sustainability

MDPI

Article

Advanced Authentication Scheme with Bio-Key Using Artificial Neural Network

Zia ur Rehman [1,*], Saud Altaf [1], Shafiq Ahmad [2], Mejdal Alqahtani [2], Shamsul Huda [3] and Sofia Iqbal [4]

[1] University Institute of Information Technology, Pir Mehr Ali Shah Arid Agriculture University, Rawalpindi 46000, Pakistan; saud@uaar.edu.pk
[2] Industrial Engineering Department, College of Engineering, King Saud University, P.O. Box 800, Riyadh 11421, Saudi Arabia; ashafiq@ksu.edu.sa (S.A.); almejdal@ksu.edu.sa (M.A.)
[3] School of Information Technology, Deakin University, Burwood, VIC 3128, Australia; shamsul.huda@deakin.edu.au
[4] Pakistan Space & Upper Atmosphere Research Commission, Islamabad 44000, Pakistan; sofiaiqbal.suparco@gmail.com
* Correspondence: ziaraja@gmail.com

Abstract: The improvements in the field of health monitoring have revolutionized our daily lifestyle by developing various applications that did not exist before. However, these applications have serious security concerns; they also can be taken good care of by utilizing the Electrocardiogram (ECG) as potential biometrics. The ECG provides robustness against forgery attacks unlike conventional methods of authentication. Therefore, it has attained the utmost attention and is utilized in several authentication solutions. In this paper, we have presented an efficient architecture for an advanced authentication scheme that utilized a binarized form (bio-key) of ECG signal along with an Artificial Neural Network (ANN) to enhance the authentication process. In order to prove the concept, we have developed the testbed and acquired ECG signals using the AD8232 ECG recording module under a controlled environment. The variable-length bio-keys are extracted using an algorithm after the feature extraction process. The extracted features along with bio-keys are utilized for template formation and also for training/testing of the ANN model to enhance the accuracy of the authentication process. The performance of authentication results depicted high authentication accuracy of 98% and minimized the equal error rate (EER) to 2%. Moreover, our scheme outperformed comparative peers' work in terms of accuracy and EER.

Keywords: ANN; ECG; advance authentication; WBAN

Citation: Rehman, Z.u.; Altaf, S.; Ahmad, S.; Alqahtani, M.; Huda, S.; Iqbal, S. Advanced Authentication Scheme with Bio-Key Using Artificial Neural Network. *Sustainability* **2022**, *14*, 3950. https://doi.org/10.3390/su14073950

Academic Editor: Ripon Kumar Chakrabortty

Received: 17 February 2022
Accepted: 22 March 2022
Published: 26 March 2022

1. Introduction

Wearable medical devices paved the way to provide ubiquitous health care services that have enhanced the quality of life as compared to past years. These devices provide seamless monitoring in a way that one can perform their daily life's routine and work comfortably without being bothered, and enable a variety of applications from routine to clinical scenarios. However, the security of data became vitally important in the case of a healthcare scenario.

Biometrics provides unique features that can be utilized for authentication purposes. It includes Iris, Fingerprint, gait, etc, The electrocardiogram (ECG) (as shown in Figure 1) is one of the biometric traits that measure the dynamic electrical activity of the human heart [1]. It is considered an efficient method that can be utilized for identity recognition. However, the innovation of Machine Learning (ML) techniques has opened a new perspective in authentication approaches [2]. The verification models have been constructed using ML techniques for the identification of ECG data [3,4].

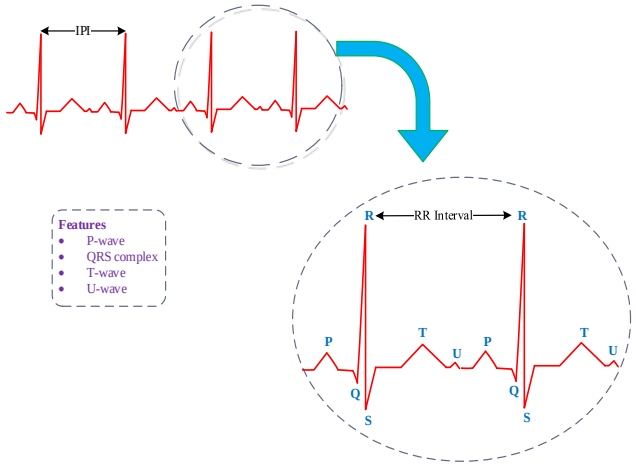

Figure 1. The ECG signal with different features.

The ECG-based authentication schemes mostly utilize fiducial, non-fiducial, and a fusion of both features for identity recognition purposes. Whereas fiducial feature points are related to the morphology of the signal, such as *p*, QRS, T waves, non-fiducial features represent statistical features analysis, such as kurtosis, autocorrelation, average, mean, etc. [5–7]. Recently, techniques have been proposed in the literature that utilized a fusion of both types of features and proved promising results [8,9].

The ML-based authentication scheme using an ECG signal proposed by Akleem et al. [10] applied a regression model into subsets of the dataset. After breaking the ECG dataset into smaller parts, the authors applied a decision tree (DT) model and achieved accuracy up to 92%. In another study [11], authors utilized convolutional kernels to achieve better classification by combining two functions, namely margin loss and center loss, in the training process. The results depicted improved accuracy and a lower equal error rate (EER).

Similarly, Donida et al. utilized a convolutional neural network (CNN) for biometric authentication and binarized the ECG signal to speed up the matching process [12]. Moreover, the authentication schemes [13–15] also utilized CNN as a classification method after extracting features from ECG signals. Hammad et al. [16] proposed a multimodal biometric scheme that fused both ECG and Fingerprints data to apply the CNN feature extraction method. The authors used a Q-Gaussian multi-support vector machine (QG-MSVM) in the authentication phase to enhance performance.

The authentication solutions pertaining to the anonymous lightweight category [17,18] and hybrid approaches, such as [19], along with other cryptographic schemes and RNN based biometrics schemes, [20] also exist in the literature. However, our main focus is, to sum up, authentication schemes based on ML techniques [21,22]. This work is specifically related to ANN-based authentication schemes [23,24].

The main contributions are summarized as follows:

- We have proposed a new architecture for an advanced authentication scheme that utilized a binarized form (bio-key) of ECG signals in combination with ANN to improve the authentication process.
- We have designed a testbed using the AD8232 ECG recording module and acquired ECG signals of 47 subjects (including males and females) under a controlled environment.
- The bio-keys are generated using an algorithm and the template is constructed along with selected ECG features. These selected features besides bio-keys are further utilized for training/testing of the ANN model to enhance the accuracy of the authentication process.
- The performance results of the proposed authentication scheme depicted high precision (98.1%), authentication accuracy (98%), and minimized equal error rate (EER) (0.02).

- The performance comparison results proved that the proposed authentication scheme outstands with peer schemes. This proved that it is highly applicable, efficient, and robust.
- The rest of the article is organized as follows: section II unveiling the proposed authentication scheme; section III detailing experimentation, performance evaluation, and comparison with peers; section IV covering the discussion; and, finally, the conclusion in section V.

2. Proposed Authentication Scheme

The proposed scheme's architecture (as depicted in Figure 2) contains three major stages of the scheme namely preprocessing, enrollment, and authentication stages. The raw ECG signal is firstly preprocessed to remove noise and other related artifacts, such as baseline wandering, muscles noise, etc. The next step involves feature extraction and bio-key generation from the cleaned ECG signal. The enrollment stage starts right after the features extraction and bio-key generation. It comprises template construction and template storage that is further utilized in ANN classification, through which an authentication decision is made.

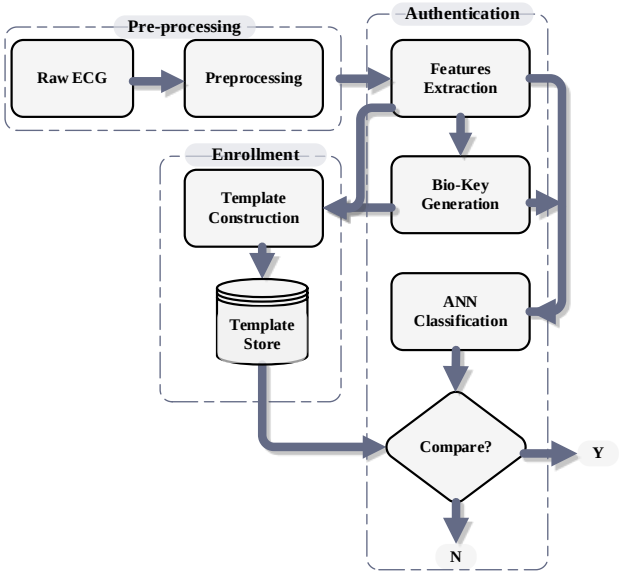

Figure 2. The architecture of the proposed scheme.

2.1. Preprocessing

In this step we remove baseline wandering from the ECG signal, which is caused due to breathing and electrically charged electrodes. It requires a high pass filter with a cut-off frequency greater than the lowest frequency in the ECG signal. It cancels low-frequency components from the signal and is usually set to under 0.5 Hz. However, the frequency content of a baseline wander can be increased due to increased body movement during stress tests or exercise. The high pass filter is designed using Equation (1).

$$H\left(e^{j\omega}\right) = \begin{cases} 0, & 0 < |\omega| < \omega_c \\ 1, & \omega_c < |\omega| < \pi \end{cases} \quad (1)$$

where $\omega_c = 2\pi f_c$ and f_c is cutoff frequency, ω = frequency.

The power line noise is also introduced into the ECG signal due to seamless electromagnetic field interference of supply lines and can be removed by applying an infinite impulse response (IIR) notch filter, as depicted in Equation (2). After removing the baseline

wander, power line noise is also removed by designing a filter using a notch frequency set to 60 HZ and bandwidth to 120. Thus, the net result is the removal of power line noise.

$$H(z) = \frac{\left(1 - z_1 z^{-1}\right)\left(1 - z_2 z^{-1}\right)}{(1 - p_1 z^{-1})(1 - p_2 z^{-1})} = \frac{1 - 2cos(\omega_0)z^{-1} + z^{-2}}{1 - 2ecos(\omega_0)z^{-1} + r^2 z^{-2}} \quad (2)$$

where z refers to complex conjugated pair, ω_0 refers to interfering frequency.

2.2. Feature Extraction

This is a process that transforms ECG signal into low dimensional feature space. It is normally divided into two categories, namely fiducial features and non-fiducial features. The fiducial features involved fixed reference points present in ECG signals, such as *p*-wave, QRS wave, and T-wave. It also requires calculations regarding amplitude and temporal distance among fiducial points. These points are very sensitive to noise and require high precision. The non-fiducial features, on the other hand, examine the frequency domain of the ECG signal and are less sensitive to noise, e.g., calculation of mean, standard deviation, variance, kurtosis, etc. We have utilized both fiducial and non-fiducial features for the authentication process. The extracted features are 'Rpeaks', 'HeartRate', 'Peaks Interval (Pinter)', 'Average', and 'Kurtosis'.

2.3. Bio-Key Generation

Once features are extracted from the ECG signal, the Inter-Pulse-Interval (IPI) is utilized to formulate a key of varying length. The process commences firstly by generating a bio-key after computing IPI values, secondly, applying the gray coding, and lastly, the output bits of gray coding are concatenated to get the result. The pseudocode of bio-key extraction is depicted in Algorithm 1. The uniqueness of extracted bio-keys is determined by calculating hamming distance (HD) and Entropy (H) using Equations (3) and (4).

$$d^{HD}(i,j) = \sum_{k=0}^{n-1} \left[y_{i,k} \neq y_{j,k} \right] \quad (3)$$

where y is a series of numbers

$$H(X) = -\sum_{i=1}^{n} p_i log_2 p_i \quad (4)$$

where p denotes the probability

Algorithm 1 Pseudo-code algorithm used for bio-key extraction.

1. The raw ECG signal is collected from the subject.
2. The signal is pre-processed using noise removal techniques.
3. After noise removal, R-peaks are preserved and all other frequency components are removed.
4. The IPI is quantified up to the length of the signal and its equivalent binary representations.
5. The gray coding is applied to reduce the difference between IPI bits
6. The concatenation operation is applied to get the final variable-length bio-key.

2.4. Template Construction & Store

During the enrollment process, the template is created by mixing the bio-key generated from the ECG with extracted features, such as peaks interval (PInter), average, and kurtosis. The bio-key can have values in the range of [0, 1] and are extracted by the manipulation of fiducial features; therefore, the next step is to store it in a file that can be used in the matching process.

2.5. Authentication

The authentication phase begins once features are extracted and a bio-key is generated after it. The ANN serves as the core of the authentication stage by using a feed forward neural network with backpropagation. The features (PInter, average, kurtosis, and bio-key) were used to formalize the training dataset for two purposes, i.e., training and validation. The neural network starts with inputs, bias, and the sum of the multiplication of weights. The mathematical form of the model is shown in Equation (5).

$$Y_k = f\left(\sum_{j=1}^{n} w_{jk} Z_j + w_{k0}\right) \; for \; k = 1, 2, \ldots\ldots l \tag{5}$$

where $Z_j = f\left(\sum_{i=1}^{d} w_{ij} x_i + w_{j0}\right) \; for \; j = 1, 2, \ldots\ldots n$; x_i are network inputs, w_{ij} represents weights, w_{j0} represents an initial bias of the hidden node, while f is the transfer function. Z_j represents hidden layers' output while Y_k represents network output, w_{jk} is weights and w_{k0} is the bias of the output layer.

We have distributed data with the ratio of 70% for training, whereas the remaining 30% is distributed equally for testing and validation purpose. The PInter values are utilized during the training phase by the ANN model until the binary stream is produced with the help of varying weights in the backpropagation algorithm. The input data from an individual user is provided to the ANN with existing weights of training phase results in binary stream output that is further compared with pre-stored bio-keys from the template store in the next step.

2.6. Criteria for Authentication

The criteria set for authentication is 80% or more, i.e., detailed as:

1. During the comparison, if a match is found in the template store with accuracy of more than or equal to 80% then it is authenticated
2. Otherwise, a person is considered an intruder

2.7. Performance Evaluation

The performance of authentication criteria is measured through the following metrics:

- Performance accuracy defines the percentage of correct prediction over a total number of testing samples.
- Equal Error Rate (EER): It is utilized for determining the threshold value among FAR and FRR.

$$Precision = \frac{TP}{TP + FP} * 100 \tag{6}$$

$$Sensitivity = \frac{TP}{TP + FN} * 100 \tag{7}$$

$$\text{Specitivity} \; = \frac{\text{TN}}{\text{FP} + \text{TN}} * 100 \tag{8}$$

$$\text{F} \; - \; \text{Score} \; = \frac{2 * \text{Sensitivity} \; * \; \text{Precision}}{(\text{Sensitivity} \; + \; \text{Precision})} \tag{9}$$

$$\text{Accuracy} \; = \frac{\text{Number of Correct Predictions}}{\text{Total number of test samples}} * 100 \tag{10}$$

$$\text{False Acceptance Rate (FAR)} = \frac{\text{FP}}{\text{TN} + \text{FP}} \tag{11}$$

$$\text{False Rejection Rate (FRR)} = \frac{\text{FN}}{\text{TP} \; + \; \text{FN}} \tag{12}$$

where TP refers to true positive, TN = true negative, FP = false positive, FN = false negative.

3. Experimentation and Results

The algorithm is developed using Matlab 2016b running on the Windows 10 operating system. We have designed a testbed to collect ECG signals from 47 subjects including both males and females. We utilized the AD8232 sensor for ECG recording along with Arduino UNO (acting as coordinator) attached to a Computer. The testbed diagram is shown in Figure 3. We have used 100 recordings, which are sampled at a frequency of 360 samples/s. In total, 70% of records are utilized for training and 30% for testing purposes. The ECG signal recordings are made with the consent of volunteers (subjects), as shown in Figure 4.

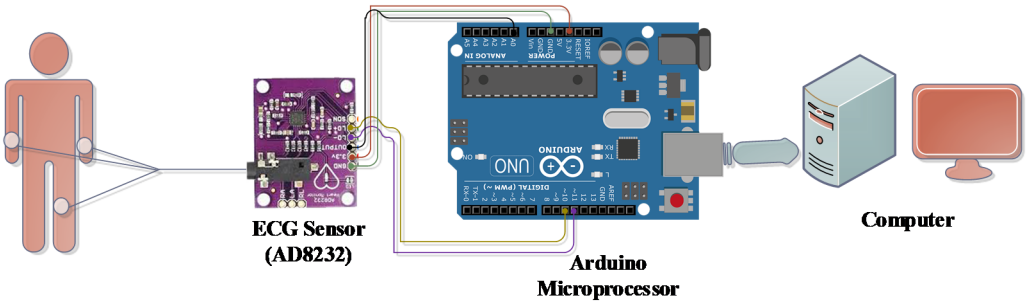

Figure 3. The testbed utilized for experimentation.

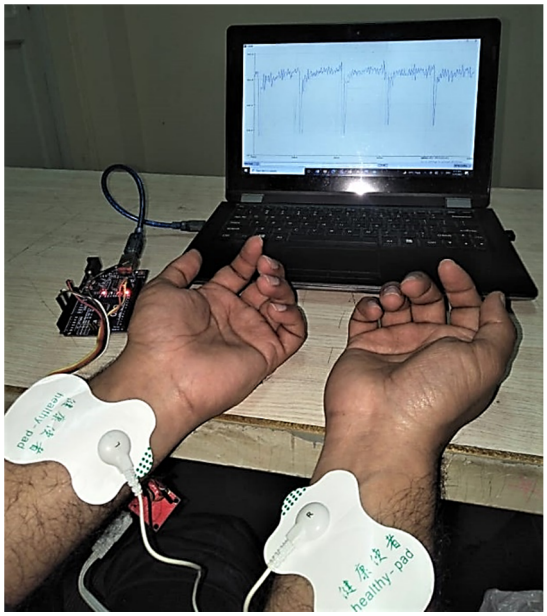

Figure 4. The ECG recording using the AD8232 Sensor.

3.1. Experimental Setup

The experiment started by preprocessing ECG signals, as depicted in Figure 5. The features were extracted and the bio-key for each individual was generated using the pseudocode algorithm. The output of the pseudocode is depicted (in blue) in Figure 6 as a single case. To ensure the degree of uncertainty and uniqueness, the Hamming distance (HD) and key entropy H(X) were calculated for all ECG recordings in general, but the comparison among the few records was made as a single-case (as depicted in Figures 7 and 8, respectively). Furthermore, four subjects are selected at random and their bio-keys are extracted after time interval 't' and then HD and H(X) are calculated, which showed higher HD value and closer H(X) value. It is worth mentioning here that a higher HD value means more different keys and H(X) closer to 1 means higher uncertainty, which is also desired.

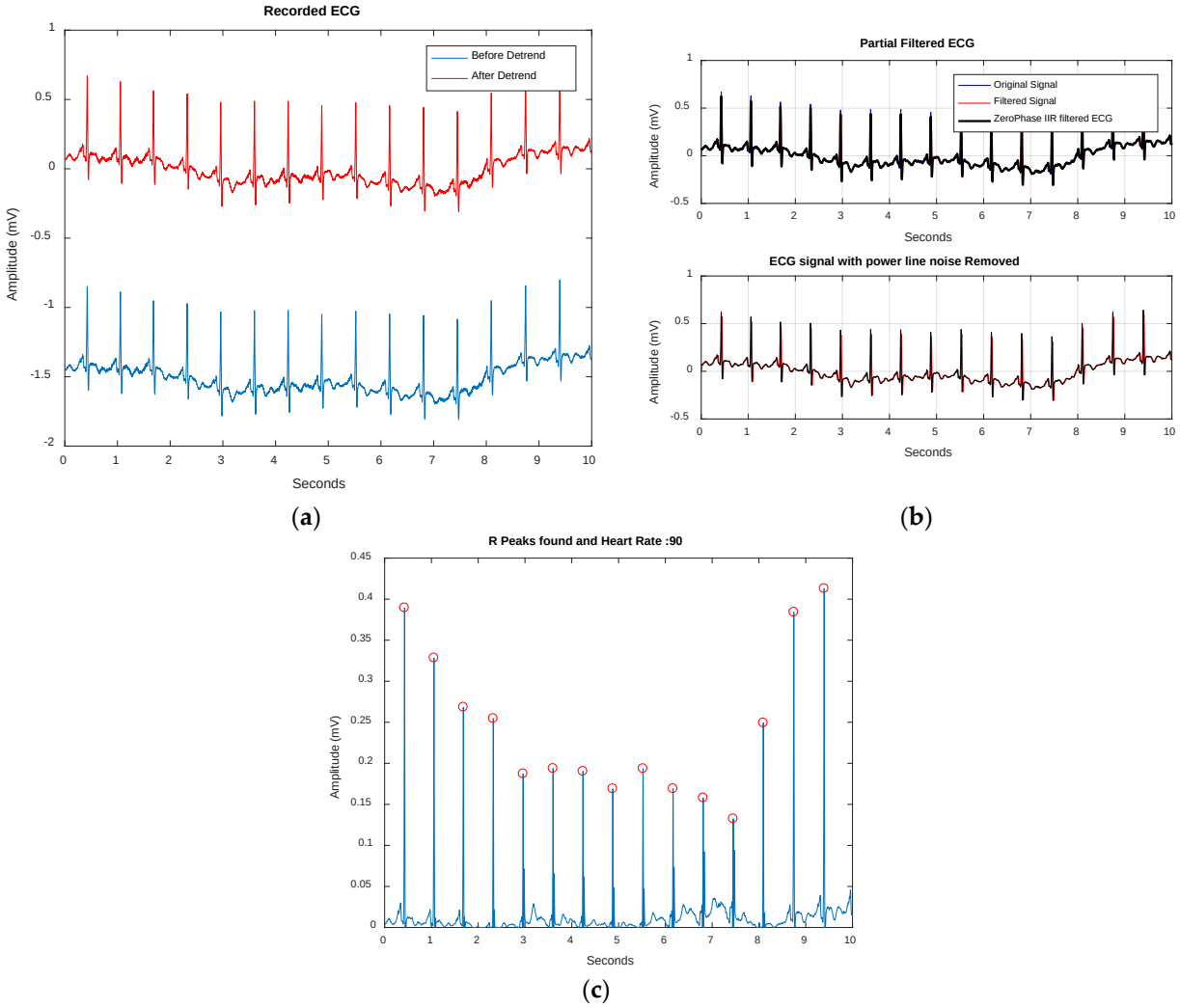

Figure 5. The preprocessing stage of the ECG signal is depicted as: (**a**) detrending of signal; (**b**) baseline wander and power line noise removed; (**c**) Rpeaks identified after noise removal.

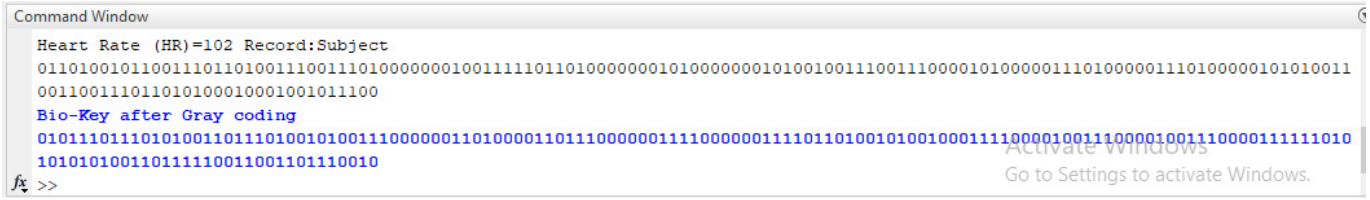

Figure 6. The bio-key extracted (in blue) using pseudocode.

The features (PInter, average, kurtosis, and bio-key) were simulated using Matlab scripts to produce a Neural Network (NN) model. The bio-key/stream was set as target data while the other three served as input data. The hidden layers and their initial weights were set, along with transfer functions to compute error criteria. Table 1 depicted the extracted features samples that were used for classification and training purposes.

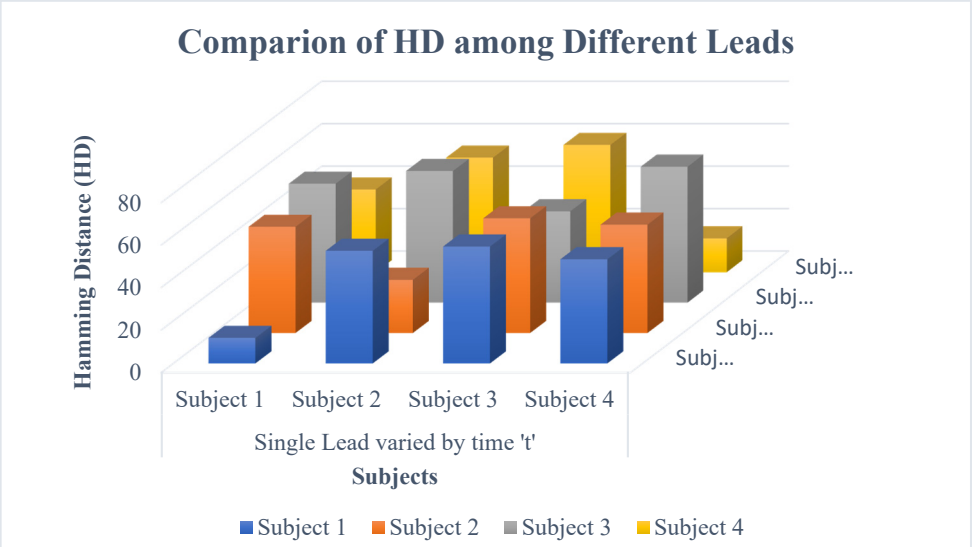

Figure 7. The Hamming distance calculated among bio-keys generated with the same lead but varied by time 't'.

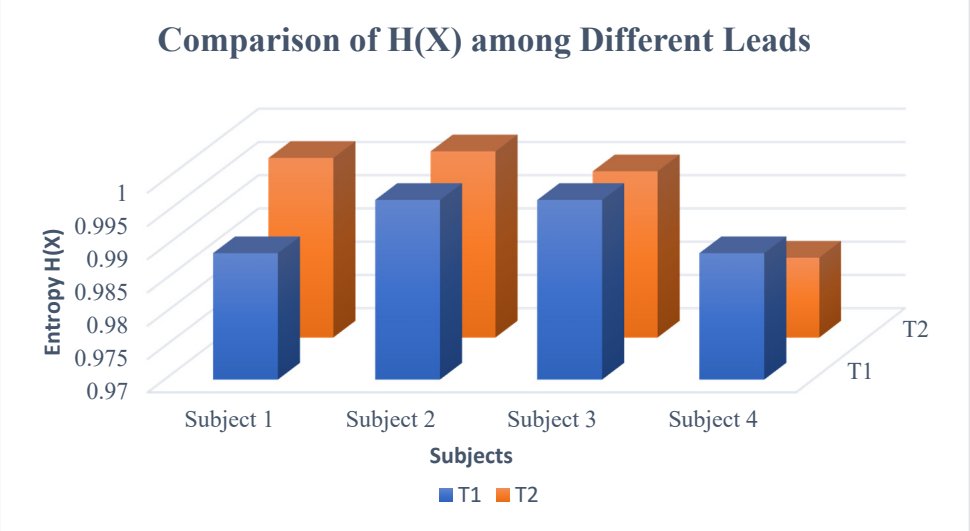

Figure 8. The entropy calculations among generated bio-keys with the same lead but varied by the time 't', i.e., t1 and t2.

Table 1. The extracted features samples.

Samples	Pinter	Average	Kurtosis	Bio-Key
S1	[1 × 18 double]	5.97×10^{-4}	47.5186	110110101110110110110010010110010010110010010110110100 1100111100110101011101110000101101101100100110100111111
S2	[1 × 16 double]	4.05×10^{-4}	47.9453	101001011110101101110011101110001000111100001011101010111 1100111110110001100110010101011101010101000010100011001011 011010101010100010000101
S3	[1 × 18 double]	5.30×10^{-4}	87.3044	100111001000011011110001010000000111011010011011011001001101 0110000101001010100100111001110010110011
S4	[1 × 19 double]	3.18×10^{-4}	83.3642	100111001000100010011110000010010000111010011010100111001000011 0010001100000110011001110010011110000111001001101 1

We have a varied number of hidden layers ([4 × 8 × 3], [4 × 12 × 3], and [4 × 15 × 3]) to attain a dissimilar form of architecture and its impact on data validation results, as shown

in Table 2. It is observed through Table 2 that the architecture [4 × 12 × 3] performed better in terms of Mean Squared Error (MSE). Furthermore, better efficacy is achieved in the same architecture due to less classification error rate as compared with other architectures. However, as a case study, the [4 × 12 × 3] architectural model is depicted in Figure 9 and its corresponding confusion matrices are depicted in Figure 10.

Table 2. The validation results by varying NN architecture.

Arch	Sample	MSE	No. of Epoch	Accuracy	Classification Error
[4 × 8 × 3]	S1	7.79×10^{-2}	71	92.3	7.7
	S2	7.45×10^{-2}	76	92.4	7.6
	S3	7.99×10^{-2}	102	91.9	8.1
	S4	7.01×10^{-2}	65	90.2	9.8
[4 × 12 × 3]	S1	8.29×10^{-2}	143	97.4	2.6
	S2	9.05×10^{-2}	186	97.5	2.5
	S3	7.49×10^{-2}	110	97.6	2.4
	S4	9.291×10^{-2}	168	97.7	2.3
[4 × 15 × 3]	S1	7.99×10^{-2}	405	92.9	7.1
	S2	7.15×10^{-2}	398	90.2	9.8
	S3	6.91×10^{-2}	312	89.1	10.9
	S4	7.19×10^{-2}	399	91.5	8.1

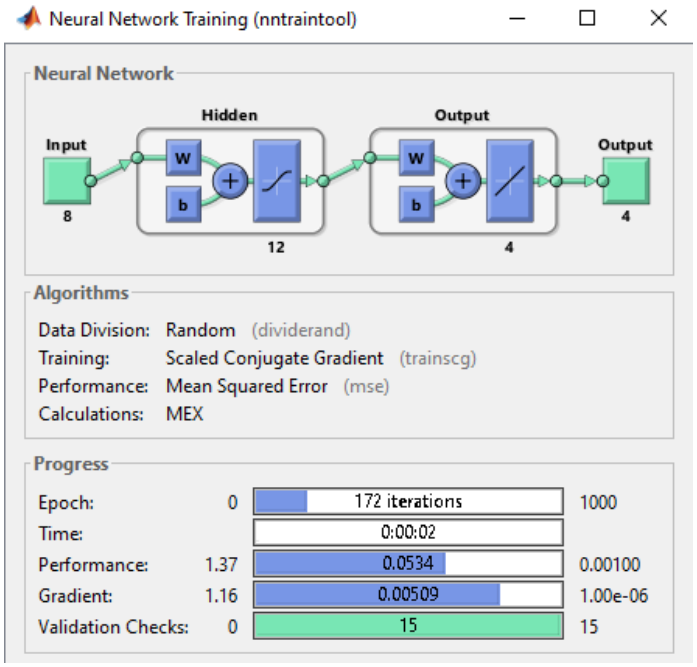

Figure 9. The ANN architecture [4 × 12 × 3].

The confusion grid (as shown in Figure 10) contained training data analysis among target and output classes. The data was divided into four classes both horizontally and vertically to highlight the testing accuracy of the validation process. The cells in green depicted accurately classified groups of trail classes. Moreover, the data represented in red cells were incorrectly classified, or, in other words, were invalidated during the testing process. The overall percentage was depicted in blue depending on the number of test cases classified correctly or incorrectly, as highlighted in green and red cells.

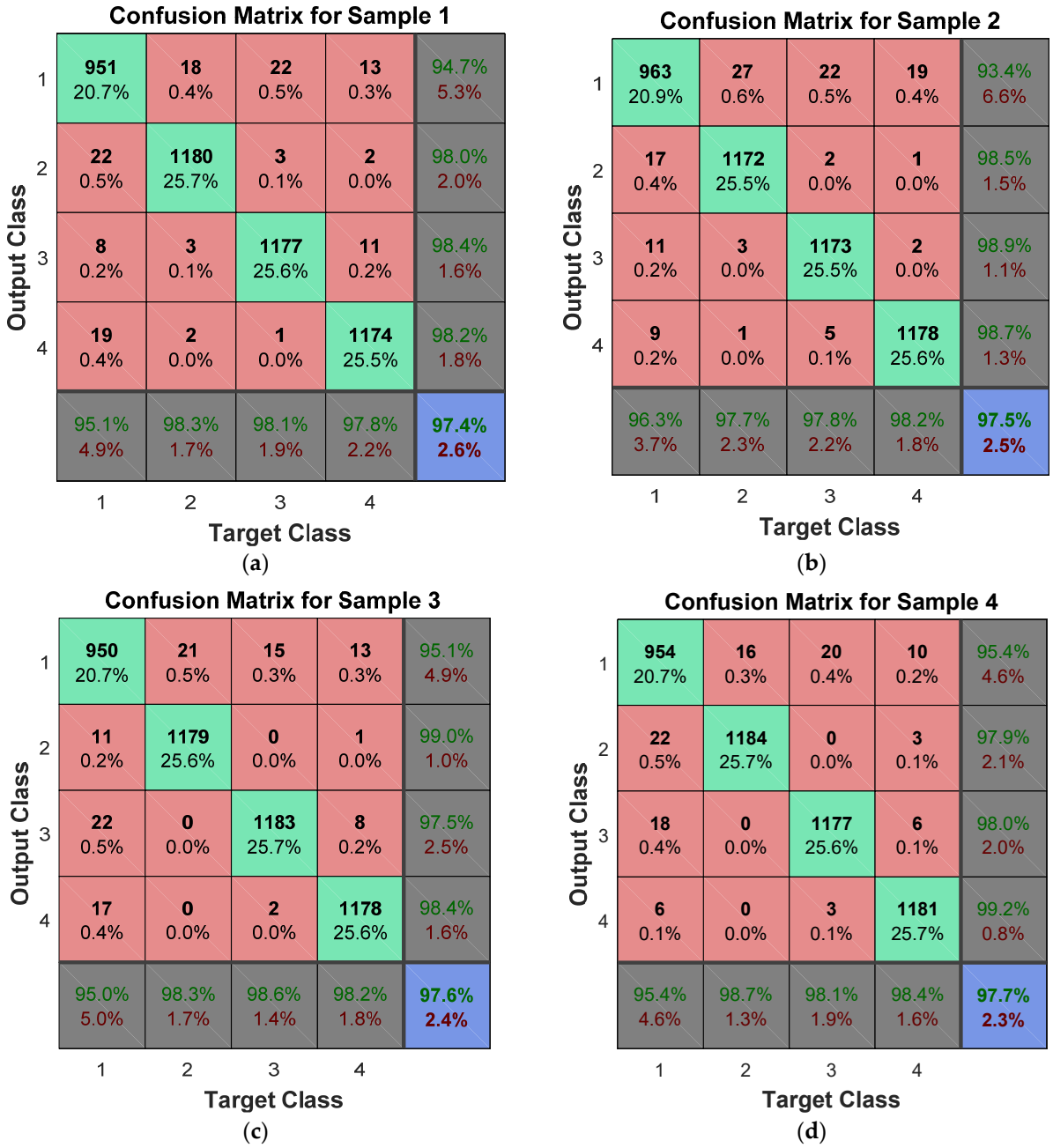

Figure 10. The confusion matrix depicted as: (**a**) Sample 1; (**b**) Sample 2; (**c**) Sample 3; and (**d**) Sample 4.

It is apparent from Figure 10 that the testing trails for each class were 1200 as depicted in green cells. Similarly, by analyzing sample 1, the datasets wrongly identified were low comparative to cells in green. For instance, there were 22 types of wrongly classified trials sample in output class 2 and target class 1. Similarly, in the same target class, the output classes 3 and 4 had 8 and 19 types, respectively, that were wrongly classified, comprising the data validation accuracy of 95.1% shown in grey with an error rate of 4.9% overall. Similarly, the data validation accuracy and error rate of other target classes were calculated, and accumulated output data validation accuracy of 97.4% with an error rate of 2.6% was achieved. The maximum accuracy was achieved at sample 4 97.7% with a minimized error rate of 2.3%, which is considered as an achievement.

3.2. ECG Authentication

Out of 47 subjects, 40 were considered authorized and 7 as imposter. The performance accuracy is achieved to 98% and FAR of 0.02 where FRR = 0. In our proposed work only 2% of imposters are wrongly identified as authorized. As the matching process of the proposed scheme returns a decision (either Y or N), therefore a detection error trade-off (DET) graph cannot be generated and we have to consider FAR only (FRR = 0). Moreover, the EER is considered equal to FAR, i.e., 0.02 or 2%. The details of performance evaluation results are depicted in Figure 11.

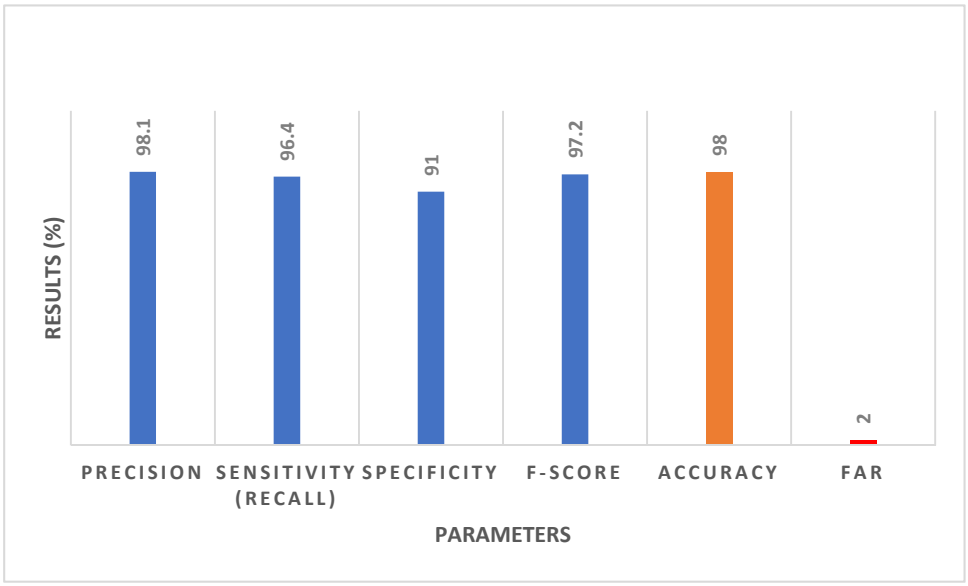

Figure 11. The performance results based on authentication criteria.

3.3. Comparison with Peers

The comparison of our scheme with related peer works is summarized in Table 3 It is obvious from the given table that our scheme has outperformed in terms of accuracy and EER. It is also evident that our scheme outperformed due to improvements made in the matching process by introducing the binary streams in it. The comparison is also made clear in Figure 12.

Table 3. The comparison results with peers.

Ref	Accuracy (%)	EER
[8]	96.6	0.03
[10]	92.7	0.03
[16]	96.56	0.035
[11]	95.99	0.047
[Our]	98.0	0.02

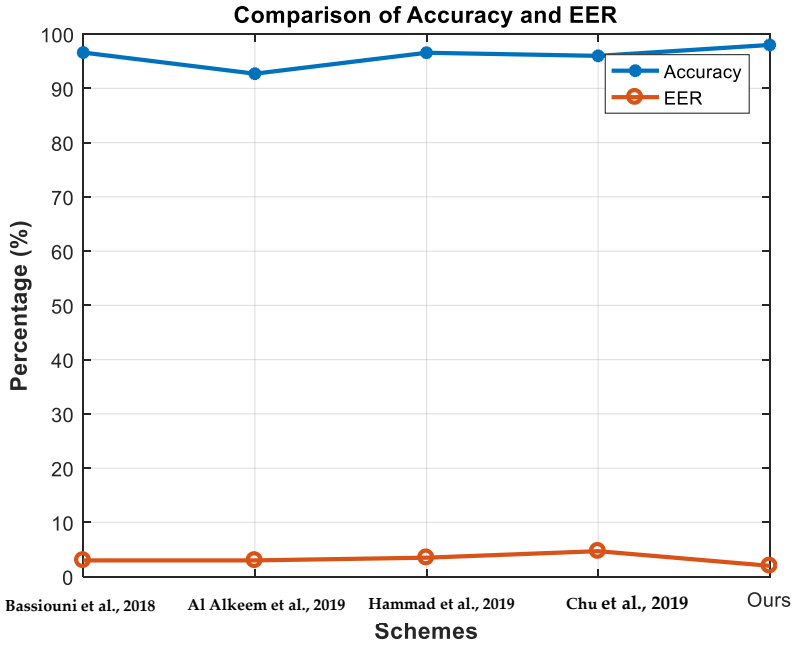

Figure 12. The comparison of accuracy (%) and EER (%) with peers.

4. Discussion

The proposed authentication scheme is implemented through the data collected through the AD8232 ECG sensor. The ECG signals are preprocessed using the Equations (1) and (2) and features are extracted afterward, which are used for biometrics. The bio-keys are extracted with the help of the algorithm discussed in Table 1. The bio-keys extracted from the features are variable, distinct, random, and difficult to predict. The bio-keys acquired through this process are verified for randomness and uncertainty property by using Equations (3) and (4). The fact is made prominent through the output of HD comparison results (in Figure 7) computed among selected subjects, which depicted greater differences with each other.

It is worth mentioning that even bio-keys extracted from IPI values (in Figure 6) computed from different subjects varied by time interval have produced more dynamic and different results, which is desirable. Similarly, the comparison of Entropy H(X) (Figure 8) depicted results are closer to one, which means a higher degree of uncertainty that is further desirable.

Furthermore, the bio-key along with extracted features (PInter, average, and kurtosis) are also utilized for template formation and stored in a database. The sample features in Table 1 showed the excerpts of results, which are further utilized for training and testing purposes. The different architectural models for ANN have been computed and found that [8 × 12 × 4] have yielded better results compared to other models, as shown in Table 2. The ANN model showed the training state in Figure 9. The confusion matrices for each sample have been computed and depicted in Figure 10. As discussed in the previous section, the data validation accuracy and error rate for each class have been calculated besides the net data validation accuracy and error rate. The aggregate accuracy achieved for sample 1 to sample 4 is very consistent from 97.4% to 97.7%, along with a consistent error rate from 2.6% to 2.3%, respectively. The proficiency of data validation results has been increased and imprecision has been reduced to an optimal level. Hence, the results validated the analysis and trained samples data.

Moreover, the outcome of the ANN model was the bio-stream that was further utilized in the matching process. The performance of authentication criteria was judged with the help of parameters detailed in Figure 11. These parameters are calculated using the Equations (6)–(12). The authentication accuracy is measured to 98% with FAR = 0.02, which is further evidence that the proposed scheme has achieved higher accuracy. It is

also worth mentioning here that FAR = 0.02 (FRR = 0), therefore, EER is considered equal to FAR in our case. The achieved results were also compared against the performance of peers, as highlighted in Table 3 and made prominent with the help of Figure 12. The proposed scheme achieved better performance accuracy and EER as compared to peer works. Therefore, we claim that our scheme is more efficient as compared to peer works.

5. Conclusions and Future Direction

We have proposed an authentication scheme that utilized ECG signals along with the ANN technique and bio-key. The proposed authentication scheme is implemented by using the AD8232 ECG sensor for data collection. We designed an algorithm to extract a variable-length bio-key using IPI values of ECG signal. This newly added feature is further utilized in template construction and training/validation of the ANN model. The different ANN architectures were tested and found [$4 \times 12 \times 3$] architecture demonstrated better results than others. The output of the ANN model is utilized in the template matching process. The performance results of our scheme achieved accuracy to 98%, precision to 98.1%, and minimized the equal error rate (EER) to 2%. The performance comparison results proved that the proposed authentication scheme is applicable and efficient in terms of accuracy and EER.

We have planned to work on a multimodal authentication scheme by fusing two or more physiological signals and application of ML techniques as a possible future extension.

Author Contributions: Conceptualization, Z.u.R., M.A., S.A. (Shafiq Ahmad) and S.A. (Saud Altaf); methodology, Z.u.R., S.A. (Saud Altaf) and M.A.; software, Z.u.R.; validation, Z.u.R., S.A. (Shafiq Ahmad) and S.I.; formal analysis, Z.u.R., M.A. and S.A. (Saud Altaf); investigation, Z.u.R.; resources, S.A. (Saud Altaf); data curation, S.A. (Saud Altaf), M.A. and S.A. (Shafiq Ahmad); writing—original draft preparation, Z.u.R., S.H. and S.I.; writing—review and editing, S.A. (Saud Altaf); visualization, Z.u.R. and S.A. (Saud Altaf), M.A.; supervision, S.H.; project administration, M.A.; funding acquisition, M.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by King Saud University, grant number RSP2022R426, and the APC was funded by RSP2022R426.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors extend their appreciation to King Saud University for funding this work through Researchers Supporting Project number (RSP2022R426), King Saud University, Riyadh, Saudi Arabia.

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

References

1. Elshahed, M.A. Personal identity verification based ECG biometric using non-fiducial features. *Int. J. Electr. Comput. Eng.* **2020**, *10*, 3007–3013. [CrossRef]
2. Xin, Y.; Kong, L.; Liu, Z.; Chen, Y.; Li, Y.; Zhu, H.; Gao, M.; Hou, H.; Wang, C. Machine Learning and Deep Learning Methods for Cybersecurity. *IEEE Access* **2018**, *6*, 35365–35381. [CrossRef]
3. Zhang, J.; Li, H.; Li, J. Key Establishment Scheme for Wireless Sensor Networks Based on Polynomial and Random Key Predistribution Scheme. *Ad Hoc Netw.* **2017**, *71*, 68–77. [CrossRef]
4. Ribeiro Pinto, J.; Cardoso, J.S.; Lourenco, A. Evolution, current challenges, and future possibilities in ECG Biometrics. *IEEE Access* **2018**, *6*, 34746–34776. [CrossRef]
5. Teodoro, F.G.S.; Peres, S.M.; Lima, C.A.M. Feature selection for biometrie recognition based on electrocardiogram signals. In Proceedings of the 2017 International Joint Conference on Neural Networks (IJCNN), Anchorage, AK, USA, 14–19 May 2017; pp. 2911–2920. [CrossRef]
6. Hejazi, M.; Al-Haddad, S.A.R.; Hashim, S.J.; Aziz, A.F.A.; Singh, Y.P. Non-fiducial based ECG biometric authentication using one-class Support Vector Machine. In Proceedings of the 2017 Signal Processing: Algorithms, Architectures, Arrangements, and Applications (SPA), Poznan, Poland, 7 September 2017; pp. 190–194. [CrossRef]

7. Tobore, I.; Li, J.; Kandwal, A.; Yuhang, L.; Nie, Z.; Wang, L. Statistical and spectral analysis of ECG signal towards achieving non-invasive blood glucose monitoring. *BMC Med. Inform. Decis. Mak.* **2019**, *19*, 266. [CrossRef] [PubMed]
8. Bassiouni, M.M.; El-Dahshan, E.S.A.; Khalefa, W.; Salem, A.M. Intelligent hybrid approaches for human ECG signals identification. *Signal Image Video Process.* **2018**, *12*, 941–949. [CrossRef]
9. Kim, S.K.; Huh, J.H. Artificial neural network blockchain techniques for healthcare system: Focusing on the personal health records. *Electronics* **2020**, *9*, 763. [CrossRef]
10. Al Alkeem, E.; Kim, S.K.; Yeun, C.Y.; Zemerly, M.J.; Poon, K.F.; Gianini, G.; Yoo, P.D. An enhanced electrocardiogram biometric authentication system using machine learning. *IEEE Access* **2019**, *7*, 123069–123075. [CrossRef]
11. Chu, Y.; Shen, H.; Huang, K. ECG Authentication method based on parallel multi-scale one-dimensional residual network with center and margin loss. *IEEE Access* **2019**, *7*, 51598–51607. [CrossRef]
12. Donida Labati, R.; Muñoz, E.; Piuri, V.; Sassi, R.; Scotti, F. Deep-ECG: Convolutional Neural Networks for ECG biometric recognition. *Pattern Recognit. Lett.* **2019**, *126*, 78–85. [CrossRef]
13. Zhao, Z.; Zhang, Y.; Deng, Y.; Zhang, X. ECG authentication system design incorporating a convolutional neural network and generalized S-Transformation. *Comput. Biol. Med.* **2018**, *102*, 168–179. [CrossRef] [PubMed]
14. Zhang, Q.; Zhou, D.; Zeng, X. HeartID: A Multiresolution Convolutional Neural Network for ECG-Based Biometric Human Identification in Smart Health Applications. *IEEE Access* **2017**, *5*, 11805–11816. [CrossRef]
15. Ibtehaz, N.; Chowdhury, M.E.H.; Khandakar, A.; Kiranyaz, S.; Rahman, M.S.; Tahir, A.; Qiblawey, Y.; Rahman, T. EDITH:ECG biometrics aided by Deep learning for reliable Individual auTHentication. *ArXiv* **2021**, *e-prints*. arXiv:2102.08026.
16. Hammad, M.; Wang, K. Parallel score fusion of ECG and fingerprint for human authentication based on convolution. *Comput. Secur.* **2019**, *81*, 107–122. [CrossRef]
17. Rehman, Z.U.; Altaf, S.; Iqbal, S. An Efficient Lightweight Key Agreement and Authentication Scheme for WBAN. *IEEE Access* **2020**, *8*, 175385–175397. [CrossRef]
18. Rehman, Z.U.; Altaf, S.; Iqbal, S. Survey of Authentication Schemes for Health Monitoring: A Subset of Cyber Physical System. In Proceedings of the 2019 16th International Bhurban Conference on Applied Sciences and Technology, IBCAST 2019, Islamabad, Pakistan, 8–12 January 2019; pp. 653–660.
19. Rehman, Z.U.; Altaf, S.; Ahmed, S.; Huda, S.; Al-Shayea, A.M.; Iqbal, S. An Efficient, Hybrid Authentication using ECG and Lightweight Cryptographic Scheme for WBAN. *IEEE Access* **2021**, *9*, 133809–133819. [CrossRef]
20. Salloum, R.; Kuo, C.-C.J. ECG-based biometrics using recurrent neural networks. In Proceedings of the 2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), New Orleans, LA, USA, 5–9 March 2017; pp. 2062–2066.
21. Kim, S.K.; Yeun, C.Y.; Damiani, E.; Lo, N.W. A machine learning framework for biometric authentication using electrocardiogram. *IEEE Access* **2019**, *7*, 94858–94868. [CrossRef]
22. Hosseinzadeh, M.; Vo, B.; Ghafour, M.Y.; Naghipour, S. *Electrocardiogram Signals-Based User Authentication Systems Using Soft Computing Techniques*; Springer: Dordrecht, The Netherlands, 2020; Volume 54, ISBN 0123456789.
23. Aileni, R.M.; Pasca, S.; Florescu, A. EEG-brain activity monitoring and predictive analysis of signals using artificial neural networks. *Sensors* **2020**, *20*, 3346. [CrossRef] [PubMed]
24. Diab, M.O.; Seif, A.; Sabbah, M.; El-Abed, M.; Aloulou, N. A review on ecg-based biometric authentication systems. In *Hidden Biometrics*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 17–44.