




Article

Efficiently Updating ECG-Based Biometric Authentication Based on Incremental Learning

Junmo Kim ^{1,†}, Geunbo Yang ^{1,†}, Juhyeong Kim ¹, Seungmin Lee ², Ko Keun Kim ^{3,*} and Cheolsoo Park ^{1,*}

¹ Department of Computer Engineering, Kwangwoon University, Seoul 01897, Korea; wnsah1008@kw.ac.kr (J.K.); 2016722051@kw.ac.kr (G.Y.); kjoohyu@kw.ac.kr (J.K.)

² School of Electrical Engineering, College of Creative Engineering, Kookmin University, Seoul 02707, Korea; smlee27@kookmin.ac.kr

³ AI Lab, LG Electronics, Seoul 06763, Korea

* Correspondence: kokeun.kim@lge.com (K.K.K.); parkcheolsoo@kw.ac.kr (C.P.)

† These authors contributed equally to this work.

Abstract: Recently, the interest in biometric authentication based on electrocardiograms (ECGs) has increased. Nevertheless, the ECG signal of a person may vary according to factors such as the emotional or physical state, thus hindering authentication. We propose an adaptive ECG-based authentication method that performs incremental learning to identify ECG signals from a subject under a variety of measurement conditions. An incremental support vector machine (SVM) is adopted for authentication implementing incremental learning. We collected ECG signals from 11 subjects during 10 min over six days and used the data from days 1 to 5 for incremental learning, and those from day 6 for testing. The authentication results show that the proposed system consistently reduces the false acceptance rate from 6.49% to 4.39% and increases the true acceptance rate from 61.32% to 87.61% per single ECG wave after incremental learning using data from the five days. In addition, the authentication results tested using data obtained a day after the latest training show the false acceptance rate being within reliable range (3.5–5.33%) and improvement of the true acceptance rate (70.05–87.61%) over five days.

Keywords: ECG; authentication; biometrics; incremental learning; SVM; incremental SVM



Citation: Kim, J.; Yang, G.; Kim, J.; Lee, S.; Kim, K.K.; Park, C. Efficiently Updating ECG-Based Biometric Authentication Based on Incremental Learning. *Sensors* **2021**, *21*, 1568. <https://doi.org/10.3390/s21051568>

Academic Editors: Paddy J. French and Marios Sophocleous

Received: 31 December 2020

Accepted: 12 February 2021

Published: 24 February 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Biometrics has been widely applied in various consumer electronic products such as mobile phones and wearable devices to authenticate users with high performance [1,2]. For example, authentication systems based on fingerprint, iris, and face recognition are replacing passwords, given their reliability with adequate processing speed and better security than traditional authentication methods [3–7]. However, such biometric information is vulnerable to external attacks because common biometric features are physically exposed [8–11].

In contrast, electrocardiogram (ECG) signals, which exhibit unique physiological characteristics across subjects related to the placement and size of the heart, are difficult to spoof because the underlying biometric features are concealed during authentication and can only be obtained from physical measurements on the subject [12–14]. Since Biel et al. [15] first studied using ECG signal processing for the biometric recognition, ECG-based biometric authentication has received great attention as a next-generation promising technique and been implemented with various approaches to improve the authentication performance for the past few decades [16–18]. However, ECG signals of a person may vary according to his/her physical state or health condition, possibly leading to authentication failure in some cases [19–21].

Therefore, it is essential to design a robust method that handles the ECG intrasubject variability for accurate authentication. In order to achieve a reliable authentication result

with the robustness to the non-stationarity of ECG, continuously recording and learning ECG data from the user can be one of the solutions. In this study, we applied incremental learning to efficiently and continuously update the user recognition model after every authentication attempt by the user. To the best of our knowledge, no study has considered incremental learning for ECG-based authentication.

Incremental learning performs continuous training as more input data become available to the existing model for extending its knowledge [22]. In recent years, large amounts of data or the data stream are produced constantly, thus raising the importance of efficiently training these data. The trained model can efficiently learn new patterns embedded in such data with the incremental learning while simultaneously preserving the previous model and preventing performing the retraining process from scratch. The main advantage of this method is that it can reduce the scale of the large size training set in the restricted memory and shorten the training time [23]. Furthermore, a system implementing incremental learning can accumulate knowledge throughout its life cycle. To date, incremental learning has been successfully integrated into various machine learning algorithms such as decision trees, neural networks, and support vector machines (SVMs) [24–28].

We propose a method for ECG-based biometric authentication with incremental learning of features. The method provides continuous training using new ECG signals as they become available and dynamically updates the existing authentication model while maintaining the previous authentication knowledge by implementing an incremental SVM [29].

The rest of this paper is organized as follows. In Section 2, we present the background and related works of ECG authentication and an incremental SVM algorithm for the proposed authentication method. The authentication scheme comprising acquisition and preprocessing of ECG signals, feature extraction, and incremental learning is detailed in Section 3. In Section 4, we report and analyze the experimental results. Section 5 provides a discussion of the proposed method and findings, and we draw conclusions in Section 6.

2. Background and Related Works

2.1. Electrocardiogram

Electrocardiogram, also known as ECG, is the record of electrical activity of the heart including depolarization and repolarization of the atrium and ventricle. ECG is composed of three fiducial entities: P wave, QRS complex, and T wave. The P wave and QRS complex are produced by the depolarization of the atrial and ventricle, respectively, and the T wave is produced by the repolarization of the ventricle. The basic waveform of ECG is shown in Figure 1. The ECG waveform varies from person to person owing to differences in the size and position of the heart, sex, age and other factors. Due to these characteristics, fiducial information such as angle, amplitude and interval of the entities of ECG describes the uniqueness of the individual [30].

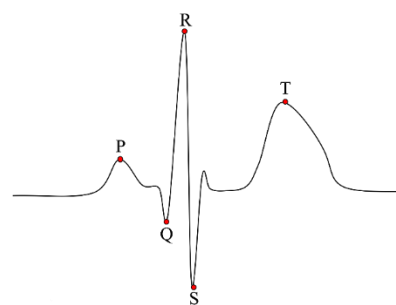


Figure 1. The basic waveform of electrocardiograms (ECG) with five fiducial points.

2.2. Related Works

Table 1 presents several recent works on ECG authentication. Most of the ECG authentication methods used three well-known ECG databases: Physikalisch-Technische

Bundesanstalt (PTB) [31], the Check Your Bio-signals Here initiative (CYBHi) [32] and MIT-BIH [33]. Some of the methods collected ECG data sets by themselves [15,34].

Table 1. Summary of the studies of the ECG-based authentication method. SVM—support vector machine, ACC—accuracy, CNN—convolutional neural network, DWT—discrete wavelet transform, FAR—false acceptance rate, PSD—power spectral density, DCT—discrete cosine transform, PCA—principal component analysis.

| Authors | Database | Feature Extraction | Authentication Model | Performance | |
|--------------------|--------------------|--|----------------------------|-------------|------------------|
| Rezgui et al. [35] | MIT-BIH | 21 Fiducial and 10 morphological descriptors | SVM | ACC: | 98.8% |
| Labati et al. [36] | PTB | CNN | Softmax | ACC: | 100% |
| Juan et al. [20] | PTB self-collected | 8 Fiducial | Template Matching | FAR: | 1.29% 1.41% |
| Choi et al. [37] | MIT-BIH PTB | 8 Fiducial | SVM | ACC: | 95.9% |
| Ergin et al. [38] | MIT-BIH PTB | Fiducial, WT and PSD | Decision tree and BayesNet | F1-score: | 0.972 |
| Hammad et al. [39] | PTB CYBHi | ResNet-Attention | Softmax | ACC: | 98.85% 99.27% |
| Chiu et al. [40] | QT DB [41] | DWT | Euclidean distance | ACC: | 81% |
| Biel et al. [15] | Self-collected | Siemens ECG apparatus | PCA | ACC: | 98% |
| Pinto et al. [42] | Self-collected | DCT | SVM | ACC: | 94.9% |
| Hammad et al. [43] | MIT-BIH | Fiducial | CNN | ACC: | 99% |

The extraction of features from ECG data can be classified into two categories: handcrafted and non-handcrafted. There are various handcrafted techniques for feature extraction such as using fiducial information [44–46], wavelet transform [40,47–49], and discrete cosine transform [42,50]. These approaches involve several processes such as feature normalization or removal of the noise designed by subjective decisions of the researchers. Thus, some researchers have implemented the authentication method with non-handcrafted extraction. With the advent of recent works of deep learning, non-handcrafted and data-driven feature extraction approaches using deep neural networks such as convolutional neural network (CNN) [36,51] or long short-term memory (LSTM) [52] can enable bypassing the additional steps.

Since a single biometric method cannot always guarantee high authentication performance [53], some studies adopted a multimodal-based method in order to provide more stable performance, such as a combination of ECG and fingerprint or photoplethysmography (PPG) [54–56].

2.3. Incremental SVM

The SVM is a supervised machine learning algorithm for classification and regression problems. The SVM classifier is trained using samples belonging to two or more categories and maximizes the margin around a decision boundary. As the SVM has demonstrated high performance without large training data sets, it has been widely used in a variety of applications, such as spam categorization [57], object recognition [58], and cancer localization [59]. However, the SVM training speed decreases rapidly as the size of the data set increases [60,61].

The incremental SVM extends the original SVM formulation to enable online learning while maintaining the previously trained model and efficiently updating it as more input data become available. As new data arrive, the conventional SVM should fully train all the existing data to reflect the latest information in the classifier. In contrast, the incremental SVM is retrained only using the new data, updating the model without complete retraining. Although the classification performance of the incremental SVM is similar to that of the

conventional SVM, the incremental approach is more efficient in terms of training speed and number of floating-point operations during training [62].

The incremental SVM classifier is designed by solving a quadratic program on the Karush–Kuhn–Tucker (KKT) conditions to find the optimal solution:

$$\begin{aligned} \alpha_i = 0 &\rightarrow |f(x_i)| > 1 \\ 0 < \alpha_i < C &\rightarrow |f(x_i)| = 1 \\ \alpha_i = C &\rightarrow |f(x_i)| < 1 \end{aligned} \quad (1)$$

where α_i is the Lagrange multiplier for the constraint of the objective function, $f(x)$ is the optimal separating function, and C is a regularization parameter that decides the degree of fitting to the training samples. If there is any violation of the KKT conditions during each incremental step, the coefficients of the samples change their values for the SVM classifier to keep satisfying the conditions. Hence, new samples are properly learned by the previously trained classifier.

For the proposed ECG-based authentication, we adopted the incremental SVM proposed by Cauwenberghs and Poggio [63]. This SVM manages data in four categories (Figure 2): set U of unlearned vectors that are going to be trained, set R of reserve vectors exceeding the margin, set S of margin support vectors within the margin, and set E of error support vectors violating the margin. During incremental learning, new training samples with $|f(x)| > 1$ (i.e., correctly classified) are assigned directly to set R , as they do not affect the SVM solution. Other samples initially become unlearned vectors in set U and are eventually assigned to set S or E . The KKT conditions must be simultaneously satisfied for all the training samples while integrating the unlearned samples into the SVM solution. The KKT conditions are maintained by modifying the coefficients of the margin vectors, and this process may result in the migration of samples to the other category in binary classification.

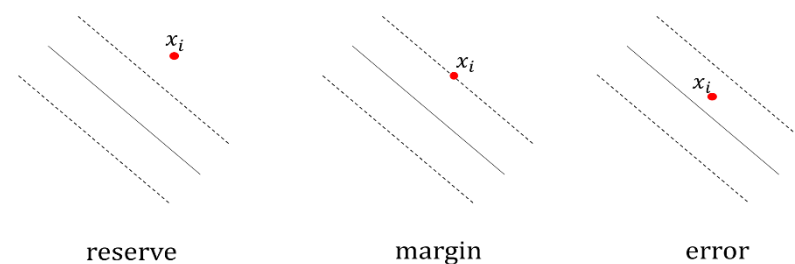


Figure 2. Sample states according to Karush–Kuhn–Tucker (KKT) conditions.

The incremental SVM stores training data because vectors other than the support vectors may become support vectors after the boundary update by incremental learning. As the number of trained samples increases, the memory required to store all the vectors also increases, thus prolonging training. To improve efficiency, the reserve vectors that are far from the decision boundary, and thus less likely to shift to the other category, may be discarded.

3. Proposed ECG-Based Authentication

The proposed authentication method and its evaluation are illustrated in Figure 3 and comprise acquisition and preprocessing of ECG signals, feature extraction, incremental learning, and performance evaluation.

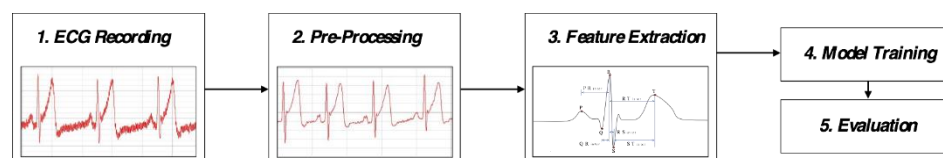


Figure 3. Scheme to implement and evaluate the proposed ECG-based authentication.

3.1. ECG Signal Acquisition and Preprocessing

We recorded single-channel ECG signals from 11 male subjects aged from 22 to 42 for 10 min over six days. This experiment was conducted after obtaining the consent of all subjects and approved by Institutional Review Board (IRB). The recording and reference channels were placed on the left and right arms and the ground channel on the left ankle of the subject, forming the Einthoven's triangle. The subject sat on a chair without moving during the ECG measurements. The MP36 system (Biopac Systems, Goleta, CA, USA) was used for the acquisition of the ECG signals at a sampling frequency of 1000 Hz. As the pre-processing step, we applied low-pass and high-pass filters to set a finite-impulse-response bandpass filter of order 5383 between 1 and 35 Hz [39,43,64] for the elimination of the baseline drift and high frequency noise.

The synchronized average of the ECG signals from each of the 11 subjects is shown in Figure 4, showing unique features in the ECG signals. Figure 5 illustrates the variation of the daily ECG waveform of the subject 10 for six days. Furthermore, the average root-mean-square error of ECG from days 2 to 6 with respect to the ECG of day 1 is presented in Table 2, showing the difference between the ECG of day 1 and those of days 2 to 6.

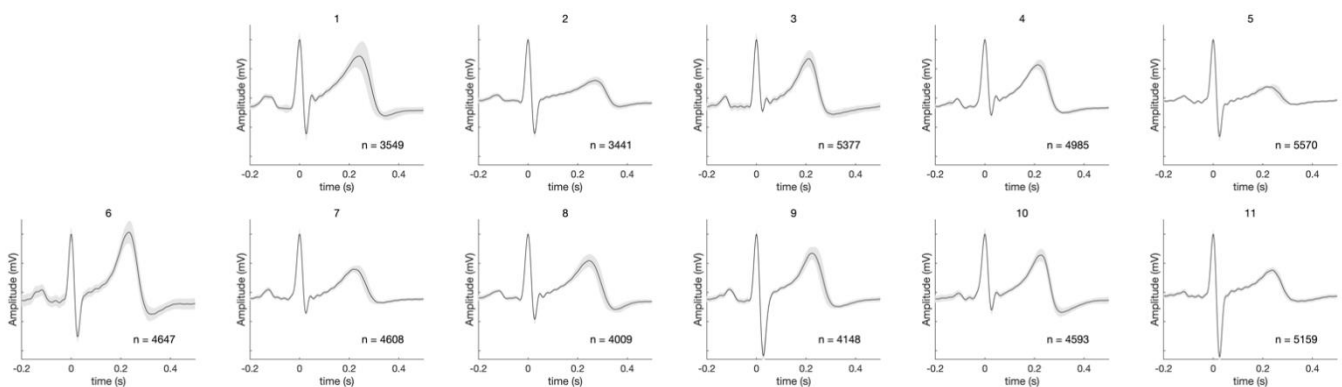


Figure 4. Synchronized average of ECG signals from 11 subjects. The shaded areas represent the standard deviation in the signals.

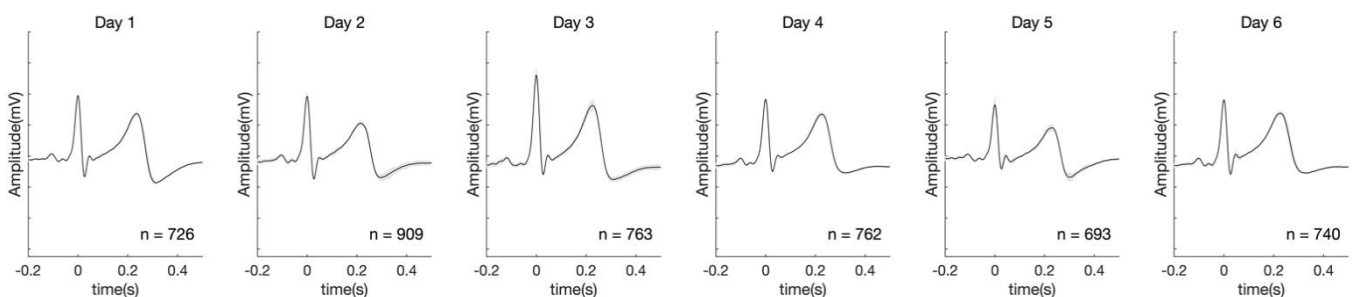


Figure 5. Synchronized average of ECG signals of the subject 10 for six days. The shaded areas represent the standard deviation in the signals.

Table 2. The average root-mean-square error of the ECG from day 2 to day 6 with respect to the ECG of day 1.

| RMSE | Day 2 | Day 3 | Day 4 | Day 5 | Day 6 |
|------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|
| | 0.12346 ± 0.06493 | 0.15085 ± 0.09276 | 0.16848 ± 0.07744 | 0.25785 ± 0.30352 | 0.20714 ± 0.14167 |

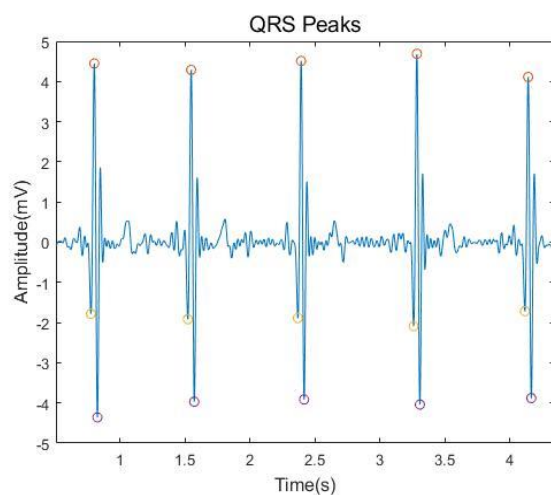
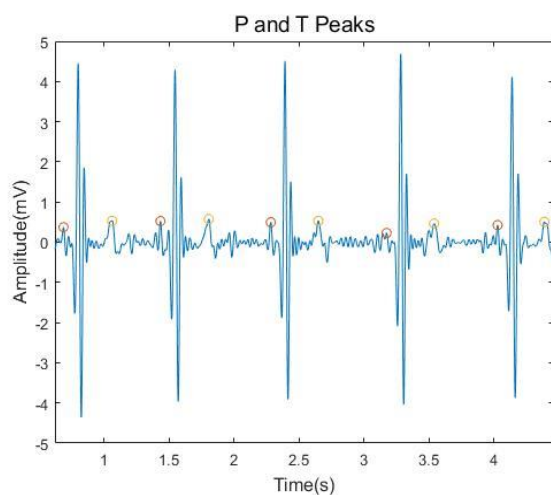
3.2. Feature Extraction

Typically, an ECG wave shows five fiducial points: P, Q, R, S and T peaks. Different combinations of peak patterns can be used as features to distinguish ECG data across subjects. Figures 6 and 7 depict the peak detections of the QRS complex and P and T peaks. To automatically detect the Q, R, and S peaks, we used the real-time QRS detection algorithm proposed by Pan and Tompkins [65]. In addition, we separately extracted the P and T peaks by searching the maxima within

$$R_{loc} - \frac{RR_{int}}{6} < P_{loc} < R_{loc} - \frac{RR_{int}}{10}, \quad (2)$$

$$R_{loc} + \frac{RR_{int}}{10} < T_{loc} < R_{loc} + \frac{RR_{int}}{2} \quad (3)$$

where RR_{int} is the average length of RR interval, R_{loc} , P_{loc} and T_{loc} are the locations of R, P and T peak, respectively [66,67].

**Figure 6.** Detected Q, R and S peaks of an ECG signal.**Figure 7.** Detected P and T peaks of an ECG signal.

After the detection of five peaks, we extracted 13 features per ECG wave including three angles, four amplitudes, and six temporal features, which are illustrated in Figure 8: PR, QR, RS, RT amplitudes, PR, QR, RS, RT, ST, RR intervals, and angles of Q, R and S peaks [68].

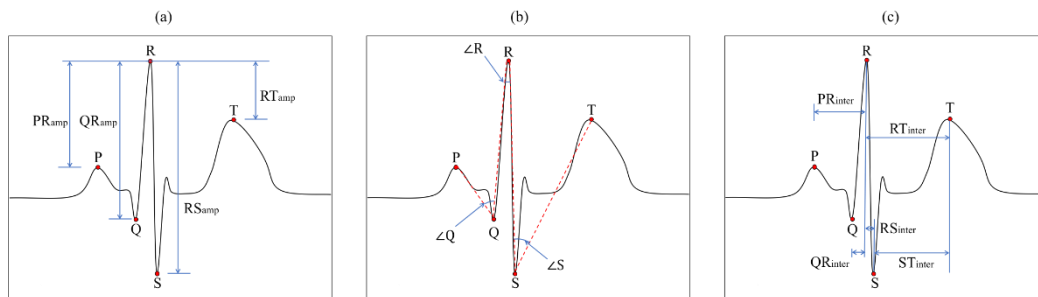


Figure 8. ECG features for the authentication: four amplitudes (a), three angles (b), and six temporal features (c) including RR interval.

3.3. Incremental Learning

In order to train the authentication model per subject, we obtained 11 initial incremental SVM classifiers that were designed using the corresponding training set of day 1. As the data set consisted of the authentication target (positive class) and 10 imposters (negative class), there was an imbalance between two classes, which degraded the authentication performance. In order to overcome this problem, the data augmentation for the positive class was conducted using the synthetic minority over-sampling technique (SMOTE) algorithm [69] in order to solve the imbalance. Each authentication model performs binary classification, either recognizing the target user's ECG data or not.

After initial training, we used the data from days 2 to 5 for incremental learning. During this learning process, each training sample was evaluated by the existing SVM model to check its classification correctness. If the sample was positively classified, it became a reserve vector and the training terminated. Otherwise, margin vector coefficients were changed to maintain the KKT conditions in response to the perturbation induced by the misclassified sample. Then, the sample became either a margin vector or an error vector. After learning data incrementally, new information could be integrated into the existing SVM model without fully retraining on the complete training set.

3.4. Performance Measures

We used various evaluation measures to determine the authentication performance based on the true positives TP , false positives FP , true negatives TN , and false negatives FN . The true positives (true negatives) indicated the number of positive (negative) samples that were classified correctly. The false positives (false negatives) indicated the number of positive (negative) samples that were misclassified.

Specifically, we used three widely used evaluation measures, namely, accuracy ACC , false acceptance rate (FAR), and true acceptance rate (TAR):

$$ACC = \frac{TP + TN}{TP + TN + FP + FN} \quad (4)$$

$$FAR = \frac{FP}{TN + FP} \quad (5)$$

$$TAR = \frac{TP}{TP + FN} \quad (6)$$

where FAR reflected the incorrectly accepted attempts by an adversary, and TAR reflected the correctly accepted attempts by the authentication target.

4. Results

In this section, we designed two different evaluation schemes and tested our proposed ECG-based authentication algorithm, evaluated by using the data of day 6 and data recorded a day after the latest update as the test set. The evaluation based on the data of day 6 was conducted to compare the proposed algorithm with the conventional SVM. As this evaluation result could be affected by the data-to-data similarities, meaning the day 5 recordings would be more similar to the day 6 data than those of the day 1, we designed another experiment based on the latest available data to demonstrate the effectiveness of the incremental learning. In each evaluation, the test set consisted of data corresponding to one authentication target and 10 imposters (i.e., data from the other subjects). The evaluation proceeded until the classification of every single beat of the test set terminated. This process was repeated until the data from every subject were classified against those of all the other subjects. We evaluated the authentication method by an implementation on MathWorks MATLAB R2019b running on a Mac OS X 10.15 computer with Intel Core i7 CPU at 2.9 GHz and 16 GB memory.

In this paper, we used the radial basis function (RBF) as kernel function of the SVM, as it outperforms other kernel functions [70]. The hyperparameters of the SVM are box constraint C and kernel scale σ . The optimal hyperparameters should be determined before training the model to obtain the best performance. The search for the optimized values of the hyperparameters was conducted using Bayesian optimization, which was applied to the data recorded on day 1. This provided the optimal values of the hyperparameters as $C = 7$ and $\sigma = 2$, which are depicted in Figure 9 [71].

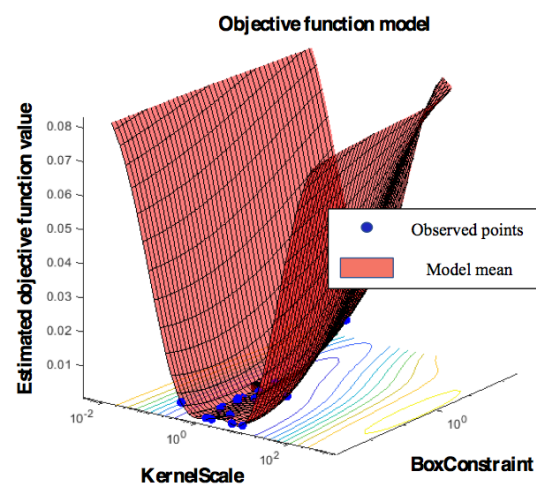


Figure 9. Objective function values for hyperparameter tuning using Bayesian optimizer. The optimal SVM parameters are $C = 7$ (box constraint) and $\sigma = 2$ (kernel scale).

To visualize the updating decision boundary of the incremental SVM as more data became available, the two most representative features obtained from the ReliefF algorithm [72] (i.e., angle of S and RR interval) and the corresponding decision boundaries for subject 4 are depicted in Figure 10. The decision boundaries changed as incremental learning proceeded. As the incremental SVM integrated new data, the support vectors that defined the classification boundary were updated by varying their coefficients to maintain the KKT conditions.

Figure 11 shows the individual performance (a) and the average performance (b) evaluated using the data of day 6 in terms of the accuracy, FAR, and TAR of every subject over the five-day incremental learning. The initial classifier trained using the data of day 1 achieved 90.62% accuracy, 6.49% FAR and 61.32% TAR, on average. As the SVM classifier learned data incrementally on the other days, the authentication result showed enhanced performance: the accuracy increased to 95.1%, TAR increased to 87.61% and FAR decreased to 4.39%.

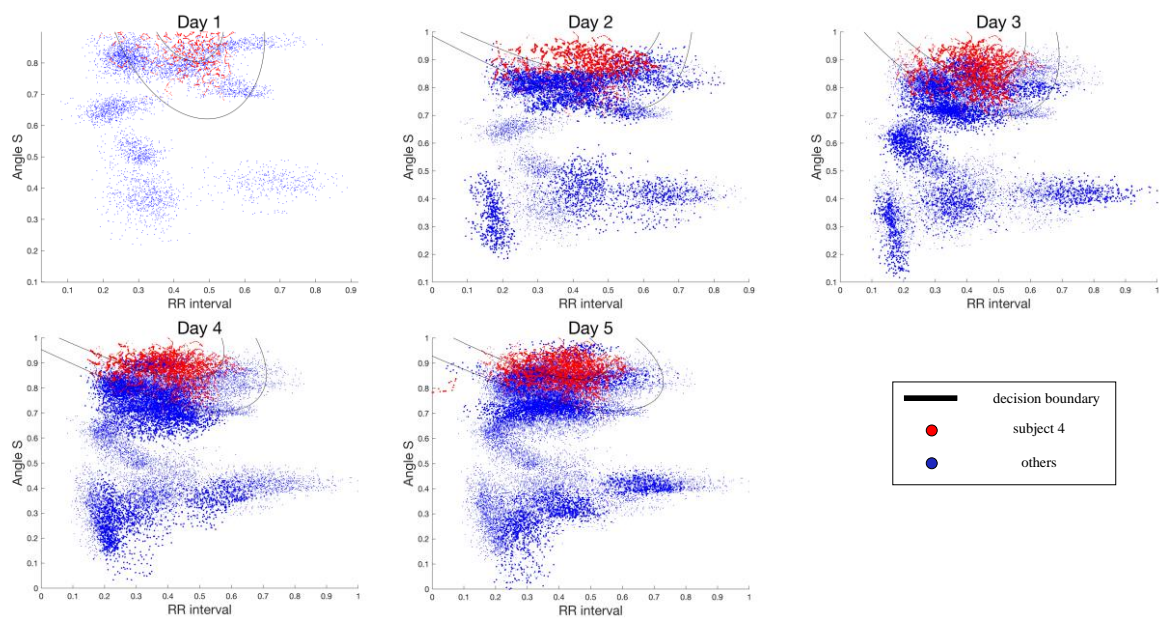


Figure 10. Updating decision boundary of incremental SVM for subject 4 data set over five-day incremental learning. The darker dots from days 2 to 5 represent the incrementally trained data.

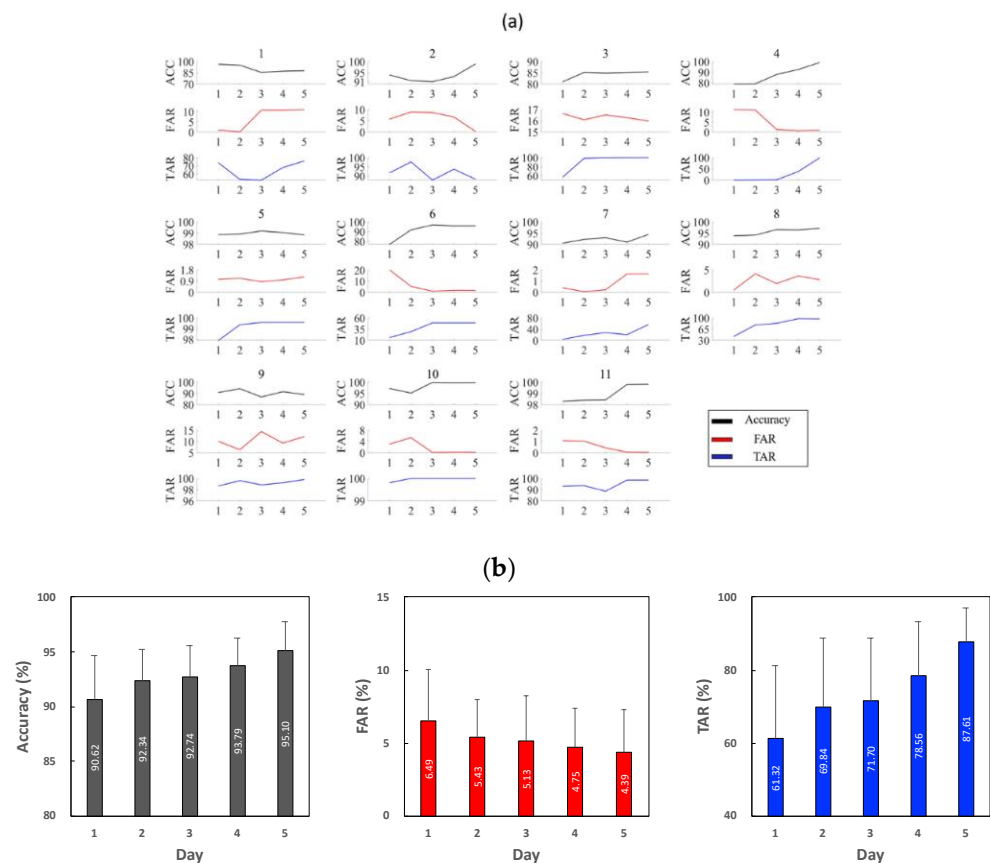


Figure 11. The accuracy, false acceptance rate (FAR) and true acceptance rate (TAR) of 11 subjects over five days of incremental learning (a) and the average (b) tested using the data of day 6.

The experiment result over the five-day incremental learning as evaluated using the data recorded a day after the latest training is presented in Figure 12. Although there was a slight decrease of the performance when the evaluation was conducted using the data of

day 5, the average accuracy across all subjects increased from 92.25% to 95.1%. The average TAR also gradually increased from 70.05% to 87.61%. The average FAR decreased from 5.33% to 3.5% until day 3, which was evaluated using the data of day 4. Then it slightly increased from 3.5% to 4.39% until the last incremental update.

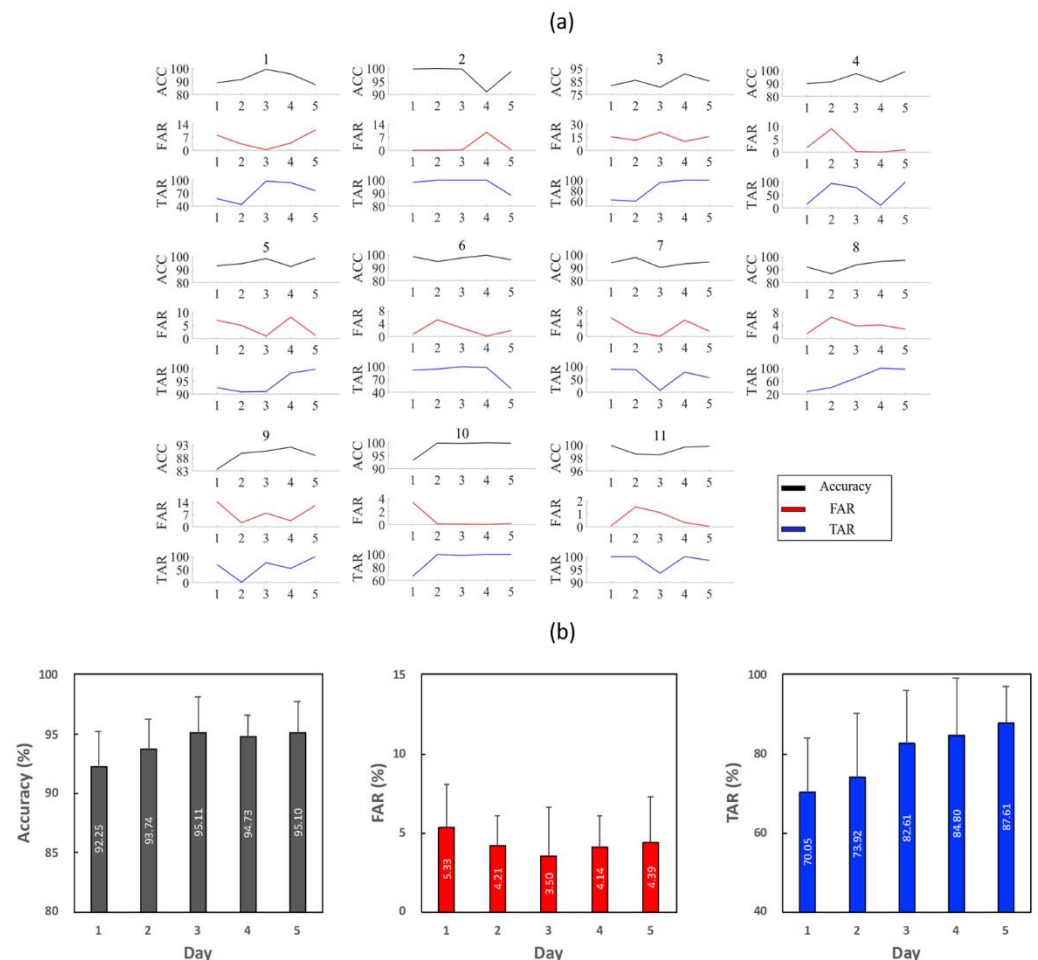


Figure 12. The accuracy, FAR and TAR of 11 subjects over five days of incremental learning (a) and the average (b) tested using the data recorded a day after the latest training.

5. Discussion

In Figure 12b, note that in terms of accuracy the authentication performance of FAR and TAR increased after the five days incremental learning. However, the accuracy slightly decreased when the evaluation was conducted using the data of day 5, and FAR increased about 0.89% from day 3 (tested using the data of day 4) to day 5 (tested using the data of day 6). Additionally, as seen in both Figures 11a and 12a, some subjects had a minor decrease of authentication performance after training new ECG data incrementally. Since the pattern of the ECG signal could vary, depending on various reasons such as the emotional or physical conditions of the authentication target user, the pattern of the evaluated data might have been slightly different from the trained ones, resulting in the deterioration in the authentication performance. Nevertheless, FAR remained between 3% and 6% during the total training process, which indicated the model was still stable and reliable for the authentication task [73].

For a benchmark test, we compared the incremental SVM and the original SVM with full training in terms of the authentication performance and the training efficiency. Both SVMs with the RBF kernel were trained by the data of days 1 to 5 using the same hyperparameters described in Figure 9 (i.e., $C = 7$, $\sigma = 2$). The evaluation results tested using the data of day 6 are illustrated in Figure 13, showing that the accuracy of the incremental

SVM was comparable with that of the fully trained SVM (95.1% and 95.12%). Likewise, FAR and TAR were similar between incremental learning and fully training methods: 4.39% and 4.4% FAR, 87.61% and 87.98% TAR, respectively.

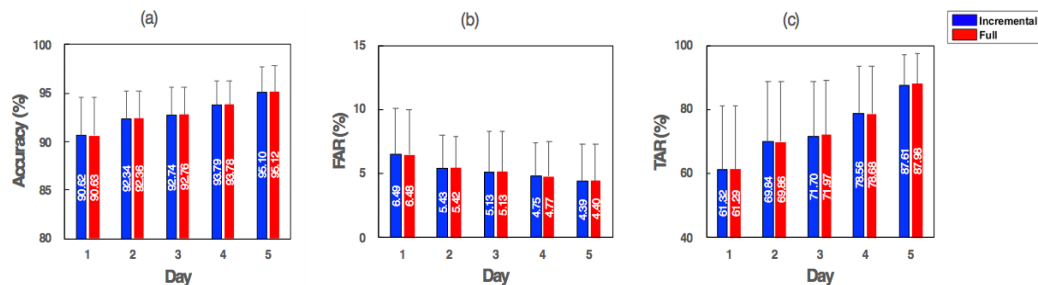


Figure 13. The result of the benchmark test with the incremental learning and full training in terms of (a) the accuracy, (b) FAR and (c) TAR.

Table 3 lists the training time of the incremental SVM and the original SVM. The training time was obtained while varying the number of arriving samples. Overall, incremental learning provided a much faster training than the fully training method. Specifically, incremental learning required 0.102–0.714 s to integrate one new sample, whereas the fully trained one required 0.713–3.294 s. When adding 100 new samples, the incremental training required 13.015–35.133 s and the other required 82.799–401.554 s for their computations. The training time across all subjects differed slightly in both methods since the SVM models had different numbers of the margin vectors and the error vectors and the training time of the SVM depended on the number of those vectors [29,61]. Table 3 shows that the difference in the training time between the two learning approaches increased as the number of new data increased. To integrate new information into the existing SVM model, the original SVM should repeat training using all the available data. On the other hand, the incremental SVM only modifies the coefficients of the margin vectors if an arriving sample is misclassified, thus reducing the training time efficiently.

Table 3. Training time (s) using the incremental learning and full training while varying the number of arriving samples.

| Subject | Incremental Learning | | | Full Training | | |
|---------|----------------------|------------|-------------|---------------|------------|-------------|
| | 1 Sample | 10 Samples | 100 Samples | 1 Sample | 10 Samples | 100 Samples |
| 1 | 0.541 | 3.995 | 27.184 | 2.022 | 20.279 | 241.554 |
| 2 | 0.630 | 3.233 | 25.382 | 0.713 | 7.101 | 82.799 |
| 3 | 0.213 | 3.320 | 17.190 | 2.570 | 25.502 | 322.653 |
| 4 | 0.367 | 5.661 | 35.133 | 1.225 | 12.762 | 192.827 |
| 5 | 0.289 | 4.347 | 34.006 | 1.901 | 18.343 | 229.996 |
| 6 | 0.234 | 2.116 | 13.015 | 1.306 | 13.181 | 161.457 |
| 7 | 0.252 | 3.208 | 26.130 | 2.185 | 21.436 | 262.371 |
| 8 | 0.102 | 2.332 | 20.584 | 1.497 | 15.139 | 187.970 |
| 9 | 0.156 | 1.994 | 17.990 | 3.294 | 31.457 | 401.554 |
| 10 | 0.610 | 4.711 | 28.913 | 0.951 | 9.294 | 107.644 |
| 11 | 0.714 | 3.381 | 21.442 | 1.120 | 9.227 | 113.987 |

In addition, the authentication method using the template update [74] was implemented and evaluated, which was similar to the proposed algorithm in terms of the continuous learning process. The evaluation was conducted by using the data obtained a day after the latest training as the test set. Figure 14 presents the comparison of FAR between the two methods, showing that our proposed algorithm obtained better performance than that using the template. Furthermore, as the model trained more data, the method using the template update had a problem of forgetting previous knowledge. However,

incremental SVM maintained its knowledge by categorizing all training vectors in reserve, margin, or error sets.

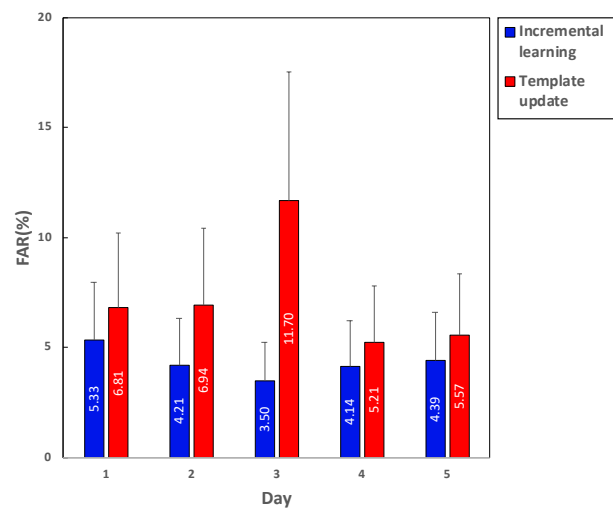


Figure 14. The result of the benchmark test with the incremental learning and template update in terms of FAR.

Figure 15 shows the results of the proposed method and previous works [35,39] on ECG authentication using MIT-BIH and CYBHi databases. Using MIT-BIH, the proposed method obtained 97.7% accuracy, which was comparable (only 1% lower) with [35], although our method used seven fewer features. Furthermore, the proposed method yielded an accuracy of 99.4% using CYBHi, an almost identical performance with [39] (0.1% higher).

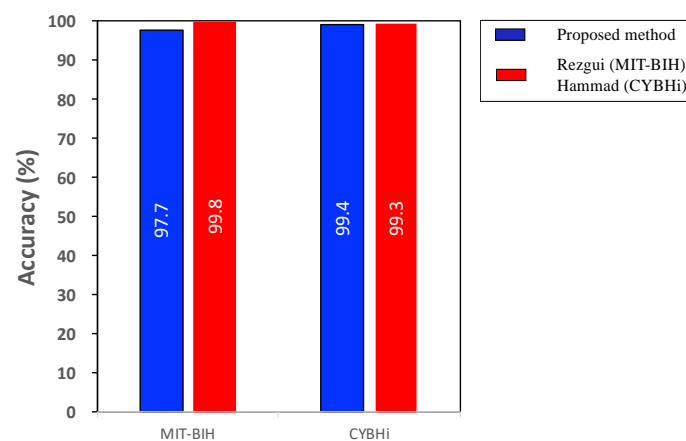


Figure 15. The evaluation result of the proposed method using MIT-BIH and Check Your Bio-signals Here initiative (CYBHi) databases. The experiment using MIT-BIH is compared with [35] and the other using CYBHi with [39].

Table 4 details the training information of the authentication models, including the average number of training data samples, the proportions between the two classes (authentication target vs. others), and the training time of the incremental SVM per day. Although the number of arriving samples was similar over the five days, the training time significantly increased as more data became available and was stored, given the time required to calculate the kernel matrix of all the data [75]. Furthermore, the more data the incremental SVM learned, the more memory the authentication model occupied. Thus, our further work will focus on reducing the training time and memory by discarding some reserve vectors that are far from the decision boundary of SVM classifier.

Table 4. Averaged characteristics of training data and training time of the incremental learning. R, S, and E indicate the number of reserve vectors, margin support vectors, and error support vectors, respectively.

| Day | Positive (%) | Negative (%) | Total | Training Time (s) | R | S | E |
|-----|---------------|---------------|---------------|-------------------|---------------|---------|-------------|
| 1 | 51.79 ± 6.2 | 48.21 ± 6.2 | 10,930 ± 1142 | 85.867 ± 25.6 | 10,348 ± 1059 | 37 ± 16 | 544 ± 420 |
| 2 | 51.14 ± 10.3 | 48.86 ± 10.3 | 10,525 ± 1408 | 157.070 ± 92.2 | 19,966 ± 1891 | 50 ± 23 | 1438 ± 1155 |
| 3 | 52.03 ± 4.65 | 47.97 ± 4.65 | 10,893 ± 914 | 344.520 ± 263.3 | 29,739 ± 2325 | 62 ± 33 | 2546 ± 1966 |
| 4 | 52.21 ± 3.19 | 47.79 ± 3.19 | 11,752 ± 653 | 525.066 ± 412.5 | 40,396 ± 2934 | 81 ± 28 | 3623 ± 2757 |
| 5 | 50.30 ± 14.49 | 49.70 ± 14.49 | 10,254 ± 1660 | 569.601 ± 582.5 | 49,808 ± 4057 | 85 ± 33 | 4461 ± 3367 |

6. Conclusions

We proposed an ECG-based authentication method providing incremental learning from arriving ECG data as they became available. The proposed algorithm was compared with the conventional ones, the original SVM and template update method. Compared to the original SVM, the proposed algorithm yielded almost identical performance with much a faster training process. In addition, it was demonstrated that the conventional continuous learning algorithm, the template update method, was outperformed by the proposed incremental learning approach. The proposed method was also compared with the previous studies on ECG authentication using MIT-BIH and CYBHi databases. The proposed algorithm achieved an accuracy of 97.7% and 99.4% using MIT-BIH and CYBHi, respectively, showing that the method could be as reliable as the others. We showed that our proposed algorithm could be reliable authentication method in terms of FAR and TAR, with the advantage of training new data incrementally. To the best of our knowledge, this is the first ECG-based authentication method implementing incremental learning, which is suitable to applications with data accumulation.

Author Contributions: Conceptualization, J.K. (Junmo Kim) and G.Y.; software, J.K. (Juhyeong Kim); validation, J.K. (Junmo Kim) and G.Y.; formal analysis, J.K. (Junmo Kim); resources, J.K. (Junmo Kim) and G.Y.; writing—original draft preparation, J.K. (Junmo Kim); writing—review and editing, J.K. (Junmo Kim), G.Y. and C.P.; supervision, C.P. and K.K.K.; project administration, S.L. and C.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by an Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korean Government (MSIT) (No.2019-0-00426, Development of active kill-switch and biomarker-based defense system for life-threatening IoT medical devices).

Institutional Review Board Statement: The study was conducted according to the guidelines of the Declaration of Helsinki, and approved by the Institutional Review Board of Kwangwoon University (IRB No. 7001546-20200102-HR(SB)-001-03, 17 Jan 2020).

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: The data are not publicly available due to ethical.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

1. Frischholz, R.W.; Dieckmann, U. BioID: A multimodal biometric identification system. *Computer* **2000**, *33*, 64–68. [[CrossRef](#)]
2. Hou, D.; Hou, R.; Hou, J. ECG Beat Classification on Edge Device. In Proceedings of the 2020 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 4–6 January 2020; pp. 1–4.
3. Holder, J.R.E.H.; Robinson, L.O.; Laub, J.H. *The Fingerprint Sourcebook*; Dept. Justice, Office Justice Programs, Nat. Inst. Justice: Washington, DC, USA, 2011.
4. Prabhakar, S.; Pankanti, S.; Jain, A.K. Biometric recognition: Security and privacy concerns. *IEEE Secur. Priv. Mag. Mar.* **2003**, *1*, 33–42. [[CrossRef](#)]
5. Ross, A.; Jain, A.K. Human recognition using biometrics: An overview. *Ann. Télécommun. Jan.* **2007**, *62*, 11–35.
6. Jang, Y.J.; Noh, H.K.; Kim, B.; Sim, J.Y.; Park, H.J. An Ultrasonic Scanner to Probe 3-D Finger Skin Structures for Biometric Recognition. *IEIE Trans.* **2019**, *8*, 161–169. [[CrossRef](#)]
7. Ponnusamy, V.; Sridhar, A.; Baalajji, A.; Sangeetha, M. A Palm Vein Recognition System based on a Support Vector Machine. *IEIE Trans.* **2019**, *8*. [[CrossRef](#)]
8. Zhang, Y.; Xia, P.; Luo, J.; Ling, Z.; Liu, B.; Fu, X. Fingerprint attack against touch enabled devices. *Proc. SPSM* **2012**, *12*, 57–68.
9. Duc, N.M.; Minh, B.Q. Your face is not your password. *Black Hat.* **2009**, *4*, 158.
10. Li, Y.; Xu, K.; Yan, Q.; Li, Y.; Deng, R.H. Understanding OSN based facial disclosure against face authentication systems. *Proc. AS ACCS* **2014**, *14*, 413–424.
11. Ruiz-Albacete, S.V.; Tome-Gonzalez, P.; Alonso-Fernandez, F.; Galbally, J.; Fierrez, J.; Ortega-Garcia, J. Direct Attacks Using Fake Images in Iris Verification. In *Biometrics and Identity Management*; Springer: Berlin/Heidelberg, Germany, 2008; pp. 181–190.
12. Israel, S.A.; Irvine, J.M.; Cheng, A.; Wiederhold, M.D.; Wiederhold, B.K. ECG to identify individuals. *Pattern Recognit.* **2005**, *38*, 133–142. [[CrossRef](#)]
13. Fatemian, S.Z.; Hatzinakos, D. A new ECG feature extractor for biometric recognition. In Proceedings of the 2009 16th International Conference on Digital Signal Processing, Santorini, Greece, 5–7 July 2009; pp. 1–6.
14. Hoekema, R.; Gérard, G.J.; Van Oosterom, A. Geometrical aspects of the interindividual variability of multilead ECG recordings. *IEEE Trans. Biomed. Eng.* **2001**, *48*, 551–559. [[CrossRef](#)]
15. Biel, L.; Pettersson, O.; Philipson, L.; Wide, P. ECG analysis: A new approach in human identification. *IEEE Trans. Instrum. Meas.* **2001**, *50*, 808–812. [[CrossRef](#)]
16. Carreiras, C.; Lourenço, A.; Fred, A.; Ferreira, R. ECG signals for biometric applications—Are we there yet? In Proceedings of the 2014 11th International Conference on Informatics in Control, Automation and Robotics (ICINCO), Vienna, Austria, 1–3 September 2014; Volume 2, pp. 765–772.
17. Hammad, M.; Luo, G.; Wang, K. Cancelable biometric authentication system based on ECG. *Multimed. Tools Appl.* **2018**, *12*, 1–31. [[CrossRef](#)]
18. Li, R.; Yang, G.; Wang, K.; Huang, Y.; Yuan, F.; Yin, Y. Robust ECG biometrics using GNMF and sparse representation. *Pattern Recognit. Lett.* **2020**, *129*, 70–76. [[CrossRef](#)]
19. Odinaka, I.; Lai, P.; Kaplan, A.D.; O’Sullivan, J.A.; Sirevaag, E.J.; Rohrbaugh, J.W. ECG Biometric Recognition: A Comparative Analysis. *IEEE Trans. Inf. Forensics Secur.* **2012**, *7*, 1812–1824. [[CrossRef](#)]
20. Arteaga-Falconi, J.S.; Al Osman, H.; El Saddik, A. ECG authentication for mobile devices. *IEEE Trans. Instrum. Meas.* **2016**, *65*, 591–600. [[CrossRef](#)]
21. Samona, Y.; Pintavirooj, C.; Visitsattapongse, S. Study of ECG variation in daily activity. In Proceedings of the 2017 10th Biomedical Engineering International Conference (BMEiCON), Hokkaido, Japan, 31 August–2 September 2017; pp. 1–5.
22. Gepperth, A.; Hammer, B. Incremental learning algorithms and applications. *Eur. Symp. Artif. Neural Netw.* **2016**, *1*, 1–13.
23. Xu, J.; Xu, C.; Zou, B.; Tang, Y.Y.; Peng, J.; You, X. New Incremental Learning Algorithm with Support Vector Machines. *IEEE Trans. Syst. Man Cybern. Syst.* **2019**, *49*, 2230–2241. [[CrossRef](#)]
24. Utgoff, P.E. Incremental induction of decision trees. *Mach. Learn.* **1989**, *4*, 161–186. [[CrossRef](#)]
25. Falcari, T.; Saotome, O.; Pires, R.; Campo, A.B. Evaluation of multi-class support-vector machines strategies and kernel adjustment levels in hand posture recognition by analyzing sEMG signals acquired from a wearable device. *Biomed. Eng. Lett.* **2020**, *10*, 275–284. [[CrossRef](#)]
26. Huang, M.L.; Wu, Y.S. Classification of atrial fibrillation and normal sinus rhythm based on convolutional neural network. *Biomed. Eng. Lett.* **2020**, *10*, 183–193. [[CrossRef](#)]
27. Xiao, R.; Wang, J.; Zhang, F. An approach to incremental SVM learning algorithm. In Proceedings of the 12th IEEE International Conference on Tools with Artificial Intelligence. ICTAI 2000, Vancouver, BC, Canada, 15 November 2000; pp. 268–278.
28. Polikar, R.; Upda, L.; Upda, S.S.; Honavar, V. Learn++: An incremental learning algorithm for supervised neural networks. *IEEE Trans. Syst. Man Cybern. C.* **2001**, *31*, 497–508. [[CrossRef](#)]
29. Diehl, C.P.; Cauwenberghs, G. SVM incremental learning, adaptation and optimization. *Proc. Int. Jt. Conf. Neural Netw.* **2003**, *4*, 2685–2690.
30. Lugovaya, T. Biometric Human Identification Based on Electrocardiogram. Master’s Thesis, Faculty of Computing Technologies and Informatics, Electrotechnical University “LETI”, Saint-Petersburg, Russia, 2005.
31. Bousseljot, R.; Kreiseler, D.; Schnabel, A. Nutzung der EKG-Signaldatenbank CARDIODAT der PTB über das Internet. *Biomed. Tech.* **1995**, *1*, S317. [[CrossRef](#)]

32. Da Silva, H.P.; Lourenço, A.; Fred, A.; Raposo, N.; Aires-deSousa, M. Check your biosignals here: A new dataset for off-the-person ECG biometrics. *Comput. Methods Programs Biomed.* **2014**, *113*, 503–514. [[CrossRef](#)]
33. Goldberger, A.L.; Amaral, L.A.; Glass, L.; Hausdorff, J.M.; Ivanov, P.C.; Mark, R.G.; Mietus, J.E.; Moody, G.B.; Peng, C.K.; Stanley, H.E. Physiobank physiotoolkit and physionet: Components of a new research resource for complex physiologic signals. *Circulation* **2000**, *101*, e215–e220. [[CrossRef](#)]
34. Chan, A.D.C.; Hamdy, M.M.; Badre, A.; Badee, V. Wavelet Distance Measure for Person Identification Using Electrocardiograms. *IEEE Trans. Instrum. Meas.* **2008**, *57*, 248–253. [[CrossRef](#)]
35. Rezgui, D.; Lachiri, Z. ECG biometric recognition using SVM-based approach. *IEE J. Trans. Electric. Electron. Eng.* **2016**, *11*, S94–S100. [[CrossRef](#)]
36. Labati, R.D.; Muñoz, E.; Piuri, V.; Sassi, R.; Scotti, F. Deep-ECG: Convolutional neural networks for ECG biometric recognition. *Pattern Recognit. Lett.* **2018**, *126*, 78–85. [[CrossRef](#)]
37. Choi, H.S.; Lee, B.H.; Yoon, S.R. Biometric authentication using noisy electrocardiograms acquired by mobile sensors. *IEEE Access* **2016**, *4*, 1266–1273. [[CrossRef](#)]
38. Ergin, S.; Uysal, A.K.; Gunal, E.S.; Gunal, S.; Gulmezoglu, M.B. ECG based biometric authentication using ensemble of features. In Proceedings of the 2014 9th Iberian Conference on Information Systems and Technologies (CISTI), Barcelona, Spain, 18–21 June 2014; pp. 1–6.
39. Hammad, M.; Pławiak, P.; Wang, K.; Acharya, U.R. ResNet-Attention model for human authentication using ECG signals. *Expert Syst.* **2020**, *10*, e12547. [[CrossRef](#)]
40. Chiu, C.C.; Chuang, C.M.; Hsu, C.Y. A Novel Personal Identity Verification Approach Using a Discrete Wavelet Transform of the ECG Signal. In Proceeding of the International Conference on Multimedia and Ubiquitous Engineering (MUE 2008), Busan, Korea, 24–26 April 2008; pp. 201–206.
41. Laguna, P.; Mark, R.G.; Goldberg, A.; Moody, G.B. A database for evaluation of algorithms for measurement of QT and other waveform intervals in the ECG. In Proceedings of the IEEE Computers in Cardiology, Lund, Sweden, 7–10 September 1997; pp. 673–676.
42. Pinto, J.R.; Cardoso, J.S.; Lourenço, A.; Carreiras, C. Towards a continuous biometric system based on ECG signals acquired on the steering wheel. *Sensors* **2017**, *17*, 2228. [[CrossRef](#)] [[PubMed](#)]
43. Hammad, M.; Zhang, S.; Wang, K. A novel two-dimensional ECG feature extraction and classification algorithm based on convolution neural network for human authentication. *Future Gener. Comput. Syst.* **2019**, *101*, 180–196. [[CrossRef](#)]
44. Liu, J.; Yin, L.; He, C.; Wen, B.; Hong, X.; Li, Y. Amultiscale autoregressive model-based electrocardiogram identification method. *IEEE Access.* **2018**, *6*, 18251–18263. [[CrossRef](#)]
45. Krasteva, V.; Jekova, I.; Abächerli, R. Biometric verification by cross-correlation analysis of 12-lead ECG patterns: Ranking of the most reliable peripheral and chest leads. *J. Electrocardiol.* **2017**, *50*, 847–854. [[CrossRef](#)] [[PubMed](#)]
46. Hammad, M.; Ibrahim, M.; Hadhoud, M. A novel biometric based on ECG signals and images for human authentication. *Int. Arab J. Inf. Technol.* **2016**, *13*, 959–964.
47. Karimian, N.; Guo, Z.M.; Tehranipoor, M.; Forte, D. Highly Reliable Key Generation from Electrocardiogram (ECG). *IEEE Trans. Biomed. Eng.* **2017**, *64*, 1400–1411. [[CrossRef](#)]
48. Tan, R.; Perkowski, M. Toward Improving Electrocardiogram (ECG) Biometric Verification using Mobile Sensors: A Two-Stage Classifier Approach. *Sensors* **2017**, *17*, 410. [[CrossRef](#)]
49. Pathoumvanh, S.; Airphaiboon, S.; Hamamoto, K. Robustness study of ECG biometric identification in heart rate variability conditions. *IEEJ Trans. Electron. Eng.* **2014**, *9*, 294–301. [[CrossRef](#)]
50. Kalai Zaghoulani, E.; Benzina, A.; Attia, R. ECG based authentication for e-healthcare systems: Towards a secured ECG features transmission. In Proceedings of the 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), Valencia, Spain, 26–30 June 2017; pp. 1777–1783.
51. Luz, E.J.D.S.; Moreira, G.J.P.; Oliveira, L.S.; Schwartz, W.R.; Menotti, D. Learning deep off-the-person heart biometrics representations. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 1258–1270.
52. Lynn, H.M.; Pan, S.B.; Kim, P. A Deep Bidirectional GRU Network Model for Biometric Electrocardiogram Classification Based on Recurrent Neural Networks. *IEEE Access* **2019**, *7*, 145395–145405. [[CrossRef](#)]
53. Clarke, N.L.; Furnell, S.M.; Rodwell, P.M.; Reynolds, P.L. Acceptance of subscriber authentication methods for mobile telephony devices. *Comput. Secur.* **2002**, *21*, 220–228. [[CrossRef](#)]
54. Hammad, M.; Wang, K. Parallel score fusion of ECG and fingerprint for human authentication based on convolution neural network. *Comput. Secur.* **2019**, *81*, 107–122. [[CrossRef](#)]
55. Mancilla-Palestina, D.E.; Jimenez-Duarte, J.A.; Ramirez-Cortes, J.M.; Hernandez, A.; Gomez-Gil, P.; Rangel-Magdaleno, J. Embedded System for Bimodal Biometrics with Fiducial Feature Extraction on ECG and PPG Signals. In Proceedings of the 2020 IEEE International Instrumentation and Measurement Technology Conference (I2MTC), Dubrovnik, Croatia, 25–28 May 2020; pp. 1–6.
56. Hammad, M.; Liu, Y.; Wang, K. Multimodal biometric authentication systems using convolution neural network based on different level fusion of ECG and fingerprint. *IEEE Access* **2018**, *7*, 26527–26542. [[CrossRef](#)]
57. Drucker, H.; Wu, D.; Vapnik, V.N. Support vector machines for spam categorization. *IEEE Trans. Neural Netw.* **1999**, *10*, 1048–1054. [[CrossRef](#)]

58. Pontil, M.; Verri, A. Support vector machines for 3d object recognition. *IEEE Trans. Pattern Anal. Mach. Intell.* **1998**, *20*, 637–646. [[CrossRef](#)]
59. Artan, Y.; Haider, M.A.; Langer, D.L.; Van der Kwast, T.H.; Evans, A.J.; Yang, Y.; Wernick, M.N.; Trachtenberg, J.; Yetik, I.S. Prostate Cancer Localization With Multispectral MRI Using Cost-Sensitive Support Vector Machines and Conditional Random Fields. *IEEE Trans. Image Process.* **2010**, *19*, 2444–2455. [[CrossRef](#)] [[PubMed](#)]
60. Anguita, D.; Boni, A.; Pace, S. Fast training of support vector machines for regression. In Proceedings of the IEEE-INNS-ENNS International Joint Conference on Neural Networks. IJCNN 2000. Neural Computing: New Challenges and Perspectives for the New Millennium, Como, Italy, 27–27 July 2000; Volume 5, pp. 210–214.
61. Dong, J.X.; Krzyzak, A.; Suen, C.Y. Fast SVM Training Algorithm with Decomposition on Very Large Data Sets. *IEEE Trans. Pattern Anal.* **2005**, *27*, 1088–1099.
62. Domeniconi, C.; Gunopulos, D. Incremental Support Vector Machine Construction. In Proceedings of the 2001 IEEE International Conference on Data Mining, San Jose, CA, USA, 29 November–2 December 2001; pp. 589–592.
63. Cauwenberghs, G.; Poggio, T. Incremental and decremental support vector machine learning. *Adv. Neural Inf. Process. Syst.* **2001**, *13*, 409–415.
64. Singh, B.; Singh, P.; Budhiraja, S. Various Approaches to Minimise Noises in ECG Signal: A Survey. In Proceedings of the 2015 Fifth International Conference on Advanced Computing & Communication Technologies, Haryana, India, 21–22 February 2015; pp. 131–137.
65. Pan, J.; Tompkins, W.J. A real-time QRS detection algorithm. *IEEE Trans. Biomed. Eng. Mar.* **1985**, *32*, 230–236. [[CrossRef](#)]
66. Drew, B.J.; Califf, R.M.; Funk, M.; Kaufman, E.S.; Krucoff, M.W.; Laks, M.M.; Macfarlane, P.W.; Sommarginen, C.; Swiryn, S.; Van Hare, G.F. Practice standards for electrocardiographic monitoring in hospital settings: An American Heart Association scientific statement from the councils on cardiovascular nursing, clinical cardiology, and cardiovascular disease in the young: Endorsed by the international society of computerized electrocardiology and the American Association of Critical-Care Nurses. *Circulation* **2004**, *110*, 2721–2746.
67. Hammad, M.; Maher, A.; Wang, K.; Jiang, F.; Amrani, M. Detection of abnormal heart conditions based on characteristics of ECG signals. *Measurement* **2018**, *125*, 634–644. [[CrossRef](#)]
68. Singh, Y.N.; Singh, S.K. Evaluation of Electrocardiogram for Biometric Authentication. *J. Inf. Secur.* **2012**, *3*, 39–48. [[CrossRef](#)]
69. Chawla, N.V.; Bowyer, K.W.; Hall, L.O.; Kegelmeyer, W.P. SMOTE: Synthetic minority over-sampling technique. *J. Artif. Intell. Res.* **2011**, *16*, 321–357. [[CrossRef](#)]
70. Yekkehkhany, B.; Safari, A.; Homayouni, S.; Hasanlou, M.A.; Homayouni, S.; Hasanlou, M. A comparison study of different kernel functions for SVM-based classification of multi-temporal polarimetry SAR data. In *International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences—ISPRS Archives*; ISPRS: Hanover, Germany, 2014.
71. Prescott, A.R.; Snoek, J.; Larochelle, H. Practical Bayesian Optimization of Machine Learning Algorithms. In Proceedings of the NIPS 2012, Lake Tahoe, CA, USA, 3–8 December 2012; pp. 2951–2959.
72. Robnik-Šikonja, M.; Kononenko, I. Theoretical and empirical analysis of relieff and rrelieff. *Mach. Learn.* **2003**, *53*, 23–69. [[CrossRef](#)]
73. Rui, Z.; Yan, Z. A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification. *IEEE Access* **2019**, *7*, 5994–6009. [[CrossRef](#)]
74. Chun, S.Y. Small Scale Single Pulse ECG-based Authentication using GLRT that Considers T Wave Shift and Adaptive Template Update with Prior Information. In Proceedings of the 23rd International Conference on Pattern Recognition (ICPR), Cancun, Mexico, 4–8 December 2016; pp. 3038–3043.
75. Abdiansah, A.; Wardoyo, R. Time complexity analysis of support vector machines (SVM) in LibSVM. *Int. J. Comput. Appl.* **2015**, *128*, 28–34. [[CrossRef](#)]