PPGPass: Nonintrusive and Secure Mobile Two-Factor Authentication via Wearables

Yetong Cao* Qian Zhang† Fan Li* Song Yang* Yu Wang‡
* School of Computer Science and Technology, Beijing Institute of Technology, China
† School of Software and BNRist, Tsinghua University, China
‡ Department of Computer and Information Sciences, Temple University, USA

***Abstract*—Mobile devices are promising to apply two-factor authentication in order to improve system security and enhance user privacy-preserving. Existing solutions usually have certain limits of requiring some form of 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 in wrist-worn wearables to extract individual characteristics of PPG signals. In order to realize both nonintrusive and secure, we design a two-stage algorithm to separate clean heartbeat signals from PPG signals contaminated by motion artifacts, which allows verifying users without intentionally staying still during the process of authentication. In addition, to deal with non-cancelable issues when biometrics are compromised, we design a repeatable and non-invertible method to generate cancelable feature templates as alternative credentials, which enables to defense against man-in-the-middle attacks and replay attacks. To the best of our knowledge, PPGPass is the first nonintrusive and secure mobile two-factor authentication based on PPG sensors in wearables. We build a prototype of PPGPass and conduct the system with comprehensive experiments involving multiple participants. PPGPass can achieve an average F1 score of 95.3%, which confirms its high effectiveness, security, and usability.**

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

I. Introduction

In recent years, two-factor authentication is widely deployed by mobile devices to further improve system security and enhance user privacy-preserving. It provides an additional line of defense besides traditional commonly used authentication approaches. For example, when a user wants to log in 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. As mobile devices have increasing relations with personally and financially sensitive information during people's daily behaviors like messaging, health caring, and payment, currently mobile two-factor authentication is taking over more importance.

Given the need of 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], but it has proven ineffective against advanced statistical attacks [14]. 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. Fig. 1 shows the working paradigm of PPGPass. Users register their features of PPG signals as cancelable templates stored in the system database. When a user wants to access, new incoming PPG signals will be collected and the system verifies if the signals belong to the same person from the stored templates. Thus identifying authorized users and malicious attackers as the second layer of security.

Specifically, PPGPass focuses on three goals. 1) **Nonintrusive authentication**: PPG signals are easy to be disturbed by hand motions. The user is usually required to remain stationary

Fan Li is the corresponding author. The work of Fan Li is partially supported by the National Natural Science Foundation of China (NSFC) under Grant No. 61772077 and Beijing Natural Science Foundation under Grant No. 4192051. The work of Song Yang is partially supported by NSFC under Grant No. 61802018 and Beijing Institute of Technology Research Fund Program for Young Scholars.

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 user extra involvement. 2) **High accuracy authentication**: We select 40 geometric features in the angle domain from single and multiple cardiac cycles, which reflect consistent and intrinsic individual characteristics to support high accuracy authentication. 3) **Secure authentication when biometrics are compromised**: We design a repeatable and non-invertible method to generate cancelable feature templates as alternative credentials, which provides solutions to defense against man-in-the-middle (MITM) attacks and replay attacks.

The advantages of PPGPass are two-fold. First, it could be easily applied to existing wrist-worn wearables without extra hardware and cost, which enables every device to authentication 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. 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 geometric features in the angle domain from single cardiac cycle and multiple cardiac cycles, and 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 MITM attacks and replay attacks.
- We conduct extensive experiments with multiple participants using our prototype. The results show that PPGPass can achieve an average F1 score of 95.3%, which confirms its efficiency and robustness.

The rest of this paper is organized as follows. Section II surveys related work. Section III introduces PPG sensors, design challenges, overview, and workflow. Section IV presents details of data preprocessing. Section V describes geometric feature extraction and classification. Section VI gives how to re-register new credentials when biometrics are compromised. Section VII shows evaluation results. Finally, Section VIII concludes the paper and discusses future work.

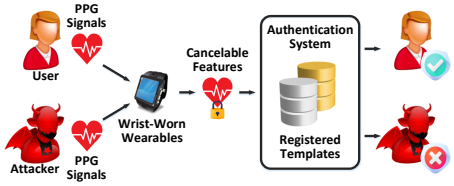


Fig. 1. Working paradigm of PPGPass. A nonintrusive and secure mobile two-factor authentication system using PPG signals via wrist-worn wearables.

II. 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 [15]. Cardiac Scan [16] uses geometric and nonvolitional 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, Fourier series analysis and semi-discrete decomposition methods are applied to extract discriminable features [17]. CardioCam [18] 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 [19] propose a PPG-based authentication system utilizes the statistical differences to detect MAs and reduce MAs by using a special moving average filter. 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 [20]–[22]. However, these methods can only work well for only a limited range of artifacts. They cannot be applied directly with users' signatures writing or passwords/PINs/patterns inputs to realize simultaneous two-factor authentication.

Cancelable Authentication: To deal with noncancelable issues when biometrics are compromised, the direct way 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 [23]. Brain Password [24] 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 [25]–[27]. 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

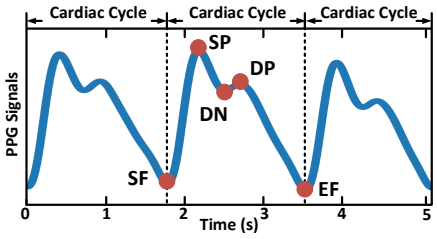


Fig. 2. Fiducial points in PPG signals.

over a Bluetooth channel between an enrolled phone and a login device [28], [29]. While they may not easy to be compatible with standard web browsers. Proximity-Proof [30] 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 [31], [32], are also leveraged to recognize and verify users. Acoustic sensing has been widely applied in many mobile applications(e.g., relative positioning [33], [34], driving motion detection [35]). In addition, EchoPrint [36] focuses on leveraging facial features obtained from both acoustic signals and vision for authentication. However, such methods might fail by ambient disturbing noise or intrusive signals.

III. Preliminaries

A. 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 [16], which results in a sharp increase in PPG signals because blood absorbs more light than surrounding tissue [37]. 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 [16]), 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.

B. 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 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 precisely 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, what kinds of features to extract is critical. Commonly used heartbeat features, such as HRV, are strongly influenced by specific states (e.g., emotions) [38]. Thus, they are not sufficient for high accuracy of authentication, especially in the presence of MAs. In this work, we extract a set of geometric features based on fiducial points from the angle domain that reflects the consistent characteristics of individual heartbeats.

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 [23]. 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.

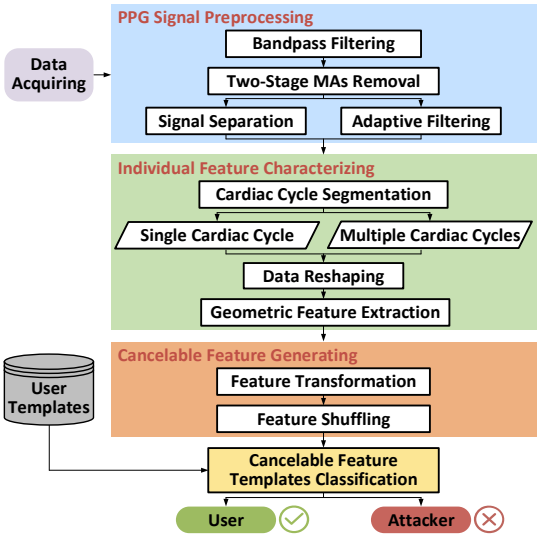


Fig. 3. Overview of PPGPass.

C. Overview & Workflow

The overview of PPGPass is shown in Fig. 3, which consists of three parts: *PPG Signal Preprocessing*, *Individual*

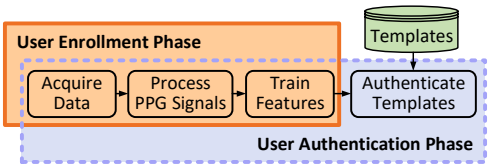


Fig. 4. Workflow of PPGPass.

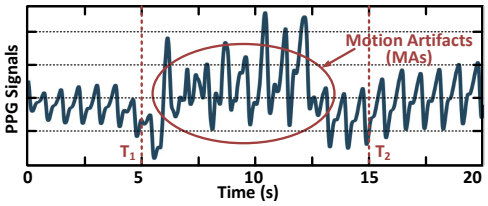


Fig. 5. PPG signals contaminated by MAs.

Feature Characterizing, and *Cancelable Feature Generating*. PPG signals are continuously acquired via wrist-worn devices. In *PPG Signal Preprocessing*, firstly the original signals 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*, firstly PPGPass 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, PPGPass uses a random forest classifier to efficiently identify users and attackers.

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 PPG signals from every new user via wrist-worn wearables and the signals are processed by *PPG Signal Preprocessing*, *Individual Feature Characterizing*, and *Cancelable Feature Generating*. Note that, this phase is conducted on personal wrist-worn wearables at user-end locally. Then, the generated cancelable feature templates are sent from the user-end to the server-end. At the server-end, all the features are trained by a random forest classifier and stored as user templates in the system. This process is similar to open a new bank account, where a user provides personal information (PPG signals) for the bank to verify this user in the future. In *User Authentication Phase*, like in the user enrollment phase, PPGPass nonintrusively acquires PPG signals from a user and processes the signals. Then, the server authenticates users referring to the user templates by the random forest classifier. 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.

IV. PPG Signal Preprocessing

A. 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 nonintrusive 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) [22], we continue to process PPG signals by the designed algorithm in the following, which aims to further effectively remove MAs in PPG signals.

B. 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 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 [21] 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.

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 $S(t)$:

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

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:

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

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 $H_X(\tau) = \mathbb{E}\left\{X(k)X(k+\tau)^{\mathrm{T}}\right\}$. 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.

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) [22] adaptive filtering to remove MAs. The effectiveness of the two-stage MAs removal algorithm is investigated in Section VII-C, which lays the foundation for PPGPass to authenticate users using PPG sensors in wrist-worn wearables.

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 [22], we choose the best output data as clean heartbeat signals by comparing their skewness and kurtosis.

V. Individual Feature Characterizing

A. 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.

B. Data Reshaping

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. In order to achieve high authentication accuracy, we extract geometric features based on the shape of heartbeat signals.

Due to the dynamic nature of biometrics, signal lengths and amplitudes between cycles present nonstationary over time. If geometric features are extracted directly from the time domain, such differences will influence the uniqueness of features. So, we transform signals from the time domain (x, y) to angle domain $(\dot{x}, \dot{y}, \dot{z})$ [39]:

$$\begin{aligned} &\dot{x} = \omega x - \rho y, \\ &\dot{y} = \omega y + \rho x, \\ &\dot{z} = -\sum_{i\in\{sf,sp,dn,dp,ef\}} a_i \Delta\theta_i exp\left(-\frac{\Delta\theta_i^2}{2b_i^2}\right) - (z - z_0), \end{aligned} \tag{6}$$

where $\omega = 1 - \sqrt{x^2 + y^2}$, ρ is the instantaneous heart rate. $\Delta\theta_i = (\theta - \theta_i)\, mod\, 2\pi$, where θ_i is the the fiducial point position and the instantaneous angular position $\theta = tan^{-1}(y/x)$. a_i and b_i are constant model parameters, z represents signals in the five fiducial points $\{SF, SP, DN, DP, EF\}$, and $\{sf, sp, dn, dp, ef\}$ are X-axis values of the five fiducial points. In our case, the baseline component z_0 can be ignored because we only analyze one cycle at a time.

C. Feature Extraction

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

TABLE I
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}.
	$\boldsymbol{\sum_{sp}^{dp} \lvert S - y_{spsp}\rvert}$, $\boldsymbol{\sum_{dn}^{dp} \lvert S - y_{spsp}\rvert}$, $\frac{\boldsymbol{\sum_{sp}^{dn} \lvert S-y_{spsp}\rvert}}{\boldsymbol{\sum_{sf}^{sf} \lvert S-y_{spsp}\rvert}}$, $\frac{\boldsymbol{\sum_{sp}^{dn} \lvert S-y_{spsp}\rvert}}{\boldsymbol{\sum_{sp}^{sf} \lvert S-y_{spsp}\rvert}}$	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**.

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.

D. Feature Training and Classification

1) Training: As PPGPass aims to allow users to re-register new credentials when biometrics (PPG signals or feature templates) are compromised, instead of the original extracted geometric features, the input features for a random forest classifier are cancelable features, which will be described in detail in Section VI. 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.

2) Classification: Initially, training templates are stored in the system during the user enrollment phase. Then, 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 (Section IV), individual feature characterizing (Section V), and cancelable feature generating (Section VI), resulting cancelable feature templates. During classification, the random forest classifier is applied to verify the current template against pre-stored templates and identify users.

VI. CANCELABLE FEATURE GENERATING

A. 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 MITM attacks or 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 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 hereditary diseases might be inferred from cardiac motions. When using biometrics as inputs for authentication, users have a concern about invasion of privacy.

B. Feature Transformation

To solve the above issues, instead of using the extracted geometric features (denoted as a vector $\boldsymbol{v}$), we aim to fuse the features by a transform function $\mathbb{F}(*)$. Such a transforming process has two design guidelines as follows.

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. 6.

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:
$$Dist(\mathbb{F}_1(\boldsymbol{v_1}), \mathbb{F'}_1(\boldsymbol{v_1})) \geq \lambda, \tag{7}$$
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 $\mathbb{F}_2$):
$$Dist(\boldsymbol{v_1}, \boldsymbol{v_2}) \geq \lambda \Rightarrow Dist(\mathbb{F}_1(\boldsymbol{v_1}), \mathbb{F}_2(\boldsymbol{v_2})) \geq \lambda. \tag{8}$$

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 transformed 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 matching of minimum cost in G by the Hungarian method, in which the similarity measurement $Dist(*)$ is the found minimum cost:
$$Dist(\boldsymbol{v_1}, \boldsymbol{v_2}) = minimize \sum_{i,j \in 1,2,...,N} d(\bar{p}_i, \bar{q}_j). \tag{9}$$

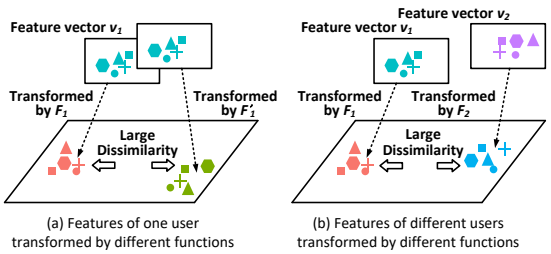


Fig. 6. Illustration of feature transformation strategies.

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.

VII. Evaluation

A. Experimental Setting

To validate the authentication performance of PPGPass, because existing manufactures 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. 7. The prototype consists of an integrated PPG sensor (with green and infrared light LEDs) and an adjustable wristband. Note that the prototype is completely harmless to the human body, and we use a sample rate at $400Hz$.

B. 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. Every participant sits comfortably in a chair, wearing the prototype on the dominant hand to conduct three conditions: signatures writing, passwords inputs, and patterns inputs. 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. Totally, we collect 3780 samples (7 participants $\times$ 6 sessions $\times$ 30 repetitions $\times$ 3 conditions) for analysis. The collected samples are manually labeled. During authentication, each participant acts as an owner and the rest act as attackers.

In order to obtain data under continuous contact between the wrist and 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.

C. 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 that

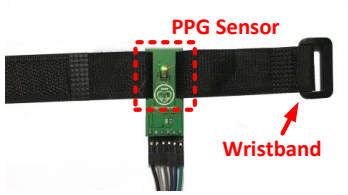
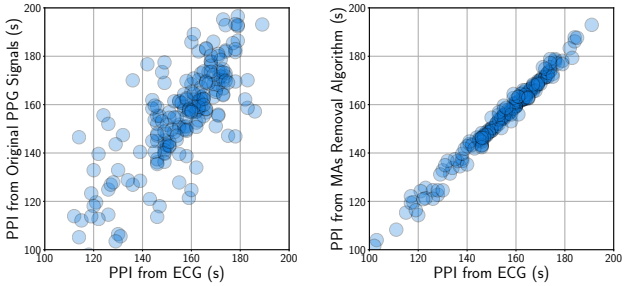


Fig. 7. Prototype of a wrist-worn device with a PPG sensor.

obtained from the ECG signals. As shown in Fig. 8, 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.



(a) PPI from original PPG signals (b) PPI after MAs removal

Fig. 8. Scatter plot of PPI estimates.

D. Metrics

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

E. Overall Performance

We first compare F1 score, recall, and precision with different cardiac cycles in feature extraction under the three conditions. Fig. 9 shows that F1 score of signatures writing achieve 91.5%, 93.7%, 93.9%, 93.2%, 93.0%, and 92.3% for 1 cycle, 2 cycles, 4 cycles, 6 cycles, 8 cycles, and 10 cycles, respectively. For conditions of passwords inputs and patters inputs, F1 score achieve 95.5%, 97.2%, 97.6%, 97.6%, 98.2%, 97.0%, and 89.6%, 93.3%, 94.5%, 95.5%, 95.5%, 94.8% for different cycles, respectively. The recall and precision of the three conditions under different cycles have similar trends. The results indicate that along with the increase of cycles in feature extraction, the performance of PPGPass first improves and then goes stable. When 4 cardiac cycles in feature extraction is used, the overall accuracy of PPGPass achieves the best performance. The average F1 score, recall, and precision for 4 cycles of the three conditions are all above 95%. The results demonstrate that our system can accurately verify users.

F. Time Duration

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. 10 shows that F1 score of $4s$, $6s$, $8s$, $10s$, 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 accuracies 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 achieving high accuracy. The results show that users can be authenticated nonintrusively and efficiently.

G. Classifier Impact

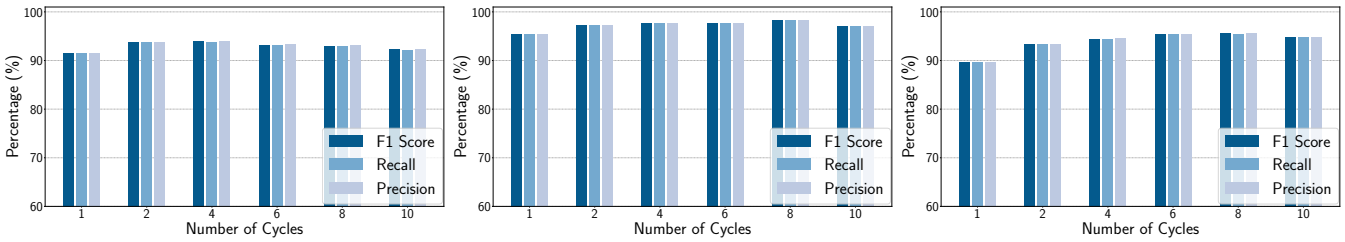
We compare the performance of 4 commonly used classifiers: Random Forest (RF), Naive Bayes (NB), Decision Trees (DT), and Logistic Regression (LR). We apply 4 cycles in feature extraction and $4s$ sensing time. F1 scores of different testing set sizes are shown in Fig. 11. Along with the increasing size 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.

H. Long-Term Study

Long-term performance is a critical aspect of authentication systems. Fig. 12 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.

I. Cancelability

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



(a) Signatures writting (b) Passwords inputs (c) Patterns inputs

Fig. 9. Overall performance of PPGPass under three conditions.

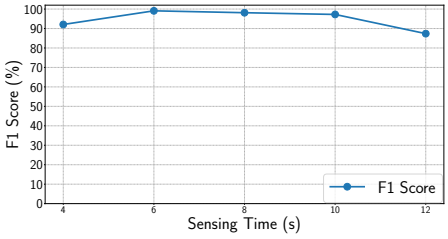


Fig. 10. Time duration.

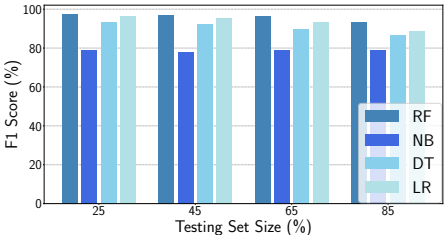


Fig. 11. Impact of classifiers.

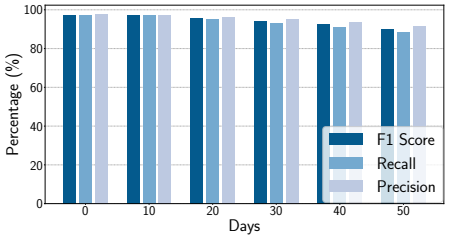


Fig. 12. Performance in a long-term study.

TABLE II
PERFORMANCE OF REVOCABILITY

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

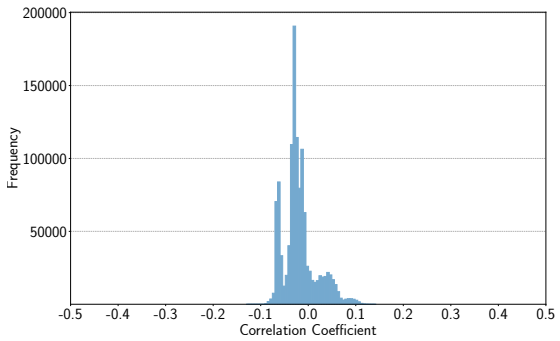


Fig. 13. Dependence between previous and new transformed features.

achieve high accuracy. As shown in Table II, 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 attackers. 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 can defense against MITM attacks and replay attacks and thus presents revocability.

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. 13, the results center at zero, mainly ranging between $[-0.1, 0.1]$, which indicates that the previous features and new features are highly independent.

VIII. Conclusion and Future Work

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 the proposed system, we plan to conduct experiments with more participants under more intense motions (such as continuous and intense on-screen keyboard typing) in a longer time. Thirdly, we plan to test participants in different states, such as different emotions, cardiac disease, and before and after exercise. Overall, we would like to explore more observations and solutions for PPGPass in our future work.

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] 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.

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

[16] 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.

[17] 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.

[18] 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.

[19] 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.

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

[21] Z. L. Zhang and Z. Yi, "Robust extraction of specific signals with temporal structure," *Neurocomputing*, 2006.

[22] 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.

[23] V. M. Patel, N. K. Ratha, and R. Chellappa, "Cancelable biometrics: A review," *IEEE Signal Processing Magazine*, 2015.

[24] 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.

[25] O. Ouda, N. Tsumura, and T. Nakaguchi, "Tokenless cancelable biometrics scheme for protecting iriscodes," in *IEEE International Conference on Pattern Recognition (ICPR)*, 2010.

[26] 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.

[27] R. M. Bolle, J. H. Connell, and N. K. Ratha, "Biometric perils and patches," *Pattern Recognition (PR)*, 2002.

[28] 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.

[29] 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.

[30] 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.

[31] Z. Yang, Z. Zhou, and Y. Liu, "From RSSI to CSI: Indoor localization via channel response," *ACM Computing Surveys*, 2013.

[32] 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.

[33] 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.

[34] H. Chen, F. Li, and Y. Wang, "Soundmark: Accurate indoor localization via peer-assisted dead reckoning," *IEEE Internet of Things Journal*, 2018.

[35] 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.

[36] 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.

[37] 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.

[38] M. Zhao, F. Adib, and D. Katabi, "Emotion recognition using wireless signals," in *ACM International Conference on Mobile Computing and Networking (MobiCom)*, 2017.

[39] 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.