Biometric Authentication Using the Unique Characteristics of the ECG Signal

Tomas Repcik[1], Veronika Polakova[1], Vojtech Waloszek[1], Michal Nohel[1], Lukas Smital[1], Martin Vitek[1], Radim Kolar[1]

[1]Brno University of Technology, Faculty of Electrical Engineering and Communication, Department of Biomedical Engineering, Brno, Czech Republic

Abstract

ECG is a biological signal specific for each person that is hard to create artificially. Therefore, its usage in biometry is highly investigated. It may be assumed that in the future, ECG for biometric purposes will be measured by wearable devices. Therefore, the quality of the acquired data will be worse compared to ambulatory ECG. In this study, we proposed and tested three different ECG-based authentication methods on data measured by Maxim Integrated wristband. Specifically, 29 participants were involved. The first method extracted 22 time-domain features – intervals and amplitudes from each heartbeat and Hjorth descriptors of an average heartbeat. The second method used 320 features extracted from the wavelet domain. For both methods a random forest was used as a classifier. The deep learning method was selected as the third method. Specifically, the 1D convolutional neural network with embedded feed-forward neural network was used to classify the raw signal of every heartbeat. The first method reached an average false acceptance rate (FAR) 7.11% and false rejection rate (FRR) 6.49%. The second method reached FAR 6.96% and FRR 21.61%. The third method reached FAR 0.57% and FRR 0.00%.

1. Introduction

Identification and verification of subjects are required in many different areas and industries to provide a relatively high level of security. For this purpose, biometric are used. Commonly used biometric traits are the iris, fingerprint, face and voice. Nowadays, a falsification of these signals is an issue. ECG is a biological signal which is hard to falsify and therefore its potential in biometry is investigated [1].

2. Materials & Methods

The experimental data consisted of 775 20s Lead I ECG records with sampling frequency 512 Hz. These records were manually extracted from several measurements of 29 participants. Each volunteer was measured for three minutes by Maxim Integrated wristband (MAXREFDES101#: Health Sensor Platform 2.0) in a sitting position. Next, to capture also inter-measurement variability, at least 5 measurements (with one hour pause between them) were performed on each participant.

The goal of our study was to recognize a specific person from the others based on one short ECG recording. To be more specific, we chose a real-world scenario of a company using a biometric system. There were three assumptions in our experiment. First, there are two categories of persons – authorised persons and intruders. Second, we can collect more records of the authorised persons, because they are part of our company unlike intruders. This is important as it prevents imbalance between classification classes. Third, we can never collect ECG of all possible intruders.

With respect to these assumptions three random participants were supposed to be authorised persons and had over 90 recordings each. The remaining participants played a role of intruders, but records of only 14 of them were used for training (following the third assumption).

Three different algorithms were tested on our data – classification based on time-domain features, wavelet-domain features and deep learning approach.

2.1. Time-domain features

The time domain approach is based on features extracted from fiducial points and Hjorth descriptors (Figure 3.). There are 14 interval features, 2 amplitude features, 5 Hjorth features, and one feature related to interval variability. All the features show certain interpersonal differences and the combination of features has high discrimination ability.

First, the recording signal is filtered by an advanced Wiener filter designed for muscle noise reduction [2]. Then, the fiducial points (Figure 1.) are detected by wavelet transform based algorithm [3].

ISSN: 2325-887X DOI: 10.22489/CinC.2020.321

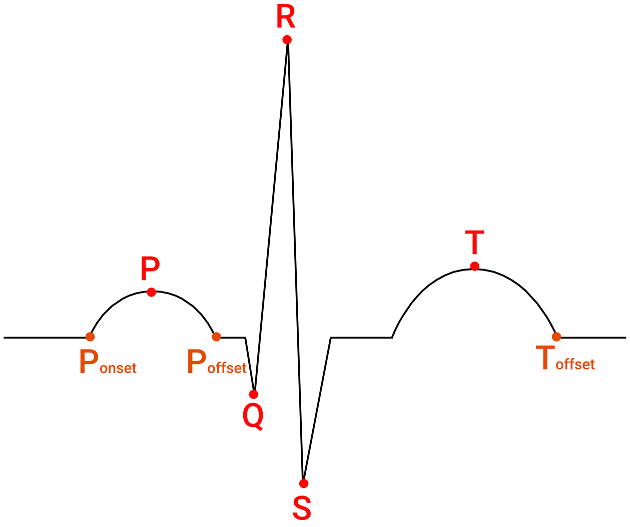

Figure 1. ECG fiducial points

Intervals between fiducial points (QR, RS, RT, PR, P_{onset}R, P_{offset}R, length of P wave, PQ, P_{onset}Q, P_{offset}Q, QT_{offset}, ST_{offset}, ST, PT) are extracted from each heartbeat [4], outliers are deleted (two shortest and two longest intervals of the recording) and mean value of intervals is computed and used as the feature (Figure 2.).

Amplitude features (RT and RP amplitude) are voltage difference between R peak and T (or P) wave top [4]. Again, mean value is computed from all heartbeats in the recording excluding outliers.

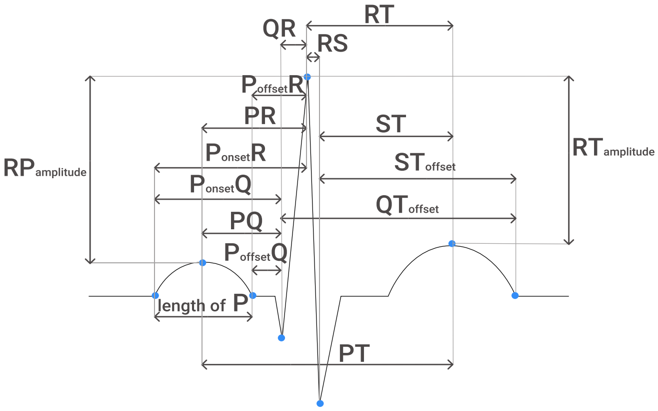

Figure 2. Interval and amplitude features

Hjorth descriptors (activity, mobility and complexities with order from one to three) [5] of an average heartbeat are computed. The average heartbeat is obtained by averaging of all undistorted heartbeats (aligned according to R peak) in the filtered and normalized ECG record.

The last feature is a standard deviation of PR intervals divided by mean PR interval in recording.

2.2. Wavelet-domain features

This method is based on extracted features from the wavelet transform [1]. The first step is preprocessing of data, which consists of signal filtering for removal drift and powerline interference. Then every record is filtered by FIR bandpass filter with band limited to the frequency range between 1 and 40 Hz. The signal is split into individual heartbeats cycles by an R detector. Each cycle contains 301 discrete sampling points. Cycles of each individual record are reduced to one cycle by averaging all cycles to reduce the effect of signal variation and to reduce noise in the signal. The amplitude of all ECG signals is normalized into values in the range of [-1, 1]. Heartbeats are aligned according to R peaks in order to obtain a representative ECG beat of the person.

Such a signal is used as an input to discrete wavelet transform. Coefficients of discrete wavelet transform of these averaged beats are considered as features (Figure 3.). The Daubechies wavelets (db3, db4, db5) are chosen with three, four and five levels of decomposition.

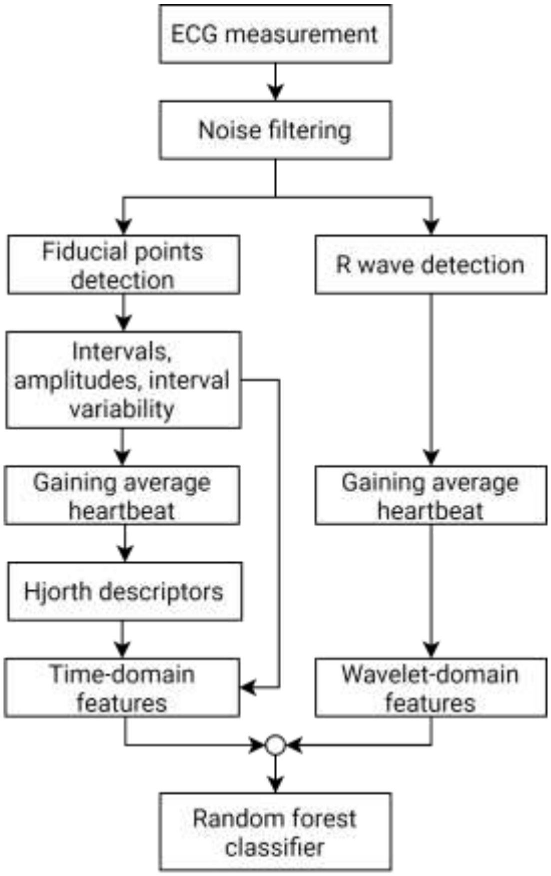

Figure 3. Time-domain and wavelet-domain algorithm diagram

2.3. Deep learning

The third approach uses deep learning methods. Previous methods use whole measurement to extract time / frequency domain features, which are used in machine learning models.

In means of deep learning, the different approach was taken. With use of the convolutional neural network (CNN), every single heartbeat is used as a signature for a specific person. The goal is to teach CNN to look for unique properties of every single ECG wave and in accordance to them identify our authorised person.

The proposed algorithm can be based on any arbitrary R wave detector. In our specific case, the Pan-Tompkins QRS wave detector is used [6]. Every R wave is centred to the closest highest value. Whole ECG wave is then extracted with 100 samples before the R peak and 200 samples after the R peak, which is approximately 600 milliseconds in time domain. This number of samples must be constant, due to an input of the CNN, which cannot be changed. After the extraction, the one ECG pattern continues to the min-max normalisation to get a scale from 0 to 1, which is the most convenient scale for the neural networks in general.

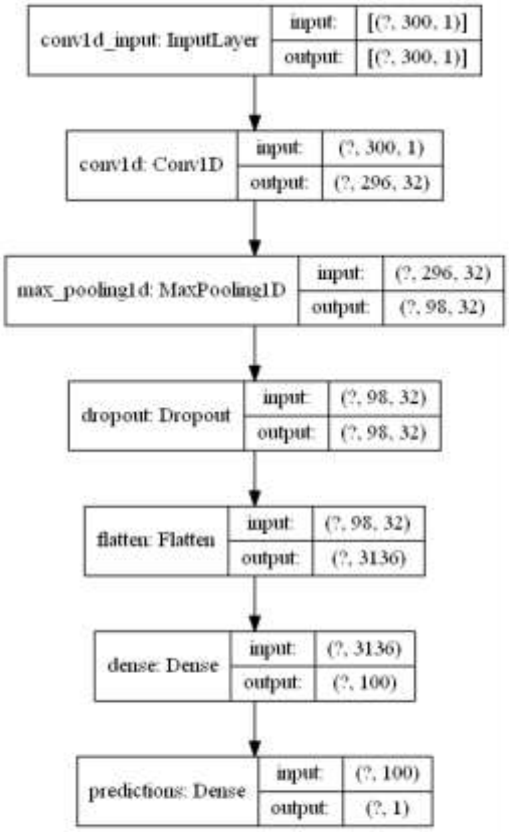

Figure 4. The architecture of the CNN. The question mark represents dynamic change of the batch size.

TensorFlow 2.0 is used as a framework for implementation and training of the CNN. The structure of the CNN is simple and efficient. 1D convolutional layer with 32 kernel filters, 1D max-pooling and embedded 2 dense layers to flatten output of the convolutional part are used in the architecture (Figure 4.). The problem is defined as a classification problem, so 0 represents intruder and 1 is the authorised person.

The model is trained with a random pick of people and our authorised person. The ratio of our authorised ECGs waves is too low in comparison with other people. Therefore, the weights for the classification are calculated from total counts of the ECG waves for our authorised person and intruders. Batch size is adapted to these counts, so our authorised persons ECG has a high chance to appear in the batch. The number of epochs is fixed, but at the end of every epoch, false acceptance rate (FAR) and false rejection rate (FRR) are calculated from a testing dataset created by people, which the CNN has never seen. The best results are saved. If the model reached 0 % for FAR and FRR, the training stopped.

3. Results

The results are summarized in Table 1.: Each time, one authorized person was examined against the intruders. The features extracted from 75 % of records of the authorized person and all records of 14 randomly selected intruders formed a training set. The remaining records of the authorized person and all records of the other 12 intruders were used for testing purposes. For the time domain and wavelet-domain method a random forest classifier was used. CNN already combines feature extraction and classification in its architecture. In total we applied models on three authorized persons with IDs 1205, 2200, 1003. In order not to affect results by a random selection of intruders the training and testing datasets were generated several times and the results were averaged.

Table 1. Results for sampling rate 512 Hz. IDs represent tested individuals.

	time-domain		wavelet-domain		deep learning	
ID	FAR	FRR	FAR	FRR	FAR	FRR
1205	7.57	10.43	6.52	33.66	0.00	0.00
2200	10.31	8.56	9.71	26.23	1.72	0.00
1003	3.46	0.48	4.66	4.96	0.00	0.00

3.1. Discussion

The Table 1. represents the average results for each method. Time-domain method and wavelet-domain show significant false acceptance rate, which means that, in some cases, one intruder out of ten would be accepted. The percentage however is not that high, this authentication approach could be used as an additional security, e.g. combined with fingerprints.

The false rejection rate is acceptable in the time-domain approach, in the worst-case scenario the person would have to repeat the authentication ECG recording once in 10 cases. On the contrary, the wavelet-domain FRR is too high for real performance.

The deep learning approach results are very promising. This level of accuracy in authentication is highly acceptable. It is still not as accurate as fingerprint biometry, but the potential usage of this method in person authentication is obvious. For the higher reliability and transparency of this method, it would be needed to gather more data, mainly for simulation of intruders.

Acknowledgments

This work has been funded by the United States Office of Naval Research (ONR) Global, award number N62909-19-1-2006. The authors wish to thank LCDR Joshua Swift from ONR Code 342 and Dr. Stephen O'Regan from ONR Global Central and Eastern European Office for their support.

References

[1] N. Belgacem et al., "ECG based human authentication using wavelets and random forest," *International Journal on Cryptography and Information Security*, vol. 2, no. 2, June,2012.

[2] L. Smital et al., "Adaptive wavelet Wiener filtering of ECG signals," *IEEE Trans. Biomed. Eng*., vol. 60, no. 2, pp. 437-445, 2013.

[3] M. Vítek et al., "A wavelet-based ECG delineation with improved P wave offset detection accuracy," *Proc. 20th Bienn. Int. EURASIP Conf. BIOSIGNAL 2010*, Brno, Czech Republic, pp. 160-165, 2010

[4] Y. N. Singh, P. Gupta, "ECG to individual identification," *2008 IEEE Second International Conference on Biometrics: Theory*, Applications and Systems, pp. 1-8, Sep. 2008

[5] A. Rizal, S. Hadiyoso, "ECG signal classification using Hjorth descriptor," *2015 International Conference on Automation, Cognitive Science, Optics, Micro Electro-Mechanical System, and Information Technology (ICACOMIT)*, pp. 87-90, Oct. 2015

[6] J. Pan, W.J. Tompkins, "A real-time QRS detection algorithm," *IEEE Trans. Biomed. Eng.*, vol. BME-32, no. 3, pp. 230–236, Mar. 1985.

Address for correspondence:

Tomas Repcik
Department of Biomedical Engineering
Technicka 3082/12, 616 00 Brno
xrepci01@vutbr.cz