This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2023.3285796

A Secure, Flexible and PPG-based Biometric Scheme for Healthy IoT Using Homomorphic Random Forest

Liping Zhang, Anzi Li, Shukai Chen, Wei Ren and Kim-Kwang Raymond Choo, *Senior Member, IEEE*

***Abstract*—Advances in the Internet of Things such as biosensing and camera-capturing technologies have also resulted in biometric-based authentication approaches becoming more viable. Photoplethysmography (PPG), for example, can be leveraged to provide better biometric features for continuous authentication, in comparison to other biometrics such as fingerprint. However, the fewer morphological features in PPG signals can complicate the accurate authentication of PPG signals. Furthermore, one has to also consider transmission security and PPG template storage security. These two considerations are typically not taken into consideration in most existing PPG-based authentication schemes. Therefore, we design a secure PPG-based biometric system to achieve accurate authentication with biometric privacy protection. In our design, Homomorphic Random Forest is adopted to classify the homomorphically encrypted biometric features, thus protecting the user's PPG biometrics from being compromised in authentication. Furthermore, beat qualification screening is set up to avoid the interference of unqualified signals, and 19 features with the least redundancy from the 541 features extracted are selected as the biometric features of the user. Doing so allows us to ensure the accuracy of authentication, as demonstrated in our evaluations using five PPG databases collected by three different collection methods (contact, remote, and monitor). In addition, our experiments adopt PPG signals acquired from remote cameras, which are not considered in other PPG-based biometric systems. The experimental results show that the average accuracy of our biometric system is 96.4%, the F1 score is 96.1%, the EER is 2.14%, and the authentication time is about 0.5s.**

***Index Terms*—Biometric system, Photoplethysmography, Homomorphic encryption, Random forest, Feature extraction**

I. Introduction

HUMAN authentication using physiological or behavioral features, i.e. biometrics, has gained increasing applications in security-concerning activities. Compared to conventional knowledge-based (e.g., PIN, password) and property-based (e.g., smart card) authentication, biometric-based authentication has shown its better robustness against guesswork, hacking, or theft attacks [1]. Over the past decade, many biometrics have proven to be convenient in many authentication scenarios, including iris, face, fingerprint, palmprints, etc [2]–[5]. However, these biometrics are not available for continuous authentication [6] as they require voluntary input from the user.

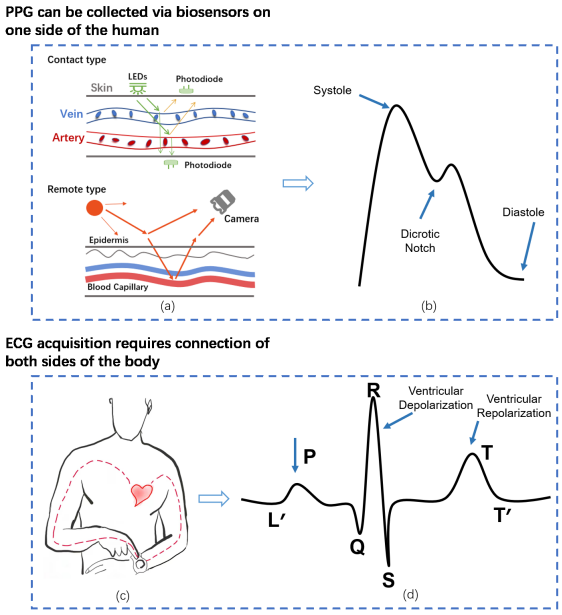

Fig. 1. (a) PPG signal acquisition method. (b) Typical PPG waveform. (c) ECG signal acquisition method. (d) Typical ECG waveform.

In healthcare systems and remote Internet of Things (IoT) medical services, the demand for continuous authentication has motivated researchers to explore newly available biometrics. In recent studies, electrocardiogram (ECG) and photoplethysmograph (PPG), as two important physiological signals in healthcare systems, have been proven possible for continuous authentication. As shown in Fig.1(a)(b), unlike ECG signals acquisition that need to connect both sides of the body, the PPG signals can be easily collected via biosensors from earlobes, fingertips, wrists, and other different positions on one side of the human body [7]–[9]. Moreover, PPG signal acquisition can also be achieved via remote PPG technology [10], which means that common consumer-grade cameras can achieve convenient signal acquisition without contact-specific sensors. The PPG-based authentication can be applied in various application scenarios to provide secure and convenient identity authentication. For example, a smartwatch captures the driver's PPG signals in real-time, enabling continuous authentication without any additional action by the driver [11], [12].

Liping Zhang, Anzi Li, and Shukai Chen are with the School of Computer Science, China University of Geosciences, Wuhan, 430074, China; e-mail: carolyn321@163.com.

Wei Ren is with the School of Computer Science China University of Geosciences, Wuhan, 430074, China; Nanchang Innovation Institute, Peking University, Nanchang, China. e-mail: weirencs@cug.edu.cn.

Kim-Kwang Raymond Choo is with the Department of Information Systems and Cyber Security, the University of Texas at San Antonio, San Antonio, TX 78249-0631, USA.

In addition, the use of PPG biometrics can complement other authentication methods to achieve multi-factor authentication [13].

Despite the convenience of continuous authentication and signal acquisition, PPG-based authentication is still facing many challenges. As shown in Fig.1(b)(d), the PPG signal has fewer morphological features than the ECG signal, and the signal quality is poor due to the low signal-to-noise ratio of the acquired PPG, which poses a challenge for accurate authentication based on the PPG signal.

Another challenge of PPG-based authentication is how to provide biometric privacy protection during the authentication process. Due to the permanence of the PPG signal, it cannot be changed after a compromise, which allows the adversary to obtain the user's private information by launching some attacks using the compromised PPG signals. Therefore, Cancelability [14] should be provided to achieve updates of PPG templates, thus preventing the adversary from obtaining the real PPG signal by compromising the PPG templates stored in the server or device. Furthermore, the PPG signals should also be protected during the transmission processes involved in authentication to prevent the adversary from obtaining the user's biometric privacy by eavesdropping. However, the existing researches on PPG-based authentication mainly focus on how to improve the accuracy of authentication, while ignoring the security requirements of biometric privacy protection during the authentication process.

Motivated by the above challenges, we design a secure PPG-based biometric system. In our design, the most unique features are selected and the Random Forest (RF) classifier is employed to achieve accurate authentication of PPG signals. Furthermore, homomorphic cryptography is introduced into the RF classifier to provide cancelability and secure signal transmission, thus achieving the protection of PPG signals during the authentication process.

- To improve authentication accuracy, Principle component analysis (PCA), and Max-Relevance and Min-Redundancy (mRMR) are employed to select the PPG biometric features, and the RF classifier is chosen to achieve accurate authentication of PPG signals. In our design, 541 features were extracted from a single PPG beat that passed quality screening, and then PCA and mRMR were used to select the most unique features for human identification, which ensures that there are sufficiently effective biometric features for authentication.
- To protect the PPG signals during the authentication process, the homomorphic encryption method is introduced into the RF classifier to realize cancelability and secure transmission. Moreover, in our design, the evaluation of PPG signals can be performed on ciphertext by using homomorphism random forest, ensuring that even the authentication server cannot access the real biometric features, thus protecting the user's biometric information.
- We performed extensive experiments on five datasets, where the PPG signals were acquired by different collection methods, such as contact and remote. To the best of our knowledge, we are the first to implement PPG signal authentication via a remote camera, which expands the practical application scenario of PPG-based authentication. The experimental results show that our authentication method achieves an average accuracy of 96.4% and the EER of 2.14%, indicating that the proposed PPG-based biometric system has high stability and authentication accuracy for PPG signals collected by various methods.

II. Related Works

This section briefly describes the existing methods of PPG-based authentication and the relevant researches on PPG biometric protection.

The feasibility of using PPG for authentication has been investigated in the previous work of Bonissi, Spacho et al. [15], [16], and their study illustrated that the differences between individuals are sufficient for human authentication. Subsequently, based on their work, many methods such as template matching, Fourier analysis, and pattern recognition have been investigated to achieve efficient PPG authentication.

Umang Yadav et al. [17] adopted template matching method to realize PPG authentication. In their design, continuous wavelet transform (CWT) and direct linear discriminant analysis (DLDA) were employed to generate user PPG templates, and Pearson distance was used to perform template matching operations. Although their method achieves a low error rate(EER 0.5%-6%), the authentication accuracy of this method depends on the selection of the thresholds, making it difficult to be widely applied. Fourier transforms as another approach has been adopted in both recently published researches [18], [19] to extract features from the time domains and frequency domains of PPG signals. These extracted features were used as unique identification features to distinguish users. However, the features extracted by the above method are less stable and also susceptible to noise interference, resulting in unstable authentication accuracy.

Pattern recognition methods are very popular in PPG authentication, especially machine learning technologies such as Support Vector Machines (SVM), Random Forest (RF), and K-Nearest Neighbor (K-NN). Guannan Wu et al. [20] proposed a two-step authentication method using a fingertip PPG sensor device. They first extracted five features of morphology and then conducted experiments on 40 individuals using K-NN, and SVM, respectively. The accuracy rate of their method is 91.93% for K-NN and 92.56% for SVM. Tianming Zhao [21] et al. also employed SVM and Gradient Boosting Decision Tree (GBT) for PPG authentication, and the experimental results demonstrated that GBT had better results on their collected data. Karimian et al. [22] used three different machine learning techniques, SVM, Self-organizing Map (SOM), and K-NN to compare the impact of two types of features(non-fiducial feature, fiducial features) of PPG signals on the authentication accuracy. They concluded that the method based on non-fiducial feature extraction outperformed the other, achieving an accuracy of 99.84%. However, PPG authentication based on machine learning also faces some unsolved problems such as small data size, poor data quality, or overfitting.

Recently, many deep learning models have been employed for PPG-based authentication. Hwang et al. [7] designed a two-layer convolutional neural network to find unique and time-stable features, which achieved 100% single-session authentication accuracy. Subsequently, they further introduced the LSTM technology into the PPG-based biometric [23] to achieve stable performance. However, deep learning models need to be trained in separate servers or resources before they can be implemented in local devices. It also takes a long time to train the raw data.

To achieve accurate PPG authentication, some studies [24], [25] have focused on how to reduce the possible noise interference caused by motion. Cao et al. [24] proposed a two-stage Motion Artifacts (MAs) removal algorithm to separate clean heartbeat signals from PPG signals. Pu et al. [25] also presented an MA removal algorithm to reduce noise interference and obtain more pure PPG signals. Although the above schemes [7], [15]–[23], [25] continuously improve the authentication accuracy, none of them provide PPG biometric protection during the authentication process.

To protect the PPG signals from being compromised by the adversary in the authentication process, the security of biometrics should be fully considered in the design of the PPG-based biometric systems. Cao et al. [24] proposed a repeatable and irreversible method to generate cancelable feature templates as alternative credentials that can resist man-in-the-middle attacks. Although their approach can construct new cancelable templates after a feature template has been compromised, the issue of when to update the template remains unresolved. This means that the adversary can still pass the authentication using the compromised PPG template within the interval of template updates. In addition, to provide secure transmission of PPG signals during the authentication process, Nakayama et al. designed [26] a secure communication channel using Galvanic Coupling to achieve the protection of transmitted PPG signals. However, their approach relies on the special channel and is therefore difficult to apply widely.

Although efforts have been made to achieve PPG biometric protection, existing PPG-based biometric systems generally fail to meet the requirements of PPG biometric protection both in transmission and storage. In this study, we present a secure PPG-based biometric system using homomorphic encryption, in which the PPG biometric features are transmitted and stored in ciphertext form.

III. Our Proposed Secure PPG-Based Biometric Framework And Application

In this section, the framework and application scenarios of the proposed PPG-based biometric system are presented.

The framework of our proposed secure PPG-based biometric system is shown in Figure 2. First, appropriate signal acquisition methods are selected according to different application scenarios. For example, a camera can be used for authentication when a wrist-based acquisition device (e.g. a smartwatch) is not available. Then, the raw PPG signals will be transmitted via Bluetooth to a platform such as a mobile phone, or computer for further processing.

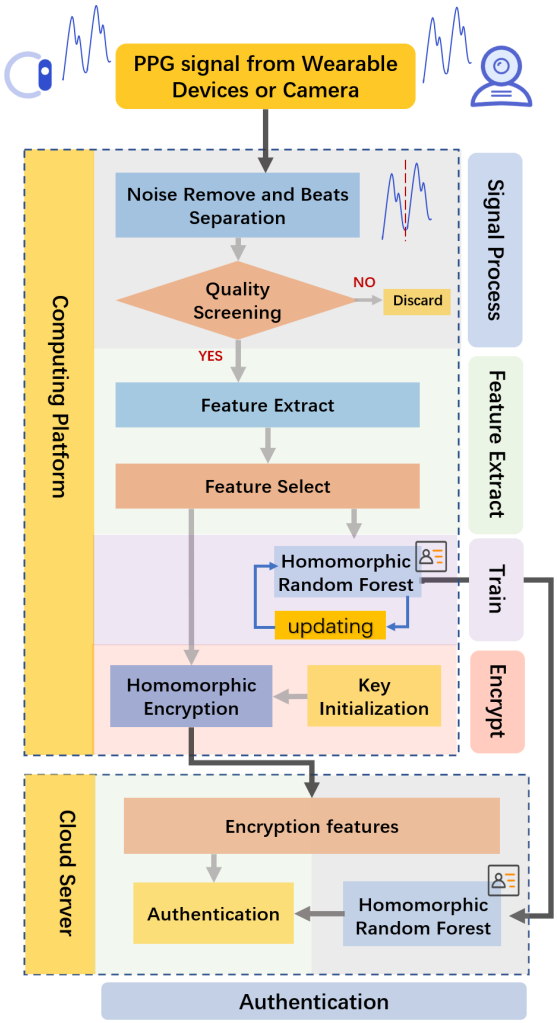

Fig. 2. Secure PPG-based biometric system framework

The PPG signal processing will be performed on a platform with computing power, where the data is first denoised to remove high-frequency noise and retain the cleaner PPG signal. Then, the continuous PPG signals are split into single beats using the beat separation algorithm, and the PPG features will be generated in the single beats. In each beat, fiducial point detection is first performed, and then, a quality screening is applied to eliminate the unqualified beats, thus avoiding the impact of the unqualified beats on the authentication.

Once the signal processing is completed, the biometric system will carry out the feature extraction process, including two steps: extraction and feature selection. In the extraction step, a total of 541 features were extracted for each beat. Next, a feature selection process is performed to reduce feature dimensionality and remove redundancy. After that, the unique biometric features of the user are successfully extracted from the processed PPG signals, which will be used for training and authentication.

The subsequent authentication process is divided into two phases: encryption and authentication. In the encryption phase, the selected features are first homomorphically encrypted, and

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2023.3285796

then the encrypted ciphertext is sent to the server. Note that the user's biometric features are transmitted in ciphertext during the transmission process. In the authentication phase, on the server side, the received encrypted biometric features are reasoned and evaluated using a homomorphic random forest. In this case, even the server does not have access to the real biometric information of the user. It is important to note that training on ciphertext to obtain an authentication model is difficult to achieve the desired goal, therefore in our system training is first performed locally on the user using plaintext and then the trained model is sent to the server. In addition, to improve the accuracy of authentication, the training set is adaptively updated to meet the requirements of the application.

Our proposed secure PPG-based biometric system not only achieves the protection of biometric features but also can be applied to various scenarios. For example, our proposed system can provide continuous authentication for users wearing smart wearable devices, and the authentication process does not require user interaction. In addition, the authentication results can be sent to other devices via Bluetooth or other communication protocols for various application requirements. Especially, the PPG signals can be collected using a common consumer-grade camera that extracts the PPG signal from the face skin video. As shown in Figure 3, in our proposed PPG-based biometric system, the remote PPG signals acquired by a camera are used for authentication. This design is suitable for some application scenarios without PPG sensors.

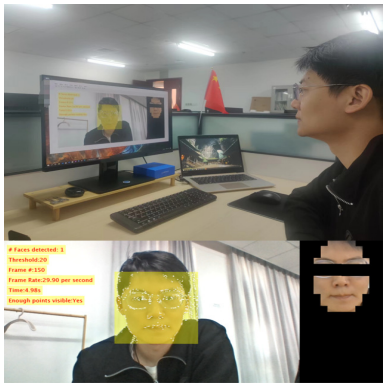

Fig. 3. PPG signals were collected using a computer camera

IV. Implementation Of PPG-Based Secure Biometric System

In this section, we present the implementation details of our proposed secure PPG-based biometric system and explain how the proposed system achieves accurate authentication with biometric features protection by applying homomorphic cryptographic random forests. The proposed PPG authentication mainly includes three phases: the signal process phase, the feature extraction phase, and the authentication phase. In the signal process phase, the raw PPG signals are processed to obtain cleaner PPG signals by signal denoising, beat separation, fiducial points detection, and beat quality screening steps. In the feature extraction phase, the user's unique PPG biometric features are extracted from previously processed PPG signals using our proposed feature extraction and selection methods. The final authentication phase includes three steps: encryption, classification, and adaptive updating, which realize the secure and accurate authentication of PPG signals. The details of our proposed PPG-based biometric system are given below.

A. Signal Process

The signal processing phase consists of four steps: signal denoising, beat segmentation, fiducial points detection, and beat quality screening. The purpose of this phase is to obtain cleaner PPG signals from the original PPG signals that will be used for the next step of feature extraction.

1) Signal Denoising: After acquiring the PPG signal, the trend is first removed using a rolling average method. Here, a window size of 1.01 seconds is used as a rolling average. Then we adopt a low-pass filter to remove the high-frequency noise.

Algorithm 1 The Beats Separation Algorithm

INPUT: preprocessed signal $\mathcal{S}$,max bpm $\mathcal{U}$, sampling rate $\mathcal{F}$, smoothing window size $\mathcal{W}$.

1. Estimates the minimum interval between the beats.
$$\mathcal{G} = 60 \cdot \frac{\mathcal{F}}{\mathcal{U}}$$
2. Moving average for signal $\mathcal{S}$.
$$A = moving\_average(S, W)$$
3. Find the index of the relative minima of S and A.
$$mins^{(S)} = arg\_rel\_min(S)$$
$$mins^{(A)} = arg\_rel\_min(A)$$
4. Separate individual beats.
$$S_i = \{s_{i-g}, \cdots, s_{i+g}\}$$
$$j = \underset{s_{i-g},\cdots,s_{i+g}}{\arg\min} S_i$$
$$B = B + \{j\}$$

where $i \in mins^A$.

OUTPUT: The set of beats B $= \{b_1, b_2 \ldots, b_n\}$

2) Beat Separation: Since the features are extracted in one beat, beat separation is required to obtain a single beat after denoising. In our design, we employ an algorithm 1 to separate continuous PPG signals into several single beats [27]. The algorithm 1 first estimates the minimum interval between the beats $\mathcal{G}$ which is used to initially segment the signal. Then a moving average algorithm is performed on the denoised signal $\mathcal{S}$ to remove some random perturbations. After that, the index of the relative minimum of the signal is found using the arg_rel_min function. Finally, according to the index of $\mathcal{A}$ complete the beat separation.

3) Fiducial Points Detection: After separating several individual beats, the system detects fiducial points in each beat, which are selected as part of the final feature. Three fiducial points are generated from the extremes of the first and second order derivatives of the PPG signal: diastolic peak, systolic peak, and dicrotic notch. As shown in Figure 4, these fiducial points mentioned above have unique physiological characteristics, and more features such as t_{a1} , t_{sp}, t_{b2}, $A2/A1$, etc. can be obtained from them.

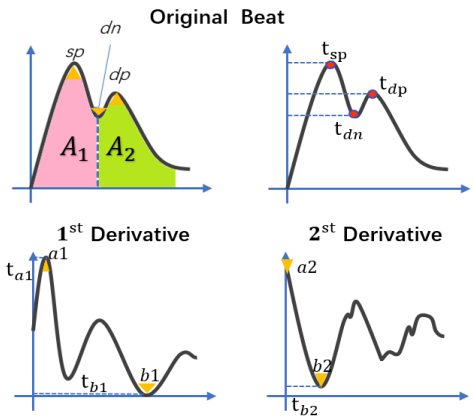

Fig. 4. Fiducial points and related features of ppg signals

4) Beat Quality Screening: The PPG signals acquired by various devices such as biosensors or cameras may be of poor quality due to motion, friction, bad contact, and other reasons [28], thus limiting the extraction of complete features from each beat. Since the accuracy of authentication can be affected by poor quality beats, so we add a screening step to eliminate the unqualified beats. Three standards are used to determine a qualified signal.

- The number of beats per minute is between 30 and 120.
- The number of maxima is 3 or more.
- The dynamic time warping (DTW) [29] distance from the standard waveform is less than 2. The DTW of the standard waveform is the average of the data set.

B. Feature Extraction

In our PPG-based biometric system, four groups of features introduced in [27] - statistics, curve width, frequency domain, and fiducial point - are employed as unique biometric features of the user. Moreover, we resample all beats to a sampling rate of 1,000Hz and normalize them so that the amplitude lies in a fixed range.

The statistical features used in our biometric system include minimum, maximum, maximum-minimum difference, and beat length. The curve width feature is the width of the beat curve over a predetermined set of heights. For the frequency domain, the computed discrete Fourier transform coefficients are adopted as features. Consequently, including the fiducial features mentioned in IV-A, a total of 541 features can be extracted on a beat.

However, too many features may lead to performance degradation, so feature selection is added to reduce the feature dimensionality and remove redundancy. This selection process involves the following three steps:

- Reduce the number of features by using principal component analysis (PCA) [30] for both frequency domain and curve width features. Then we retain the n components that describe 99% of the variance percentage of the corresponding feature set.
- Select the top 60% of the most important features by the Max-Relevance and Min-Redundancy (mRMR) [31].
- Generate the final biometric features by choosing the top 60% features ranked by Relative Mutual Information (RMI) [32].

Thereafter, the feature extraction and selection steps are completed, and the final number of features obtained on one beat for each user is between 18 and 22, which depends on the dataset.

C. Authentication

In our design, a random forest model based on classification is developed to achieve secure and accurate authentication. The users' PPG features obtained from the above steps are divided into training and test sets according to 7:3.

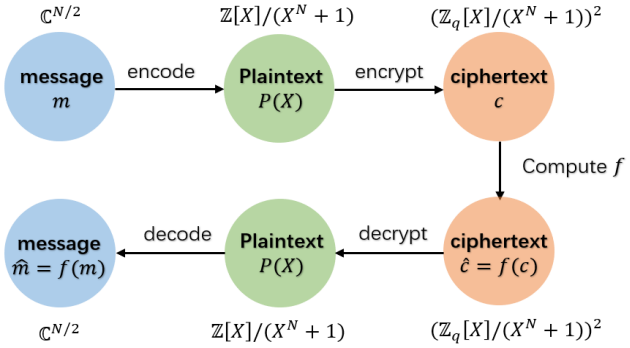

Fig. 5. Overview of CKKS

The entire authentication process consists of three steps: Encryption, Classification, and Adaptive Update. In the encryption step, the PPG features extracted from the user's PPG signals are encrypted using the CKKS scheme [33] which is an effective homomorphic encryption (HE) method. Figure 5 illustrates the framework of the CKKS scheme. Here, the N is a power of two, $S = 2N$, $\mathcal{R} = \mathbb{Z}[X]/(X^N+1)$ and $\phi_S(X) = X^N + 1$, which is S-th cyclotomic polynomial of degree N. As shown in Fig. 5, a message $m \in \mathbb{C}^{N/2}$ is first encoded into a plaintext polynomial $p(X) \in \mathcal{R}$. Next, the plaintext $p(X)$ is further encrypted into a ciphertext c using a public key. Here, the ciphertext c is a couple of polynomials. On this ciphertext, the operations such as addition, multiplication, and rotation can be performed directly. Since the HE method can achieve authentication on the ciphertext without decryption, the calculation results can also be stored in an encrypted form. Furthermore, in the proposed PPG-based biometric system, the key generation and encryption are performed locally by the user, and then the encrypted features are sent to the server. In this case, the adversary or even the server cannot compromise the user's real PPG biometric features.

Next, a Random Forest Classifier is performed on the server side to complete the authentication process. In the Random Forest (RF) classifier, the classifier is trained on plaintext features and does not support the authentication of ciphertext, so it needs to be modified to achieve the direct evaluation of ciphertext. In our design, Homomorphic Random Forest (HRF) [34] is chosen since it achieves inference and prediction results on cryptographic data by introducing DNNs

modeling [35] and homomorphism. Algorithm 2 illustrates the procedure of homomorphic random forest evaluation. In this algorithm, the homomorphic random forest is composed of trees $(T(l) = (\tau(l), t(l), V(l), b(l), W(l), \beta(l)))$ with input $x \in X$ and a polynomial activation function $P \in R[X]$. In addition, Homomorphic random forests can realize fast homomorphic evaluation using a Single Instruction Multiple Data (SIMD) manner. Therefore, our proposed PPG-based system achieves secure and efficient authentication by using the homomorphic random forest and CKKS scheme.

Algorithm 2 Homomorphic Random Forest Evaluation

INPUT: $(\tau(l), t(l), V(l), b(l), W(l), \beta(l)), x \in X, P \in \mathbb{R}[X]$

Client:

1. The client will prepare the data before sending it to the server. The input of each tree is replicated, for $l = 1, \cdots, L$

$$\tilde{x}^{(C)} \leftarrow (x_\tau|0|x_\tau) \in \mathbb{R}^{2K-1}$$

2. All inputs are concatenated

$$\tilde{x} \leftarrow (\tilde{x}^{(1)}|...|\tilde{x}^{(L)})|0, \cdots, 0) \in \mathbb{R}^{N/2}$$

3. After preprocessing the client encrypts the data

$$\tilde{x} \leftarrow Encrypt(\tilde{x})$$

Server:

4. Thresholds are prepared similarly to the inputs, bias needs only to be padded. For $l = 1, \cdots, L$

$$\tilde{t}^{(l)} \leftarrow (t_\tau|0|t_\tau)$$
$$\tilde{b}^{(l)} \leftarrow (b_\tau|0, \cdots, 0)$$

5. Perform the comparisons

$$\tilde{t} \leftarrow (\tilde{t}^{(1)}| \cdots |\tilde{t}^{(L)}|0, \cdots, 0)$$
$$\tilde{b} \leftarrow (\tilde{b}^{(1)}| \cdots |\tilde{b}^{(L)}|0, \cdots, 0)$$
$$u \leftarrow P(\tilde{x} - \tilde{t})$$
$$v \leftarrow P(PackedMatrixMultiplication(W_1^{(1)}, \cdots, W_1^{(L)}) + \tilde{b})$$

6. Compute leaf scores in parallel, for $c = 1, \cdots, C$

$$\tilde{W}_c^{(l)} \leftarrow (\alpha_l|0, \cdots, 0) \quad \text{for } l = 1, \cdots, L$$
$$\tilde{W}_c \leftarrow (\tilde{W}_c^{(1)}| \cdots |\tilde{W}_c^{(L)}|0, \cdots, 0)$$
$$\beta_c \leftarrow \sum_{l=1}^{L} \alpha_l \beta_c^{(l)}$$

7. Compute the score of each class

$$\hat{y} \leftarrow DotProduct(\tilde{W}_c + \beta_c)$$

OUTPUT: $\hat{y} \in \mathbb{R}^C$

Finally, the adaptive update mechanism is designed to reduce the impact on authentication accuracy caused by changes in the PPG signals over time. Specifically, after several successful rounds of authentication, the authenticated PPG signals are added to the training set, and the new classifier is retrained so that the authentication model can continuously evolve to achieve continuous authentication.

D. Security Analysis

As shown in Figure 6, an adversary can launch various attacks to obtain the user's PPG biometric information through insecure communication channels, compromised servers, or lost local devices such as a smartwatch. To solve the above problems, instead of directly using the extracted PPG features as training and testing data, we adopt encrypted PPG features to make the biometric system meet the principle of biometric security [36].

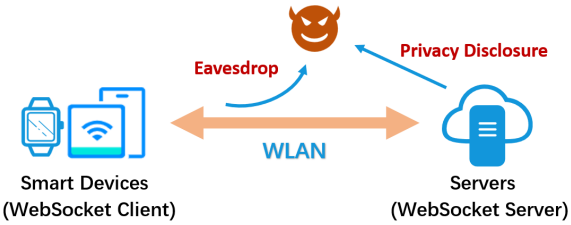

Fig. 6. Possible security threats in practical authentication scenarios

Biometric protection: Biometrics, especially PPG signals, inherently carry some private information. For instance, health status can be inferred from cardiac movement. This means that an adversary can obtain the user's private information by compromising the biometric. Therefore, when using biometric as an input for authentication, the biometric protection should be considered to avoid privacy leakage.

To achieve the biometric protection, the CKKS scheme is employed to encrypt the extracted PPG features in our design. According to the security of homomorphic encryption, the ciphertext generated in our biometric system does not reveal any information. Therefore, even if the adversary obtains the encrypted features through the communication channel, he cannot obtain the real PPG biometric features of the user. Similarly, the server cannot compromise the user's real PPG biometrics from the encrypted biometric features. In addition, since the key is always kept locally and does not need to be distributed or sent, the security of the key is guaranteed. From the above analysis, our proposed biometric system achieves the biometric protection during the authentication process.

Cancellable: When a biometric is compromised, an adversary can successfully pass the authentication by launching a replay attack. Unlike passwords, which can be changed or reset, biometrics are permanently linked to the user and cannot be revoked or replaced. If lost or compromised, the biometrics cannot be used again for authentication. Therefore, a secure biometric system needs to satisfy cancelability, i.e., the biometric template used for authentication can be replaced.

In our proposed PPG-based biometric system, cancellability is achieved by key updates. In our design, once the PPG biometric features are compromised, new encrypted PPG features will be generated by re-initializing and replacing the key locally. According to the property of homomorphic encryption [37], the ciphertext generated using an updated key is completely different from that of the previous ciphertext encrypted with the old key. Therefore, our proposed PPG-based biometric system provides the cancellable property by updating the key used in homomorphic encryption.

Unlinkable: In biometric systems, if there is a linkage between the multiple biometric templates generated, it is possible for an adversary to derive new templates or perform cross-matching attacks across multiple databases. Furthermore, the adversary may be able to determine whether multiple transformed instances come from the same biometric

signal. Obviously, the unlinkable property should be provided to prevent the adversary from inferring the new biometric from the replaced one.

In our proposed PPG-based biometric system, when an encrypted PPG biometric feature is compromised, a new one will be generated to replace the compromised one. According to the security of homomorphic encryption, there is no association between the encrypted PPG biometric features generated by different keys, so the new encrypted PPG biometric features cannot be inferred from the old ones. Therefore, our proposed PPG-based biometric system achieves unlinkability.

V. Evaluation And Discussion

This section describes the experimental setup, the database, and the metrics. Furthermore, our proposed PPG-based biometric is compared with five other related PPG-based biometric systems [7], [21], [23], [24], [38].

A. Experimental Setup

The evaluation experiments were conducted on a 64-bit Windows OS laptop with a 1.60GHz Intel(R) Core(TM) i5-8250U CPU and 16GB RAM, using Python 3.7.3. The simulation of Homomorphic encryption is completed under Python Tenseal library [39].

B. Databases

To evaluate our proposed PPG-based biometric system, five databases were adopted including four publicly available databases (PRRB [40], MIMIC [41], [42], BIDMC [43], [44], Oxford University Fingertip Video Signal [27]) and one of our own collections. Table I briefly introduces the information about these databases. Notably, these databases include various PPG signals collected by different acquisition methods and sampling rates, thus providing more types of PPG signals to evaluate the availability of the proposed PPG-based biometric system.

TABLE I
INTRODUCTION TO THE FIVE DATABASES USED IN OUR EXPERIMENTS

Dataset	Subjects	Sampling Rate	Collection Method
PRRB	42	300 Hz	Anesthesia
MIMIC	50	125 Hz	Bedside Monitors
BIDMC	53	125 Hz	Bedside Monitors
Oxford	15	500 Hz	Smartphone Camera Reflection
Ours	10	30 Hz	Computer Camera Remote Capture

In our experiments, the rPPG toolbox [45] is employed to acquire remote PPG signals from the faces of 10 individuals(including 5 males and 5 females) via a regular camera on a laptop, and these remote PPG signals constitute our dataset. The PPG signals collected in Oxford dataset were acquired from body parts at the fingertips. While the PPG signals of the MIMIC dataset and BIDMC dataset were collected in the ICU via a bedside monitor. The PRRB dataset includes 29 children and 13 adults, and the PPG signals were recorded during their surgery and anesthesia.

C. Metrics

Accuracy: the percentage of correct predicted results to the total sample. It reflects the correctness of the biometric system.

F1 score = $2 \cdot precision \cdot recall / (precision + recall)$. This parameter considers both precision and recall rate and reflects the general authentictaion accuracy of biometric system.

Receiver Operating Characteristic (ROC) Curve: This curve represents the balance of True Postive Rate (TPR) and False Positive Rate (FPR). The smallest distance from the poin to the top-left corner of the ROC curve corresponds to the best authentication accuracy.

Equal Error Rate (EER): This parameter can be obtained from the ROC curve when the True Positive Rate (TPR) is equal to the False Positive Rate (FPR). It reflects the robustness against false predicitions.

D. Performance

Table II presents the accuracy and F1 score of our scheme for the five PPG datasets mentioned above. As shown in Table II, our proposed biometric system achieved 100% accuracy and F1 score on PRRB. For MIMIC, the accuracy and F1 score were 92.5% and 92.3%, respectively. For BIDMC, the accuracy and F1 score were reported as 97.2% and 97.2%, while for Oxford, the accuracy and F1 score were 96.7% and 96.4%, respectively. Last, our proposed system obtained a 95.6% accuracy and a 95.3% F1 score on our own PPG dataset. According to the experimental results, our proposed biometric system achieved 100% accurate authentication on PRRB, and the accuracy and F1 score on BIDMC and Oxford datasets were also satisfactory. Furthermore, for MIMIC, the authentication performance was limited due to the data scale but also acceptable. Last but not least, our proposed biometric system also exhibited high robustness on our own dataset, where the rPPG is used for authentication for the first time. In summary, our proposed PPG-based biometric system achieves high authentication accuracy for different PPG datasets.

TABLE II
AUTHENTICATION ACCURACY AND F1 SCORE OF THE PROPOSED PPG-BASED BIOMETRIC SYSTEM

Dataset	Accuracy	F1 score
PRRB	100%	100%
MIMIC	92.5%	92.3%
BIDMC	97.2%	97.2%
Oxford	96.7%	96.4%
Ours	95.6%	95.3%

We also evaluate the EER of our biometric system. Figure 7 shows the ROC curve and the corresponding EER for five different datasets mentioned above. From Figure 7, the EER obtained on PPRB, MIMC, BIDMC, the Oxford dataset, and our own dataset were 0%, 4.2%, 2.5%, 1.2%, and 2.8%, respectively. According to the experimental results, our proposed PPG-based biometric system achieves zero error on PPRB, and exhibits high robustness against false predicitions on all five datasets.

To explore the effects of dataset size in our proposed biometric system, we further compared the learning curve for the

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2023.3285796

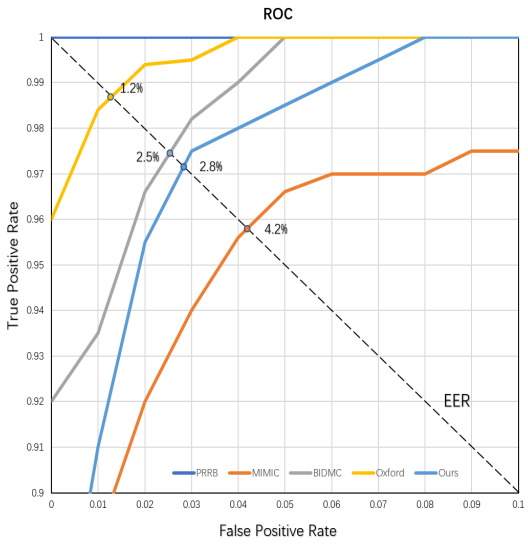

Fig. 7. ROC curve and the corresponding EER for five different datasets

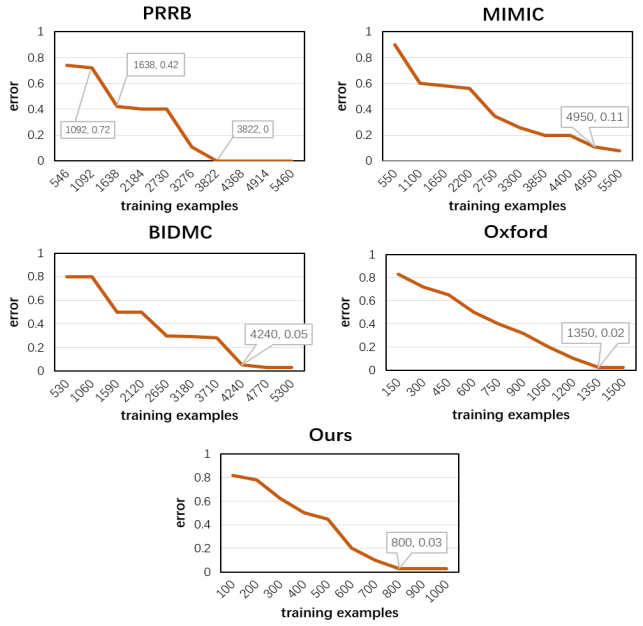

Fig. 8. the learning curve for five datasets

above five datasets as the training scale changes. The learning curve is the correlation between a learner's performance on a task and the number of attempts or time required to complete that task. Its vertical axis represents the error rate, which refers to a measure of the degree of error in a model's prediction of the true model. As shown in Figure 8, for PRRB, the error rate was around 70% when the sample number is below 1092, and then it decreases to 42% when the sample number is 1638. After the sample number increases to 2730, the error rate on PRRB starts to decrease and drops to 0% when the sample number reaches 3622. Similar to PRRB, the error rate of MIMIC and BIDMC also decreases in steps. For MIMIC, the error rate was below 11% when the sample number is over 4950, and for BIDMC, the error rate drops to 5% with 4240 samples involved. Meanwhile, the error rate decreases steadily on the Oxford dataset and ours. For the Oxford dataset, a 2% error rate is achieved when the sample number is bigger than 1350, while a relatively low error rate (3%) was reached after 800 for our dataset. To sum up, the training scale affects the error rate of our proposed PPG-based biometric system. When the sample number increases, the error rate decreases until it has reached the local minimum. In our experience, a relatively appropriate amount of training is for a person to have at least 100 heartbeats, which is about a 1 to 2 minute signal.

E. Time Duration

To evaluate the time efficiency of our proposed PPG-based biometric system, we conducted experiments on the time overhead of each step. An important factor affecting the running time is the signal quality; if the signal quality is poor, it will take more time to filter to get a sufficient number of beats. In addition, the key initialization and encryption steps are the most time-consuming part of the authentication. Table III shows the average authentication time overhead for a single beat.

From the table III, we can see that the time for both signal processing and feature extraction is the shortest for PRRB. In addition, the authentication process is the most time-consuming, and the key generation time is around 2.5 seconds. For all the five datasets, there is almost no difference in the authentication time, all around 3 seconds.

TABLE III
COMPARISON OF THE TIME OVERHEAD OF A SINGLE PPG BEAT OVER THREE STEPS IN DIFFERENT DATASETS

Dataset	Signal Process	Feature Extraction	Authentication
PRRB	0.008s	0.006s	2.973s
MIMIC	0.022s	0.009s	2.997s
BIDMC	0.015s	0.008s	2.911s
Oxford	0.017s	0.008s	3.017s
Ours	0.021s	0.007s	2.980s

TABLE IV
COMPARISON OF TIME SPENT USING RF AND HRF

Dateset	RF	HRF
PRRB	0.026s	0.039s
MIMIC	0.028s	0.040s
BIDMC	0.026s	0.039s
Oxford	0.027s	0.039s
Ours	0.028s	0.039s

We further compared the classification time of ordinary random forest (RF) and homomorphic random forest(HRF). As shown in Table IV, HRF takes slightly more time compared to RF due to the evaluation of the ciphertext, but the difference is not significant, only about 0.01s. According to our experimental results, the time consumption using HRF is mainly in the initialization of the key and encryption steps. Moreover, our

TABLE V
COMPARISON WITH STATE-OF-THE-ART SOLUTIONS IN TERMS OF ACCURACY, ROBUSTNESS, AND SECURITY

Method	Subject	Accuracy	F1 score	EER	Collection	Security
[7]	42	100%	*	0.1%	PRRB dataset	*
[21]	20	90%	*	*	wrist wearable device	*
[23]	42	100%	*	0.1%	PRRB dataset	*
[24]	7	*	95.3%	*	wrist wearable device	✓
[38]	56	100%	*	0.1%	professional equipment	*
Ours	170	96.4%	96.1%	2.14%	Five datasets	✓

proposed biometric system has excellent efficiency in signal processing, feature extraction, and classification. In practical applications, keys do not change frequently, and in this case, the average time required to authenticate a beat is within 0.5s, which is an acceptable time.

F. Comparative Analysis

In this subsection, we compared our proposed PPG-based biometric system with other five related PPG-based biometric systems [7], [21], [23], [24], [38] in terms of accuracy, F1 scores, and EER. We also discussed and analyzed our method and the methods of their solution.

Two PPG-based biometric systems proposed by Hwang et al. [7], [23] were tested on the PRRB dataset, one system achieved 100% single-session accuracy with an EER of 0.1%, and the other had similar results. Since both systems are based on convolutional neural networks, a long training time is required. Furthermore, neither of these two biometric systems considers the security of the PPG signals during the authentication process. Compared with these two PPG-based biometric systems [7], [23], our system provides biometric protection while achieving their authentication accuracy.

In the authentication approach presented by Zhao et al. [21], the user pulse signals acquired by PPG sensors in commercial wrist wearable devices were adopted to perform continuous authentication. Their authentication scheme achieves more than 90% accuracy in a scenario with 20 participants using general fiducial point features. Although their scheme contributes to Motion Artifact(MA) rejection, the protection of biometric features is not considered. Compared with Zhao et al.'s scheme [21], our proposed biometric system extracts more comprehensive features from PPG signals and provides biometric protection.

Cao et al. [24] proposed a new mobile two-factor authentication system using PPG signals collected by a wrist wearable device. In their design, the cancellable property was considered to provide biometric template protection. However, only seven individuals are involved in their experiments and the average F1 score is 95.3% due to the usage of random forests. Compared to their method, our proposed PPG-based biometric system achieves a higher F1 score of 96.4%, and more subjects are adopted in our experiments, which reflects higher stability and usability of authentication. In addition, in their design, the real PPG features were projected to generate cancelable feature templates by finding suitable transformation functions. In this case, the accuracy of authentication is highly dependent on the reliability of the transformation functions. But how to obtain and evaluate the transformation function is a difficult task.

In Sancho et al.'s biometric scheme [38], the experiments were performed on MIMIC database and obtained an EER of 8% on 56 subjects. In their design, the matching is done by comparing the Manhattan distance and the Euclidean distance between the input and the stored template. If the results are within a predetermined threshold value, the authentication passes. Compared to their scheme [38], our proposed PPG-based biometric system achieves a lower EER with biometric protection.

As summarized in Table III, our proposed PPG-based biometric system achieves satisfactory results on five different datasets, with an accuracy of 96.4%, F1 score of 96.1%, and EER of 2.14%. In addition, the homomorphic encryption method is used in our design to ensure the security of biometric features and protect the privacy of users. Compared with other five related solutions, our proposed system fully considers the security requirements of biometric system while improving the authentication accuracy, and then supports more application scenarios.

The PPG signal is changed by mood, movement, or other human activities. In addition, PPG sensors on wearable devices can also change the PPG signals due to factors such as friction, and signals acquired by rPPG technology under different lighting conditions and at different ages face the same problem. This paper focuses on how to design a secure and efficient PPG-based authentication scheme, and the above issues will be fully considered in the future work to further improve the robustness of the authentication.

VI. CONCLUSION

This paper presented a biometric system whose implementation is based on homomorphic random forests. The system is designed to support continuous PPG authentication with biometric protection through adaptive updating of classification models. In our design, PCA and mRMR are employed to realize the accurate extraction of unique human biometrics from PPG signals, and a beat quality screening step is designed to improve the accuracy of authentication. Furthermore, a

homomorphic random forest model is employed in our biometric system to evaluate the encrypted features, thus providing biometric protection during the authentication process. The security analysis demonstrated that the proposed PPG-based biometric system achieves irreversibility, cancelability, and unlinkability – key properties in a biometric system. Compared with other related works, our proposed biometric system achieves high accuracy of authentication with biometric protection and can be implemented in a wider range of application scenarios (e.g., remote PPG authentication using a common consumer-grade camera).

ACKNOWLEDGMENT

The research was financially supported by the National Natural Science Foundation of China (No. 62172303), the Open Research Project of the Hubei Key Laboratory of Intelligent GeoInformation Processing (No. KLIGIP-2019B09), the Knowledge Innovation Program of Wuhan - Basic Research (No. 2022010801010197), the Opening Project of Nanchang Innovation Institute, Peking University (No. NCII2022A02), and the Foundation of Anhui Engineering Research Center for Intelligent Applications and Security of Industrial Internet (IASII22-02). K.-K. R. Choo was supported only by the Cloud Technology Endowed Professorship.

REFERENCES

[1] Wencheng Yang, Song Wang, Nor Masri Sahri, Nickson M Karie, Mohiuddin Ahmed, and Craig Valli. Biometrics for internet-of-things security: A review. *Sensors*, 21(18):6163, 2021.

[2] Jianze Wei, Huaibo Huang, Yunlong Wang, Ran He, and Zhenan Sun. Towards more discriminative and robust iris recognition by learning uncertain factors. *IEEE Transactions on Information Forensics and Security*, 17:865–879, 2022.

[3] Jian Zhao, Shuicheng Yan, and Jiashi Feng. Towards age-invariant face recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2020.

[4] Ajay Kumar and Yingbo Zhou. Human identification using finger images. *IEEE Transactions on image processing*, 21(4):2228–2244, 2011.

[5] Shuping Zhao and Bob Zhang. Joint constrained least-square regression with deep convolutional feature for palmprint recognition. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 52(1):511–522, 2020.

[6] Muhammad Shahzad and Munindar P Singh. Continuous authentication and authorization for the internet of things. *IEEE Internet Computing*, 21(2):86–90, 2017.

[7] Dae Yon Hwang, Bilal Taha, Da Saem Lee, and Dimitrios Hatzinakos. Evaluation of the time stability and uniqueness in ppg-based biometric system. *IEEE Transactions on Information Forensics and Security*, 16:116–130, 2020.

[8] Mohamed and Elgendi. On the analysis of fingertip photoplethysmogram signals. *Current cardiology reviews*, 2012.

[9] Sukgyu Koh, Bo Ram Cho, Jong-il Lee, Soon-O Kwon, Suwoong Lee, Joon Beom Lim, Soo Beom Lee, and Hyeok-Dong Kweon. Driver drowsiness detection via ppg biosignals by using multimodal head support. In *2017 4th International Conference on Control, Decision and Information Technologies (CoDIT)*, pages 0383–0388, 2017.

[10] Wenjin Wang, Albertus C. den Brinker, Sander Stuijk, and Gerard de Haan. Algorithmic principles of remote ppg. *IEEE TRANSACTIONS ON BIOMEDICAL ENGINEERING*, 64(7):1479–1491, JUL 2017.

[11] Denisse Castaneda, Aibhlin Esparza, Mohammad Ghamari, Cinna Soltanpur, and Homer Nazeran. A review on wearable photoplethysmography sensors and their potential future applications in health care. *International journal of biosensors & bioelectronics*, 4(4):195, 2018.

[12] Emanuele Maiorana, Chiara Romano, Emiliano Schena, and Carlo Massaroni. Biowish: Biometric recognition using wearable inertial sensors detecting heart activity. *IEEE Transactions on Dependable and Secure Computing*, 2023.

[13] Xinyan Zhou, Jiaqi Pan, Zenan Zhang, Xiaoyu Ji, and Haiming Chen. Gesture-related two-factor authentication for wearable devices via ppg sensors. *IEEE Sensors Journal*, 2023.

[14] Arpita Sarkar and Binod K. Singh. A review on performance,security and various biometric template protection schemes for biometric authentication systems. *MULTIMEDIA TOOLS AND APPLICATIONS*, 79(37-38):27721–27776, OCT 2020.

[15] Angelo Bonissi, Ruggero Donida Labati, Luca Perico, Roberto Sassi, Fabio Scotti, and Luca Sparagino. A preliminary study on continuous authentication methods for photoplethysmographic biometrics. In *2013 IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications*, pages 28–33. IEEE, 2013.

[16] Petros Spachos, Jiexin Gao, and Dimitrios Hatzinakos. Feasibility study of photoplethysmographic signals for biometric identification. In *2011 17th international conference on digital signal processing (DSP)*, pages 1–5. IEEE, 2011.

[17] Umang Yadav, Sherif N Abbas, and Dimitrios Hatzinakos. Evaluation of ppg biometrics for authentication in different states. In *2018 International Conference on Biometrics (ICB)*, pages 277–282. IEEE, 2018.

[18] Chunying Liu, Jijiang Yu, Yuwen Huang, and Fuxian Huang. Time–frequency fusion learning for photoplethysmography biometric recognition. *IET Biometrics*, 11(3):187–198, 2022.

[19] Farnaz Farid, Mahmoud Elkhodr, Fariza Sabrina, Farhad Ahamed, and Ergun Gide. A smart biometric identity management framework for personalised iot and cloud computing-based healthcare services. *Sensors*, 21(2):552, 2021.

[20] Guannan Wu, Jian Wang, Yongrong Zhang, and Shuai Jiang. A continuous identity authentication scheme based on physiological and behavioral characteristics. *Sensors*, 18(1):179, 2018.

[21] Tianming Zhao, Yan Wang, Jian Liu, Jerry Cheng, Yingying Chen, and Jiadi Yu. Robust continuous authentication using cardiac biometrics from wrist-worn wearables. *IEEE Internet of Things Journal*, 2021.

[22] Nima Karimian, Mark Tehranipoor, and Domenic Forte. Non-fiducial ppg-based authentication for healthcare application. In *2017 IEEE EMBS international conference on biomedical & health informatics (BHI)*, pages 429–432. IEEE, 2017.

[23] Dae Yon Hwang, Bilal Taha, and Dimitrios Hatzinakos. Variation-stable fusion for ppg-based biometric system. In *ICASSP 2021-2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 8042–8046. IEEE, 2021.

[24] Yetong Cao, Qian Zhang, Fan Li, Song Yang, and Yu Wang. Ppgpass: Nonintrusive and secure mobile two-factor authentication via wearables. In *IEEE INFOCOM 2020-IEEE Conference on Computer Communications*, pages 1917–1926. IEEE, 2020.

[25] Limeng Pu, Pedro J Chacon, Hsiao-Chun Wu, and Jin-Woo Choi. Novel robust photoplethysmogram-based authentication. *IEEE Sensors Journal*, 22(5):4675–4686, 2022.

[26] F. Nakayama, P. Lenz, S. Banou, M. Nogueira, and K. R. Chowdhury. A continuous user authentication system based on galvanic coupling communication for s-health. *Wireless Communications and Mobile Computing*, 2019(7):1–11, 2019.

[27] Giulio Lovisotto, Henry Turner, Simon Eberz, and Ivan Martinovic. Seeing red: Ppg biometrics using smartphone cameras. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops*, pages 818–819, 2020.

[28] T. Chatterjee, A. Ghosh, and S. Sarkar. Signal quality assessment of photoplethysmogram signals using quantum pattern recognition and lightweight cnn architecture. 2022.

[29] Meinard Müller. Dynamic time warping. *Information retrieval for music and motion*, pages 69–84, 2007.

[30] Michael E Tipping and Christopher M Bishop. Probabilistic principal component analysis. *Journal of the Royal Statistical Society: Series B (Statistical Methodology)*, 61(3):611–622, 1999.

[31] Hanchuan Peng, Fuhui Long, and Chris Ding. Feature selection based on mutual information criteria of max-dependency, max-relevance, and min-redundancy. *IEEE Transactions on pattern analysis and machine intelligence*, 27(8):1226–1238, 2005.

[32] Brian C Ross. Mutual information between discrete and continuous data sets. *PloS one*, 9(2):e87357, 2014.

[33] Jung Hee Cheon, Andrey Kim, Miran Kim, and Yongsoo Song. Homomorphic encryption for arithmetic of approximate numbers. In *International conference on the theory and application of cryptology and information security*, pages 409–437. Springer, 2017.

[34] Daniel Huynh. Cryptotree: fast and accurate predictions on encrypted structured data. *arXiv preprint arXiv:2006.08299*, 2020.

[35] Gérard Biau, Erwan Scornet, and Johannes Welbl. Neural random forests. *arXiv preprint arXiv:1604.07143*, 2016.
[36] Vishal M Patel, Nalini K Ratha, and Rama Chellappa. Cancelable biometrics: A review. *IEEE Signal Process. Mag.*, 32(5):54–65, 2015.
[37] Abbas Acar, Hidayet Aksu, A. Selcuk Uluagac, and Mauro Conti. A survey on homomorphic encryption schemes: Theory and implementation. *ACM COMPUTING SURVEYS*, 51(4), SEP 2018.
[38] Jorge Sancho, Álvaro Alesanco, and José García. Biometric authentication using the ppg: a long-term feasibility study. *Sensors*, 18(5):1525, 2018.
[39] Ayoub Benaissa, Bilal Retiat, Bogdan Cebere, and Alaa Eddine Belfedhal. Tenseal: A library for encrypted tensor operations using homomorphic encryption, 2021.
[40] Walter Karlen, M Turner, Erin Cooke, Guy Dumont, and J Mark Ansermino. Capnobase: Signal database and tools to collect, share and annotate respiratory signals. In *2010 Annual meeting of the society for technology in anesthesia*, page 27. Society for Technology in Anesthesia, 2010.
[41] Alistair EW Johnson, Tom J Pollard, Lu Shen, Li-wei H Lehman, Mengling Feng, Mohammad Ghassemi, Benjamin Moody, Peter Szolovits, Leo Anthony Celi, and Roger G Mark. Mimic-iii, a freely accessible critical care database. *Scientific data*, 3(1):1–9, 2016.
[42] B Moody, G Moody, M Villarroel, G Clifford, and I Silva III. Mimic-iii waveform database (version 1.0). *PhysioNet*, 2020.
[43] Marco AF Pimentel, Alistair EW Johnson, Peter H Charlton, Drew Birrenkott, Peter J Watkinson, Lionel Tarassenko, and David A Clifton. Toward a robust estimation of respiratory rate from pulse oximeters. *IEEE Transactions on Biomedical Engineering*, 64(8):1914–1923, 2016.
[44] Ary L Goldberger, Luis AN Amaral, Leon Glass, Jeffrey M Hausdorff, Plamen Ch Ivanov, Roger G Mark, Joseph E Mietus, George B Moody, Chung-Kang Peng, and H Eugene Stanley. Physiobank, physiotoolkit, and physionet: components of a new research resource for complex physiologic signals. *circulation*, 101(23):e215–e220, 2000.
[45] Daniele Di Lernia, Gianluca Finotti, Manos Tsakiris, Giuseppe Riva, and Marnix Naber. Remote photoplethysmography (rppg) in the wild: Remote heart rate imaging via online webcams. 2022.

Liping Zhang received the Ph.D. degree in information security from Huazhong University of Science and Technology, Wuhan, China, in 2009.

She is Associate Professor of Information and Network Security at China University of Geosciences, Wuhan. Her research interests include network security, key management and distribution, and privacy protection. Dr. Zhang has published over 30 research papers, most of which are refereed international journal papers including IEEE/ACM/IET journal papers.

Dr. Zhang is the principal grant holder of three externally funded research projects.

Anzi Li received the BSc degree in information security from China University of Geosciences in 2021 .He is currently a postgraduate researchstudentininformation securityat ChinaUniversityof Geosciences. Hisresearchinterests include ECG, PPG authentication, communicationssecurityandbiological privacy protection.

Shukai Chen received the BSc degree in network engineering from PLA Army Engineering University in 2020. He is currently a postgraduate research student in electronic engineering (computer science) at China University of Geosciences. His research interests include ECG authentication, communications security and network security.

Wei Ren (Member, IEEE) received the Ph.D. degree in computer science from Huazhong University of Science and Technology, Wuhan, China.

He is currently a Full Professor with the School of Computer Science, China University of Geosciences, Wuhan, China. He was with the Department of Electrical and Computer Engineering, Illinois Institute of Technology, Chicago, IL, USA, in 2007 and 2008, the School of Computer Science University of Nevada Las Vegas, Las Vegas, NV, USA, in 2006 and 2007, and the Department of Computer Science, The Hong Kong University of Science and Technology, Hong Kong, in 2004 and 2005. He has published over 100 refereed papers, one monograph, and four textbooks.

Prof. Ren has obtained ten patents and five innovation awards. He is a Distinguished Member of the China Computer Federation.

Kim-Kwang Raymond Choo (Senior Member, IEEE) received the Ph.D. degree in information security from Queensland University of Technology, Brisbane, QLD, Australia, in 2006.

He currently holds the Cloud Technology Endowed Professorship with The University of Texas at San Antonio (UTSA), San Antonio, TX, USA. He also has a courtesy appointment with the University of South Australia, Adelaide, SA, Australia.