig. 9.

1) The new fused features transformed by function $\mathbb{F}_1$ of a feature vector $\boldsymbol{v_1}$ of one person should be distinct from the previous fused features transformed by function $\mathbb{F'}_1$, which is analogical to the case where using the previously used passwords cannot be allowed to log in after resetting new passwords:
$$Dist(\mathbb{F}_1(\boldsymbol{v_1}), \mathbb{F'}_1(\boldsymbol{v_1})) \geq \lambda, \quad (7)$$
where $Dist(*)$ is an operator to define the similarity between two feature vectors, and λ is a threshold.
2) To reduce false acceptance rate, distinguishable feature vectors from different people ($\boldsymbol{v_1}$ and $\boldsymbol{v_2}$) should maintain distinct after being fused by their corresponding transform functions ($\mathbb{F}_1$ and $\mathbb{F}_2$):
$$Dist(\boldsymbol{v_1}, \boldsymbol{v_2}) \geq \lambda \Rightarrow Dist(\mathbb{F}_1(\boldsymbol{v_1}), \mathbb{F}_2(\boldsymbol{v_2})) \geq \lambda. \quad (8)$$

Based on the above discussion, we aim to find the maximal dissimilarity between two fused feature vectors during feature transformation. We first design similarity measurement $Dist(*)$. We denote two feature vectors as $\boldsymbol{v_1} = \{p_1, p_2, ..., p_i, ..., p_N\}$ and $\boldsymbol{v_2} = \{q_1, q_2, ..., q_j, ..., q_N\}$, where N is the number of extracted features. We normalize each element and the normalized results are presented as $\bar{\boldsymbol{v_1}}$ and $\bar{\boldsymbol{v_2}}$. Then, we construct a complete bipartite graph $G = (V, E)$, where V are divided into two disjoint sets corresponding to the two vectors, respectively. The weight of each edge in E is the Euclidean norm of its connecting vertexes, denoted as $d(\bar{p}_i, \bar{q}_j)$. Next, in order to measure the similarity between the two vectors, we find a perfect

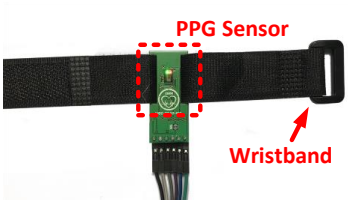


Fig. 10. Prototype of a wrist-worn device with a PPG sensor.

matching of minimum cost in G by the Hungarian method, in which the similarity measurement $Dist(*)$ is the found minimum cost:

$$Dist(\boldsymbol{v_1}, \boldsymbol{v_2}) = minimize \sum_{i,j \in 1,2,\ldots,N} d(\bar{p}_i, \bar{q}_j). \quad (9)$$

We use a transform function $\mathbb{F}$ to project a feature vector $\boldsymbol{v}$ onto another space: $\mathbb{F}(\boldsymbol{v}) = \boldsymbol{H}\boldsymbol{v}$, where $\boldsymbol{H}$ is a vector whose entries are independent realizations of Gaussian variables. In practice, we generate a large number of functions and then find a function that has the maximum $Dist(*)$ between feature vectors. Additionally, note that after transforming, in order to avoid linkability between the previous features and current features, we further shuffle the order of the features.

6.3 Re-instate Cancelable Features

After we propose the transformation method to generate cancelable feature templates, another problem arises, *when to re-instate (re-register) the cancelable features*. Of course, when a user requests to cancel and re-instate the account, the system will reallocate a transform function and issue a new identifier for the user. In addition, the system will lock the account when detecting user spoofing. Specifically, timestamp discrepancy identification, feature transformation method, and the elaborated recognition model effectively protect the second factor. Although a determined adversary can manage to compromise the first factor, he/she can only try to use his/her cardiac trait to pass the system by chance. In other words, a practical threat is that an adversary defeats the first factor but not the second factor. As discussed in Section 5.4.4, we can detect such attacks as he/she reached maximum attempts.

7 Evaluation

7.1 Experimental Setting

To validate the authentication performance of PPGPass, because existing manufacturers do not provide direct access to raw PPG signals, we develop a proof-of-concept prototype in a wrist-worn device using an off-the-shelf PPG sensor, which is shown in Fig. 10. The prototype consists of an integrated MAX30105 PPG sensor (with green and infrared light LEDs) and an adjustable wristband. The prototype is connected to a laptop equipped with Intel Core i7 CPU running at 3.2 GHz and 16 G memory. Note that the prototype is completely harmless to the human body, and we use a sample rate at $400Hz$.

TABLE 2
Success rate of attacks and attack detect rate for each participant's account.

Participant ID	1	2	3	4	5	6	7
FAR (%)	0.00	0.00	3.33	6.66	3.33	0.00	3.33
ADR (%)	100.00	100.00	96.66	93.33	96.66	100.00	96.66

7.2 Data Collection

PPG signals are collected from 7 healthy participants (4 males and 3 females), aged between 21 and 27. None of them has a history of heart disease. This study is conducted with the approval of the ethics committee of the facility. During data collection, we ask the participants to wear the prototype on the dominant hand and perform signature writing, password inputting, and pattern inputting, respectively. Each participant performs 6 sessions. In each session, PPG signals are collected repeatedly 30 times for each condition. At the same time, an ECG sensor (AD8232) is used to offer baselines. In addition, to ensure diversity, we ask users to collect data in various scenarios (e.g., sit, stand, in vehicles). In order to obtain data under continuous contact between the wrist and the PPG sensor in the process, we generate binary data from the collected PPG signals as an indication of error. When signals present one or more error bits, such unreasonable data will be discarded. Totally, we collect over 7600 samples for analysis. The collected samples are manually labeled.

7.3 Metrics

We use the following metrics to evaluate the effectiveness of our user authentication system:

False acceptance rate (FAR) & false recognition rate (FRR): FAR is the percentage of identification instances in which unauthorized persons are incorrectly accepted. FRR is the percentage of identification instances in which authorized persons are incorrectly rejected.

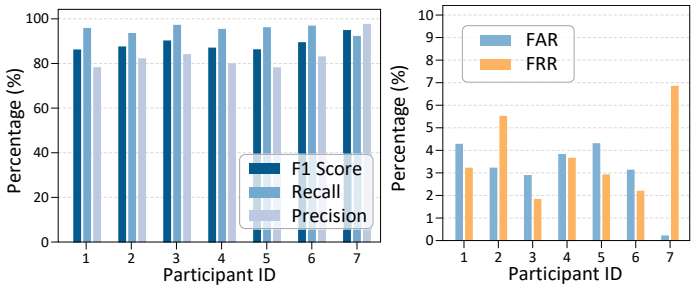
Recall & precision: Recall is the ratio of correctly predicted positives values to the actual positive values. Precision is the ratio of correctly predicted positive values to the total predicted positive values.

F1 score: As the ratio of the positive and negative class is unbalanced, we use F1 score to measure the accuracy of PPGPass, which is nonsensitive to class distribution: $F1 = 2 * precision * recall/(precision + recall)$.

7.4 Overall Performance

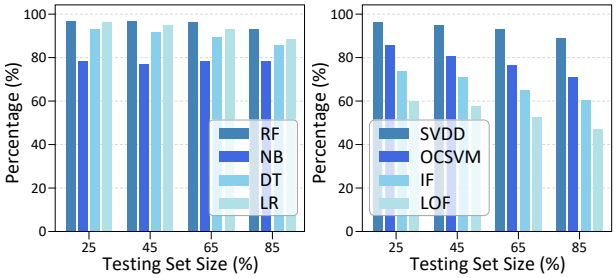
We evaluate the security and usability of PPGPass from two aspects. The first is how accurate is PPGPass in identifying legitimate users and adversaries. The second is how accurate is PPGPass in distinguishing different users.

We conduct an experiment to evaluate the effectiveness of PPGPass under the presence of user spoofing. As discussed in Section 3.3.2, a practical threat is the random attack that the adversary somehow eavesdrops the passcode and provides his/her own cardiac traits to try to impersonate a legitimate user. We process PPG data from each participant and construct an adversary detector for each user using his/her data. We ask the remaining six participants (adversaries) to provide their cardiac traits and try to pass



(a) F1 score, recall, and precision (b) FAR and FRR

Fig. 11. Performance in distinguishing legitimate users.



(a) User Differentiator (b) Adversary Detector

Fig. 12. Impact of Classifiers.

TABLE 3
Comparison with well-established related work.

Work	Credentials	Device	Require user effort	Address MA	Cancelability	Performance
[19]	Cardiac motion	Doppler radar sensor	Yes	No	No	BAC: 98.61%
[21]	Cardiac features	Cameras	Yes	No	No	TPR: 99% FPR: 4%
[22]	Cardiac features	Wrist-worn PPG device	No	Only mitigate mild MA	No	Accuracy: 90% FRR: 4%
[40]	Acoustic features & facial landmarks	Mobile phone	Yes	No	No	BAC: 93.75%
[28]	Brainwave	Head-mounted ECG device	Yes	Only remove ambulation-related MA	Yes	f-score: 95.46%
PPGPass (our work)	Cardiac features	Wrist-worn PPG device	No	Yes	Yes	FAR: 3.11% FRR: 3.73%

the system by chance. Up to five authentication attempts can be made. Overall, each participant's account was attacked 30 times. Table 2 shows the success rate of attacks (FAR) and attack detection rate (ADR) for each participant's account. We can observe that the FAR of all participants are less than 6.66%. Moreover, the ADR reaches to over 93.33%, and the ADR of participant 1, 2, and 6 reaches 100%. The result suggests that our proposed scheme is highly efficient and is secure when the firs factor is compromised.

Then, we conduct five-fold cross-validation to evaluate PPGPass in differentiating multiple users. Fig 11 shows the detailed F1 score, recall, precision, FAR, and FRR for each participant. We can observe that all participant receive recall more than 93.27%, which indicates that most of the cardiac traits are correctly distinguished. Besides, the average FAR is 3.11% and the average FRR is 3.73%, indicating that PPGPass performs well in distinguishing a legitimate user from others.

7.5 Comparative Study

A comparison between our work and the well-established related work is given in Table 3. We find it is difficult to compare the performance of related work due to different evaluation metrics and different datasets. Besides, some approaches did not explicitly report the training dataset size and testing dataset size. Thus, we summarize the results provided by these works in the *Performance* column. Moreover, we compare our design with the well-established related work in terms of authentication credentials, the sensing device, the requirement for user effort, ability to address MA, and cancelability. The result shows that the proposed method has a decent performance comparable to the other methods and has advantages of requiring zero user effort, addressing MA, and supporting cancelable biometric. Furthermore, it can be easily deployed in any PPG-mounted wearable devices.

7.6 Issue Study

7.6.1 *Impact of Classifiers*

We evaluate the performance of the user differentiator with 4 commonly used classifiers: Random Forest (RF), Naive Bayes (NB), Decision Trees (DT), and Logistic Regression (LR). We apply 4 cycles in feature extraction and 4 s sensing time. F1 scores of different testing set sizes are shown in Fig. 12 (a). Along with the increasing size of the testing set, F1 scores of all classifiers slightly go descending. RF has the highest F1 score among all the classifiers achieving 97.2%. The results show that RF has the best performance and is adopted in PPGPass.

We also evaluate the performance of the adversary detector with 4 commonly used one-class classifiers, including Support Vector Domain Description (SVDD), One-Class Support Vector Machines (OCSVM), Isolation Forest (IF), and Local Outlier Factor (LOF). All classifiers are implemented with default values. As shown in Fig. 12 (b), SVDD receives the best performance and is adopted in this work.

7.6.2 *Impact of Training Data Length*

To evaluate the time efficiency of PPGPass, we obtain its response time, which usually is related to signal sensing time. So, we restrict different sensing times in the experiment. During authentication, we extract features from all adjacent 4 cardiac cycles and make a decision on each of these features. When all of them are verified to the same user, this user is approved. Fig. 13 shows that F1 score of $4s$,

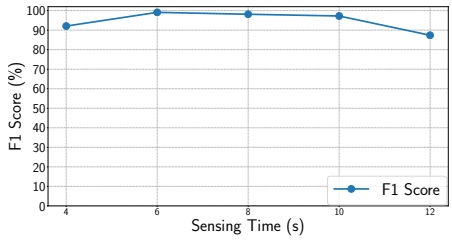


Fig. 13. Impact of data length.

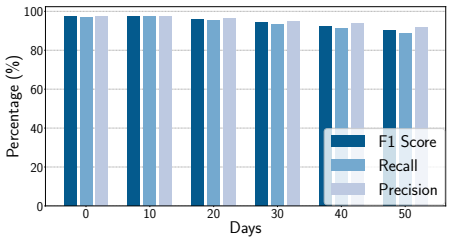


Fig. 14. Performance in a long-term study.

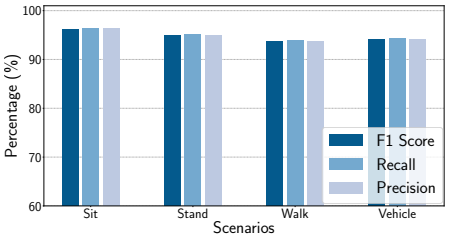


Fig. 15. Performance in three usage scenarios.

6s, 8s, 10s, and 12s sensing times are 92.1%, 99.1%, 98.1%, 97.2%, and 87.4%, respectively. The recall and precision have similar performance, whose corresponding values are 91.8%, 99.1%, 98.0%, 97.0%, 86.8%, and 92.4%, 99.1%, 98.2%, 97.4%, 87.9%, respectively. We observe that when sensing time is 4s, the system reaches accuracy above 90%, and the average system response time is 1.8s. Normally, the three conditions take time varying between 2-6s. Thus, the sensing time and condition completion time can be approximately synchronized for achieving high accuracy. The results show that users can be authenticated nonintrusively and efficiently.

7.6.3 *Long-Term Study*

Long-term performance is a critical aspect of authentication systems. Fig. 14 shows the F1 score of PPGPass among all the participants over 50 days. After training, the data of the testing set are collected on the same day, 10 days later, 20 days later, 30 days later, 40 days later, and 50 days later, respectively. We observe that the corresponding F1 score achieve 97.3%, 97.2%, 95.7%, 94.2%, 92.4%, and 90.1%, respectively. The F1 score is declined by 7.4%. The recall and precision have similar trends. They are declined by 8.7% and 6.0%, respectively. We conclude that the performance of the system has no significant descending in the long-term study, and PPGPass is robust against time change.

7.6.4 *Usage Study in Real Environments*

To validate that PPGPass can work robustly in various usage scenarios, we ask the participants to sit, stand, and walk in the controlled lab and sit in a moving vehicle to collect data. We focus on the typical condition of password input. PPG signals are continuously recorded using our prototype. The evaluation model is trained with 75% data collected in four cases and tested with the rest 25% data. Fig. 15 shows the results. Participants' upper body is almost static in the cases of sit and stand, which both receive F1 score over 95%. When walking and sitting in a moving vehicle, participants' upper body is unstable, which introduces variations to the collected data. Specifically, recall, precision, and F1 score of data collected during walking reach 93.73%, 93.82%, and 93.88%, respectively. Also, recall, precision, and F1 score of data collected during sitting in a moving vehicle reach 94.12%, 94.26%, and 94.19%, respectively. The results are acceptable in real-word experiment, and can be improved by enriching the training data set.

7.7 Authentication Performance in Combination With Conventional Authentication Schemes

Our design goal is to add cardiac traits as the second layer of security to existing mobile authentication schemes. Here we consider three commonly used authentication scenarios, enter passwords, draw patterns, and input signatures. Each participant is asked to collect PPG data in the three scenarios, and PPG features are extracted from 1 to 6 cardiac cycles. Fig. 16, Fig. 17, and Fig. 18 show the authentication results of enter passwords, draw patterns, and input signatures, respectively. Clearly, the number of feature extraction cycles plays an important role in the success of user identity verification. Along with the increase of cycles in feature extraction, the performance of PPGPass first improves and then goes stable. Particularly, when we use 4 cardiac cycles in feature extraction, the overall accuracy of PPGPass achieves the best performance.

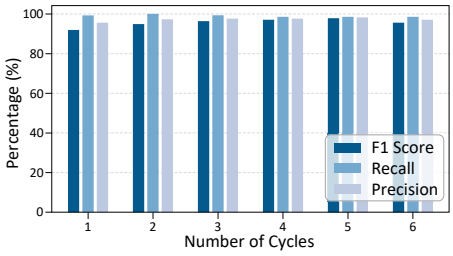
Moreover, we can observe that three scenarios are highly secure. The F1 score, recall, and precision for 4 cycles of the three scenarios are greater than 90%, and both FAR and FRR of the three scenarios are less than 5%. All these results confirm the soundness and security of PPGPass.

7.8 Efficiency of Two-Stage MAs Removal Algorithm

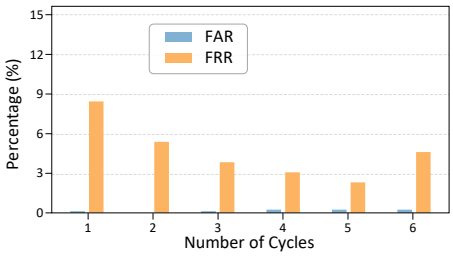
To evaluate the performance of the two-stage MAs removal algorithm, we use peak-to-peak intervals (PPIs) to measure accuracy in identifying the boundaries of each heartbeat cycle. We compare the PPIs estimated by the algorithm to those obtained from the ECG signals. After applying our proposed method, the mean absolute error decreases from 13.27 seconds to 3.59 seconds. As shown in Fig. 19, the coordinates of the scatter plot are the PPIs derived from ECG and PPG signals, respectively. Points on the diagonal have identical PPIs, and the distance to the diagonal is proportional to the error. We observe that after removing MAs, all points are clustered around the diagonal. Hence, the two-stage MAs removal algorithm can effectively restore heartbeat signals and provide a basis for PPGPass.

7.9 Effectiveness of Data Augmentation

To validate how well the data augmentation methods perform, we compare the authentication performance without and with data augmentation. We set the data augmentation rate to be five. The Authentication models with and without data augmentation are evaluated with the same dataset. Fig. 20 shows the comparing results under three conditions. As illustrated in Fig. 20 (b), performance with data augmentation outperforms performance without data

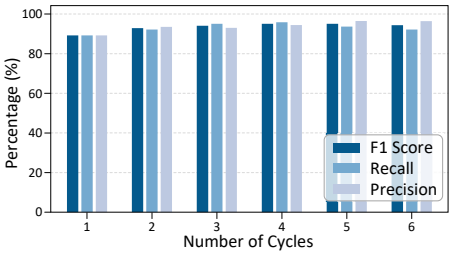


(a) F1 score, recall, and precision

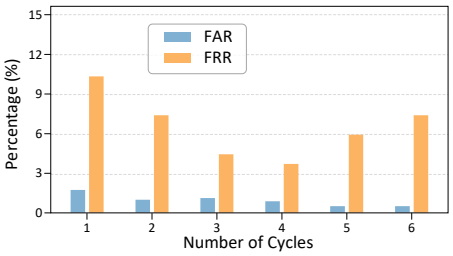


(b) FAR and FRR

Fig. 16. Performance under password input.

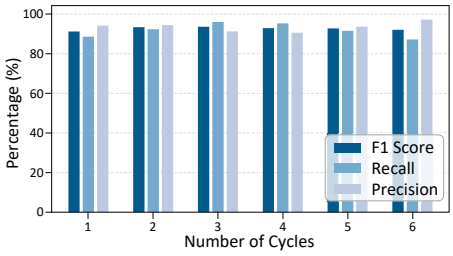


(a) F1 score, recall, and precision

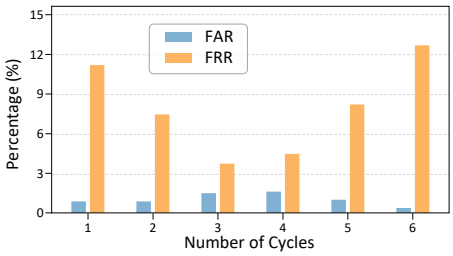


(b) FAR and FRR

Fig. 17. Performance under pattern input.

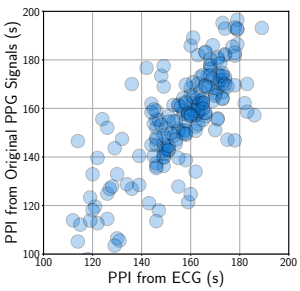


(a) F1 score, recall, and precision

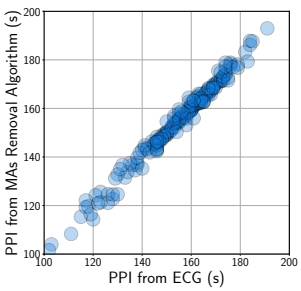


(b) FAR and FRR

Fig. 18. Performance under signature input.



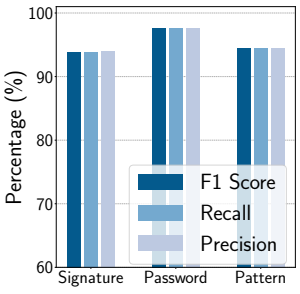
(a) PPI from original PPG signals



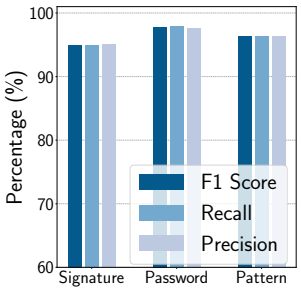
(b) PPI after MAs removal

Fig. 19. Scatter plot of PPI estimates.

augmentation (Fig. 20 (a)). Specifically, the authentication F1 score of writing signature, inputting passwords, and inputting patterns increased by 1.10%, 0.12%, and 1.84%. We believe the results can be further improved by higher data augmentation rates.



(a) Performence without data augmentation



(b) Performence with data augmentation

Fig. 20. Results without and with data augmentation.

TABLE 4
Performance of Revocability

Features	F1 Score	Recall	Precision
Previous Features	94.6%	94.7%	94.6%
New Features	96.1%	93.7%	98.6%

7.10 Cancelability

7.10.1 Revocability

First, we aim to prove features transformed by a new function is distinguished from features transformed by the previous function. Second, we aim to show that applying features transformed by a new function can still achieve high accuracy. As shown in Table 4, the average F1 score, recall, and precision of the previous transformed features under the three conditions are 94.6%, 94.7%, and 94.6%, respectively. When evaluating the performance of new transformed features, treat the previous features as adversaries. The average F1 score, recall, and precision of the new transformed features under the three conditions are 96.1%, 93.7%, and 98.6%, respectively. The results demonstrate that the process of generating cancelable features does not degrade the efficiency of the system. In addition, PPGPass is shown to have robustness against the attacks using the previous signals when biometrics are compromised, which provides solutions to re-instate the account and protects privacy information.

7.10.2 Unlinkability

We use Pearson's correlation coefficient to evaluate dependence between the previous and new transformed features (comparing each pair of normalized features from the previous features and new features). As shown in Fig. 21, the results center at zero, mainly ranging between $[-0.1, 0.1]$, which indicates that the previous features and new features are highly independent.

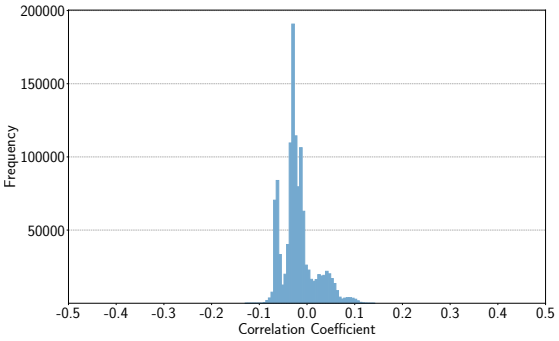


Fig. 21. Dependence between previous and new transformed features.

8 Conclusion

We propose PPGPass, a novel nonintrusive and secure mobile two-factor authentication system, which leverages PPG sensors in wrist-worn devices. Specifically, it can remove MAs in PPG signals, characterize individual heartbeat signals, and generate cancelable feature templates when biometrics are compromised. It is compatible with existing wearables and other authentication techniques. We build a prototype of PPGPass and evaluate its performance with multiple participants. The results show that it can achieve high accuracy, which provides an additional line of defense. We also evaluate its long-term performance and its cancelability against attacks, which demonstrate the robustness and sustainability of PPGPass.

In future work, firstly, we are aware that PPG signals are sensitive to acquisition locations and skin colors. So, we plan to examine the impact of these factors of PPG sensors in wrist-worn wearables. Secondly, to further evaluate the performance of PPGPass, we plan to recruit more participants and collect divers data. Specifically, we plan to conduct experiments with more participants under more intense motions (such as continuous and intense on-screen keyboard typing) in a longer duration. Moreover, we plan to test participants in different states, such as different emotions, cardiac disease, and before and after exercise. Thirdly, we plan to evaluate PPGPass with people suffering from heart disease, which might cause drastically cardiac status changes and impact the system performance. Overall, we would like to explore more observations and solutions for PPGPass in our future work.

Acknowledgments

The work of Fan Li is partially supported by the National Natural Science Foundation of China (NSFC) under Grant No. 62072040, 61772077, and the Beijing Natural Science Foundation under Grant No. 4192051. The work of Qian Zhang is partially supported by NSFC under Grant No. 62002193. The work of Song Yang is partially supported by NSFC under Grant No. 61802018.

References

[1] O. Riva, C. Qin, K. Strauss, and D. Lymberopoulos, "Progressive authentication: Deciding when to authenticate on mobile phones," in *USENIX Conference on Security symposium (USENIX Security)*, 2012.

[2] F. Schaub, R. Deyhle, and M. Weber, "Password entry usability and shoulder surfing susceptibility on different smartphone platforms," in *ACM International Conference on Mobile and Ubiquitous Multimedia*, 2012.

[3] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge attacks on smartphone touch screens," in *Usenix Conference on Offensive Technologies*, 2010.

[4] Duo. [Online]. Available: https://duo.google.com/about/

[5] Encap security. [Online]. Available: https://www.encapsecurity.com/

[6] Google 2-step verification. [Online]. Available: https://www.google.com/ landing/2step/

[7] Fingerprint biometrics hacked again. [Online]. Available: http://www. ccc.de/en/updates/2014/ursel

[8] N. M. Duc and B. Q. Minh, "Your face is not your password," in *Black Hat Briefings*, 2009.

[9] L. Zhang, T. Sheng, Y. Jie, and Y. Chen, "VoiceLive: A phoneme localization based liveness detection for voice authentication on smartphones," in *ACM Conference on Computer and Communications Security (CCS)*, 2016.

[10] A. Levy, B. Nassi, Y. Elovici, and E. Shmueli, "Handwritten signature verification using wrist-worn devices," *ACM International Conference on Ubiquitous Computing (UbiComp)*, 2018.

[11] L. Lu, J. Yu, Y. Chen, H. Liu, Y. Zhu, Y. Liu, and M. Li, "LipPass: Lip reading-based user authentication on smartphones leveraging acoustic signals," in *IEEE Conference on Computer Communications (INFOCOM)*, 2018.

[12] J. Chauhan, Y. Hu, S. Seneviratne, A. Misra, A. Seneviratne, and Y. Lee, "BreathPrint: Breathing acoustics-based user authentication," in *ACM International Conference on Mobile Systems, Applications, and Services (MobiSys)*, 2017.

[13] M. Shahzad, A. X. Liu, and A. Samuel, "Secure unlocking of mobile touch screen devices by simple gestures: You can see it but you can not do it," in *ACM International Conference on Mobile Computing and Networking (MobiCom)*, 2013.

[14] H. Chen, F. Li, W. Du, S. Yang, M. Conn, and Y. Wang, "Listen to your fingers: User authentication based on geometry biometrics of touch gesture," *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, vol. 4, no. 3, 2020.

[15] C. Bo, L. Zhang, T. Jung, J. Han, X.-Y. Li, and Y. Wang, "Continuous user identification via touch and movement behavioral biometrics," in *2014 IEEE 33rd International Performance Computing and Communications Conference (IPCCC)*. IEEE, 2014, pp. 1–8.

[16] V.-D. Stanciu, R. Spolaor, M. Conti, and C. Giuffrida, "On the effectiveness of sensor-enhanced keystroke dynamics against statistical attacks," in *ACM Conference on Data and Application Security and Privacy*, 2016.

[17] Y. Cao, Q. Zhang, F. Li, S. Yang, and Y. Wang, "Ppgpass: Nonintrusive and secure mobile two-factor authentication via wearables," in *IEEE INFOCOM 2020-IEEE Conference on Computer Communications*. IEEE, 2020, pp. 1917–1926.

[18] Z. Zhao, L. Yang, D. Chen, and Y. Luo, "A human ECG identification system based on ensemble empirical mode decomposition," *Sensors*, 2013.

[19] F. Lin, C. Song, Y. Zhuang, W. Xu, C. Li, and K. Ren, "Cardiac Scan: A non-contact and continuous heart-based user authentication system," in *ACM International Conference on Mobile Computing and Networking (MobiCom)*, 2017.

[20] N. S. G. R. Salanke, N. Maheswari, A. Samraj, and S. Sadhasivam, "Enhancement in the design of biometric identification system based on photoplethysmography data," in *International Conference on Green High Performance Computing*, 2013.

[21] J. Liu, C. Shi, Y. Chen, H. Liu, and M. Gruteser, "Cardiocam: Leveraging camera on mobile devices to verify users while their heart is pumping," in *Proceedings of the 17th Annual International Conference on Mobile Systems, Applications, and Services*, 2019.

[22] T. Zhao, Y. Wang, J. Liu, Y. Chen, J. Cheng, and J. Yu, "Trueheart: Continuous authentication on wrist-worn wearables using ppg-based biometrics," in *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications*, 2020, pp. 30–39.

[23] T. Zhao, Y. Wang, J. Liu, and Y. Chen, "Your heart won't lie: PPG-based continuous authentication on wrist-worn wearable devices," in *ACM International Conference on Mobile Computing and Networking (MobiCom)*, 2018.

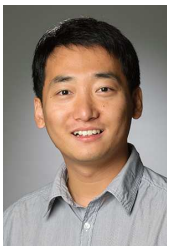
[24] K. A. Reddy and V. J. Kumar, "Motion artifact reduction in photoplethysmographic signals using singular value decomposition," 2007.

[25] Z. L. Zhang and Z. Yi, "Robust extraction of specific signals with temporal structure," *Neurocomputing*, 2006.
[26] M. R. Ram, K. V. Madhav, E. H. Krishna, N. R. Komalla, and K. A. Reddy, "A novel approach for motion artifact reduction in PPG signals based on AS-LMS adaptive filter," *IEEE Transactions on Instrumentation and Measurement*, 2012.
[27] V. M. Patel, N. K. Ratha, and R. Chellappa, "Cancelable biometrics: A review," *IEEE Signal Processing Magazine*, 2015.
[28] F. Lin, K. W. Cho, C. Song, W. Xu, and Z. Jin, "Brain Password: A secure and truly cancelable brain biometrics for smart headwear," in *ACM International Conference on Mobile Systems, Applications, and Services (MobiSys)*, 2018.
[29] O. Ouda, N. Tsumura, and T. Nakaguchi, "Tokenless cancelable biometrics scheme for protecting iriscodes," in *IEEE International Conference on Pattern Recognition (ICPR)*, 2010.
[30] R. Nalini K, S. Chikkerur, honathan H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," *IEEE Transactions Pattern Analysis and Machine Intelligence (TPAMI)*, 2007.
[31] R. M. Bolle, J. H. Connell, and N. K. Ratha, "Biometric perils and patches," *Pattern Recognition (PR)*, 2002.
[32] A. Czeskis, M. Dietz, T. Kohno, W. Dan, and D. Balfanz, "Strengthening user authentication through opportunistic cryptographic identity assertions," in *ACM Conference on Computer and Communications Security (CCS)*, 2012.
[33] N. Gunson, D. Marshall, H. Morton, and M. Jack, "User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking," *Computers and Security*, 2011.
[34] D. Han, Y. Chen, T. Li, R. Zhang, Y. Zhang, and T. Hedgpeth, "Proximity-Proof: Secure and usable mobile two-factor authentication," in *ACM International Conference on Mobile Computing and Networking (MobiCom)*, 2018.
[35] Z. Yang, Z. Zhou, and Y. Liu, "From RSSI to CSI: Indoor localization via channel response," *ACM Computing Surveys*, 2013.
[36] Y. Zheng, Y. Zhang, K. Qian, G. Zhang, Y. Liu, C. Wu, and Z. Yang, "Zero-effort cross-domain gesture recognition with Wi-Fi," in *ACM International Conference on Mobile Systems, Applications, and Services (MobiSys)*, 2019.
[37] H. Chen, F. Li, X. Hei, and Y. Wang, "CrowdX: Enhancing automatic construction of indoor floorplan with opportunistic encounters," *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, 2018.
[38] H. Chen, F. Li, and Y. Wang, "Soundmark: Accurate indoor localization via peer-assisted dead reckoning," *IEEE Internet of Things Journal*, 2018.
[39] Y. Xie, F. Li, Y. Wu, S. Yang, and Y. Wang, "D3-guard: Acoustic-based drowsy driving detection using smartphones," in *IEEE Conference on Computer Communications (INFOCOM)*, 2019.
[40] B. Zhou, J. Lohokare, R. Gao, and F. Ye, "EchoPrint: Two-factor authentication using acoustics and vision on smartphones," in *ACM International Conference on Mobile Computing and Networking (MobiCom)*, 2018.
[41] T. Zhao, J. Liu, Y. Wang, H. Liu, and Y. Chen, "PPG-based finger-level gesture recognition leveraging wearables," in *IEEE Conference on Computer Communications (INFOCOM)*, 2018.
[42] M. Zhao, F. Adib, and D. Katabi, "Emotion recognition using wireless signals," in *ACM International Conference on Mobile Computing and Networking (MobiCom)*, 2017.
[43] A. Baayer, N. Enneya, and M. Elkoutbi, "Enhanced timestamp discrepancy to limit impact of replay attacks in MANETs," 2012.
[44] P. E. McSharry, G. D. Clifford, L. Tarassenko, and L. A. Smith, "A dynamical model for generating synthetic electrocardiogram signals," *IEEE Transactions on Biomedical Engineering*, 2003.
[45] J. Thickstun, Z. Harchaoui, D. P. Foster, and S. M. Kakade, "Invariances and data augmentation for supervised music transcription," in *2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2018, pp. 2241–2245.
[46] B. McFee, E. J. Humphrey, and J. P. Bello, "A software framework for musical data augmentation." in *ISMIR*, vol. 2015, 2015, pp. 248–254.
[47] Y. Li, H. Hu, and G. Zhou, "Using data augmentation in continuous authentication on smartphones," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 628–640, 2019.
[48] D. Kiyasseh, G. A. Tadesse, L. N. T. Nhan, L. Van Tan, L. Thwaites, T. Zhu, and D. Clifton, "Plethaugment: Gan-based ppg augmentation for medical diagnosis in low-resource settings," *IEEE Journal of Biomedical and Health Informatics*, vol. 24, no. 11, pp. 3226–3235, 2020.

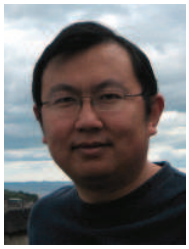
Yetong Cao received the BEng degree in computer science and technology from Shandong University, Shandong, China, in 2017. She is now working toward the PhD degree in the School of Computer Science and Technology, Beijing Institute of Technology. Her research interests include mobile computing and ubiquitous computing.

Fan Li received the PhD degree in computer science from the University of North Carolina at Charlotte in 2008, MEng degree in electrical engineering from the University of Delaware in 2004, MEng and BEng degrees in communications and information system from Huazhong University of Science and Technology, China in 2001 and 1998, respectively. She is currently a professor at School of Computer Science in Beijing Institute of Technology, China. Her current research focuses on wireless networks, ad hoc and sensor networks, and mobile computing. Her papers won Best Paper Awards from IEEE MASS (2013), IEEE IPCCC (2013), ACM MobiHoc (2014), and Tsinghua Science and Technology (2015). She is a member of ACM and IEEE.

Qian Zhang is a Postdoc researcher in School of Software, Tsinghua University, China. She received her Ph.D. degree in School of Computer Science, Beijing Institute of Technology, China, her MS degree in Computer Science, Illinois Institute of Technology. Her research interests include mobile computing, smart sensing, and mobile crowd sensing.



Song Yang received the Ph.D. degree from Delft University of Technology, The Netherlands, in 2015. From August 2015 to July 2017, he worked as postdoc researcher for the EU FP7 Marie Curie Actions CleanSky Project in Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen (GWDG), Göttingen, Germany. He is currently an associate professor at School of Computer Science in Beijing Institute of Technology, China. His research interests focus on data communication networks, cloud/edge computing and network function virtualization.



Yu Wang is currently a Professor in the Department of Computer and Information Sciences at Temple University. He holds a Ph.D. from Illinois Institute of Technology, an MEng and a BEng from Tsinghua University, all in Computer Science. His research interest includes wireless networks, smart sensing, and mobile computing. He has published over 200 papers in peer reviewed journals and conferences. He has served as general chair, program chair, program committee member, etc. for many international conferences (such as IEEE IPCCC, ACM MobiHoc, IEEE INFOCOM, IEEE GLOBECOM, IEEE ICC), and served as Editorial Board Member for several international journals, including IEEE Transactions on Parallel and Distributed Systems. He is a recipient of Ralph E. Powe Junior Faculty Enhancement Awards from Oak Ridge Associated Universities (2006), Outstanding Faculty Research Award from College of Computing and Informatics at the University of North Carolina at Charlotte (2008), Fellow of IEEE (2018), and ACM Distinguished Member (2020).