sensors

MDPI

Article

An Approach to Biometric Verification Based on Human Body Communication in Wearable Devices

Jingzhen Li, Yuhang Liu, Zedong Nie *, Wenjian Qin, Zengyao Pang and Lei Wang

Shenzhen Institutes of Advanced Technology, Chinese Academy of Science, Shenzhen 518055, China; lijz@siat.ac.cn (J.L.); yh.liu2@siat.ac.cn (Y.L.); wj.qin@siat.ac.cn (W.Q.); dl.yang@siat.ac.cn (Z.P.); wang.lei@siat.ac.cn (L.W.)

* Correspondence: zd.nie@siat.ac.cn; Tel.: +86-755-8639-2295; Fax: +86-755-8639-2299

Academic Editors: Giancarlo Fortino, Hassan Ghasemzadeh, Wenfeng Li, Yin Zhang and Luca Benini
Received: 13 October 2016; Accepted: 4 January 2017; Published: 10 January 2017

Abstract: In this paper, an approach to biometric verification based on human body communication (HBC) is presented for wearable devices. For this purpose, the transmission gain S21 of volunteer's forearm is measured by vector network analyzer (VNA). Specifically, in order to determine the chosen frequency for biometric verification, 1800 groups of data are acquired from 10 volunteers in the frequency range 0.3 MHz to 1500 MHz, and each group includes 1601 sample data. In addition, to achieve the rapid verification, 30 groups of data for each volunteer are acquired at the chosen frequency, and each group contains only 21 sample data. Furthermore, a threshold-adaptive template matching (TATM) algorithm based on weighted Euclidean distance is proposed for rapid verification in this work. The results indicate that the chosen frequency for biometric verification is from 650 MHz to 750 MHz. The false acceptance rate (FAR) and false rejection rate (FRR) based on TATM are approximately 5.79% and 6.74%, respectively. In contrast, the FAR and FRR were 4.17% and 37.5%, 3.37% and 33.33%, and 3.80% and 34.17% using K-nearest neighbor (KNN) classification, support vector machines (SVM), and naive Bayesian method (NBM) classification, respectively. In addition, the running time of TATM is 0.019 s, whereas the running times of KNN, SVM and NBM are 0.310 s, 0.0385 s, and 0.168 s, respectively. Therefore, TATM is suggested to be appropriate for rapid verification use in wearable devices.

Keywords: biometric verification; human body communication; threshold-adaptive template matching; weighted Euclidean distance; transmission gain S21; wearable device

1. Introduction

Body sensor networks (BSNs), which also referred to as body area networks (BANs), are wireless networks for interconnecting wearable nodes/devices centered on an individual person's workspace [1,2]. With the rapid development of microprocessor technologies and wireless communication, BSNs have emerged as a revolutionary technology and have demonstrated great potential in healthcare monitoring (blood pressure monitoring [3], blood glucose monitoring [4], etc.), emotion recognition (negative emotional state of fear [5], etc.), sport performance monitoring [6], physical/virtual social interactions [7], and so on [8–10]. However, because wearable devices usually carry user's personal information, information leakage from wearable devices in BSNs is regarded as a challenge, which may bring about an immeasurable loss [11]. Therefore, the information security of wearable devices should be strictly considered [12].

Biometric verification, which uses the human physiological or behavioral trait to achieve personal verification, is widely used in information security [13,14]. Compared with conventional verifications, such as digital password, personal identification number and IC card, biometric verification has the advantages of being much more difficult to forget, lose, steal, copy or forge [15]. Thus far, biometric

verification using fingerprint, face, iris, vein, voice, electroencephalograph (EEG), electrocardiogram (ECG) and gait, among others, has been an active research topic in recent years [16–19]. Mathur et al. demonstrated the methodology of fingerprint verification in a wearable system [20]. However, the identification performance will be reduced when the finger is moist. Klonovs et al. introduced a mobile biometric verification system utilizing EEG recordings headset [21]. However, the EEG recordings headset is not suitable to wear for a long time. Peter et al. proposed an ECG-based authentication protocol to identify sensor nodes attached to the same human body [22]. Choudhary et al. presented a biometric verification approach based on the photoplethysmographic (PPG) signal for BSNs [23]. Derawi et al. collected the user's gait as biometric trait through a wireless monitor [24]. However, the wireless monitor is so complicated that it is difficult to wear. Kim et al. presented a multimodal verification approach that uses face, teeth and voice modalities as biometric traits for mobile device [25]. However, the power of multimodal verification is too large to be used in wearable devices. Other biometric verifications, such as iris, hand and vein verification, are difficult to integrate into wearable devices due to the limitation of wearable devices' size [26–28]. Therefore, a new approach to biometric verification is necessary in wearable devices [29].

Human body communication (HBC), which uses the human body itself as a transmission medium, provides a potential personal verification solution for wearable devices [30]. Specifically, due to the thickness differences of biological tissues in human body, the transmission gain S21, which reflects the variation of transmission characteristics at different frequencies, are different while the signal is coupled into the human body. Therefore, the transmission gain S21 may be used as a biometric trait to achieve personal verification. This is the theoretical foundation of biometric verification based on HBC. Considering that the location of a specified wearable device is usually fixed (e.g., a wristband is worn on the forearm), the HBC sensor, which is attached to the wearable device, can collect the biometric trait in the fixed location. In other words, the biometric verification based on HBC is readily integrated into different wearable devices. Thus, biometric verification based on HBC may be a promising technology in wearable devices [31].

Thus far, few investigations have characterized the biometric verification based on HBC. Nakanishi et al. presented a verification approach that uses a pseudo white noise as an input signal to acquire human biometric trait [32]. However, the identification performance is low due to the influence of randomness from white noise. Rasmussen et al. proposed a biometric based on the human body's response to an electric square pulse signal, and used the pulse-response biometric as an additional verification mechanism [33]. However, all sample data are used in both learning and verification by the researchers, which may lead to a higher risk of confidence level. The authors of this article also made a preliminary research on biometric verification based on HBC [34]. However, the amount of computation in [34] is so large that it is inappropriate for rapid verification in wearable devices.

In this work, we aim to study the biometric verification based on HBC for wearable devices. The contribution and originality of this paper is summarized as follows. Firstly, the transmission gain S21 is proposed as the biometric trait for different individuals. Secondly, to achieve the rapid verification, a threshold-adaptive template matching (TATM) algorithm based on weighted Euclidean distance is employed. Furthermore, in order to evaluate TATM algorithm, the identification performance of TATM is compared with K-nearest neighbor (KNN) classification [35], support vector machines (SVM) [36], and naive Bayesian method (NBM) classification [37]. The remainder of this paper is organized as follows. In Section 2, we will demonstrate the validity of biometric verification method based on HBC through numerical simulation. In Section 3, the experimental setup will be introduced. Section 4 is about measurement result and analysis. TATM algorithm will be reported in Section 5. Section 6 gives a detailed analysis of identification performance. Finally, the conclusions are drawn in Section 7.

2. Modeling Biometric Verification Based on HBC

2.1. Forearm Modeling

As demonstrated in Figure 1, in order to evaluate the feasibility of biometric verification based on HBC, three different forearm models, namely, Model A, Model B and Model C, are established. These models are abstracted as cylinders. The length and diameter of all models are 300 mm and 56 mm, respectively. Furthermore, each model includes, from outside to inside, skin, fat, muscle, cortical bone and bone marrow [38]. The thicknesses of tissue layers for different models are listed in Table 1. Specifically, the thicknesses of fat and muscle for Model A are 2.30 mm and 17.86 mm, respectively. Compared with Model A, the thickness of fat in Model B is increased, whereas the thickness of muscle is decreased. In addition, the thickness of fat in Model C is 7.60 mm, and the thickness of muscle is about 12.56 mm. Details of simulation setup are as follows. A transmitting electrode and a receiving electrode are attached on the surface of model. A voltage source with an output impedance of 50 Ω is fed to the transmitting electrode. In order to acquire the transmission gain S21 in the frequency range 0.3 MHz to 1500 MHz conveniently, a Gaussian signal, of which the pulse width was 0.25 ns, is adopted in the simulation. In addition, there is a load with impedance of 50 Ω in receiving electrode. The simulations are performed using commercial electromagnetic modeling software XFDTD based on the finite-difference time-domain (FDTD) method.

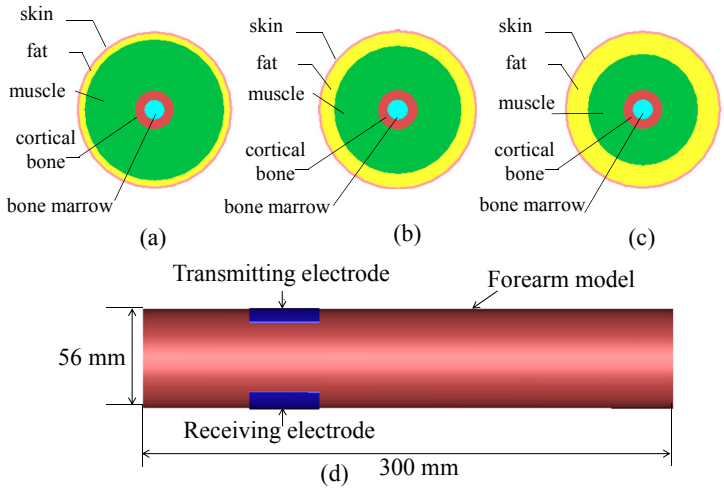

Figure 1. (**a**) The cross-section of Model A; (**b**) the cross-section of Model B; (**c**) the cross-section of Model C; and (**d**) transmitting electrode and receiving electrode.

Table 1. Thicknesses of difference tissue layers (mm).

	Model A	Model B	Model C
Skin	0.84	0.84	0.84
Fat	2.30	4.76	7.60
Muscle	17.86	15.4	12.56
Cortical bone	3.36	3.36	3.36
Bone marrow	3.64	3.64	3.64

2.2. Simulation Result

Figure 2 shows the transmission gain S21 (in dB) of three forearm models. The gains of three forearm models are somewhat different when the frequency is below 200 MHz. The gain of Model A is about −3 dB at 150 MHz, whereas the gain of Model C is −5.3 dB. The gains of all models are similar in the frequency range 200 MHz to 530 MHz. However, the gains are quite different when the frequency is 530 MHz to 750 MHz and 900 MHz to 1500 MHz. For instance, the gain of Model C

is the smallest at 630 MHz, about −28 dB, whereas the gain of Model A is approximately −23 dB at 630 MHz. In addition, the gain of Model C is more than −26.5 dB at 1000 MHz, whereas the gain of Model A is about −30 dB. From Figure 2, it can be revealed that the transmission gain S21 of each forearm model is different, which is related with the thicknesses of tissue layers, as demonstrated in Figure 1. Thus, considering the difference of biological tissues for each individual, the transmission gain S21 is an optional biometric trait to achieve personal verification.

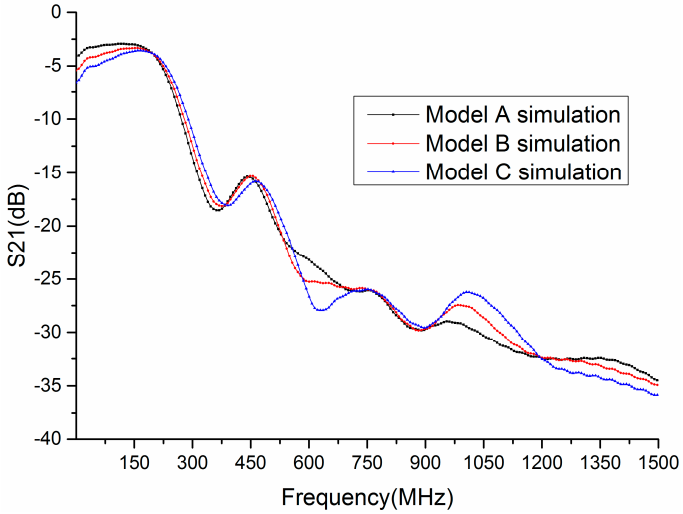

Figure 2. Transmission gain S21 of different models in FDTD simulations.

3. Experimental Setup

3.1. Experimental Equipment

The experimental equipment includes a vector network analyzer (VNA, Agilent E5061A), a transmitting electrode and a receiving electrode. In order to ensure that the electrodes are in close contact with the skin, the electrodes are attached on a plastic clip, as shown in Figure 3a. The VNA is adopted to acquire the transmission gain S21 of volunteer. Figure 3b illustrates the measurement location of volunteer. The transmitting electrode and receiving electrode are placed on the volunteer's forearm. The distance between electrode and wrist is 6 cm. The transmitting electrode is connected to the Port 1 of VNA through cable. Similarly, the receiving electrode is connected to the Port 2 of VNA.

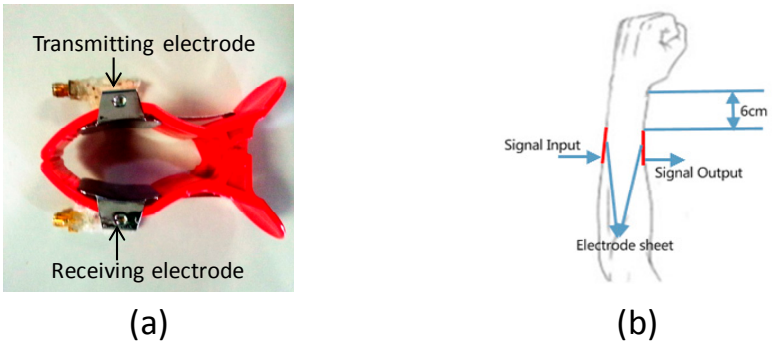

Figure 3. (**a**) Electrodes and plastic clip; and (**b**) measurement location.

3.2. Experimental Setup

In our study, ten volunteers (average age of 24 years) with body weights of 50 kg to 80 kg and body heights of 165 cm to 180 cm were selected. Written informed consent was obtained from all volunteers. Figure 4 shows the experimental scenario. Two experiments were carried out in this work.

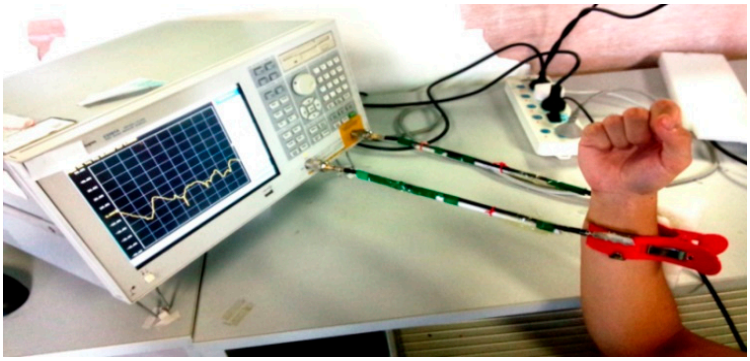

Figure 4. Experimental scenario.

Table 2 lists the detailed setup for Experiments 1 and 2. In Experiment 1, we aimed to find the chosen frequency for biometric verification based on HBC. For this purpose, the transmission gain S21 in the frequency range 0.3 MHz to 1500 MHz was investigated. The measurement was done 60 times (groups) per day for each volunteer and repeated for 3 days. Specifically, the measurement was done 10 times per hour for 6 hours each day. Moreover, 1601 sample data are acquired in each time. Thus, 2,881,800 sample data are acquired in Experiment 1.

According to Experiment 1, it can be known that the chosen frequency for biometric verification is from 650 MHz to 750 MHz. In Experiment 2, we aimed to obtain the sample data used for learning and verification at the chosen frequency. In Experiment 2, the measurement was done 6 times (groups) per day for each volunteer and was repeated for 5 days. Furthermore, 21 sample data are acquired each time. Therefore, 6300 sample data are acquired in Experiment 2.

Table 2. Experimental setup.

	Frequency Bands	Volunteers	Days	Times per Day	Sample Data per Time	Total
Experiment 1	0.3 MHz–1500 MHz	10	3	60	1601	2,881,800
Experiment 2	650 MHz–750 MHz	10	5	6	21	6300

4. Measurement Results and Analysis

4.1. Feasibility of Biometric Verification Based on HBC

Figure 5a depicts the transmission gain S21 (in dB) of five volunteers at the same time. As shown in Figure 5a, it is interesting to observe that there is a significantly difference among five volunteers in the frequency range 500 MHz to 1500 MHz. Moreover, as the frequency increases, the difference is become more discernible. Therefore, it can be inferred that the biometric verification based on HBC is feasible due to the difference of transmission gain S21 between individuals. Figure 5b describes the transmission gain S21 of one volunteer at four different times. It can be observed that the transmission gain S21 is almost the same when the frequency is from 0.3 MHz to 1000 MHz, which means that the transmission gain S21 of the same individual is steady over a period of time.

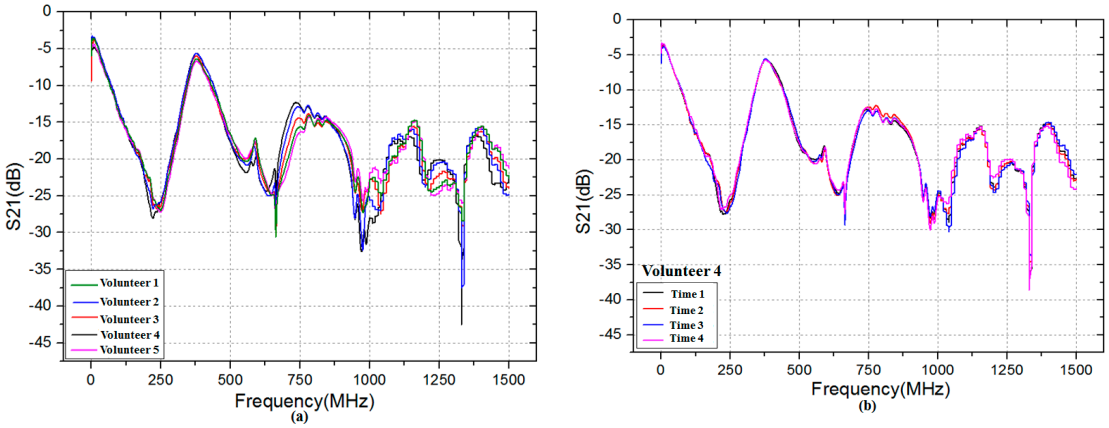

Figure 5. Transmission gain S21 in the frequency range 0.3 MHz to 1500 MHz: (**a**) five volunteers at the same time; and (**b**) Volunteer 4 at four different times.

4.2. Chosen Frequency for Biometric Verification

In order to decrease the number of sample data, it is critical to determine the HBC frequency for biometric verification, which is of great benefit to achieve rapid verification in wearable devices. For this purpose, the standard deviation of transmission gain S21 for ten volunteers in the frequency range 0.3 MHz to 1500 MHz is investigated in this section. In addition, the standard deviation of transmission gain S21 for one volunteer at nine different times is also studied. The standard deviation calculation is shown as Equation (1).

$$s_i = \left(\frac{\sum_{i=1}^{n} (x_i - \overline{x})^2}{n-1} \right)^{\frac{1}{2}} \quad (1)$$

where s_i is the standard deviation, x_i is the value of i-th sample data, $\overline{x}$ is the average value of sample data, and n is the sample times; n is 10 in the former calculation and n is 9 in the latter calculation.

Figure 6 illustrates the standard deviation of transmission gain S21 when the frequency is 0.3 MHz to 1500 MHz. The black curve represents the standard deviation among ten volunteers, and the red curve shows the standard deviation of a volunteer at nine different times. As demonstrated in Figure 6, the standard deviation among ten volunteers is equal to or less than 0.9 when the frequency is below 600 MHz. However, the standard deviation is greater than 1.3 when the frequency is 650 MHz to 750 MHz and 950 MHz to 1050 MHz. furthermore, the standard deviation is up to 2.1 at 700 MHz. Thus, it is indicated that there is a distinguishable difference among volunteers in aforementioned frequency range. On the other hand, the standard deviation of a volunteer (Volunteer 4) at nine different times is less than 0.6 in the frequency range 290 MHz to 950 MHz. As the frequency increases, the standard deviation is become larger. Thus, it can be deduced that the chosen frequency for biometric verification based on HBC should be from 650 MHz to 750 MHz, in which the standard deviation of ten volunteers is more than 1.3, but the standard deviation of a volunteer at nine different times is approximately 0.4.

In order to better understand the statistic characteristics of biometric verification based on HBC in the frequency range 650 MHz to 750 MHz, the coefficient of variation, which can reflect the relative dispersion of data, is adopted in this section. The calculation of coefficient of variation is shown as Equation (2).

$$\mathrm{CV} = \left| \frac{s_i}{\overline{x}} \right| \times 100\% \quad (2)$$

where CV is the coefficient of variation, s_i is the standard deviation of sample data, and $\overline{x}$ is the average value of sample data.

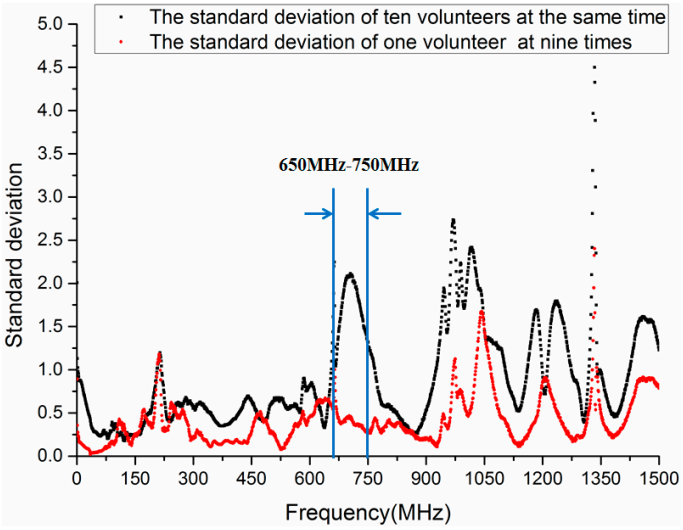

Figure 6. Standard deviation of transmission gain S21 in the frequency range 0.3 MHz to 1500 MHz.

As shown in Figure 7, the coefficient of variation of ten volunteers is more than 8% when the frequency is 664 MHz. As the frequency increases, the coefficient of variation has a feature of sustained rise in the frequency range 665 MHz to 715 MHz. In addition, the coefficient of variation is 12.5% at 715 MHz and is 9.5% at 750 MHz. However, the coefficient of variation of one volunteer at nine different times is approximately 2.5% when the frequency is 650 MHz to 750 MHz. Thus, it is indicated that the frequency 650 MHz to 750 MHz may be appropriate for biometric verification based on HBC.

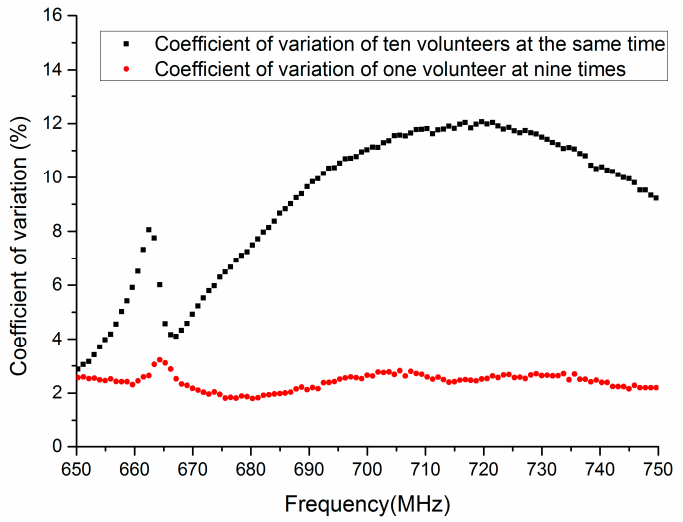

Figure 7. The coefficient of variation of transmission gain S21 in the frequency range 650 MHz to 750 MHz.

4.3. Transmission Gain S21 at Chosen Frequency

To achieve rapid verification, the number of sample data for human biometric trait should not be too high. In this paper, 21 sample data are acquired in each time (group) via VNA when frequency is from 650 MHz to 750 MHz. The frequency interval between each sample data is 5 MHz. Figure 8 shows the transmission gain S21 (21 sample data) in the frequency range 650 MHz to 750 MHz. As shown in Figure 8, there is a significantly difference among volunteers at the chosen frequency. In contrast, the difference of one volunteer at four times is small. Therefore, those 21 sample data can be regarded as human biometric trait.

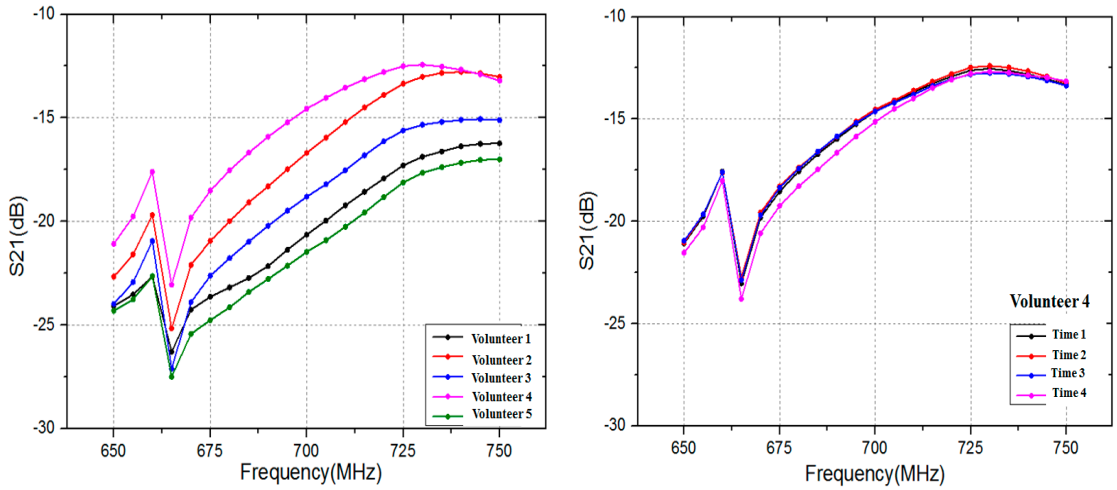

Figure 8. Transmission gain S21 in the frequency range 650 MHz to 750 MHz: (**a**) five volunteers at the same time; and (**b**) Volunteer 4 at four different times.

5. TATM Algorithm Proposed

5.1. Template Building

In this paper, a threshold adaptive template matching (TATM) algorithm based on weighted Euclidean distance is proposed to achieve personal verification. Figure 9 illustrates the process of the TATM algorithm. In general, the personal verification is divided into two steps: learning and verification [39]. In the first step, the error data need to be cleaned from the template library before the matching template is built. The second step is to determine the correlation between sample data and matching template. It is worth noting that the data used for matching template building and verification are obtained via Experiment 2. Specifically, 18 groups of data for each volunteer, obtained during the first three days, are used as template library to build the matching template, and the remaining groups (12 groups) are used to verification. Moreover, each group includes 21 sample data.

However, the sample data are unsteady in a certain range owing to the influence of VNA and ambient environment. Moreover, the change of experimental condition sometimes has a great impact on sample data. Therefore, the error data should be removed from the template library. In this paper, a simple and effective method is adopted to remove the error data from template library. Firstly, the sample data of 18 groups for each volunteer are taken as the initial template library *lib*1, as shown in Equation (3).

$$\begin{cases} lib1 = \begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{m1} & x_{m2} & \cdots & x_{mn} \end{pmatrix}_{m \times n} \\ y_j = \frac{1}{m} \sum_{i=1}^{m} x_{ij},\ 1 \le j \le n \\ M_1 = \begin{pmatrix} y_1 & y_2 & \cdots & y_n \end{pmatrix}_{1 \times n} \end{cases} \tag{3}$$

where m represents the number of feature vectors in each initial template library and the value of m is 18. n represents the number of feature points in each feature vector, and the value of n is 21. M_1 is the initial matching template which consists of 21 feature points.

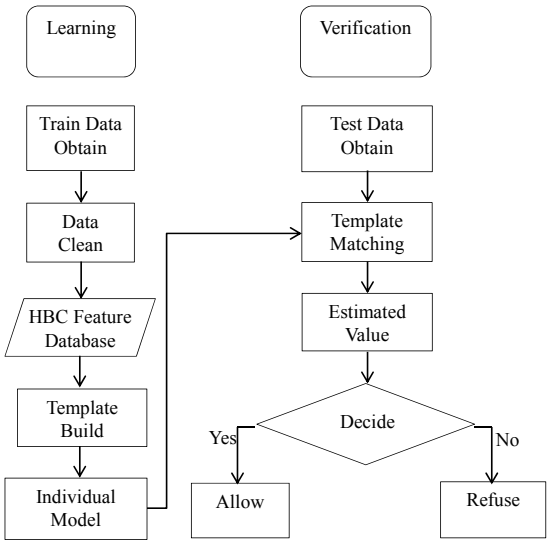

Figure 9. Flow diagram of TATM algorithm.

Secondly, the Euclidean distance between the initial matching template M_1 and each feature vector that belongs to the template library is calculated. The feature vector will be excluded when the Euclidean distance is greater than the threshold T_1. The calculation of Euclidean distance is represented in Equation (4).

$$\begin{cases} S_i = \begin{pmatrix} x_{i1} & x_{i2} & \cdots & x_{in} \end{pmatrix}_{1\times n} \\ S_i \in lib1,\ 1 \le i \le m \\ D_1 = ||S_i - M_1||_2 = \sqrt{(S_i - M_1)^T (S_i - M_1)} \\ D_1 = \begin{cases} \ge T_1,\ delete \\ \le T_1,\ save \end{cases} \end{cases} \tag{4}$$

where S_i is the feature vector of initial template library $lib1$, D_1 is the Euclidean distance between M_1 and S_i, and T_1 is the Euclidean distance threshold. The value of threshold T_1 can be set to 2 in this paper.

A new template library $lib2$ is obtained after the error data are removed from $lib1$. Subsequently, the matching template M_2 is generated according to Equation (5). This template is the final feature vector of individual, which represents individual's behavioral trait.

$$\begin{cases} lib2 = \begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{(m-r)1} & x_{(m-r)2} & \cdots & x_{(m-r)n} \end{pmatrix}_{(m-r)\times n} \\ y'_j = \frac{1}{m-r} \sum_{i=1}^{m-r} x'_{ij},\ 1 \le j \le n \\ M_2 = \begin{pmatrix} y'_1 & y'_2 & \cdots & y'_n \end{pmatrix}_{1\times n} \end{cases} \tag{5}$$

where $lib2$ is $(m-r) \times n$ Matrix, r is the number of feature vectors which have been cleaned, and M_2 is the matching template used for verification.

5.2. Verification

Considering that the weights of feature points are different in a feature vector, TATM based on weighted Euclidean distance is proposed in this work. Compared with classical Euclidean distance

calculation method, the calculations are more precise. The calculation of TATM based on weighted Euclidean distance is performed as follows. The difference between maximum max_{1i} and minimum min_{1i} of sample data, which belong to template library *lib*2 at the same frequency, is calculated. The reciprocal of difference is used as the corresponding feature point weight C_i, as shown in Equation (6).

$$\begin{cases} max_{1j} = \max\left(x_{1j}\ ,\ x_{2j}\ ,\ \cdots\ ,\ x_{(m-r)j}\right),\ 0 \le j \le n \\ min_{1j} = \min\left(x_{1j}\ ,\ x_{2j}\ ,\ \cdots\ ,\ x_{(m-r)j}\right),\ 0 \le j \le n \\ C_j = 1/\left(max_{1j} - min_{1j}\right) \end{cases} \tag{6}$$

According to the value of matching template M_2, the distance between the feature vector in template library *lib*2 and matching template M_2 is calculated. Then, the maximal value of distance max_2 is set to threshold T_2, as shown in Equation (7).

$$\begin{cases} D_{2i} = \sqrt{\sum_{j=1}^{n} C_j\left(x_{ij} - M_{2j}\right)^2},\ 0 \le i \le m - r \\ max_2 = \max\left(D_{21}, D_{22}, D_{23}, \ldots, D_{2(m-r)}\right) \\ T_2 = max_2 \end{cases} \tag{7}$$

where j is the j-th feature point in a feature vector, and D_{2i} is the value of Euclidean distance between matching template M_2 and i-th feature vector in *lib*2.

In terms of Equation (7), it is revealed that the threshold and weight are defined by matching template. The advantage of this method is that it does not required many experiments to find the suitable value. T_2 is utilized as the verification threshold in TATM algorithm to confirm whether the user is the authorized person. In verification mode, the test sample will be divided into two classes: the *I*-related and the *I*-non-related. Under the premise of the acceptable false acceptance rate (FAR), this method can get the smallest false rejection rate (FRR). The final determination condition is shown as Equation (8).

$$\begin{cases} D = \sqrt{\sum_{j=1}^{n} C_j\left(Fdata_j - M_{2j}\right)^2} \\ D\begin{cases} \ge T_2,\ I - \text{non} - \text{related} \\ < T_2,\ I - \text{related} \end{cases} \end{cases} \tag{8}$$

where $Fdata_j$ is the j-th sample data in test feature vector, and D is the distance between test data and matching template M_2.

6. Algorithm Evaluation

6.1. Effect of Data Cleaning

Figure 10 demonstrates the variance of 21 feature points in the frequency range 650 MHz to 750 MHz. As demonstrated in Figure 10, the variance of feature points is reduced after data cleaning. The maximum and minimum values are 0.23 and 0.05 before data cleaning, and 0.1736 and 0.0365 after data cleaning, respectively. Therefore, the data cleaning method adopted in this paper is effective at removing error data from template library.

On the other hand, the variance of feature points is different at different frequencies after data cleaning. Specifically, the variances of these feature points are 0.0365, 0.1401, 0.1266, 0.1395, 0.1736, and 0.1289, respectively, at frequencies 650 MHz, 665 MHz, 670 MHz, 705 MHz, 740 MHz, and 750 MHz. It is revealed that feature points are not invariable values. A smaller variance of feature point means that the biometric trait is more stable, which is of great help to improve the accuracy of personal verification. Therefore, the weight of feature point of which the variance is relatively small should be

set to a higher value to highlight its importance. In contrast, the weight should be decreased if the variance of feature point is large.

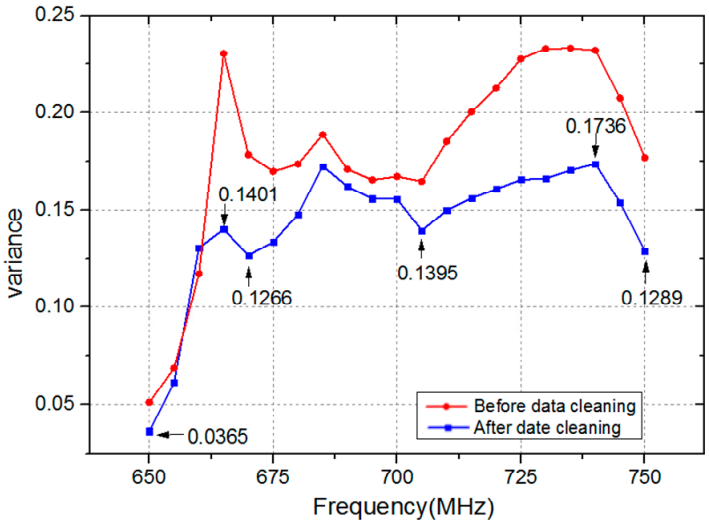

Figure 10. The variance of feature points after data cleaning.

To better understand the influence of Euclidean distance threshold T_1 on data cleaning, the false acceptance rate (FAR) and false rejection rate (FRR) are acquired at different threshold T_1. FAR reflects the rate at which the imposters are accepted into the system, and FRR reflects the rate at which the authorized users are denied entry into the system. The calculations of FAR and FRR are shown as Equations (9) and (10). Table 3 lists the FAR and FRR at different Euclidean distance threshold T_1.

$$\text{FAR} = \frac{false\ acceptance\ samples}{total\ acceptance\ samples} \times 100\% \tag{9}$$

$$\text{FRR} = \frac{false\ rejection\ samples}{total\ acceptance\ samples} \times 100\% \tag{10}$$

As listed in Table 3, the Euclidean distance threshold T_1 has a great impact on data cleaning when it is less than 5. Furthermore, the FAR is 5.79% and the FRR is 6.74% when the Euclidean distance threshold T_1 is equal to 2. However, the FRR is up to 36.8% and 13.3%, respectively, when the Euclidean distance threshold T_1 is 1.5 and 2.5. Therefore, considering the relatively low FAR and FRR, the Euclidean distance threshold T_1 can be set to 2 in this paper.

Table 3. Influence of Euclidean distance threshold T_1.

Threshold T_1	**1**	**1.5**	**2**	**2.5**	**3**	**3.5**	**4**	**5**	**6**	**7**
FAR	1.09%	5.24%	5.79%	8.26%	15.2%	14.5%	17.6%	17.4%	17.4%	17.4%
FRR	77.7%	36.8%	6.74%	13.3%	3.33%	4.17%	4.17%	5.0%	5.0%	5.0%

6.2. The EER

In this section, 120 groups of data obtained during Days 4 and 5 in Experiment 2 are adopted to calculate the FAR, FRR and equal error rate (EER). Figure 11 shows the values of FAR and FRR when the verification threshold T_2 is from 0.8 to 2.8. As shown in Figure 11, the range of FRR is from 80% to 0.5%, and the range of FAR is from 0.1% to 18%. Furthermore, the EER is 7.06% when the FAR is equal to FRR at verification threshold $T_2 = 1.91$.

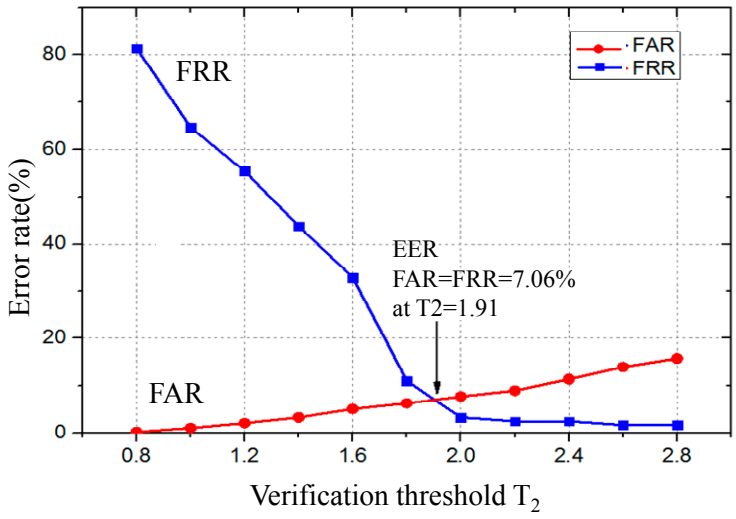

Figure 11. FAR and FRR for different verification threshold T_2.

6.3. Algorithm Comparison

In this paper, the TATM based on weighted Euclidean distance is compared with K-nearest neighbor (KNN) classification, support vector machines (SVM) and naive Bayesian method (NBM). All algorithms are implemented by MATLAB on a personal computer. Furthermore, the SVM is achieved by the LIBSVM which is a library designed by Taiwan University [40], and the KNN and NBM are acquired from MATLAB function library. A total of 120 groups of sample data are used as the test data. The FAR and FRR of different algorithms are listed in Table 4. Additionally, the running time of algorithm is listed in Table 5.

Table 4. FAR and FRR of different algorithms.

Volunteer	TATM		KNN		SVM		NBM	
	FAR	FRR	FAR	FRR	FAR	FRR	FAR	FRR
1	0.95%	0	7.41%	8.33%	0	0	0	16.67%
2	15.24%	0	8.33%	33.33%	7.41%	58.33%	7.41%	41.67%
3	3.81%	25%	4.63%	66.67%	5.56%	25.0%	10.19%	41.67%
4	1.89%	0	3.70%	8.33%	2.78%	8.33%	3.70%	8.33%
5	0	8.33%	0	25%	0	33.33%	0	41.67%
6	13.21%	0	6.48%	50.0%	5.56%	8.33%	4.63%	25.0%
7	6.67%	25%	0.93%	58.33%	1.85%	91.67%	0.93%	25.0%
8	3.77%	9.09%	3.70%	33.33%	10.19%	16.67%	3.70%	41.67%
9	12.38%	0%	6.48%	91.67%	3.70%	91.67%	7.41%	100%
10	0	0	0	0	0	0	0	0
Average	5.79%	6.74%	4.17%	37.5%	3.37%	33.33%	3.80%	34.17%

Table 5. Running time of different algorithms

Algorithm	TATM	KNN	SVM	NBM
Running time (s)	0.019	0.310	0.0385	0.168

As illustrated in Table 4, for Volunteers 1, 4, and 10, KNN shows a good performance of low FAR and FRR. However, KNN has a disappointing result for other volunteers. The FRR is more than 50% for Volunteers 3, 6, 7, and 9. Thus, the KNN is unsuitable for biometric verification based on HBC. The FRR obtained by SVM is more than 10% for Volunteers 2, 3, 5, 6, 7, 8, and 9. Moreover, the FRR

of Volunteers 7 and 9 is 91.67%. The FRR of SVM is so large that it is inappropriate for verification. Similarly, the NBM also shows a bad performance, and the FRR is greater than 10% for eight volunteers in the measurement. On the other hand, the TATM shows a good performance for different volunteers (Table 4). The average values of FAR and FRR are 5.79% and 6.74%, respectively. Furthermore, as listed in Table 5, the running time of TATM is the shortest (0.019 s), whereas the running time of KNN is up to 0.310 s, while the running times of SVM and NBM are 0.0385 s and 0.168 s, respectively. Thus, it can be concluded that the TATM is more suitable for rapid verification owing to it has lower FRR and shorter running time.

The influence of the number of feature vectors on FAR and FRR is investigated next. Figure 12 describes the FAR and FRR with different numbers of feature vectors. In Figure 12a, it can be observed that the FAR of three algorithms is less than 6% when the number of feature vectors is 18. Additionally, as demonstrated in Figure 12b, the FRR is sensitive to the numbers of feature vectors. The FRRs of all algorithms are greater than 50% when the numbers of feature vectors is equal to 3. However, the FRR of SVM and NBM is approximately 25%, and the FRR of TATM is only 6.74% when the number of feature vectors is 18. Thus, compared with SVM and NBM, TATM presents a lower FRR.

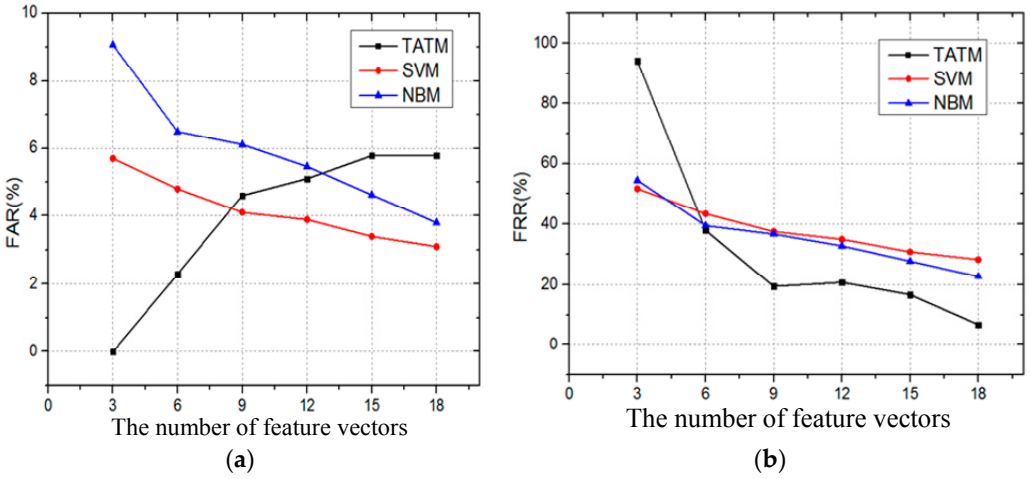

Figure 12. The influence of the number of feature vectors: (**a**) FAR; and (**b**) FRR.

Table 6 lists the EER, running time, and computational memory of biometric verification based on HBC in previous works. In [34], the EER of 0.56% is achieved by SVM. However, the number of feature vectors is 160, and the number of feature points for each feature vector is up to 1600. Furthermore, the running time and computational memory of SVM in Reference [34] are approximately 9.941 s and 91 MB. In Reference [31], the EER of 25% is obtained by SVM when 40 feature vectors and each feature vector includes 100 feature points are adopted. In our paper, the EER of 7.06% is achieved by TATM when 18 feature vectors are utilized. Furthermore, the number of feature points in each feature vector is only 21. Additionally, the running time and computational memory of TATM in this article are 0.019 s and 2 MB, respectively. Thus, it is concluded that TATM can provide a rapid verification with a relatively low running time and computational memory.

Table 6. Comparison with previous works.

	[34]	[31]	This Article
The number of feature vectors	160	40	18
Feature point in each feature vector	1600	100	21
Algorithm	SVM	SVM	TATM
EER	0.56%	25%	7.06%
Running time	9.941 s	-	0.019 s
Computational memory	91 MB	-	2 MB

6.4. Discussion

As listed in Table 4, it is worth noting that both the FAR and FRR of Volunteer 10 are equal to zero, which may be associated with the volunteer herself. Specifically, the forearm of Volunteer 10 is thinner than the other volunteers, which led to her transmission gain S21 being quite different.

On the whole, as listed in Table 4, The FRR of KNN, SVM, and NBM is high even when the parameters of algorithms were varied, which may be related with the number of training data [27]. In the learning groups, the training data for each volunteer (18 groups of data) are fewer than those of others (162 groups of data), so a volunteer's classification area is narrower and might overlap with those of other volunteers, which leads to a high FRR.

However, the FRR of TATM is relatively low, which is associated with the verification threshold T_2. The verification threshold T_2 is threshold-adaptive in this paper, namely, the verification threshold T_2 of each volunteer is mainly dependent on the number of each volunteer's own training data rather than those of others. Thus, the TATM shows low FRR.

7. Conclusions

This paper proposes a rapid biometric verification for application in wearable devices. The transmission gain S21 of individual is measured in the frequency range 0.3 MHz to 1500 MHz. The results indicate that there is significantly different transmission gain S21 among individuals, and the transmission gain S21 for the same individual is steady over a period of time. Furthermore, it is also revealed that the chosen frequency for biometric verification based on HBC is 650 MHz to 750 MHz. In addition, a threshold-adaptive template matching (TATM) algorithm based on weighted Euclidean distance is proposed in this paper. In order to achieve rapid verification, 18 groups of data, each group including 21 sample data, are used as the template library. In terms of template library, the matching template used for personal verification is built after the data cleaning. Meanwhile, the weights of feature points are calculated. The results show that the TATM algorithm presents a good performance with relative lower FAR and FRR, 5.79% and 6.74%, respectively. In contrast, the FAR and FRR were 4.17% and 37.5%, 3.37% and 33.33%, and 3.80% and 34.17%, respectively, using KNN, SVM, and NBM. In addition, the running time of TATM is the shortest (0.019 s), while the running times of KNN, SVM and NBM are 0.310 s, 0.0385 s, and 0.168 s, respectively. Compared with other algorithms, the TATM based on weighted Euclidean distance has lower FRR and shorter running time. Therefore, the TATM proposed in this paper may be a potential solution for rapid verification for wearable devices. In the near future, the biometric verification based on HBC and the TATM algorithm will be achieved in a wearable prototype.

Acknowledgments: This work was supported by the National Natural Science Foundation of China under Grant No. 61403366 and No. U1505251; Guangdong Science and Technology Plan Project under Grant No. 2015A020214018 and No. 2015B020233004; Shenzhen Basic Research Project Fund under Grant No. JCYJ20150401150223630; Shenzhen Technology Development Project Fund under Grant No. CXZZ20150505093829778 and Shenzhen Public Technology Service Platform Improvement Project of Biomedical Electronics.

Author Contributions: Jingzhen Li and Zengyao Pang performed the experiments and wrote the paper; Zedong Nie provided the initial idea of this research and provided many useful comments; Yuhang Liu and Wenjian Qin worked for the data collection and analysis; and Lei Wang modified the grammar.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

The algorithms of KNN, NBM and SVM are introduced as follows.

A.1. KNN

KNN is usually used for clustering with the advantage of simple principle and fast running speed for large datasets. The main idea of KNN is that the datasets are divided into different categories by the iterative process. The detailed steps for KNN are as follows.

(1) The dataset X and the number of clustering N (N > 1) are set at initialization time. N objects are randomly selected as the initial cluster centers in dataset X.
(2) The Euclidean distance between each object and the cluster centers is calculated. According to the principle of minimum distance, datasets will be divided into N classes again.
(3) The average value of each class is used as a new clustering center.
(4) If the new clustering center is equal to the cluster center, the iterative process stops; otherwise, repeat Step 2 and Step 3.

A.2. NBM

NBM, which is based on the probability density function, is an efficient and simple classification algorithm. NBM can be used to describe the relation between conditional probability and classification in the system, as shown in Equation (A1).

$$\mathrm{P(B|A)} = \frac{\mathrm{P(A|B)P(B)}}{\mathrm{P(A)}} \tag{A1}$$

Compared with the other classification methods, NBM has lower time complexity and higher accuracy. As a well-developed classification method, NBM has been widely used in classification. The steps of NBM are as follows.

(1) $\mathrm{X} = \{a_1, a_2, \ldots, a_m\}$ and $\mathrm{C} = \{y_1, y_2, \ldots, y_n\}$ are set as a sorting item and collection of categories, respectively. C is trained in advance.
(2) The Conditional probability $\mathrm{P}(y_i|\mathrm{X})$ for the sorting item X is calculated by Equation (A2).

$$\mathrm{P}(y_i|\mathrm{X}) = \frac{P(X|y_i)}{P(X)},\ 0 < i \leq n \tag{A2}$$

(3) The value of $\mathrm{P}(y_k|\mathrm{X})$ is obtained through Equation (A3).

$$\mathrm{P}(y_k|\mathrm{X}) = \max\{\mathrm{P}(y_1|X), \mathrm{P}(y_2|X), \ldots \mathrm{P}(y_n|\mathrm{X})\} \tag{A3}$$

A.3. SVM

SVM is a data mining algorithm based on statistical theory. The mechanism of SVM is to obtain an optimal separating hyperplane to meet the requirements of classification. The optimal separating hyperplane ensures the accuracy of the classification. In addition, it has the largest distance of the classification point at optimal separating hyperplane. The two-class classification problem is taken as an example.

First, a training data set is acquired, as shown in Equation (A4).

$$\begin{cases} (x_i\ ,\ y_i),\ i = 1, 2, \ldots, l \\ \quad \mathrm{x} \in \mathrm{R},\ y_i = \pm 1 \end{cases} \tag{A4}$$

To solve two-class classification problem, the separating hyperplane is obtained.

$$\omega \cdot x + \mathrm{b} = 0 \tag{A5}$$

In order to classify all the samples correctly, the Equation (A6) needs to be satisfied.

$$y_i[(\omega \cdot x_i + b)] \geq 1,\ i = 1, 2, \ldots l \tag{A6}$$

The classification interval is set to $2/||\omega||$. Thus, the problem of constructing the hyperplane is transformed into solving the constraint problem.

$$\min\varnothing(\mathrm{x}) = \frac{1}{2}||\omega||^2 = \frac{1}{2}(\omega' \cdot \omega) \tag{A7}$$

In order to solve the constrained optimization problem, the Lagrange function is introduced, as shown in Equation (A8).

$$\mathrm{L}(\omega, \mathrm{b}, \mathrm{a}) = \frac{1}{2}||\omega|| - a(y((\omega \cdot x) + b) - 1) \tag{A8}$$

where $\mathrm{a} > 0$ is Lagrange multiplier. The solution of the optimization problem is determined by the saddle point of the Lagrange function. This solution's partial derivatives of b and ω are 0 at the saddle point. The quadratic programming (QP) problem is transformed into a dual problem.

$$\begin{cases} \max \mathrm{Q}(\mathrm{a}) = \sum\limits_{j=1}^{l} a_j - \frac{1}{2} \sum\limits_{i=1}^{l} \sum\limits_{j=1}^{l} a_i a_j y_i y_j (x_i \cdot x_j) \\ s.t. \sum\limits_{j=1}^{l} a_j y_j = 0 \; i, j = 1, 2, \ldots, l \; a_j \geq 0 \end{cases} \tag{A9}$$

The solution is obtained by Equations (A8) and (A9).

$$\begin{cases} a^* = \left(a_1^*, a_2^*, \ldots, a_l^*\right)^T \\ \omega^* = \sum\limits_{j=1}^{l} a_j^* y_j x_j \\ b^* = y_i - \sum\limits_{j=1}^{l} y_j a_j^* (x_j \cdot x_i). \end{cases} \tag{A10}$$

Finally, the optimal classification function is obtained according to Equation (A5) and (A10).

$$\mathrm{f}(\mathrm{x}) = \mathrm{sgn}\{(w^* \cdot x) + b^*\} = \mathrm{sgn}\left\{\left(\sum_{j=1}^{l} a_j^* y_j (x_j \cdot x_i)\right) + b^*\right\} \tag{A11}$$

References

1. Gravina, R.; Alinia, P.; Ghasemzadeh, H.; Fortino, G. Multi-sensor fusion in body sensor networks: State-of-the-art and research challenges. *Inf. Fusion* **2016**, *35*, 68–80. [CrossRef]
2. Fortino, G.; Giannantonio, R.; Gravina, R.; Kuryloski, P.; Jafari, R. Enabling Effective Programming and Flexible Management of Efficient Body Sensor Network Applications. *IEEE Trans. Hum. Mach. Syst.* **2013**, *43*, 115–133. [CrossRef]
3. Fortino, G.; Giampa, V. PPG-based methods for non invasive and continuous blood pressure measurement: An overview and development issues in body sensor networks. In Proceedings of the IEEE International Workshop on Medical Measurements and Applications Proceedings, Ottawa, ON, Canada, 30 April–1 May 2010; pp. 10–13.
4. Choi, H.; Naylon, J.; Luzio, S.; Beutler, J.; Birchall, J.; Martin, C.; Porch, A. Design and in Vitro Interference Test of Microwave Noninvasive Blood Glucose Monitoring Sensor. *IEEE Trans. Microw. Theory Tech.* **2015**, *63*, 3016–3025. [CrossRef] [PubMed]
5. Gravina, R.; Fortino, G. Automatic Methods for the Detection of Accelerative Cardiac Defense Response. *IEEE Trans. Affect. Comput.* **2016**, *7*, 286–298. [CrossRef]
6. Ghasemzadeh, H.; Jafari, R. Coordination Analysis of Human Movements With Body Sensor Networks: A Signal Processing Model to Evaluate Baseball Swings. *IEEE Sens. J.* **2011**, *11*, 603–610. [CrossRef]
7. Fortino, G.; Galzarano, S.; Gravina, R.; Li, W. A framework for collaborative computing and multi-sensor data fusion in body sensor networks. *Inf. Fusion* **2015**, *22*, 50–70. [CrossRef]

8. Friedman, N.; Rowe, J.B.; Reinkensmeyer, D.J.; Bachman, M. The manumeter: A wearable device for monitoring daily use of the wrist and fingers. *IEEE J. Biomed. Health Inform.* **2014**, *18*, 1804–1812. [CrossRef] [PubMed]
9. Su, S.W.; Hsieh, Y.T. Integrated Metal-Frame Antenna for Smartwatch Wearable Device. *IEEE Trans. Antennas Propag.* **2015**, *63*, 3301–3305. [CrossRef]
10. Wannenburg, J.; Malekian, R. Body Sensor Network for Mobile Health Monitoring, a Diagnosis and Anticipating System. *IEEE Sens. J.* **2015**, *15*, 6839–6852. [CrossRef]
11. Ignatenko, T.; Willems, F.M.J. Biometric Systems: Privacy and Secrecy Aspects. *IEEE Trans. Inf. Forensic Secur.* **2009**, *4*, 956–973. [CrossRef]
12. Zhang, K.; Yang, K.; Liang, X.; Su, Z. Security and privacy for mobile healthcare networks: From a quality of protection perspective. *IEEE Wirel. Commun.* **2015**, *22*, 104–112. [CrossRef]
13. Lim, M.H.; Yuen, P.C. Entropy Measurement for Biometric Verification Systems. *IEEE Trans. Cybern.* **2015**, *46*, 1065–1077. [CrossRef] [PubMed]
14. Zareen, F.J.; Jabin, S. Authentic mobile-biometric signature verification system. *IET Biom.* **2016**, *5*, 13–19. [CrossRef]
15. He, D.; Wang, D. Robust Biometrics-Based Authentication Scheme for Multiserver Environment. *IEEE Syst. J.* **2014**, *9*, 816–823. [CrossRef]
16. Jain, A.K.; Ross, A.; Prabhakar, S. An introduction to biometric recognition. *IEEE Trans. Circuits Syst. Video Technol.* **2004**, *14*, 4–20. [CrossRef]
17. Hsieh, S.H.; Li, Y.H.; Tien, C.H.; Chang, C.C. Extending the Capture Volume of an Iris Recognition System Using Wavefront Coding and Super-Resolution. *IEEE Trans. Cybern.* **2016**, *46*, 3342–3350. [CrossRef] [PubMed]
18. Chih-Lung, L.; Kuo-Chin, F. Biometric verification using thermal images of palm-dorsa vein patterns. *IEEE Trans. Circuits Syst. Video Technol.* **2004**, *14*, 199–213.
19. Odinaka, I.; Lai, P.H.; Kaplan, A.D.; O'Sullivan, J.A.; Sirevaag, E.J.; Rohrbaugh, J.W. ECG Biometric Recognition: A Comparative Analysis. *IEEE Trans. Inf. Forensic Secur.* **2012**, *7*, 1812–1824. [CrossRef]
20. Mathur, S.; Vjay, A.; Shah, J.; Das, S.; Malla, A. Methodology for partial fingerprint enrollment and authentication on mobile devices. In Proceedings of the 2016 International Conference on Biometrics (ICB), Halmstad, Sweden, 13–16 June 2016; pp. 1–8.
21. Klonovs, J.; Petersen, C.K.; Olesen, H.; Hammershoj, A. ID Proof on the Go: Development of a Mobile EEG-Based Biometric Authentication System. *IEEE Veh. Technol. Mag.* **2013**, *8*, 81–89. [CrossRef]
22. Peter, S.; Reddy, B.P.; Momtaz, F.; Givargis, T. Design of Secure ECG-Based Biometric Authentication in Body Area Sensor Networks. *Sensors* **2016**, *16*, 570. [CrossRef] [PubMed]
23. Choudhary, T.; Manikandan, M.S. Robust Photoplethysmographic (PPG) Based Biometric Authentication for Wireless Body Area Networks and m-Health Applications. In Proceedings of the National Conference on Communication, Guwahati, Assam, India, 4–6 March 2016; pp. 1–6.
24. Derawi, M.; Voitenko, I. Fusion of gait and ECG for biometric user authentication. In Proceedings of the 2014 International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, Germany, 10–12 September 2014; pp. 1–4.
25. Kim, D.J.; Chung, K.W.; Hong, K.S. Person Authentication using Face, Teeth and Voice Modalities for Mobile Device Security. *IEEE Trans. Consum. Electron.* **2010**, *56*, 2678–2685. [CrossRef]
26. Sun, Z.; Zhang, H.; Tan, T.; Wang, J. Iris Image Classification Based on Hierarchical Visual Codebook. *IEEE Trans. Pattern Anal. Mach. Intell.* **2013**, *36*, 1120–1133. [CrossRef] [PubMed]
27. Farmanbar, M.; Toygar, Ö. A Hybrid Approach for Person Identification Using Palmprint and Face Biometrics. *Int. J. Pattern Recognit. Artif. Intell.* **2015**, *29*, 671–682. [CrossRef]
28. Guzman, A.M.; Goryawala, M.; Wang, J.; Barreto, A.; Andrian, J.; Rishe, N.; Adjouadi, M. Thermal Imaging as a Biometrics Approach to Facial Signature Authentication. *IEEE J. Biomed. Health Inform.* **2013**, *17*, 214–222. [CrossRef] [PubMed]
29. Mayron, L.M. Biometric Authentication on Mobile Devices. *IEEE Secur. Priv.* **2015**, *13*, 70–73. [CrossRef]
30. Nakanishi, I.; Yorikane, Y.; Itoh, Y.; Fukui, Y. Biometric Identity Verification Using Intra-Body Propagation Signal. In Proceedings of the 2007 Biometrics Symposium, Baltimore, MD, USA, 11–13 September 2007; pp. 1–6.

31. Nakanishi, I.; Inada, T.; Sodani, Y.; Shigang, L. Performance Evaluation of Intra-palm Propagation Signals as Biometrics. In Proceedings of the International Conference on Biometrics and Kansei Engineering, Tokyo, Japan, 5–7 July 2013; pp. 91–94.
32. Nakanishi, I.; Sodani, Y. SVM-Based Biometric Authentication Using Intra-Body Propagation Signals. In Proceedings of the IEEE International Conference on Advanced Video and Signal Based Surveillance, Boston, MA, USA, 29 August–1 September 2010; pp. 561–566.
33. Rasmussen, K.B.; Roeschlin, M.; Martinovic, I.; Tsudik, G. Authentication using pulse-response biometrics. In Proceedings of the Proceedings of the Network and Distributed Systems Security Symposium (NDSS), San Diego, CA, USA, 23–26 February 2014; pp. 1–14.
34. Xia, M.; Ma, J.; Li, J.; Liu, Y.; Zeng, Y.; Nie, Z. Gradient and SVM based biometric identification using human body communication. In Proceedings of the 2016 IEEE International Conference of Online Analysis and Computing Science (ICOACS), Chongqing, China, 28–29 May 2016; pp. 61–65.
35. Wu, J.; Cai, Z.; Gao, Z. Dynamic K-Nearest-Neighbor with Distance and attribute weighted for classification. In Proceedings of the 2010 International Conference on Electronics and Information Engineering (ICEIE), Kyoto, Japan, 1–3 August 2010; pp. V1-356–V1-360.
36. Shilton, A.; Palaniswami, M.; Ralph, D.; Tsoi, A.C. Incremental training of support vector machines. *IEEE Trans. Neural Netw.* **2005**, *16*, 114–131. [CrossRef] [PubMed]
37. Zhang, C.; Wang, J. Attribute weighted Naive Bayesian classification algorithm. In Proceedings of the 2010 5th International Conference on Computer Science and Education (ICCSE), Hefei, China, 24–27 August 2010; pp. 27–30.
38. Wegmueller, M.S.; Kuhn, A.; Froehlich, J.; Oberle, M.; Felber, N.; Kuster, N.; Fichtner, W. An attempt to model the human body as a communication channel. *IEEE Trans. Biomed. Eng.* **2007**, *54*, 1851–1857. [CrossRef] [PubMed]
39. Biggio, B.; Fumera, G.; Russu, P.; Didaci, L. Adversarial Biometric Recognition: A review on biometric system security from the adversarial machine-learning perspective. *IEEE Signal Process. Mag.* **2015**, *32*, 31–41. [CrossRef]
40. Chang, C.C.; Lin, C.J. Training v-support vector classifiers: Theory and algorithms. *Neural Comput.* **2001**, *13*, 2119–2147. [CrossRef] [PubMed]