Computers & Security 135 (2023) 103488

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

# A Survey of PPG's Application in Authentication

Lin Li [a], Chao Chen [b], Lei Pan [c], Leo Yu Zhang [d], Zhifeng Wang [e,*], Jun Zhang [a], Yang Xiang [a]

[a] *Swinburne University of Technology, Melbourne, 3000, VIC, Australia*
[b] *RMIT University, Melbourne, 3000, VIC, Australia*
[c] *Deakin University, Waurn Ponds, 3216, VIC, Australia*
[d] *Griffith University, Gold Coast, 4222, QLD, Australia*
[e] *Nantong First People's Hospital, Nantong, 226006, Jiangsu, China*

ARTICLE INFO

*Keywords:*
Biometrics
Physiological Signals
Photoplethysmogram
User Authentication

ABSTRACT

Biometric authentication prospered because of its convenient use and security. Early generations of biometric mechanisms suffer from spoofing attacks. Recently, unobservable physiological signals (e.g., Electroencephalogram, Photoplethysmogram, Electrocardiogram) as biometrics offer a potential remedy to this problem. In particular, Photoplethysmogram (PPG) measures the change in blood flow of the human body by an optical method. Clinically, researchers commonly use PPG signals to obtain patients' blood oxygen saturation, heart rate, and other information to assist in diagnosing heart-related diseases. Since PPG signals contain a wealth of individual cardiac information, researchers have begun to explore their potential in cyber security applications. The unique advantages (simple acquisition, difficult to steal, and live detection) of the PPG signal allow it to improve the security and usability of the authentication in various aspects. However, the research on PPG-based authentication is still in its infancy. The lack of systematization hinders new research in this field. We conduct a comprehensive study of PPG-based authentication and discuss these applications' limitations before pointing out future research directions.

## 1. Introduction

Authentication ensures the legitimacy of access to data (Wang et al., 2020a) and the identity of individuals. Authentication is useful in many areas of our lives, including commercial applications, healthcare, access control, and many more. There are three categories of authentication—knowledge-based authentication like passwords, object-based authentication, like ID cards, and biometric-based authentication, like face recognition (Jain et al., 2006). Biometric-based authentication uses physiological or behavioral characteristics extracted from a person as a source of idiosyncratic information (Huang and Wang, 2022). It does not suffer from being forgotten compared with knowledge- and object-based methods. Since each human has many idiosyncratically physical or behavioral characteristics, a wealth of individual information can be leveraged to strengthen biometric-based authentication against fabrication. The traditional features used for biometrics include fingerprint, face, iris, voice, palmprint, and many more (Jia et al., 2021). In the 2010s, biometric authentication thrived, for example, using face recognition to unlock a smartphone and fingerprint recognition to unlock a door. Nevertheless, these early versions of biometric authentication are often vulnerable to presentation attacks (Wang et al., 2020c; Kolberg et al., 2021). A presentation attack means that an attacker impersonates a legitimate user to present biometrics to an authentication system. A common scenario is using a 3D mask representing the victim's face to fool the face recognition system.

Physiological signals are considered as biometrics because they are not readily observable. Such signals include Electroencephalogram, Electrocardiogram, and Photoplethysmogram (PPG) (Wang et al., 2020b; Huang et al., 2021; Hwang et al., 2021c). Specifically, a Pentagon's product uses infrared lasers to detect people's unique heart features to authenticate individuals (Hambling, 2019); a Canadian company Nymi has developed an authentication system using wrist-worn pulse sensors as an alternative to fingerprint recognition (Eberz et al., 2017). Different from traditional biological features, physiological signal-based features are invisible on the human body's skin surface, making it challenging to be collected and analyzed by attackers from remote locations.

[*] Corresponding author.
*E-mail addresses:* linli@swin.edu.au (L. Li), chao.chen@rmit.edu.au (C. Chen), l.pan@deakin.edu.au (L. Pan), leo.zhang@griffith.edu.au (L.Y. Zhang), maisui1976@163.com (Z. Wang), junzhang@swin.edu.au (J. Zhang), yxiang@swin.edu.au (Y. Xiang).

https://doi.org/10.1016/j.cose.2023.103488
Received 22 March 2023; Received in revised form 14 July 2023; Accepted 17 September 2023
Available online 21 September 2023

Among the physiological signals, PPG is a non-invasive optical method for measuring the volume of light absorbed or reflected by microvascular in biological tissues (Natarajan et al., 2021). Furthermore, PPG has a wide range of research prospects in authentication due to its unique advantages: **Simple acquisition**—An oximeter or a camera alone can capture PPG signals from a human body. Furthermore, PPG sensors embedded in wearable devices simplify and reduce the cost of PPG signal acquisition. **Difficult to steal**—Traditional biometrics are subject to many easy attacks. Fingerprints and palmprints can be extracted from touchscreen surfaces left by a user (Vachon, 2020), while facial images can be taken at a distance. In contrast, contact-based PPG signals are not directly exposed to the attacker, making them difficult to spoof. **Live detection**—The liveliness of the users involved in the system is ensured by the natural liveness detection system because the PPG signal responds to the information of the human heartbeat.

The PPG signals differed between individuals. The signal can be affected by genetic and non-genetic factors, according to many PPG signal studies (Tegegne et al., 2020; Wang et al., 2021; Panahi et al., 2021). Differences in PPG signals are observed between individuals, empowering the upgrade from pre-set passwords to PPG signals for user authentication. PPG signals were first applied in biometrics in 2003 (Gu et al., 2003). Subsequently, the derivatives of the PPG signal were used for biometric authentication (Yao et al., 2007). The approach to individual feature matching has shifted from the initial calculation of the distance between features to deep learning classifiers (Reşit Kavsaoğlu et al., 2014).

We attempt to comprehensively investigate PPG signals in authentication applications. PPG signals used in authentication systems can effectively capture users' cardiac dynamic behaviors Gil et al. (2008), which is not possible for traditional methods like fingerprints, iris, and many alike. We found the articles from Google Scholar, IEEEXplore, ACM Digital Library, ScienceDirect, and DBLP using various search terms — "PPG", "photoplethysmogram", "security", "authentication", "biometrics", and "attack". We assessed the relevance of the articles to our investigation by examining their titles, abstracts, and keywords, ranging from the first PPG-based biometrics in 2003 to recently published articles in 2023. We kept the papers directly related to the intersection of PPG signals and cybersecurity applications. We prioritized articles with a substantial number of citations, indicating their influence and recognition within the research community. We focused on the articles published in top conferences and journals known for their rigorous review processes and wide readerships, such as the IEEE Symposium on Security and Privacy, the ACM Conference on Computer and Communications Security, Computers & Security, IEEE Transactions on Information Forensics and Security and several others. We paid attention to the paper authored by recognized experts or research groups in the field of cybersecurity. While we aimed to include recent research, we also considered foundational papers published in earlier years.

A survey of heart biometrics was presented in (Rathore et al., 2020) for user authentication with heart signals, but it suffers from a primitive coverage in PPG signals with merely six papers. A review on wearable biometric systems was presented in (Sundararajan et al., 2019) with only a few acquisition methods for PPG signals. This paper aims to present a comprehensive review of the authentication method based on PPG signals. The main contributions are summarized as follows:

- We systematically present PPG-based authentication associated with security threats. We propose a novel taxonomy to organize various systems from the technical and application perspectives to provide a comprehensive insight into PPG signals.
- We survey the most recent research on PPG-based authentication from 2003 to 2023 and summarize the view to enable future researchers to apply the PPG signals technologies.
- We discuss the challenges of PPG-based authentication to highlight open issues for immediate attention and suggest possible countermeasures for future research.

The rest of this paper is organized as follows: We propose a four-layered view of PPG-based authentication in Section 2. In Sections 3, 4 and 5, the literature review is presented on PPG-based authentication. We review the usage of PPG signals in other authentication models in Section 6. Section 7 discusses the challenges faced by PPG-based authentication and proposes the corresponding future directions. Section 8 concludes this paper.

## 2. A Novel Four-Layered View on PPG-based Authentication

In this section, we present a novel view of PPG-based authentication. Fig. 1 presents our four-layered framework generalized from the literature. The bottom layer is the signal acquisition layer for collecting PPG signals. The second layer denoises the signal with the enhancement of its signal-to-noise ratio. The third layer, called the PPG representation layer, extracts the signal's features through feature transformation and selection. The security application layer uses the extracted features for authentication. Our framework was developed through meticulous information aggregation and generalization from diverse literature sources. We aim to capture and categorize the essential facets, factors, and dimensions prevalent in the existing body of knowledge. To provide further clarity, we emphasize that our taxonomy is not merely a subjective framework based on individual expertise. Instead, it is rooted in a systematic literature analysis, ensuring its relevance and coverage of the key elements within the field. By presenting this taxonomy, we contribute a structured and organized approach to the study of PPG signals in the context of cybersecurity, enabling researchers to navigate the complexities of this domain effectively.

### 2.1. *Signal Acquisition Layer*

The signal acquisition layer includes the actions for capturing the user's PPG signal. It extracts PPG signals from the skin and converts them into electrical signals for transmission to the next layer. This layer consists of four main components — light source, skin, sensor, and storage. The blood flow in the skin is the source of the signal. The light source exposes the signal to the sensor. The sensor converts the received signal into an electrical signal to feed subsequent layers for processing. The mainstream sensors are photodetectors that convert the received light intensity into a voltage signal. A camera is regarded as a sensor for capturing rich information of light. Storage determines the carrier of the signal, including electrical and video signals. Eventually, all signals are transformed into PPG waveforms and passed to the noise reduction layer.

Depending on the sensor and acquisition types, many methods are available to capture PPG signals. We classify them as contact and remote captures. The contact type captures the signal using photodetectors, and the device remains contacting with the skin. The remote type usually acquires the PPG signal by analyzing the video obtained by the camera, which allows the signal to be acquired at a certain distance. Within these two types, there are also subtle differences in the different acquisition devices. We have compared four most common devices, including oximetry (contact), wearable devices (contact), smartphone cameras (remote), and HD cameras (remote). The oximeter and wearable devices capture reflected or projected light intensity changes primarily through light-sensitive sensors (Fong et al., 2021; Singh et al., 2021). Smartphone cameras and HD cameras capture the change of RGB value among video frames to detect the change of blood flow in human skin tissue (Aziz et al., 2021; Liu et al., 2021). Although the captured PPG signals all respond to a wealth of individual biometric information, the signal morphology acquired by various methods differs because tissues of different body parts emit different PPG signals.

For a comprehensive comparison, we summarized five evaluation dimensions of signal acquisition from the existing literature.

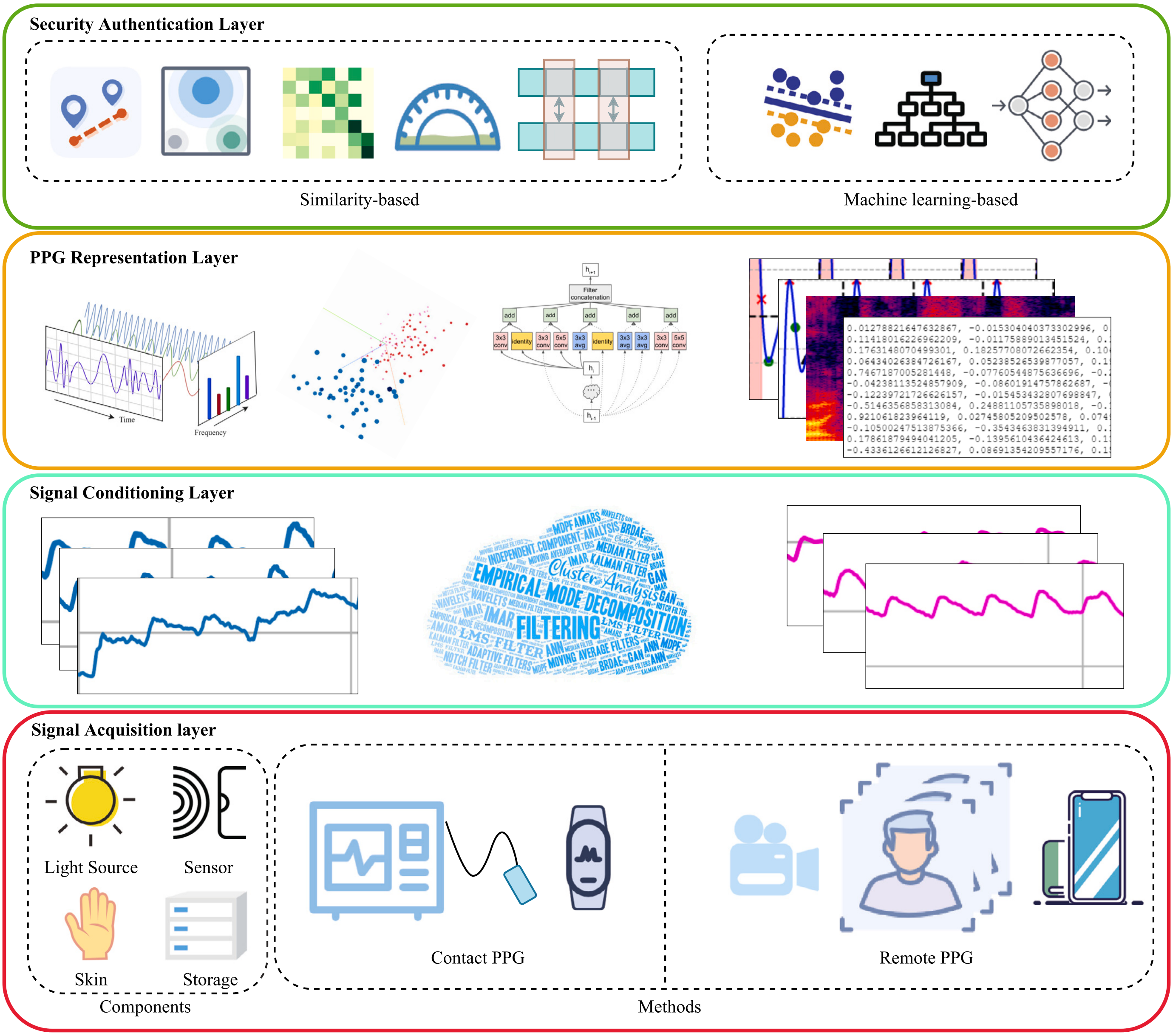

**Fig. 1.** Four-layered PPG-based authentication framework. Firstly, the PPG signal of the user can be captured using different devices. Then, the raw PPG signal is processed by signal conditioning to obtain a high-quality signal. In the third layer, features are extracted from the processed signal. Finally, each of these features is applied to different tasks according to their properties.

- **Security** refers to the level of data protection and privacy provided during signal acquisition. It encompasses aspects such as encryption, authentication mechanisms, secure transmission protocols, and protection against unauthorized access.
- **Signal Quality** focuses on the acquired signals' accuracy, reliability, and fidelity. It involves evaluating factors such as noise levels, signal-to-noise ratio, resolution, dynamic range, frequency response, and any distortions or artifacts introduced during acquisition.
- **Cost** evaluation involves assessing the financial implications of different signal acquisition methods. It includes considerations such as the initial investment required for equipment, ongoing maintenance costs, licensing fees for software or algorithms, and any additional expenses associated with the acquisition process.
- **Range** examines the ability of a signal acquisition method to capture signals from a distance. It evaluates the acquisition system's range and effectiveness in scenarios where physical proximity to the signal source may be limited.
- **Mobility** refers to the portability, flexibility, and ease of use of a signal acquisition system. It considers factors such as device size, weight, power requirements, and the ability to deploy or move the system in various settings.

Fig. 2 compares four acquisition methods in these five dimensions. The pulse oximeter obtains high-quality signals partly because it isolates the interference from external ambient light. However, a pulse oximeter needs to be clipped to a human finger, which interferes with any tasks that require finger involvement during continuous authentication. Due to the limited computational capability, oximeters transmit the captured signals to the endpoint for processing, increasing the risk of compromise. Wearable devices provide a new mode of interaction without affecting individuals' everyday lives, enabling continuous unnoticed authentication. A built-in physiological signal sensor allows

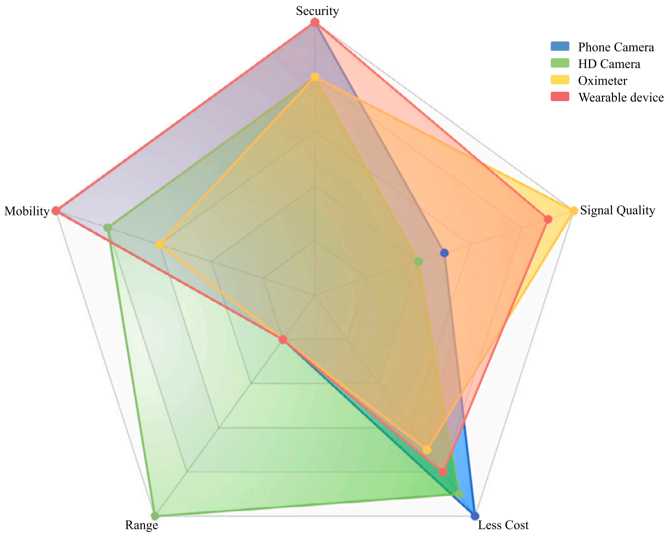

**Fig. 2.** Characteristics of different acquisition methods. We compared the four most representative devices using the two acquisition methods on five dimensions. Regarding security, smartphones, and wearable devices performed the best. Regarding signal quality, the oximeter scored the highest. Phone cameras cost the least. HD cameras can capture PPG signals at a distance. Phone cameras and wearable devices have excellent mobility.

wearable devices to capture PPG signals. Unlike the traditional acquisition of PPG signals via photodetector, a phone camera acquires PPG signals by using the flashlight as the light source and shooting the fingertip on the camera (Lovisotto et al., 2020b; Ortiz et al., 2022). The HD camera method analyzes the face video for non-contact physiological measurements (Patil et al., 2018), while the illumination usually comes from ambient light. However, the PPG signals acquired using the camera are often low quality and noisy, especially for people with dark skin tones and quick motion artifacts due to body movement. In addition, the surrounding light conditions can significantly affect the signal quality. With the popularity of smartphones, HD cameras have been built into various devices, so this acquisition method incurs no extra cost. For security reasons, the HD camera approach allows remote acquisition of PPG signals, which a malicious attacker can steal without the victim's awareness.

### 2.2. Signal Conditioning Layer

Noise is always present during any biomedical signal acquisition, no matter how well the devices are used (Mishra and Nirala, 2020). Signal conditioning has become an important task for ensuring highly accurate authentication. The signal conditioning layer receives the raw PPG signal as the input and produces a high-quality PPG signal as the output. Reducing or even eliminating noises in the signal is a primary concern when the types of noise need to be identified. The PPG signal contains rich heart-related information. Human bodies are usually assessed through statistical indicators (e.g., heartbeat interval, systolic peak) or physiological values (e.g., heartbeat rate, heart rate variability). Hence, it is challenging to pinpoint the noise.

There are four primary types of noises: low-frequency noise, high-frequency noise, cardiac arrhythmia noise, and low-amplitude PPG signals. High-frequency and low-frequency noises are more commonly present in PPG signals than the other two. Specifically, motion artifacts (MA) are the most common low-frequency noise commonly found in wearable devices. Both tissue deformation and sensor displacement may cause the appearance of motion artifacts (Nabavi and Bhadra, 2020). Another type of low-frequency noise is baseline wander noise. Under normal circumstances, the centerline of the pulse wave signal is relatively smooth, indicating that the signal's non-pulsatile component is stable. However, the acquired signal has a constantly changing amplitude value of the overall waveform due to baseline wander caused by multiple factors, such as temperature variations, the bias of the instrumentation amplifier, and breathing motion (Mishra and Nirala, 2020). High-frequency noise is normally caused by power line interference, which refers to the ambient electromagnetic signal of the instrument amplifier and the power supply obstruction of the PPG recording probe. We can filter all the high-frequency and low-frequency signals directly by using the low-pass/high-pass filter at the cost of a significant loss of the original signal. Advanced filters like adaptive filter (Arunkumar and Bhaskar, 2020) help retain the maximum information of the original signal.

### 2.3. PPG Representation Layer

The representation layer receives the cleansed signal as the input before yielding feature vectors that apply to authentication systems. Its primary objective is to extract features from the signal that are resilient to time and environmental changes while preserving the uniqueness of individual features. The PPG representation layer comprises feature transformation and feature selection. Fiducial points or statistical information can be directly extracted from the signal as feature vectors, like systolic peak, diastolic peak, and heart rate variability. The dicrotic notch is related to blood pressure (Mousavi et al., 2019), and the systolic peak is associated with cardiovascular aging (Chiarelli et al., 2019). Although these features can be acquired quickly from the raw signal, they are susceptible to changes in the surrounding environment and the physical state of the subject.

Feature transformation and feature selection are suitable for different tasks. Feature transformation converts the current feature space to a different space to acquire robust features for authentication, like from time-domain to frequency-domain. Feature selection helps remove redundant or irrelevant information. While removing the interference of useless information, feature selection also reduces features' dimensionality and computational cost.

### 2.4. Security Application Layer

The security application layer implements the authentication applications using features extracted from the PPG representation layer. PPG signals represent an individual's unique hemodynamic and cardiovascular system. Hence, PPG signals identify their owners during authentication.

The user authentication process comprises the enrollment phase and the authentication phase. During the enrollment phase, the biometric system learns the feature vectors extracted from the individual. The enrollment phase can be regarded as the training phase from the machine learning perspective. The learned templates are stored on a local device or in the cloud as individual identifiers. The authentication phase is further divided into two scenarios — verification and identification. Verification determines whether the user is consistent with the declared identity. Identification attempts to find the best matching enrollment template in the system that corresponds to the user. A biometric system can be regarded as a matching or classification problem.

At present, several methods distinguish the PPG signals of different individuals. A straightforward method uses the similarity between features to distinguish the PPG signals between individuals. A predefined threshold value determines the degree of similarity. If the similarity between features exceeds a preset threshold, the signals are considered to belong to the same individual. Distance and correlation are common approaches to measure similarity (Salanke et al., 2013; Akhter et al., 2015; Yao et al., 2007).

User authentication is typically translated into a classification problem in machine learning as the paradigm where user profiles are associated with different classes. Features manually extracted through traditional machine learning do not guarantee an adequate representation of the uniqueness of individual PPG signals. On the contrary, deep learning approaches are usually end-to-end solutions. Deep learning methods feed the training data and corresponding labels into the model before learning useful features and inferring the testing set results. Deep learning methods are often preferred over manual feature extraction when we lack profound domain knowledge to understand the feature domain.

## 3. Acquisition and Conditioning

PPG signals consist of pulse signals as repetitive waveforms and motion artifacts as bursty signals. Statistical differences (e.g., kurtosis, skewness, and standard deviation) can be applied to PPG signals for motion artifact detection (Zhao et al., 2018). According to the recoverability of cardiac signals, motion artifact is divided into two categories — distal and proximal wrist (Zhao et al., 2020). Distal wrist activity is a primary arm movement without involving the tendons and muscles of the wrist region. On the other hand, proximal wrist activities are horizontal and wrist-level movements that directly affect blood volume changes in the wrist region. Hence, proximal wrist activities may significantly impact PPG measurements from wearable devices.

Though distal wrist activity has a minor and recoverable effect on PPG signals, proximal wrist activity can have a long-lasting, intense, and non-recoverable effect on PPG measurements. Continuous near-wrist activity and accidental disease may cause sharp changes in heart conditions and affect the system's performance, resulting in a temporary reversion to a conventional authentication method like passwords. When motion artifact is scattered or present in only a few contiguous segments, it is associated with distal wrist activity so that we can reconstruct the associated pulse waveform. When motion artifact is detected in consecutive PPG signals, the motion artifact occurrence is attributed to proximal wrist activity. Therefore, motion artifact removal helps eliminate the affected PPG segments.

Mobile phone cameras have become an easy choice to acquire PPG signals because mobile devices are widely popular (Lovisotto et al., 2020b; Ortiz et al., 2022). However, poor light conditions and frequent vibrations often affect the quality of PPG signals collected by mobile phone cameras. Reliable cardiac motion patterns could only be obtained with the proper camera configuration and sufficient light entering the camera. Excessive (too low or too high) flashlight illumination reduces pixel sensitivity when capturing cardiac motion patterns from the camera. Thus, the camera configuration (i.e., flash intensity, ISO settings) needs adjustment to offset the variation of ambient light (Liu et al., 2019). Dynamically selecting the pixels in the video captured by the camera, such as only a subset of the most sensitive pixels to heart motion or removing invalid pixel points, can improve the signal-to-noise ratio of heart measurements.

Since PPG sensors consist of LED and photodetector with specific spectral sensitivity and emission wavelengths, subtle differences in such devices are common. These signals collected from different devices can be considered data from different domains. This problem can be handled by applying cross-domain adaptation methods (Lee et al., 2020), like DRANet (Lee et al., 2021) and PCS (Yue et al., 2021). They are usually applied to vision-related tasks. It is possible to eliminate the non-pulsatile component of the signal by adding an amplifier bias adjustment circuit, obtaining a high signal-to-noise ratio pulsatile component from the original PPG signal (Wan et al., 2007). Improvements from a hardware perspective result in better signal quality and make identification data processing easier.

Additional factors affecting PPG signal quality are human body posture and emotions. If data were obtained while the participant was sitting steadily, the effects of physical exercises on PPG signals were often ignored. Significant differences in the PPG signals were observed among participants in the exercise state (Salanke et al., 2013). Besides exercises, the PPG signal reflects the influence of the autonomic nervous system on cardiac activity, which can easily be altered by changes in heart rate caused by mood fluctuations. Using a Gaussian function to represent the PPG signal features approximately has excellent robustness for emotions (Sarkar et al., 2016). The classification of emotions in the datasets is based on participants' subjective perceptions.

As an authentication feature, feasibility is critical in long-term situations. The correlation coefficients of the PPG waveforms recorded during the month compared in (Patil et al., 2018) remain constant. Because of the frequent acquisition during continuous authentication, the effect of time on the signal is not considered in (Bonissi et al., 2013). Empirically, the performance of the authentication model in the cross-session case declines over time (Sancho et al., 2017; Hwang et al., 2021c,a,b). Feature selection helps identify features resilient to time (Yadav et al., 2018). Model fusion and generative adversarial networks improve the stability of the model over time (Hwang et al., 2021a,b; Liu et al., 2023; Hwang et al., 2022).

## 4. Representation Construction

Features representing PPG signals can be constructed in several different ways. Individual template vectors are built by extracting the number of peaks, time intervals, up slopes, and down slopes as features from a single-cycle PPG signal (Gu et al., 2003). In addition to these features, morphological features like the waveform area and the waveform angle were introduced in (Lee and Kim, 2015). The features are obtained directly from the original waveform, implying potential interference of external factors like baseline wander and motion artifact. This method of approximating the signal ignores the information of higher-order derivatives contained in the pulse. Because the information contained in the PPG signals cannot be fully utilized to improve recognition accuracy and reliability, Yao *et al.* (Yao et al., 2007) proposed to consider both first- and second-order derivatives of the PPG signals. The features obtained through higher-order derivatives are discriminative and sensitive to noise in the recognition task. In contrast, features from lower-order derivatives are more robust and less sensitive than those from their higher-order counterparts.

The feature transformation can obtain robust individual template vectors. Frequency-domain signals are generally more robust to time variations than time-domain signals. The Fourier transform converts the signal from the time domain to the frequency domain (Hwang et al., 2021b). However, the Fourier transform has an inherent flaw when dealing with non-smooth signals. It only obtains information about which frequency components a segment of the signal contains instead of the exact moments when each component appears. Thus, two signals with different time domains may have the same spectrogram. In this case, the short-time Fourier transform can decompose the entire time domain of the signal into an infinite number of small processes of equal length (Donida Labati et al., 2021). By setting the window length, we can obtain the frequency at a particular point in time. Nevertheless, it cannot meet the demand of the changing frequency of non-stationary signals, such as PPG signals. The components of various signals in nature at different frequencies have different time-varying characteristics. Generally, the spectral features of the lower frequency components change more slowly over time, while the higher frequency features change more rapidly. To obtain suitable frequency resolution and time resolution in different time-frequency regions, Patil *et al.* (Patil et al., 2018) used the Wavelet transform to decompose the signal across different time and frequency bands. Mel-Frequency Cepstral Coefficients work on specific frequency components according to the nonlinear Mel scale (Siam et al., 2021).

To construct individual template vectors, feature selection improves the discriminability and robustness of the features. Principal component analysis was used in (Lovisotto et al., 2020b) to remove correlations between variables in a biometric system, retaining key features that effectively distinguish PPG signals from different individuals. However, principal component analysis can only perform linear transformations on the data, resulting in weak outcomes for linearly inseparable data. Hence, kernel principal component analysis is used in (Zhang et al., 2018) to map data that cannot be linearly classified in the low-dimensional space to the high-dimensional space for principal component analysis. In addition, various algorithms are used for feature selection in biometric systems, including linear discriminant analysis (Yadav et al., 2018) and genetic algorithm (Karimian et al., 2017).

For instance, the waveform in a heartbeat cycle can be approximated by simple functions. We can use some morphological modeling approaches to describe the PPG signals for biometrics quantitatively (Cheng et al., 2019). Data need to be pre-processed before being manually extracted for features. Conversely, deep learning automates the feature selection process that helps develop a fully data-driven end-to-end biometric system with PPG signals (Luque et al., 2018; Everson et al., 2018).

## 5. PPG-based Authentication Model

It is challenging to optimize, develop, or transform the training data structure to improve classification performance. Among the similarity-based methods for identifying individual templates, the most common measure uses the Euclidean distance (Akhter et al., 2015; Gu et al., 2003). Euclidean distance represents the straight line distance between two feature points in a Euclidean space. However, the Euclidean distance is susceptible to different feature scales in the vector. The Mahalanobis distance eliminates some limitations of the Euclidean metric, such as automatically considering the scaling of the axes, correcting for correlations between different features, and providing curved and linear decision boundaries (Salanke et al., 2013). The Mahalanobis distance calculates the covariance distance between two data points. Pearson correlation is widely used to measure the degree of linear correlation between two variables (Yao et al., 2007). Among the above methods, a few outlier data in the training set can significantly affect the classification results because any similarity-based approach only needs to store a small number of training samples.

Eight machine learning-based methods are often used for user authentication based on PPG signals: linear discriminant analysis (Sarkar et al., 2016), support vector machine (Donida Labati et al., 2021; Zhao et al., 2020; Hinatsu et al., 2020; Lovisotto et al., 2020b; Karimian et al., 2017; Zhang et al., 2018), k-nearest neighbor (Reşit Kavsaoğlu et al., 2014; Donida Labati et al., 2021), random forest (Hinatsu et al., 2020; Cheng et al., 2019; Ohtsuki and Kamoi, 2016; Cao et al., 2020), gradient boosted trees (Lovisotto et al., 2020b; Zhao et al., 2018, 2020), multi-layer perceptron (Karimian et al., 2017; Siam et al., 2021), restricted Boltzmann machines (Jindal et al., 2016). These models are usually trained using the features from the feature capture layer as input and the class of the user as output.

Convolutional neural networks (CNNs) are popular for their wide range of applications in computer vision-related tasks. Recently, PPG-based user authentication has applied a CNN model (Luque et al., 2018). A typical CNN architecture consists of a convolutional layer, a pooling layer, and a fully connected layer. The target's low-level (points in the signal) and high-level features (overall trend of the signal) can be extracted by stacking the convolutional layers. Pooling layers are sampled to reduce the feature space while retaining the important features. The primary role of the fully connected layer is to classify the signal based on the features previously extracted from the convolutional and pooling layers. In a CNN, the signal from each neural network layer propagates up one layer, and the samples are processed independently each time.

However, the PPG signals are time-series data, and the information on the time dimension is valuable. LSTM adds a gate mechanism and a memory unit to Recurrent Neural Network (RNN) to capture the long-term dependence of the input sequence by recording information from different periods. Therefore, the LSTM component captures long-time contextual information (Everson et al., 2018; Hwang and Hatzinakos, 2019; Biswas et al., 2019; Hwang et al., 2021c; Ye et al., 2021). It also solves the gradient disappearance and gradient explosion problems in RNN. Many solutions like the transformer model (Vaswani et al., 2017) learn from sequence data. The current research on deep learning models in PPG-based authentication is limited and requires further exploration.

Biometric systems based on a single PPG signal are vulnerable since the acquisition equipment, and recording environment has a significant impact on the performance of the system. A PPG signal collected with a precise sensor in a controlled environment is reliable. However, if the PPG signal is unstable, an additional biometric signal can improve the result (Spachos et al., 2011). ECG can be recorded simultaneously with PPG and provide a multi-fact biometric system. The sensor can acquire the ECG and PPG signals simultaneously, thus synchronizing the ECG and PPG values. The systolic peak of PPG and the R-peak of ECG can be used to obtain the Pulse Transit Time and Pulse Arrival Time to match the user template, detecting any spoofing signal (Karimian et al., 2020). To bypass the anti-spoofing system, attackers need to measure the victim's ECG and PPG at the same time. Even if the attacker is able to generate the victim's ECG and PPG, matching them from the same time domain would be challenging. ECG signals require the user to use additional measurement equipment, increasing the system's complexity. Ultra-wideband radar can measure the user's breathing pattern and synchronize with PPG signals so that it can be used to detect unknown presentation attacks (Forouzanfar et al., 2021). Moreover, fusion-ID authenticates users by fusing PPG signals with information from motion sensors (Kumar et al., 2022).

Table 1 summarizes the concept of the user authentication-related articles we reviewed. Most studies use a single heartbeat cycle of the PPG signal as a unique identifier, as it is easier to extract individually relevant information. Permanence pertains to the ability of an authentication system to accurately identify and authenticate individuals over time, despite variations that may occur due to the passage of time or changes in an individual's mood. It implies that the system can effectively recognize and verify an individual's identity consistently, regardless of time gaps between authentication attempts or fluctuations in their emotional state. In Permanence, the evaluation of time gaps within one day is considered low level, and between one and seven days are considered medium level, longer than seven days are considered high level. Privacy concerns arise in PPG-based user authentication methods due to collecting and storing sensitive biometric data, specifically pulse or blood flow patterns. Privacy concerns also involve evaluating the potential risks of unauthorized access or data breaches associated with the methods. For example, video analytic-based data collection methods pose a higher risk of data leakage than traditional photoelectric sensor-based data collection methods.

We also found that there is no standard to evaluate PPG-based authentication. Table. 1 summarizes five evaluation metrics (Cancelability, Wearability, Continuity, Transparency, and Accessibility). To improve the practicality of PPG-based user authentication, further research is needed in these five aspects.

**Cancelability:** Biometric systems usually require biometrics to be permanent. However, once the biometric template is exposed, the threat to the identification system is permanent. Cancelability means that the template can be replaced in biometric template exposure. The raw biometric data undergo a non-invertible transformation creating a new biometric template. This transformation could be unique for each application, providing protection across systems. If a system is compromised and the biometric templates are stolen, these templates cannot be used, and a new transformation can be applied to generate new templates, essentially canceling the old ones. The most straightforward revocable authentication is to encrypt the biometrics in the device. In PPG-based user authentication, feature transformations are used to map features into different vector spaces to cancel templates. Cancelability can be quantified by two main aspects — revocability and unlinkability Bedari et al. (2021). Revocability ensures that the newly generated one will not reduce the authentication performance when a biometric template is compromised. Unlinkability refers to the inability to establish a link

**Table 1**
Outline of reviewed papers attributes on user authentication. "✓": Will work. "●": High level. "◐": Medium level. "○": Low level. Permanence: The robustness of the authentication to temporal changes, including long time intervals and mood changes. Time gaps within one day are evaluated as low level, while gaps ranging from one to seven days or mood changes are considered medium level. Gaps exceeding seven days are classified as high level. Privacy: The potential exposure level of biometric signals. For data acquisition methods, video analytics-based data collection is low level, photoelectric sensor-based methods are medium level, and integrating photoelectric sensors with authentication systems in the same device is high level. Cancelability: Whether the authentication template can be revoked/replaced. The papers that incorporated cancellable techniques have been marked. Wearability: The papers that have been marked signify the utilization of wearable devices. Transparency: If the user can perceive the authentication process. They often require wearable devices or video-based analytics. Accessibility: Whether it is suitable for all populations, especially for people with physical disabilities. S: Single pulse. C: Continuous waveform. "-": Not considered.

| Reference | Source | Assessment | Permanence | Privacy | Cancelability | Wearability | Continuity | Transparency | Accessibility |
|---|---|---|---|---|---|---|---|---|---|
| Zhang et al. (2023) | S | Data-driven | - | ● | ✓ | ✓ | ✓ | ✓ | ✓ |
| Zhou et al. (2023) | C | Data-driven | ◐ | ● | | | | | |
| Liu et al. (2023) | C | Data-driven | ● | ◐ | | | | ✓ | ✓ |
| Hwang et al. (2022) | S | Data-driven | ● | ● | | | | | ✓ |
| Wang et al. (2022) | S | Data-driven | ○ | ◐ | | | | | ✓ |
| Kumar et al. (2022) | C | Data-driven | ○ | ● | | ✓ | | ✓ | ✓ |
| Ortiz et al. (2022) | S | Data-driven | - | ◐ | | | | | ✓ |
| Ye et al. (2021) | S | Data-driven | - | ● | | | | | ✓ |
| Hwang et al. (2021a) | S | Data-driven | ● | ● | | | | | ✓ |
| Hwang et al. (2021b) | S | Data-driven | ● | ● | | | | | ✓ |
| Siam et al. (2021) | C | Data-driven | - | ● | | | | | ✓ |
| Donida Labati et al. (2021) | C | Data-driven | - | ● | | | | | ✓ |
| Hwang et al. (2021c) | S | Data-driven | ● | ● | | | | | ✓ |
| Zhao et al. (2020) | S | Data-driven | - | ● | | ✓ | ✓ | ✓ | ✓ |
| Lee et al. (2020) | S | Data-driven | ◐ | ● | | ✓ | | ✓ | ✓ |
| Hinatsu et al. (2020) | C | Data-driven | - | ● | | | | | ✓ |
| Cao et al. (2020) | S | Data-driven | ● | ● | ✓ | ✓ | | | ✓ |
| Lovisotto et al. (2020b) | S | Data-driven | ◐ | ◐ | | | | | ✓ |
| Biswas et al. (2019) | C | Data-driven | - | ● | | ✓ | | ✓ | ✓ |
| Hwang and Hatzinakos (2019) | C | Data-driven | - | ● | | | | | ✓ |
| Liu et al. (2019) | S | Data-driven | ● | ◐ | | | | | ✓ |
| Cheng et al. (2019) | S | Data-driven | - | ● | | | | | ✓ |
| Shang and Wu (2019) | C | Data-driven | - | ● | | ✓ | | ✓ | ✓ |
| Zhang et al. (2018) | S | Data-driven | - | ● | | | | | ✓ |
| Everson et al. (2018) | S | Data-driven | - | ● | | ✓ | | ✓ | ✓ |
| Luque et al. (2018) | C | Data-driven | - | ● | | | | | ✓ |
| Yadav et al. (2018) | S | Data-driven | ◐ | ● | | | | | ✓ |
| Zhao et al. (2018) | S | Data-driven | - | ● | | ✓ | ✓ | ✓ | ✓ |
| Patil et al. (2018) | C | Data-driven | ◐ | ○ | | | | ✓ | ✓ |
| Karimian et al. (2017) | S | Data-driven | - | ● | | | | | ✓ |
| Sancho et al. (2017) | S | Statistics-based | ◐ | ● | | | | | ✓ |
| Ohtsuki and Kamoi (2016) | C | Data-driven | - | ● | | ✓ | | | |
| Jindal et al. (2016) | S | Data-driven | - | ● | | ✓ | | ✓ | ✓ |
| Sarkar et al. (2016) | S | Data-driven | ● | ● | | | | | ✓ |
| Akhter et al. (2015) | C | Statistics-based | ○ | ◐ | | | | | ✓ |
| Lee and Kim (2015) | S | Data-driven | - | ● | | | | | ✓ |
| Reşit Kavsaoğlu et al. (2014) | S | Data-driven | - | ● | | | | | ✓ |
| Bonissi et al. (2013) | S | Statistics-based | - | ● | | | ✓ | | ✓ |
| Salanke et al. (2013) | S | Statistics-based | - | ● | | | | | ✓ |
| Spachos et al. (2011) | S | Data-driven | - | ● | | | | | ✓ |
| Yao et al. (2007) | S | Statistics-based | - | ● | | | | | ✓ |
| Gu et al. (2003) | S | Statistics-based | - | ● | | | | | ✓ |

between the original biometric features and the newly generated ones. If such a link is identifiable, it might be possible to recreate the original biometric data from the new features, defeating the revocation purpose. As listed in Table 1, the papers that incorporated cancellable techniques have been marked. We can find that most of the papers ignore the assessment of cancelability.

**Wearability:** Wearability refers to the suitability and practicality of incorporating biometric sensors or devices into wearable technology or accessories. This concept emphasizes the ability of these devices to comfortably and unobtrusively collect and analyze biometric data from individuals in their everyday activities. The goal is to provide seamless and continuous biometric authentication or monitoring while ensuring user comfort, convenience. With the miniaturization of physiological signal sensors, most wearable devices have these sensors built-in for healthcare. For wearable authentication, PPG signals are primarily collected by wristband devices. These wristband devices are easily accessible and usually inexpensive. In Table 1, the papers that have been marked signify the utilization of wearable devices (e.g., smartwatches and wristbands) for signal acquisition.

**Continuity:** Authentication is usually performed only on the first access in most authentication scenarios. The user identity is maintained by the credentials obtained through authentication. It may lead to security risks for subsequent operations. For example, if a legitimate user leaves the device unattended, a malicious user accessing the device will potentially access other services. Continuous authentication enables continuous verification of the user's identity for the entire duration of the session. While traditional continuous authentication methods typically rely on transient events, PPG signals are continuous waveforms that can easily provide non-intrusive continuous authentication. We have marked the papers that reported the continuous authentication performance of their methods in Table 1.

**Transparency:** Transparent authentication refers to an authentication process that is seamless, unobtrusive, and user-friendly. It aims to provide a frictionless user experience by minimizing user intervention or explicit authentication actions. In transparent authentication, the user's identity is verified in the background or implicitly through various methods or factors without requiring explicit input. Wearable device-based PPG user authentication offers the possibility of transparent user authentication. It reduces the probability of a spoofing attack since the user does not know when the authentication occurred. In Table 1, the Transparency column excludes methods that necessitate active user participation.

**Accessibility:** It refers to the authentication methods and practices designed to accommodate individuals with disabilities or impairments. It aims to ensure that individuals with diverse abilities can access and utilize digital systems securely and conveniently. In the context of accessibility authentication, traditional authentication methods may present barriers for individuals with disabilities. For example, individuals with visual impairments may encounter difficulties in entering complex passwords or reading visual authentication cues, while those with motor impairments may struggle with physical interactions like typing or using traditional input devices. PPG signals can be collected in multiple body parts like ears, forehead, fingers, and toes, implying high accessibility. From Table 1, it can be observed that all methods listed are considered accessible, except for those that necessitate gestural involvement.

## 6. Miscellaneous Authentication Models with PPG Signals

Though face recognition is the most widely used biometric feature, current face recognition systems are vulnerable to spoofing attacks. Face recognition systems may fail in front of highly realistic 3D masks because they capture local facial details to distinguish real faces from fake ones. Because PPG signals are present only in natural living tissue and absent in surface materials of any mask or printed material, facial liveness can be detected by finding PPG signals in facial videos (Chen et al., 2017). Remote photoplethysmogram (rPPG) signals are present in an organic face, resulting in the color value of facial areas in the video varying with the heart pulse. Hence, the peak amplitude of the rPPG spectrum could reflect the heartbeat intensity. The observed amplitude is susceptible to environmental noises due to illumination and camera settings. Moreover, the noise may dominate the observed signal. Cross-correlation operations of local rPPG signals at different face regions to amplify the shared heartbeat frequency can suppress the interference of non-periodic noise (Liu et al., 2018).

DeepFake (Li et al., 2020) uses a generative adversarial network to forge a face to replace the original face in the video clip. DeepFake poses a real threat to the accuracy of the multimedia information available, especially since falsifying a politician's speech may lead to harmful results. Live detection for face recognition mainly relies on detecting heart rate, while heart rate may be present in a DeepFake video clip with a slightly different pattern of PPG signals. Videos generated by DeepFake can be identified by how consistent the regular heart rate in the facial area is (Qi et al., 2020).

Handwritten signature authentication prevents fraud in financial, judicial, and administrative settings. Traditional handwritten signature authentication requires historical samples because it only compares static handwriting with the user's previous handwriting to determine the signature's authenticity. Several methods have been used to automatically generate models for spoofing handwritten signature images (Rahman et al., 2022; Li et al., 2021). PPGSign (Hafemann et al., 2019) uses the PPG signal collected from a wrist-worn wearable device to verify a user's handwritten signature. Unlike traditional PPG-based authentication, PPGSign studies the dynamic component of the PPG signals caused by hand movements. Moreover, gestures can be used to assist in authentication by changing the signal shape Zhou et al. (2023).

## 7. Research Gaps and Future Work

Many studies propose to use PPG signals for authentication because PPG signals have unparalleled advantages over traditional biometric features. However, research on PPG-based authentication is in its infancy, especially when interacting with artificial intelligent models. To help future research, we discuss the current challenges and future research directions.

### *7.1. Challenges in User Authentication*

The first challenge for PPG-based user authentication is **signal quality**. As PPG is a physiological signal, PPG signals' quality is subject to persistent changes under various factors. The variation may exaggerate potential vulnerabilities of the authentication application. The signal quality may be affected in the following two aspects:

**The influence of intrinsic factors**: PPG changes over time, implying the necessity to consider single or multiple authentication sessions. Most existing studies investigate the single session when continuous signals are measured simultaneously. However, in practical applications, many scenarios are cross-session when the enrollment and authentication phases occur across different sessions (Hwang and Hatzinakos, 2019; Lovisotto et al., 2020b; Sancho et al., 2017).
The performance of cross-sessions in authentication results is worse than that of single session (Hwang et al., 2021c,b). It indicates that the current approach is not robust to the change of PPG signals as time varies. Furthermore, human emotional changes significantly impact the PPG signals. The influence of emotions in certain situations can help resist unauthorized certifications like enforcing a convict to authenticate. When the user is anxious to authenticate, the influence of emotions is counter-productive. In studies of the effect of emotion on PPG signals, watching a video or playing a game is investigated to stimulate participants' emotions. However, watching videos and playing games introduce many uncontrollable parameters, resulting in unreproducible results and conclusions. We cannot objectively determine their true emotions through the participants' descriptions, so significant misinformation may be present in the collected data.
**The influence of external factors**: External factors that affect PPG signals include light conditions, physical movement, skin temperature, and skin tones. PPG signals are collected by following the optical principle, implying that the external lighting conditions affect the signal quality. Wearable devices are a popular choice for capturing PPG signals, but the collected PPG signals are often affected by motion artifact noises caused by the physical movement of the wearer. Moreover, skin temperature and skin tone affect the quality of the PPG signal.

The second challenge is the availability of high-quality **dataset**. Table 2 compares the publicly available datasets, focusing on the common features. These metrics were chosen according to their widespread use in the literature, their relevance to our research objectives, and their ability to provide a holistic understanding of the dataset characteristics. The information presented in the table is derived solely from the dataset descriptions. The most extensive dataset with different states has merely 170 participants' signals. It is challenging to collect

**Table 2**

Comparison of publicly available PPG datasets in different dimensions. Subjects: Number of participants in the dataset. Location: Which body part the signal was collected. F: Face. FT: Fingertip. W: Wrist. E: Ear. FH: Forehead. "●": Cross-session. "○": Single-session. Patient: The participant is under medical supervision. Relax: Participants remain as stationary as possible during signal acquisition. Exercise: Including Running, Cycling, Walking, and Climbing. Emotion: Use games or videos to stimulate participants' emotions. "-": The health status of the participants was not considered. "$X$": There were health problems among the participants. "✓": All participants are healthy.

| Reference | Subjects | Location | Time Span | Status | Storage | Acquisition Environment | Health Status |
|---|---|---|---|---|---|---|---|
| UBFC-Phys[1]<br>(Sabour et al., 2023) | 56 | F | ○ | Exercise | Video | Laboratory | ✓ |
| Biosec3<br>(Hwang et al., 2021b) | 170 | FT | ● | Exercise | Electrical signals | Office | ✓ |
| SeeingRed<br>(Lovisotto et al., 2020b) | 15 | FT | ● | Relax | Video | Laboratory | - |
| PPG-ACC<br>(Biagetti et al., 2020) | 7 | W | ○ | Exercise | Electrical signals | Laboratory | ✓ |
| UBFC-RPPG<br>(Bobbia et al., 2019) | 50 | F | ○ | Exercise | Video | Laboratory | – |
| TokyoTech<br>(Maki et al., 2019) | 9 | F | ○ | Relax | Video | Laboratory | – |
| CIME-PPG<br>(Xu et al., 2019) | 48 | FT | ○ | Exercise | Electrical signals | Laboratory | $X$ |
| PPG-DaLiA<br>(Reiss et al., 2019) | 15 | W | ● | Exercise | Electrical signals | Wild | ✓ |
| GYRO-ACC<br>(Lee et al., 2019) | 24 | W | ○ | Exercise | Electrical signals | Laboratory | ✓ |
| VIPL-HR<br>(Niu et al., 2018) | 42 | F | ○ | Exercise | Video | Laboratory | – |
| OBF<br>(Li et al., 2018) | 106 | F | ○ | Exercise | Video | Laboratory | $X$ |
| LGI-PPGI<br>(Pilz et al., 2018) | 25 | F | ○ | Exercise | Video | Wild | – |
| PPG-BP<br>(Liang et al., 2018) | 219 | FT | ○ | Relax | Electrical signals | Clinical | $X$ |
| PulseID<br>(Luque et al., 2018) | 43 | FT | ○ | Relax | Electrical signals | Office | ✓ |
| Biosec1[2]<br>(Yadav et al., 2018) | 41 | FT | ● | Exercise | Electrical signals | Office | ✓ |
| COHFACE<br>(Heusch et al., 2017) | 40 | F | ○ | Relax | Video | Laboratory | ✓ |
| Vortal[3]<br>(Charlton et al., 2016) | 57 | FT/E | ○ | Relax | Electrical signals | Laboratory | ✓ |
| MIMIC-III[4]<br>(Johnson et al., 2016) | 10,282 | FT | ● | Patient | Electrical signals | Clinical | $X$ |
| TROIKA<br>(Zhang et al., 2015) | 20 | W | ○ | Exercise | Electrical signals | Laboratory | – |
| PURE<br>(Stricker et al., 2014) | 10 | F | ○ | Exercise | Video | Laboratory | – |
| TBME<br>(Karlen et al., 2013) | 42 | FT | ○ | Patient | Electrical signals | Clinical | $X$ |
| DEAP<br>(Koelstra et al., 2011) | 32 | FT | ○ | Emotion | Electrical signals | Laboratory | ✓ |

[1] https://ieee-dataport.org/open-access/ubfc-phys-2.
[2] https://www.comm.utoronto.ca/~biometrics/PPG_Dataset/.
[3] https://peterhcharlton.github.io/RRest/vortal_dataset.html.
[4] https://physionet.org/content/mimiciii/1.4/.

an extensive data set in different states (movement status and emotions) as a physiological signal. Moreover, the interval between their measurements was only 18 days. Most existing datasets consider PPG signals collected in the resting state. The controlled environment in the experiment is different from our daily life, indicating that the signal noise in the data is significantly less than that in the real-world application.

The third challenge is the **overhead of the device**, especially in continuous authentication. Continuous authentication requires sensors to continuously monitor the user's physiological signals, implying the need for additional computational resources and energy overhead. These overheads are significant issues for resource-limited wearable devices and smartphones.

Moreover, **data leakage** is another challenge. Though PPG signals are not easily leaked, the leaked PPG signals will threaten the security of the authentication system once the leak occurs. Furthermore, the development of radar and remote PPG to collect heart rate information makes it impossible to ignore the potentially severe consequences of data leakage. Current research about cancelability focuses on the cancelable template. When a user template is compromised, it is replaced by redeploying a new one. However, it does not consider when the raw signal is leaked. In addition, the wearability and transparency of authentication require the support of wearable devices. All the authentication system components will be exposed to the adversary for stolen wearable devices.

Most existing work investigates medical-grade devices. With the popularity of wearable devices and the development of video technology, we believe that PPG signal-based security technology will be further developed in the future. Other physiological signals also receive increasing attention as promising candidates for implicit authentication systems. Some recent publications introduce biometric applications for authentication, including brain biometrics (Arias-Cabarcos et al., 2021), ECG signals (Hosseinzadeh et al., 2021), and electrical muscle stimulation (Chen et al., 2021b).

### 7.2. Attack Threats

Although it is challenging to steal unobservable PPG signals, PPG-based authentication faces potential threats. Two main types of attack threats are stealing user templates through leaked signals and attacks against user authentication AI models.

**Stealing user templates**: With the development of biomedi-cine, many studies show that contactless methods can be used to detect heartbeat signals (Dasari et al., 2021). HD cameras-collected rPPG signal is a severe threat to the PPG-based security system because of its easy-to-acquire and long-distance-use characteristics. The rPPG signal can acquire 70% of the IPI information obtained by the contact sensor (Calleja et al., 2015). When using rPPG to estimate IPI, darker skin has a higher average bit error rate, and it is more challenging to detect IPI accurately. This is due to the higher melanin content in darker skin than in lighter skin, reducing the diffuse reflection containing pulsation information, thus reducing signal quality. The head rotation also affects the accuracy of rPPG because it changes the light reflected from the skin. In addition, compression of the video causes signal artifacts that can lead to false detection of heartbeats, but it does not significantly affect the detection of IPI. Although rPPG has been successfully applied to detect 3D mask presentation attacks and DeepFake videos, it is susceptible to environmental noise due to the particularly weak signal. rPPG is often used to obtain simple time- and frequency-domain features such as HRV and IPI to attack the corresponding security systems. The camera is susceptible to the user's background environment as the victim's environment changes in real-world scenarios.

Another non-contact method of detecting heartbeat signals is based on ultra-wideband radar. It measures the heartbeat by the variation in the amplitude and the arrival time of the reflected pulses. PPG is an optical signal that cannot be detected directly by radar. This setup allows radar-based methods to detect only heart rate information such as HRV and IPI of the heartbeat. Therefore, it is used in the same way as the HD camera approach, mainly for attacking systems based on simple features such as HRV and IPI. It does not mean that the HD camera- and radar-based approach is not a threat. There is already research to obtain high-quality rPPG signals using generative models (Lu et al., 2021). Furthermore, radar information for reconstructing the ground truth PPG signal is also a possible threat. (Yamamoto et al., 2020) hypothesized the potential to reconstruct the ECG signal using the information collected by the doppler sensor. However, there is no research evidence using the doppler sensor to reconstruct PPG signals.

Once the PPG signal is compromised, it can be simulated using dynamic models. Gaussian functions can be applied to construct the mapping function that converts the attacker's PPG signals into dynamic model parameters similar to those of the victim to deceive the biometric system. We refer to this attack method as a gray-box evasion attack. The gray-box evasion attack only attracts limited attention due to its strong assumption of obtaining the victim's PPG signal in advance.

**Attacking user authentication AI models**: Currently, there are many attack methods against machine learning that have tremendous potential (Chen et al., 2021a; Lovisotto et al., 2020a). For instance, (Chen et al., 2021a) spoofs speaker recognition systems by generating adversarial examples. Adversarial examples refer to the addition of imperceptible perturbations to the original input to mislead the model and produce incorrect outputs. To the best of our knowledge, there are no defenses against PPG-based authentication adversarial examples. Traditional adversarial defenses are usually divided into two categories, detecting adversarial examples and improving the robustness of the classifier to adversarial examples (e.g., adversarial retraining and distillation). However, even with the state-of-the-art defense approach, there are still effective attacks (Rosenberg et al., 2021). Poisoning attacks on the model were performed in (Lovisotto et al., 2020a) through the update process of unsupervised templates. Since biometric systems usually adopt a self-renewal strategy, they are prone to poisoning attacks. Another attack that targets user authentication AI models is the backdoor attack. Inserting backdoors into the model makes the model trigger different results when faced with a specific symbol (Wang et al., 2019). Unlike poisoning attacks, backdoor attacks can be hidden until the input activates them. Although the backdoor attacks can be mitigated by pruning neurons (Shokri et al., 2020), the mitigation is limited, and further exploration of possible measures remains future work. Each of these approaches is a potential threat to machine learning-based biometric systems.

## 8. Conclusion

Traditional biometric authentication is susceptible to the threat of presentation attacks. Physiological signal-based authentication has recently received much attention, especially PPG signals. PPG-based authentication becomes popular because of its non-intrusiveness, capability of continuous monitoring, spoof defection, and wide availability. This paper surveys PPG-based authentication in three aspects — signal extraction, signal conditioning, and feature conversion and selection. The existing research review identifies the challenges, and future directions are proposed to match the various limitations. In addition, the attack threats against PPG-based authentication are summarized. Thus, this survey can help researchers understand PPG signal-based applications' current development in security and future research trends. Most studies in this review were conducted within the last few years, indicating a fast-growing interest in applying PPG signals among researchers in the security community. This paper shows the broad potential of using PPG signals for authentication.

## Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## Data availability

Data will be made available on request.

## References

Akhter, N., Gite, H., Rabbani, G., Kale, K., 2015. Heart rate variability for biometric authentication using time-domain features. In: Proceedings of the International Symposium on Security in Computing and Communication. Springer, Kochi, India, pp. 168–175.

Arias-Cabarcos, P., Habrich, T., Becker, K., Becker, C., Strufe, T., 2021. Inexpensive brainwave authentication: new techniques and insights on user acceptance. In: Proceedings of the 30th USENIX Security Symposium (USENIX Security 21). USENIX Association, pp. 55–72.

Arunkumar, K., Bhaskar, M., 2020. Casinor: combination of adaptive filters using single noise reference signal for heart rate estimation from PPG signals. Signal Image Video Process. 14, 1507–1515.

Aziz, M.H., Hasan, M.K., Mahmood, A., Love, R.R., Ahamed, S.I., 2021. Automated cardiac pulse cycle analysis from photoplethysmogram (PPG) signals generated from fingertip videos captured using a smartphone to measure blood hemoglobin levels. IEEE J. Biomed. Health Inform. 25, 1385–1396.

Bedari, A., Wang, S., Yang, W., 2021. Design of cancelable mcc-based fingerprint templates using dyno-key model. Pattern Recognit. 119, 108074.

Biagetti, G., Crippa, P., Falaschetti, L., Saraceni, L., Tiranti, A., Turchetti, C., 2020. Dataset from PPG wireless sensor for activity monitoring. Data Brief 29, 105044.

Biswas, D., Everson, L., Liu, M., Panwar, M., Verhoef, B.E., Patki, S., Kim, C.H., Acharyya, A., Van Hoof, C., Konijnenburg, M., Van Helleputte, N., 2019. CorNET: deep learning framework for PPG-based heart rate estimation and biometric identification in ambulant environment. IEEE Trans. Biomed. Circuits Syst. 13, 282–291.

Bobbia, S., Macwan, R., Benezeth, Y., Mansouri, A., Dubois, J., 2019. Unsupervised skin tissue segmentation for remote photoplethysmography. Pattern Recognit. Lett. 124, 82–90.

Bonissi, A., Labati, R.D., Perico, L., Sassi, R., Scotti, F., Sparagino, L., 2013. A preliminary study on continuous authentication methods for photoplethysmographic biometrics. In: Proceedings of the IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications. IEEE, Napoli, Italy, pp. 28–33.

Calleja, A., Peris-Lopez, P., Tapiador, J.E., 2015. Electrical heart signals can be monitored from the moon: security implications for ipi-based protocols. In: Proceedings of the Information Security Theory and Practice. Springer International Publishing, Cham, pp. 36–51.

Cao, Y., Zhang, Q., Li, F., Yang, S., Wang, Y., 2020. PPGPass: nonintrusive and secure mobile two-factor authentication via wearables. In: Proceedings of the Annual IEEE International Conference on Computer Communications (INFOCOM '20). IEEE, pp. 1917–1926. Virtual.

Charlton, P.H., Bonnici, T., Tarassenko, L., Clifton, D.A., Beale, R., Watkinson, P.J., 2016. An assessment of algorithms to estimate respiratory rate from the electrocardiogram and photoplethysmogram. Physiol. Meas. 37, 610.

Chen, G., Chenb, S., Fan, L., Du, X., Zhao, Z., Song, F., Liu, Y., 2021a. Who is real Bob? Adversarial attacks on speaker recognition systems. In: Proceedings of the IEEE Symposium on Security and Privacy (SP). IEEE, pp. 694–711.

Chen, Y., Sun, J., Jin, X., Li, T., Zhang, R., Zhang, Y., 2017. Your face your heart: secure mobile face authentication with photoplethysmograms. In: Proceedings of the Annual IEEE International Conference on Computer Communications (INFOCOM). IEEE, Atlanta, GA, USA, pp. 1–9.

Chen, Y., Yang, Z., Abbou, R., Lopes, P., Zhao, B.Y., Zheng, H., 2021b. User authentication via electrical muscle stimulation. In: Proceedings of the CHI Conference on Human Factors in Computing Systems. Association for Computing Machinery, New York, NY, USA.

Cheng, S., Chou, Y., Liu, J., Gu, Y., Huang, X., 2019. A novel identity authentication method by modeling photoplethysmograph waveform. In: Proceedings of the International Conference on Control, Automation and Information Sciences (ICCAIS). IEEE, Chengdu, China, pp. 1–5.

Chiarelli, A.M., Bianco, F., Perpetuini, D., Bucciarelli, V., Filippini, C., Cardone, D., Zappasodi, F., Gallina, S., Merla, A., 2019. Data-driven assessment of cardiovascular ageing through multisite photoplethysmography and electrocardiography. Med. Eng. Phys. 73, 39–50.

Dasari, A., Prakash, S.K.A., Jeni, L.A., Tucker, C.S., 2021. Evaluation of biases in remote photoplethysmography methods. npj Digit. Med. 4, 1–13.

Donida Labati, R., Piuri, V., Rundo, F., Scotti, F., Spampinato, C., 2021. Biometric recognition of PPG cardiac signals using transformed spectrogram images. In: Proceedings of the ICPR Workshop on Mobile and Wearable Biometrics (WMWB). Springer, pp. 244–257. Virtual.

Eberz, S., Paoletti, N., Roeschlin, M., Kwiatkowska, M., Martinovic, I., Patané, A., 2017. Broken hearted: how to attack ecg biometrics. In: Proceedings of the Network and Distributed System Security Symposium (NDSS '17). Internet Society, San Diego, California.

Everson, L., Biswas, D., Panwar, M., Rodopoulos, D., Acharyya, A., Kim, C.H., Van Hoof, C., Konijnenburg, M., Van Helleputte, N., 2018. Biometricnet: deep learning based biometric identification using wrist-worn PPG. In: Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS). IEEE, Florence, Italy, pp. 1–5.

Fong, D.D., Yamashiro, K.J., Vali, K., Galganski, L.A., Thies, J., Moeinzadeh, R., Pivetti, C., Knoesen, A., Srinivasan, V.J., Hedriana, H.L., Farmer, D.L., Johnson, M.A., Ghiasi, S., 2021. Design and in vivo evaluation of a non-invasive transabdominal fetal pulse oximeter. IEEE Trans. Biomed. Eng. 68, 256–266.

Forouzanfar, M., Baker, F.C., De Zambotti, M., Claudatos, S., Chai, B.B., Bergen, J., Lubin, J., 2021. Physiological synchrony: a new approach toward identifying unknown presentation attacks on biometric systems. IEEE Trans. Instrum. Meas. 70, 1–9.

Gil, E., Mendez, M., Vergara, J.M., Cerutti, S., Bianchi, A.M., Laguna, P., 2008. Discrimination of sleep-apnea-related decreases in the amplitude fluctuations of ppg signal in children by hrv analysis. IEEE Trans. Biomed. Eng. 56, 1005–1014.

Gu, Y., Zhang, Y., Zhang, Y., 2003. A novel biometric approach in human verification by photoplethysmographic signals. In: Proceedings of the 4th International IEEE EMBS Special Topic Conference on Information Technology Applications in Biomedicine. IEEE, Birmingham, UK, pp. 13–14.

Hafemann, L.G., Sabourin, R., Oliveira, L.S., 2019. Characterizing and evaluating adversarial examples for offline handwritten signature verification. IEEE Trans. Inf. Forensics Secur. 14, 2153–2166.

Hambling, D., 2019. The pentagon has a laser that can identify people from a distance—by their heartbeat. https://bit.ly/2qo5fR0.

Heusch, G., Anjos, A., Marcel, S., 2017. A reproducible study on remote heart rate measurement. arXiv preprint. arXiv:1709.00962.

Hinatsu, S., Suzuki, D., Ishizuka, H., Ikeda, S., Oshiro, O., 2020. Photoplethysmographic subject identification by considering feature values derived from heartbeat and respiration. In: Proceedings of the 42nd Annual International Conference of the IEEE Engineering in Medicine Biology Society. IEEE, pp. 902–905. Virtual.

Hosseinzadeh, M., Vo, B., Ghafour, M.Y., Naghipour, S., 2021. Electrocardiogram signals-based user authentication systems using soft computing techniques. Artif. Intell. Rev. 54, 667–709.

Huang, L., Wang, C., 2022. Pcr-auth: solving authentication puzzle challenge with encoded palm contact response. In: Proceedings of the IEEE Symposium on Security and Privacy (SP). IEEE Computer Society, Los Alamitos, CA, USA, pp. 913–927.

Huang, Y., Yang, G., Wang, K., Liu, H., Yin, Y., 2021. Learning joint and specific patterns: a unified sparse representation for off-the-person ecg biometric recognition. IEEE Trans. Inf. Forensics Secur. 16, 147–160.

Hwang, D.Y., Hatzinakos, D., 2019. PPG-based personalized verification system. In: Proceedings of the IEEE Canadian Conference of Electrical and Computer Engineering (CCECE). IEEE, Edmonton, AB, Canada, pp. 1–4.

Hwang, D.Y., Taha, B., Hatzinakos, D., 2021a. PBGAN: learning PPG representations from gan for time-stable and unique verification system. IEEE Trans. Inf. Forensics Secur. 16, 5124–5137.

Hwang, D.Y., Taha, B., Hatzinakos, D., 2021b. Variation-stable fusion for PPG-based biometric system. In: Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, pp. 8042–8046. Virtual.

Hwang, D.Y., Taha, B., Hatzinakos, D., 2022. A new score level fusion approach for stable user verification system using the PPG signal. J. Signal Process. Syst. 94, 787–798.

Hwang, D.Y., Taha, B., Lee, D.S., Hatzinakos, D., 2021c. Evaluation of the time stability and uniqueness in PPG-based biometric system. IEEE Trans. Inf. Forensics Secur. 16, 116–130.

Jain, A.K., Bolle, R., Pankanti, S., 2006. Biometrics: Personal Identification in Networked Society. Springer Science & Business Media, vol. 479. Switzerland.

Jia, W., Xia, W., Zhang, B., Zhao, Y., Fei, L., Kang, W., Huang, D., Guo, G., 2021. A survey on dorsal hand vein biometrics. Pattern Recognit. 120, 108122.

Jindal, V., Birjandtalab, J., Pouyan, M.B., Nourani, M., 2016. An adaptive deep learning approach for PPG-based identification. In: Proceedings of the 38th Annual International Conference of the IEEE Engineering in Medicine and Biology Society. IEEE, Orlando, FL, USA, pp. 6401–6404.

Johnson, A.E., Pollard, T.J., Shen, L., Li-Wei, H.L., Feng, M., Ghassemi, M., Moody, B., Szolovits, P., Celi, L.A., Mark, R.G., 2016. Mimic-iii, a freely accessible critical care database. Sci. Data 3, 1–9.

Karimian, N., Guo, Z., Tehranipoor, M., Forte, D., 2017. Human recognition from photoplethysmography (PPG) based on non-fiducial features. In: Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, New Orleans, USA, pp. 4636–4640.

Karimian, N., Woodard, D., Forte, D., 2020. Ecg biometric: spoofing and countermeasures. In: IEEE Transactions on Biometrics, Behavior, and Identity Science 2, pp. 257–270.

Karlen, W., Raman, S., Ansermino, J.M., Dumont, G.A., 2013. Multiparameter respiratory rate estimation from the photoplethysmogram. IEEE Trans. Biomed. Eng. 60, 1946–1953.

Koelstra, S., Muhl, C., Soleymani, M., Lee, J.S., Yazdani, A., Ebrahimi, T., Pun, T., Nijholt, A., Patras, I., 2011. Deap: a database for emotion analysis using physiological signals. IEEE Trans. Affect. Comput. 3, 18–31.

Kolberg, J., Grimmer, M., Gomez-Barrero, M., Busch, C., 2021. Anomaly detection with convolutional autoencoders for fingerprint presentation attack detection. In: IEEE Transactions on Biometrics, Behavior, and Identity Science 3, pp. 190–202.

Kumar, H., Mousavi, H.S., Shahsavari, B., 2022. Fusion-id: a photoplethysmography and motion sensor fusion biometric authenticator with few shot on-boarding. In: Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, pp. 3983–3987.

Lee, A., Kim, Y., 2015. Photoplethysmography as a form of biometric authentication. In: Proceedings of the IEEE Sensors Conference. IEEE, Busan, Korea (South), pp. 1–2.

Lee, E., Ho, A., Wang, Y.T., Huang, C.H., Lee, C.Y., 2020. Cross-domain adaptation for biometric identification using photoplethysmogram. In: Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, pp. 1289–1293. Virtual.

Lee, H., Chung, H., Lee, J., 2019. Motion artifact cancellation in wearable photoplethysmography using gyroscope. IEEE Sens. J. 19, 1166–1175.

Lee, S., Cho, S., Im, S., 2021. Dranet: disentangling representation and adaptation networks for unsupervised cross-domain adaptation. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 15252–15261.

Li, H., Li, H., Zhang, H., Yuan, W., 2021. Black-box attack against handwritten signature verification with region-restricted adversarial perturbations. Pattern Recognit. 111, 107689.

Li, X., Alikhani, I., Shi, J., Seppanen, T., Junttila, J., Majamaa-Voltti, K., Tulppo, M., Zhao, G., 2018. The obf database: a large face video database for remote physiological signal measurement and atrial fibrillation detection. In: Proceedings of the 2018 13th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2018). IEEE, pp. 242–249.

Li, Y., Yang, X., Sun, P., Qi, H., Lyu, S., 2020. Celeb-Df: a large-scale challenging dataset for deepfake forensics. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). IEEE, pp. 3207–3216. Virtual.

Liang, Y., Chen, Z., Liu, G., Elgendi, M., 2018. A new, short-recorded photoplethysmogram dataset for blood pressure monitoring in China. Sci. Data 5, 1–7.

Liu, C.Y., Yang, G.P., Huang, Y.W., Huang, F.X., 2023. Dual-domain and multiscale fusion deep neural network for PPG biometric recognition. In: Machine Intelligence Research, pp. 1–9.

Liu, J., Shi, C., Chen, Y., Liu, H., Gruteser, M., 2019. 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 (MobiSys '19). Association for Computing Machinery, New York, NY, USA, pp. 249–261.

Liu, S.Q., Lan, X., Yuen, P.C., 2018. Remote photoplethysmography correspondence feature for 3d mask face presentation attack detection. In: Proceedings of the European Conference on Computer Vision (ECCV '18). Springer International Publishing, Cham, pp. 577–594.

Liu, Y., Qin, B., Li, R., Li, X., Huang, A., Liu, H., Lv, Y., Liu, M., 2021. Motion-robust multimodal heart rate estimation using BCG fused remote-PPG with deep facial ROI tracker and pose constrained Kalman filter. IEEE Trans. Instrum. Meas. 70, 1–15.

Lovisotto, G., Eberz, S., Martinovic, I., 2020a. Biometric backdoors: a poisoning attack against unsupervised template updating. In: Proceedings of the IEEE European Symposium on Security and Privacy (EuroS&P). IEEE, pp. 184–197. Virtual.

Lovisotto, G., Turner, H., Eberz, S., Martinovic, I., 2020b. Seeing red: PPG biometrics using smartphone cameras. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops. IEEE, pp. 3565–3574. Virtual.

Lu, H., Han, H., Zhou, S.K., 2021. Dual-gan: joint bvp and noise modeling for remote physiological measurement. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). IEEE, pp. 12404–12413. Virtual.

Luque, J., Cortès, G., Segura, C., Maravilla, A., Esteban, J., Fabregat, J., 2018. End-to-end photoplethysmography (ppg) based biometric authentication by using convolutional neural networks. In: Proceedings of the 26th European Signal Processing Conference (EUSIPCO). IEEE, Rome, Italy, pp. 538–542.

Maki, Y., Monno, Y., Yoshizaki, K., Tanaka, M., Okutomi, M., 2019. Inter-beat interval estimation from facial video based on reliability of bvp signals. In: Proceedings of the 41st Annual International Conference of the IEEE Engineering in Medicine and Biology Society, pp. 6525–6528.

Mishra, B., Nirala, N.S., 2020. A survey on denoising techniques of PPG signal. In: Proceedings of the 2020 IEEE International Conference for Innovation in Technology (INOCON). IEEE, pp. 1–8. Virtual.

Mousavi, S.S., Firouzmand, M., Charmi, M., Hemmati, M., Moghadam, M., Ghorbani, Y., 2019. Blood pressure estimation from appropriate and inappropriate PPG signals using a whole-based method. Biomed. Signal Process. Control 47, 196–206.

Nabavi, S., Bhadra, S., 2020. A robust fusion method for motion artifacts reduction in photoplethysmography signal. IEEE Trans. Instrum. Meas. 69, 9599–9608.

Natarajan, K., Block, R.C., Yavarimanesh, M., Chandrasekhar, A., Mestha, L.K., Inan, O., Hahn, J.O., Mukkamala, R., 2021. Photoplethysmography fast upstroke time intervals can be useful features for cuff-less measurement of blood pressure changes in humans. IEEE Trans. Biomed. Eng. 1. https://doi.org/10.1109/TBME.2021.3087105.

Niu, X., Han, H., Shan, S., Chen, X., 2018. Vipl-hr: a multi-modal database for pulse estimation from less-constrained face video. In: Proceedings of the Asian Conference on Computer Vision. Springer, pp. 562–576.

Ohtsuki, T., Kamoi, H., 2016. Biometrie authentication using hand movement information from wrist-worn PPG sensors. In: Proceedings of the IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC). IEEE, Valencia, Spain, pp. 1–5.

Ortiz, B.L., Chong, J.W., Gupta, V., Shoushan, M., Jung, K., Dallas, T., 2022. A biometric authentication technique using smartphone fingertip photoplethysmography signals. IEEE Sens. J.

Panahi, F., Rashidi, S., Sheikhani, A., 2021. Application of fractional Fourier transform in feature extraction from electrocardiogram and galvanic skin response for emotion recognition. Biomed. Signal Process. Control 69, 102863.

Patil, O.R., Wang, W., Gao, Y., Xu, W., Jin, Z., 2018. A non-contact PPG biometric system based on deep neural network. In: Proceedings of the IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS). IEEE, Redondo Beach, CA, USA, pp. 1–7.

Pilz, C.S., Zaunseder, S., Krajewski, J., Blazek, V., 2018. Local group invariance for heart rate estimation from face videos in the wild. In: Proceedings of the 2018 IEEE Conference on Computer Vision and Pattern Recognition Workshops, pp. 1254–1262.

Qi, H., Guo, Q., Juefei-Xu, F., Xie, X., Ma, L., Feng, W., Liu, Y., Zhao, J., 2020. Deeprhythm: exposing deepfakes with attentional visual heartbeat rhythms. In: Proceedings of the 28th ACM International Conference on Multimedia (MM '20). Association for Computing Machinery, New York, NY, USA, pp. 4318–4327.

Rahman, A.M., Cao, Y., Wei, X., Wang, P., Li, F., Wang, Y., 2022. PPGSign: handwritten signature authentication using wearable PPG sensor. In: Proceedings of the 2022 IEEE Wireless Communications and Networking Conference (WCNC). IEEE, pp. 2721–2726.

Rathore, A.S., Li, Z., Zhu, W., Jin, Z., Xu, W., 2020. A survey on heart biometrics. ACM Comput. Surv. (CSUR) 53, 114.

Reiss, A., Indlekofer, I., Schmidt, P., Van Laerhoven, K., 2019. Deep PPG: large-scale heart rate estimation with convolutional neural networks. Sensors 19, 3079.

Reşit Kavsaoğlu, A., Polat, K., Recep Bozkurt, M., 2014. A novel feature ranking algorithm for biometric recognition with PPG signals. Comput. Biol. Med. 49, 1–14.

Rosenberg, I., Shabtai, A., Elovici, Y., Rokach, L., 2021. Adversarial machine learning attacks and defense methods in the cyber security domain. ACM Comput. Surv. (CSUR) 54, 1–36.

Sabour, R.M., Benezeth, Y., De Oliveira, P., Chappé, J., Yang, F., 2023. UBFC-Phys: a multimodal database for psychophysiological studies of social stress. IEEE Trans. Affect. Comput. 14, 622–636. https://doi.org/10.1109/TAFFC.2021.3056960.

Salanke, N.G.R., Maheswari, N., Samraj, A., 2013. An enhanced intrinsic biometric in identifying people by photoplethysmography signal. In: Proceedings of the 4th International Conference on Signal and Image Processing (ICSIP). Springer, Paris, France, pp. 291–299.

Sancho, J., Alesanco, A., Garca, J., 2017. Photoplethysmographic authentication in long-term scenarios: a preliminary assessment. In: Proceedings of the 2017 European Medical and Biological Engineering Conference. Springer, Tampere, Finland, pp. 1085–1088.

Sarkar, A., Abbott, A.L., Doerzaph, Z., 2016. Biometric authentication using photoplethysmography signals. In: Proceedings of the IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS). IEEE, Niagara Falls, NY, USA, pp. 1–7.

Shang, J., Wu, J., 2019. A usable authentication system using wrist-worn photoplethysmography sensors on smartwatches. In: Proceedings of the 2019 IEEE Conference on Communications and Network Security (CNS). IEEE, San Francisco, California, US, pp. 1–9.

Shokri, R., et al., 2020. Bypassing backdoor detection algorithms in deep learning. In: Proceedings of IEEE European Symposium on Security and Privacy (EuroS&P). IEEE, pp. 175–183.

Siam, A.I., Abou Elazm, A., El-Bahnasawy, N.A., El Banby, G.M., Abd El-Samie, F.E., 2021. PPG-based human identification using mel-frequency cepstral coefficients and neural networks. Multimed. Tools Appl. 80, 26001–26019.

Singh, S., Kozłowski, M., García-López, I., Jiang, Z., Rodriguez-Villegas, E., 2021. Proof of concept of a novel neck-situated wearable PPG system for continuous physiological monitoring. IEEE Trans. Instrum. Meas. 70, 1–9.

Spachos, P., Gao, J., Hatzinakos, D., 2011. Feasibility study of photoplethysmographic signals for biometric identification. In: Proceedings of the 17th International Conference on Digital Signal Processing (DSP). IEEE, Corfu, Greece, pp. 1–5.

Stricker, R., Müller, S., Gross, H.M., 2014. Non-contact video-based pulse rate measurement on a mobile service robot. In: Proceedings of the IEEE International Symposium on Robot and Human Interactive Communication. IEEE, pp. 1056–1062.

Sundararajan, A., Sarwat, A.I., Pons, A., 2019. A survey on modality characteristics, performance evaluation metrics, and security for traditional and wearable biometric systems. ACM Comput. Surv. (CSUR) 52, 39.

Tegegne, B.S., Man, T., van Roon, A.M., Asefa, N.G., Riese, H., Nolte, I., Snieder, H., 2020. Heritability and the genetic correlation of heart rate variability and blood pressure in > 29 000 families: the lifelines cohort study. Hypertens. 76, 1256–1262.

Vachon, P., 2020. The identity in everyone's pocket. Commun. ACM 64, 46–55.

Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A.N., Kaiser, Ł., Polosukhin, I., 2017. Attention is all you need. In: Proceedings of the Advances in Neural Information Processing Systems. NIPS, Long Beach, CA, USA, pp. 5998–6008.

Wan, Y., Sun, X., Yao, J., 2007. Design of a photoplethysmographic sensor for biometric identification. In: Proceedings of the International Conference on Control, Automation and Systems. IEEE, Seoul, Korea (South), pp. 1897–1900.

Wang, B., Liu, C., Hu, C., Liu, X., Cao, J., 2021. Arrhythmia classification with heartbeat-aware transformer. In: Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, pp. 1025–1029. Virtual.

Wang, B., Yao, Y., Shan, S., Li, H., Viswanath, B., Zheng, H., Zhao, B.Y., 2019. Neural cleanse: identifying and mitigating backdoor attacks in neural networks. In: Proceedings of IEEE Symposium on Security and Privacy (SP). IEEE, pp. 707–723.

Wang, C., Wang, Y., Chen, Y., Liu, H., Liu, J., 2020a. User authentication on mobile devices: approaches, threats and trends. Comput. Netw. 170, 107118.

Wang, M., Hu, J., Abbass, H.A., 2020b. BrainPrint: eeg biometric identification based on analyzing brain connectivity graphs. Pattern Recognit. 105, 107381.

Wang, S., Cao, J., He, X., Sun, K., Li, Q., 2020c. When the differences in frequency domain are compensated: understanding and defeating modulated replay attacks on automatic speech recognition. In: Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS '20). ACM, pp. 1103–1119. Virtual.

Wang, W., Vette, M., Wang, Q., Yang, J., Zuniga, M., 2022. Campressid: optimizing camera configuration and finger pressure for biometric authentication. In: Proceedings of the IEEE International Conference on Mobile Ad Hoc and Smart Systems (MASS). IEEE, pp. 229–235.

Xu, K., Jiang, X., Chen, W., 2019. Photoplethysmography motion artifacts removal based on signal-noise interaction modeling utilizing envelope filtering and time-delay neural network. IEEE Sens. J. 20, 3732–3744.

Yadav, U., Abbas, S.N., Hatzinakos, D., 2018. Evaluation of PPG biometrics for authentication in different states. In: Proceedings of the International Conference on Biometrics (ICB). IEEE, Gold Coast, QLD, Australia, pp. 277–282.

Yamamoto, K., Hiromatsu, R., Ohtsuki, T., 2020. Ecg signal reconstruction via Doppler sensor by hybrid deep learning model with cnn and lstm. IEEE Access 8, 130551–130560.

Yao, J., Sun, X., Wan, Y., 2007. A pilot study on using derivatives of photoplethysmographic signals as a biometric identifier. In: Proceedings of the 29th Annual International Conference of the IEEE Engineering in Medicine and Biology Society. IEEE, Lyon, France, pp. 4576–4579.

Ye, Y., Xiong, G., Wan, Z., Pan, T., Huang, Z., 2021. PPG-based biometric identification: discovering and identifying a new user. In: Proceedings of the 43rd Annual International Conference of the IEEE Engineering in Medicine and Biology Society. IEEE, pp. 1145–1148.

Yue, X., Zheng, Z., Zhang, S., Gao, Y., Darrell, T., Keutzer, K., Vincentelli, A.S., 2021. Prototypical cross-domain self-supervised learning for few-shot unsupervised domain adaptation. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 13834–13844.

Zhang, L., Li, A., Chen, S., Ren, W., Choo, K.K.R., 2023. A secure, flexible and PPG-based biometric scheme for healthy iot using homomorphic random forest. IEEE Int. Things J., 1. https://doi.org/10.1109/JIOT.2023.3285796.

Zhang, X., Qin, Z., Lyu, Y., 2018. Biometric authentication via finger photoplethysmogram. In: Proceedings of the 2nd International Conference on Computer Science and Artificial Intelligence (CSAI '18). Association for Computing Machinery, New York, NY, USA, pp. 263–267.

Zhang, Z., Pi, Z., Liu, B., 2015. TROIKA: a general framework for heart rate monitoring using wrist-type photoplethysmographic signals during intensive physical exercise. IEEE Trans. Biomed. Eng. 62, 522–531.

Zhao, T., Wang, Y., Liu, J., Chen, Y., 2018. Your heart won't lie: PPG-based continuous authentication on wrist-worn wearable devices. In: Proceedings of the 24th Annual International Conference on Mobile Computing and Networking (MobiCom '18). Association for Computing Machinery, New York, NY, USA, pp. 783–785.

Zhao, T., Wang, Y., Liu, J., Chen, Y., Cheng, J., Yu, J., 2020. Trueheart: Continuous Authentication on Wrist-Worn Wearables Using PPG-Based Biometrics. In: Proceedings of the Annual IEEE International Conference on Computer Communications (INFOCOM). IEEE, pp. 30–39. Virtual.

Zhou, X., Pan, J., Zhang, Z., Ji, X., Chen, H., 2023. Gesture-related two-factor authentication for wearable devices via PPG sensors. IEEE Sens. J.

**Lin Li** received the master's degree in computer science from the University of Melbourne, Melbourne, VIC, Australia. He is currently pursuing the Ph.D. degree with the School of Software and Electrical Engineering, Swinburne University of Technology, Melbourne, VIC, Australia. His research interests include applied AI, cyber resilience, and healthcare digital twin.

**Chao Chen** (Member, IEEE) received the Ph.D. degree in computer science from Deakin University, Geelong, VIC, Australia, in 2017. He is currently a Senior Lecturer with the College of Business and Law, RMIT University, Melbourne, VIC, Australia. He is conducting research on applying advanced analytics to solve emerging cyber security issues, such as networks traffic classification, social spam detection, insider threat detection, and machine learning security, such as inference attacks on machine learning (ML) models.

**Lei Pan** (Member, IEEE) received the Ph.D. degree in computer forensics from Deakin University, Geelong, VIC, Australia, in 2008. He is currently a Senior Lecturer with the School of Information Technology, Deakin University. He has authored 60 research papers in refereed international journals and conferences, such as the IEEE Transactions on Information Forensics and Security, the IEEE Transactions on Dependable and Secure Computing, and the IEEE Transactions on Industrial Informatics. His current research interests include cyber security and privacy.

**Leo Yu Zhang** (Member, IEEE) is currently a Senior Lecturer with the School of Information Technology, Deakin University, VIC, Australia. He received the bachelor's and master's degrees in computational mathematics from Xiangtan University, Xiangtan, China, in 2009 and 2012, respectively, and the Ph.D. degree from the City University of Hong Kong, Hong Kong, in 2016. Prior to joining Deakin, he held various research positions with the City University of Hong Kong, the University of Macau, Macau, China, the University of Ferrara, Ferrara, Italy, and the University of Bologna, Bologna, Italy. His current research interests include applied cryptography and AI related security, and he has published more than 60 refereed journal and conference articles in these fields.

**Zhifeng Wang** is a distinguished neurosurgeon. He is widely recognized for his expertise in diagnosing and treating various neurological conditions, including brain tumors, spinal cord injuries, cerebrovascular diseases, and other disorders affecting the central nervous system.

**Jun Zhang** (Senior Member, IEEE) received the Ph.D. degree in computer science from the University of Wollongong, Wollongong, NSW, Australia, in 2011. He is currently a Full Professor and the Director of the Cybersecurity Lab, Swinburne University of Technology, Melbourne, VIC, Australia. He was recognized in The Australian's top researchers special edition publication as the Leading Researcher in the field of Computer Security and Cryptography in 2020. He leads Swinburne cybersecurity research and produced excellent outcome, including many high-impact research papers and multimillion-dollar research projects. Swinburne was named in The Australian's 2021 Research Magazine, the top research institution in the field of Computer Security and Cryptography. Prof. Zhang has been serving as a Steering Committee Member of the P-TECH Program at Melbourne since 2019, which the Australian Government invested in, promoting STEM education. He devotes himself to communication and community engagement, boosting the awareness of cybersecurity.

**Yang Xiang** (Fellow, IEEE) received the Ph.D. degree in computer science from Deakin University, Geelong, VIC, Australia, in 2007. He is currently a Full Professor and the Dean of Digital Research with the Swinburne University of Technology, Melbourne, VIC, Australia. His research interests include cyber security, which covers network and system security, data analytics, distributed systems, and networking. He is also leading the Blockchain initiatives at Swinburne. In the past 20 years, he has published more than 300 research papers in many international journals and conferences. Prof. Xiang is the Editor-in-Chief of the SpringerBriefs on Cyber Security Systems and Networks. He serves as the Associate Editor for IEEE Transactions on Dependable and Secure Computing, IEEE Internet of Things Journal, and ACM Computing Surveys. He served as the Associate Editor for IEEE Transactions on Computers and IEEE Transactions on Parallel and Distributed Systems. He is the Coordinator, Asia for IEEE Computer Society Technical Committee on Distributed Processing.