Neurocomputing 506 (2022) 37–49

Contents lists available at ScienceDirect

Neurocomputing

journal homepage: www.elsevier.com/locate/neucom

ELEKTRA: ELEKTRokardiomatrix application to biometric identification with convolutional neural networks

Caterina Fuster-Barceló [a], Pedro Peris-Lopez [a,*], Carmen Camara [a]

[a] Department of Computer Science, Carlos III University of Madrid (UC3M), Madrid, Spain

ARTICLE INFO

Article history:
Received 4 May 2021
Revised 1 June 2022
Accepted 17 July 2022
Available online 22 July 2022
Communicated by Zidong Wang

Keywords:
Electrocardiogram (ECG or EKG)
Elektrokardiomatrix (EKM or ECM)
Biometry
Identification
Convolutional Neural Networks (CNN)
Computer vision

ABSTRACT

Biometric systems are an uprising technique of identification in today's world. Many different systems have been used in everyone's daily life in the past years, such as fingerprint, face scan, and others. We propose a new identification method using Elektrokardiogramms (EKGs) converted into a heatmap of a set of aligned R-peaks (heartbeats), forming a matrix called an Elektrokardiomatrix (EKM). We can build a one-against-many identification system using a Convolutional Neural Network (CNN). We have tested our proposal with one main database (the Normal Sinus Rhythm Database (NSRDB)) and two other databases, which are the MIT-BIH Arrhythmia Database (MIT-BIHDB) and the Physikalisch-Technische Bundesanstalt (PTB) Database. With the NSRDB, we have achieved an accuracy of 99.53% and offered a False Acceptance Rate (FAR) of 0.02% and a False Rejection Rate (FRR) of 0.05%. Very similar results were also obtained with the MIT-BIH and PTB databases. We have performed in-depth experimentation to test the efficiency and feasibility of our novel biometric solution. It is remarkable that with a simple CNN, which has only one convolutional layer, a max-pooling operation, and some regularisation, we can identify users with very high performance and low error rates. Consequently, our model does not need very complex architectures to offer high-performance metrics.

1. Introduction

Nowadays, biometrics techniques are widely used in everyday life. Examples range from the start of the day when an individual unlocks her phone with facial recognition or his fingerprint, to enter into his workspace with again his fingerprint, to access specific resources with an iris or retina scanner or even by the police department to gather pieces of evidence from a crime scene with latent fingerprints [1–3].

Besides, there exist different approaches in biometrics to identify a human being. Generally, there are two main groups of biometric identifiers: behavioural and physical ones [4]. Firstly, in the behavioural biometric identifiers we can find signature recognition [5], voice recognition [6], keystroke dynamics [7] and even touch-dynamics on mobile devices [8]. These behavioural recognition modalities are based on the actions of human beings or even animals. Secondly, the physiological biometrics are the well-known iris [9], face [10] and fingerprint [11] and some others such as finger veins [12], ear [13] and footprint [14] which are based on physical characteristics of a human being.

In the past years, biometrics-based on cardiac signals, called Electrocardiogram (ECG) or Elektrokardiogramm (EKG), have been introduced to some systems due to the following four key points [15]: 1) An EKG is a non-invasive technique, whereas an iris or retina scanner would be; 2) It is very rough against counterfeiting or spoofing practices because one can only be identified through its EKG if it is alive; 3) All living beings have their own EKG; and 4) An EKG also provides additional information related to psychological states and physiological status, which can be interesting for some applications [16].

The EKG is an electrical signal provoked by cardiac muscle depolarisation followed by repolarisation during each cardiac cycle (heartbeat). When the electrical activity is drawn through Voltage (V) versus time (t) in a graph, it is called an EKG. Each cycle of the heart starts with atrial depolarisation (P wave) followed by ventricle depolarisation (QRS complex) and rapid ventricle repolarisation (T wave), and finishes with the Purkinje fibbers' repolarisation (U wave) to start again. Each of these patterns is unique and represents different heart functioning phases, as shown in Fig. 1. Besides, cardiac diseases can affect the structure of the EKG. For instance, a sinus arrhythmia could affect the R-R interval into an irregular rate, or a tachycardia can affect the heartbeat's whole rate.

* Corresponding author.
E-mail address: pperis@inf.uc3m.es (P. Peris-Lopez).

https://doi.org/10.1016/j.neucom.2022.07.059
0925-2312/

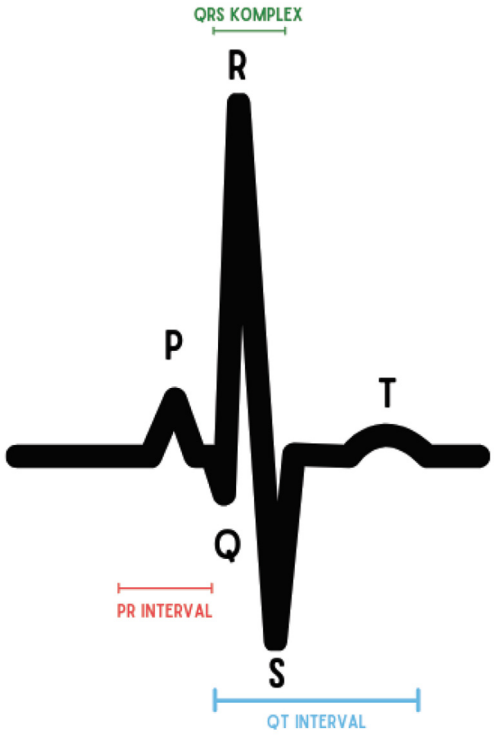


Fig. 1. Electrocardiogram with its fiducial medical points.

Due to the uniqueness of an EKG, researches on identification techniques using this signal are very numerous and have more than 20 years of experience [17,18]. The purpose of all researches is to identify users through their EKG using a huge variety of techniques in classification such as k-Nearest Neighbour (k-NN), Support Vectors Machine (SVM), Linear Discriminant Analysis Classifier (LDAC), Multilayer Perceptron (MLP), and Convolutional Neural Network (CNN) among others [19–23].

In this work, we aim to go further with the identification of users through their EKG by using the Electrocardiomatrix (Elektrokardiomatrix (EKM) or Electrocardiomatrix (ECM)) representation recently introduced in [24]. This EKM was first used for medical purposes to diagnose some heart diseases such as Atrial Fibrillation and Atrial Flutter [25–27]. As shown in Fig. 2, an EKM is a heatmap matrix of size $N \times s_p$ where N is the number of peaks (heartbeats) chosen to form the matrix[1] and s_p is the number of necessary samples to ensure that two R-peaks from the N chosen are placed in each row. In other words, in each row appears two R-peaks. Therefore, the first peak of the $n + 1$-th row is the same one as the second peak of the n-th row. Consequently, each peak from the second peak of the matrix to the peak $N - 1$ is going to be shown two times. Summarising the EKM shows the distance between peaks and their intensity. As a recent example of the use of the EKM, Salinas-Martínez et al. propose it as a powerful tool to detect cardiac anomalies [28] by using a CNN to classify the EKMs into two classes (i.e., regular or Atrial Fibrillation –AF). This way, automatic analysis is done instead of analysing the whole EKG manually.

Regarding the analysis of the signal, fiducial and non-fiducial based approaches are the two main alternatives. On the one hand, a fiducial analysis of a signal consists of using the signal with markers. Concerning the EKG, these markers or points are the well-known waves or phases of one heartbeat as shown in Fig. 1 and other relevant characteristics or points of the signal (e.g., PQ interval, RT interval, PQ amplitude or RS amplitude). An excellent example of a fiducial analysis is the study that conducts a medical professional when inspections on an EKG trace for heart diseases such as Atrial Fibrillation, Tachycardia, and others [29]. We can also find fiducial analysis in studies where users' identification is their primary goal, as in [30].

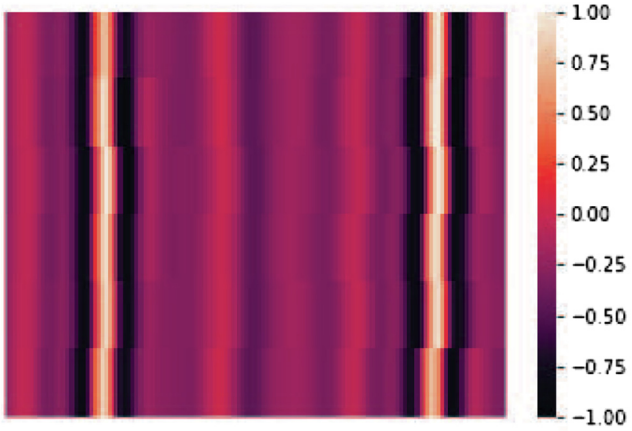


Fig. 2. Heatmap representation of an EKG.

On the other hand, the non-fiducial analysis does not focus on the signal's specific points or markers but also on the whole signal. It could be considered a general analysis. As the entire signal is taken and not some points of it, the EKG can be processed either in time, frequency, time–frequency or even as an image. Thanks to that, the identification over the signal can be performed through K-NN, SVM or a CNN between others [31–33]. It is relevant to remark that extracting features with a CNN is not a fiducial analysis. Those features extracted from a CNN are the ones that explain the data itself, not the fiducial medical points represented in Fig. 1.

Indeed, the work presented in this paper focuses on a non-fiducial analysis. The EKG will be processed in the so-called EKM which is a heatmap representation of a certain number of beats, as explained previously. Therefore, the fiducial points (R-peaks) used to construct the matrix mentioned above do not participate in the identification process. In a nutshell, the EKM images are the raw inputs to our identification system.

To construct the EKM, we need a detector of fiducial points. Particularly, what is needed is a detector of the R peaks (depicted in Fig. 1). We conduct a deep study about this procedure since detecting or not the signal's R-peaks can hardly affect the EKM generation. In the literature, we can find multiple detectors to distinguish the R-peaks of an EKG. One of the most accepted is the Pan-Tompkins detector [34], which offers a high accuracy detection. Other detectors have been developed in the past years based on different approaches such as Shannon Energy Envelope (SEE) or Hybrid Complex Wavelet (HCW) for R-peak detection and Biorthogonal Wavelet Transform (BWT) and Run-Length Encoding (RLE) for QRS complex detection [35–37].

To summarize, we show the pipeline of our method in Fig. 3. The process starts with the acquisition of the raw EKG database and ends with the users' identification. We explain every step of this pipeline in the subsequent sections.

Our main contributions with this paper are:

- We are the first contribution, to the best of our knowledge, which have proposed to use the recently presented EKG representation (the EKM) to build a robust and feasible identification system based on ECG signals.

[1] It is essential to remark that the number of chosen peaks (N) is a hyperparameter which can be tunned regarding the use of the EKM.

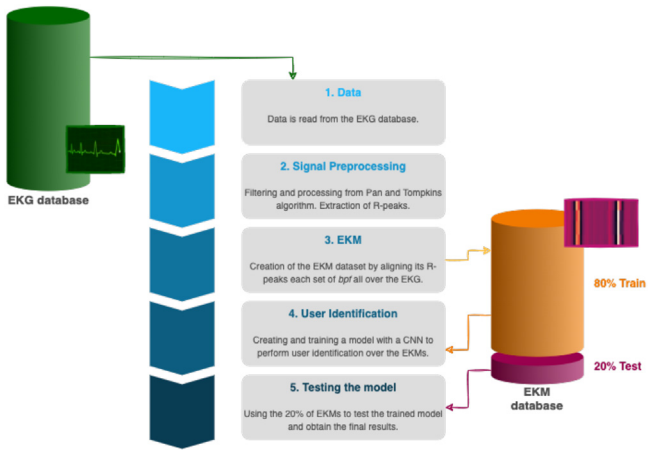


Fig. 3. Pipeline and process of ELEKTRA..

- We have designed a simple but effective CNN to test multi-class and binary identification scenarios, which can achieve tiny error rates with our ELEKTRA model.
- To guarantee reproducibility and demonstrate the feasibility of our proposal, we have used four public datasets (Normal Sinus Rhythm Database (NSRDB), MIT-BIH Arrhythmia Database (MIT-BIHDB), Physikalisch Technische Bundesanstalt (PTBDB) and Brno University of Technology ECG Quality Database (BUTQDB)) in our experiments.
- Apart from the standard performance metrics (e.g., accuracy and EER), we have also analysed the probability of an impersonation attack or the system's resistance to noisy users.
- In the comparison analysis, we have shown how our model can obtain results as good as the ones in the state-of-the-art with a simpler identification method and an efficient model.

Organisation: The rest of the article is structured as follows. In Section 2, we review the literature related to EKG biometric identification. We introduce the signal pre-processing techniques, EKG representation and the databases used in our experiments in Section 3. In Section 4, we analyse the results (multi-class and binary classification) and study the influence of several parameters such as the number of R-peaks forming the EKM or the used epochs. Finally, we extract some conclusions and compare our proposal with previous works in Section 5.

2. Related work

Identification through the EKG has been a regularly used technique in biometrics since many years ago. Already in 2001, L. Biel showed how an EKG trace obtained from just one-lead was enough to identify an individual [38]. The above result implies that the EKG can be used for biometrics in many different applications [39]. One year later, in [40] Shen et al. confirmed that it is possible to identify a person among a different group of candidates with one-lead EKG. In detail, the authors showed how to identify 20 subjects from the MIT-BIH database [41] with two different techniques, Decision Based Neural Network (DBNN) and Template Matching, and achieving an accuracy of 80% and 95%, respectively.

In the literature, we can find a wide variety of approaches for identification using EKG records. Some proposals use the raw signal after applying some filters [42], other works transform the EKG into an image and process it as a picture [43,44] or other solutions extract fiducial points of the EKG and use them directly to classify between different users as in [45] where the DETECT method is presented. The authors tested DETECT using the database of the challenge titled "You Snooze You Win" [46], and the error rates are low (FRR and FAR of 6.4×10^{-2} and 3.3×10^{-5}), and the accuracy is moderately high (i.e., 92%).

Given the outlook of identification of EKG using Neural Network (NN), there exist very different methods. One interesting work is [42] where Salloum and Kuo design an identification system based on cardiac signals and over different types of Recurrent Neural Network (RNN). As the input of their NN the authors use a vector of several consecutive heartbeats waveforms. The particular number of waveforms is a hyperparameter in the proposal. For experimentation, they use traditional RNNs, NN with Long Short-Term Memory (LSTM) units and with Gated Recurrent Unit (GRU) and test each identification proposal with two public databases: ECG-ID database [47] and the MIT-BIHDB [41]. The higher result achieved with the ECG-ID database is 100% of accuracy with an LSTM network and an input vector containing nine heartbeats. Next, the second-best result doing the same experiment but using only three heartbeats is 98.2% of accuracy. Similar results are achieved with the MIT-BIHDB.

Another striking example of identification through NN is the proposal in [44] where the identification is performed over a CNN. This CNN's input is an image containing a concatenation of several QRS complexes. This picture only contains a line (time series of several QRS segments), and the resting image is a blank space. Despite this, the performance, measured with database PTBDB [48], is comparable to the best existing works as claimed by the authors.

Concerning the use of different databases to test the identification performance, in [49] Sidek et al. tested their proposal over databases with users having abnormal cardiac conditions. Those databases are the well-known MIT-BIHDB, the MIT-BIH supraventricular arrhythmia Database (SVDB) and the Charles Sturt Diabates Complication Screening Initiative Database (DiSciRi DB). To perform the identification the authors use a Normalize-Convolute-Normalize (NCN) technique over the EKG segments and then Bayes Network (BN), MLP, Radial Basis Function (RBF) and K-NN are used as the classification algorithms. Metrics such as Sensitivity (Se) and Specificity (Sp) or Positive Predictive Value (PPV) are used to assses the performance. In terms of accuracy the results are significantly high (i.e., 96.7%, 96.4% and 99.3% for MIT-BIHDB, SVDB and DiSciRi DB databases, respectively).

In line with the wave of using NN, in [43] Hong et al. propose the combined use of MLPs and Transfer Learning[2] using the Inception-v3 network. In detail, the EKG trace (time series) is transformed into images by computing Pearson's Correlation Coefficients. Then, the Inception-v3 model is used for feature extraction, and a fully connected layer is utilised for classification. From the results, we observe that with higher sampling rates, better results are reached. For instance, the accuracy is 98.07%, and FPR is 0.69% when the sampling rate is set to 1 kHz.

One of the main obstacles of identifying users through their EKG is that many proposals used private databases in their experiments (e.g., [16] or [38],). Supporting this reasoning, in 2020, a comprehensive review of EKG-based solutions is presented in [50]. In this work, the author shows a list of the common used EKG databases, including the information whether they are public or private. From the 21 databases listed, six (30%) are public, but fifteen (70%) are private. There are just a few available databases in sites such as Physionet [48], one of the most used repositories of EKG records. Unfortunately, many works use private databases created ad hoc for that research, which hinders the results reproducibility.

[2] Transfer Learning is a broadly used technique applied in Deep and Machine Learning that consists of using a pre-trained network. Optimised weights from the pre-trained network are taken to solve a new problem with similar characteristics to the original one.

In line with the above, an interesting proposal is in [51], in which Kim and Pyun propose an identification solution based on bidirectional LSTM and tested with two public databases (NSRDB and MIT-BIHDB). The authors use as input of the LSTMs the EKG itself after filtering and normalising the EKG signal. They conduct experimentation analyses by varying the hidden units (from 125 to 250) and the beats (3, 6 or 9) used in the input. Outstanding results are achieved with the bidirectional LSTM with both databases. For example, with the proposed LSTM in the MIT-BIHDB, 99.8% of accuracy is achieved when using nine heartbeats and three hidden layers.

Last but not least, a different approach of classification with NN is the one in [52]. Their used method to treat with the EKGs is the Second Order Difference Plot (SODP), a non-linear time-series analysis method that allows extracting features. They propose a Logarithmic Grid Analysis (LGA) as a quantification method of SODP. These techniques are first applied to finally classify EKGs with K-NN. Their method is tested over three different databases: the ECG-ID database, the NSRDB, and the MIT-BIHDB. Their best results in terms of accuracy are 91.96%, 99.86% and 95.12% for each database, respectively.

3. Materials and Methods

3.1. Data

The experimentation has been performed with four public Physionet databases [48]. Each individual in the database counts a file containing the raw data and an addition file describing characteristics like the time duration or the sampling frequency.

The main data used in this study is from the NSRDB. We have chosen this database for our experimentation since it is a public database, that can be found in [53] and, what is more, the users present at this database are considered *control users* which means that they do not have any remarkable heart disease. This database includes 18 long-term EKG recordings from the Arrhythmia Laboratory at Boston's Beth Israel Hospital with no significant arrhythmias. The database involves five men aged 26 to 45 and thirteen women aged 20 to 50[3].

Our approach is also tested on MIT-BIHDB [41]. Fundamentally, we chose this database since it is a well-known database used in many previous studies (see Table 8). The MIT-BIHDB contains 48 half-our EKG recordings obtained from 47 different subjects. In detail, the database comprises 23 random patients from an ambulatory and 24 patients with significant arrhythmia. Therefore healthy and not-healthy subjects have been mixed and included in this database.

Similarly, the third chosen database is the PTBDB [54], an EKG database available at the generally used PhysioNet repository. This database contains 549 records from 290 subjects. Regarding the cardiac health of the subjects, it has approximately 18% of the subjects who are healthy, the 8% are unrecognized and the rest with different Cardiovascular Disease (CVD) such as dysrhythmia or myocarditis.

Finally, we have used the BUTQDB database in some of the experiments (i.e., see section). This database is also a public database available in [55]. This database comprises 18 long-term recordings of single-lead EKG collected from 15 subjects (nine female and six male) aged between 21 and 83 years. The participants of this database, like the ones in NSRDB, do not have significant cardiac complications. Therefore, they are all also considered *control users*.

[3] When referring to this database, names from 0 to 17 are linked to each user in alphanumeric order.

3.2. Signal Preprocessing

Before any analysis preprocessing of the EKG signal has been carried out by the following steps: a) Bandpass filtering of the signal between 5 and 15 Hz; b.) differentiation; c) rectification (squaring); and d.) moving-window integration.

To generate the EKM we need first to perform the R-peaks detection procedure. We have used the Biosignals library, which provides a set of functions (e.g., filter or event detection) commonly used in the pipeline of biosignals processing[4].

Particularly, we have used the well-known Pan and Tompkins (PT) algorithm, which employs a dynamic threshold [34] (a. Buffer initialisation; b. Detection of possible and provable *R*-peaks; and c. Exclusion of peaks ([34] criteria) and lag correction) to generate the definitive list of *R* peaks.

Using these steps with the EKG records in the database, we build a dictionary with *N* entries (being *N* the number of users of each database), and each entry contains a list of all its R-peaks.

3.3. EKG

As mentioned in Section 1, the EKM is a set of several aligned *R*-peaks of an EKG trace composing a matrix and then transformed into an image through a heatmap representation.

The EKM has already been proposed in several works for medical purposes [24,27,25,26,28]. In this article, we aim to show the feasibility of EKMs for identification (cybersecurity purposes). To the best of our knowledge, it is the first time that this approach is proposed. Next, we explain the generation procedure of the EKMs.

To create the EKM[5], first of all, we define a *window* which is an EKG segment containing the number of beats declared to be on the EKM (see Fig. 4 as illustration). To refer to this number of beats (*R*-peaks), we use a metric called beats per frame (bpf), which is the number of different beats that there appear on each frame or heatmap of the EKM. The value of bpf is a hyperparameter that depends on the problem to address. In our experiments, we test three bpf values: 7, 5 and 3.

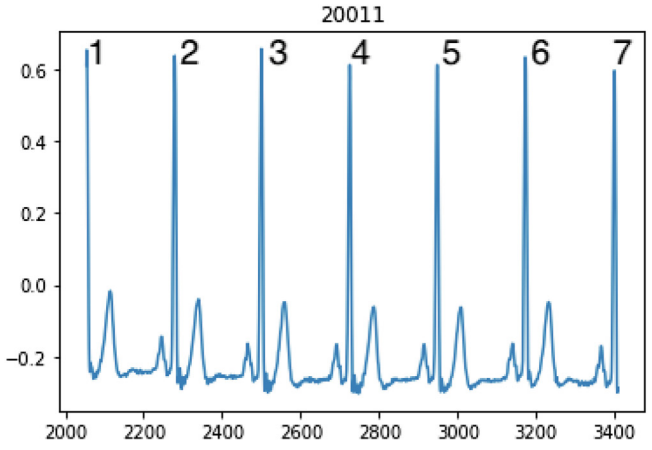
Once we have divided the EKG into windows, we need to process each of them to obtain the EKM. Precisely, we split the window into smaller segments of two peaks forming each row of the EKM. As shown in Table 1, two values delimit each segment, where the μ parameter represents the average distance between beats for the entire EKG record of a subject:

- Init Segment: Given by $p_x - \alpha_i \mu$where p_x is the sample position of the $peak_x$ and α_i is a free hyperparameter indicating the percentage of samples that are taken before p_x. For all our experiments we set α_i to 0.2.
- End Segment: Given by $p_{x+1} + \alpha_e \mu$ where p_{x+1} is the sample position of the peak consecutive to $peak_x$ and α_e is a hyperparameter which determines the percentage of samples that are taken after p_{x+1}. We set $\alpha_e = 0.3$ in our experiments.

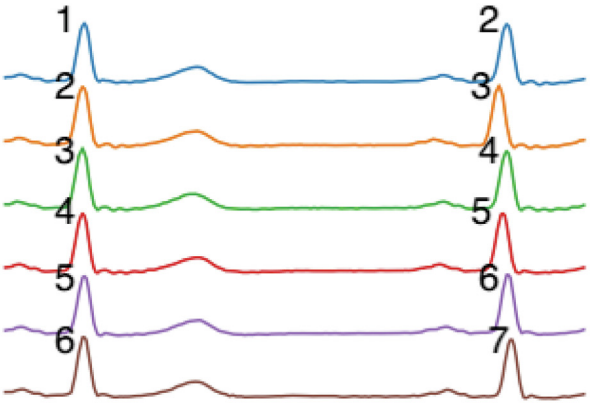
Each of the processed segments represents a row of the EKM. Note that all the peaks are aligned since the α_i, and α_e values are fixed for all the rows. The size of the EKM matrix is $bpf - 1$ rows with two peaks per row. To obtain the final image EKM representation, we need to compute a heatmap. As illustration, Fig. 5 is the representation of the plot seen in Fig. 4b.

[4] https://github.com/biosignalsplux/biosignalsnotebooks

[5] Our implementation to generate EKMs is available at:https://github.com/cfuster-barcelo/ELEKTRA-approach



(a) EKM I: Seven peaks plotted from the EKG



(b) EKM II: Alignment of seven peaks or EKG

Fig. 4. Steps I and II of the Elektrokardiomatrix.

Table 1
Segment Separation of the window

Init Segment	$p_x - \alpha_i \mu$
End Segment	$p_{x+1} + \alpha_e \mu$

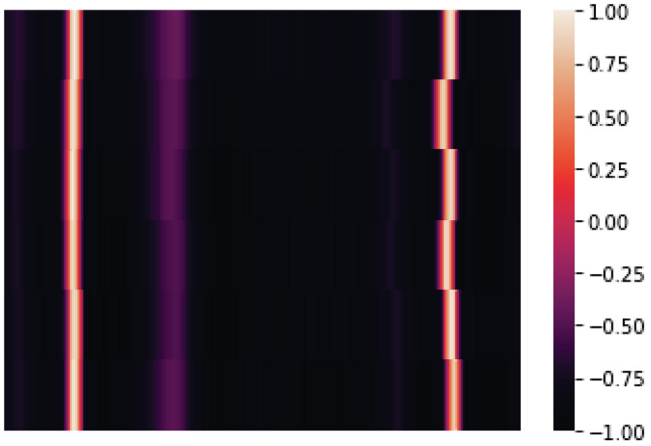


Fig. 5. EKM III: Heatmap of the EKG.

3.4. User Identification

3.4.1. EKMs databases

Following the procedure described in Section 3.3, we build several EKM datasets, one per each bpf parameter and for the databases mentioned in Section 3.1. Considering the creation of the EKM datasets, we have two different types of databases depending on how large the EKG recordings are. For large EKG recordings, such as NSRDB, we obtain EKM's images until we reach an upper threshold equal for each user in the database (i.e., 3000 images per user in our experiments). Otherwise, for shorter EKG recordings, such as the MIT-BIHDB or PTBDB, we obtain as much EKMs images as we can until we run out of signal. Once we have generated the datasets and to identify users (categorical classification problem), we have trained a CNN as it will be explained later on Section 3.4.2. As conventional, we divide the dataset into several sets:

- Train dataset: From the whole database, we use the 80% of EKMs to train the CNN for the NSRDB and a 90% for the MIT-BIHDB and PTBDB. Besides, from this training dataset another split is done in order to cross-validate the CNN parameters, creating:
  - Train dataset: (x_{train}). A 70% (for the NSRDB) or a 90% (for the MIT-BIHDB and PTBDB) of EKM samples for each user.
  - Validation data-set: (x_{val}). A 30% (for the NSRDB) or a 10% (for the MIT-BIHDB and PTBDB) of EKM samples for each user.
- Test data-set: (x_{test}). It is a 20% of the NSRDB and a 10% for the MIT-BIHDB and NSRDB. The number of images of this dataset is the resting from the training ones. It is noteworthy that the trained model never sees the testing images. Testing images are only used to test and predict once the model is trained.

The length of the EKG recordings for the MIT-BIHDB and PTBDB also influence the datasets created for each of the bpf values analyzed. Therefore the higher the value of the parameter bpf fewer images are going to be obtained for each user and dataset.

3.4.2. CNN Architecture

Nowadays, CNNs are the most used NNs for feature extraction in computer vision [56–58]. The good performance that CNNs get over image data is because convolutional layers can extract essential features from the images and the power of Graphical Process Unit (GPU) as processors.

As a proof-of-concept solution to show the feasibility of using EKMs (extracted from EKG traces) for identification purposes, we propose a simple CNN architecture that offers high performance in terms of accuracy and low error rates, as shown in Section 4. In detail, the architecture of the CNN consists of just one convolutional layer plus a fully connected layer to classify users. We have chosen to test all our work with a very simple CNN to show that our approach can identify or classify users even with an elementary architecture. Thus, we focus our approach on introducing the EKM as a valid identification method and for that purpose, we have conducted in-depth and rigorous experimentation. Fig. 6 depicts the used architecture, specifying all dimensions and layers.

The first step that the network performs can be considered as a preprocessing step. All input images are cropped to reduce the number of parameters and eliminate the image axis and white spaces, discarding irrelevant information.

Next, the second layer of the CNN is structured as follows:

- Conv2D: A 2D Convolution occurs where the kernel size is set to 3×3 kernel. After this step, we get high-level features.

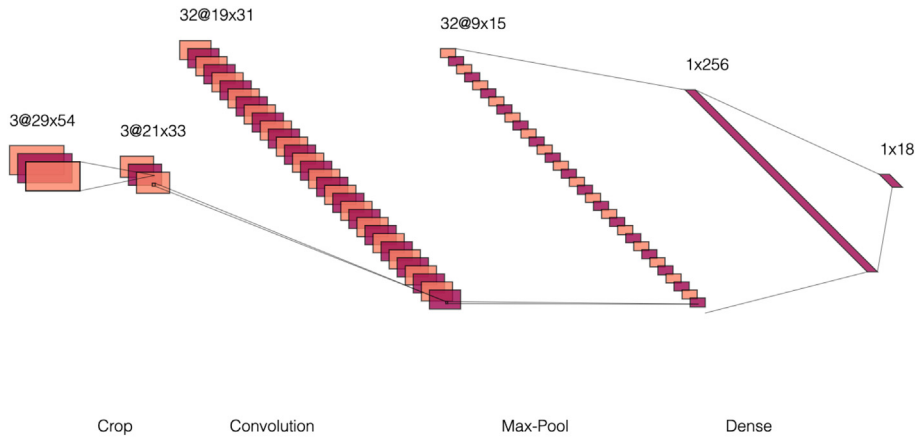


Fig. 6. CNN Architecture.

- Relu: A Rectified Linear Unit (ReLU) function is used to provide a rectified non-linear transformation.
- MaxPooling: The Pooling layer reduces the size of the samples. A kernel of size 2×2 inspects the whole image and gets the maximum value of that kernel, downsampling the images to half of its input size.
- Dropout: A dropout of 70% takes place as a regularisation technique to prevent over-fitting.

If we had another layer for our CNN in order to make it more complex, it would be the same one as the second layer. Nevertheless, our focus here is to show how our approach can identify users with satisfactory results with only one Conv2D layer for our CNN showing that an uncomplicated architecture is enough to obtain those good results with the ELEKTRA proposal.

The third layer of the network is the Fully-Connected Layer (FCL) or classification layer. This layer aims to reduce the number of features and group them into the number of classes that have to be identified (18 users in the NSRDB). Since we deal with a categorical classification problem, we use a *softmax* activation function to get the probability that an image belongs to a class[6]. The FCL consists on three steps:

- Flatten: Once the previous layers extract features, they are flattened into a column vector.
- Dense: Two dense layers are used to reduce the number of features extracted to the number of existing classes.
- Softmax: The last dense layer's output is activated by a *softmax* function to get the probability of belonging to each class.

A NN updates its parameters at each layer by optimising a cost or loss function during the training of the model. The CNN trains the model while a Categorical Cross-Entropy cost function is optimised. For this purpose, we choose the Adam optimiser since it is a widely used approach when training CNNs [59]. Our experiments train the models with different numbers of epochs and steps for epoch depending on the chosen database. In the majority of the experiments, we employ 50 epochs and 70 steps per epochs, but others, such as the ones for the MIT-BIHDB and PTBDB have 100, 150, or even 200 epochs due to the tiny EKM datasets. Also, steps per epoch (see Eq. 1) for these two commented datasets are changed depending on the number of training images:

$$Steps\,per\,epoch = \frac{length(train\,dataset)}{batch\,size} \tag{1}$$

where the batch size is set to 32.

After training each of the models used in each experiment using the training and validation datasets, we only have to test those models with the testing images that the model has never seen. We obtain all the metrics (e.g., accuracy or EER) specified in each experiment using these mentioned testing images.

4. Results

In order to show how the EKM allows the unequivocal identification of individuals, we perform several experiments varying different aspects of the network, of the EKM or even of the EKG. These experiments are willing to show how the NN adapts to the problem proposed and how user identification is possible through all the different approaches. In the following experiments, we use the NSRDB except when it is specifically indicated.

4.1. BPF Influence over User Identification with NSRDB

We launch three different experiments over the network described in Section 3.4.2 modifying the bpf parameter (i.e., $bpf = \{3, 5, 7\}$). Note that a bpf indicates how many *R*-peaks are used to generate an EKM.

After computing the EKM datasets for the three bpf values, we resize all the EKM heatmaps before introducing them to the CNN to reduce computational costs. The raw image extracted from the EKG is 57x108 pixels, including all its blank space and the margins of the picture indicating the axis values. At this step, we resize all images into 29x54 pixels. Then, as explained in Section 3.4.2, the first layer of the CNN is a cropping layer that removes all blank spaces and axis values.

We test the CNN with the three produced datasets. This experiment's main goal is to determine how many beats (R-peaks in an EKM) are enough to identify an individual. Table 2 summarises the results of these experiments. We use four common metrics to compare the proposals. Regarding the correct classification of instances, we have the Loss and Accuracy metrics. Concerning errors, we use the False Acceptance Rate (FAR), and the False Rejection Rate (FRR) commonly used in biometrics [60].

The results are very similar in the three tests with minor differences (see Table 2). The correct classification of instances is almost perfect in our system. An accuracy higher than 0.99 and loss in the range of 10^{-2} confirms this desirable property. Concerning errors, the FAR is below the FRR. That is, authorised access is *K* times more

[6] In some experiments we perform a binary classification, and some adjustments are needed, as the substitution of Softmax by a Sigmoid function.

Table 2
Metrics obtained with the CNN when varying the number of bpf into 3, 5 or 7. These results are from NSRDB with 18 users and 600 samples for testing each user.

Tests	bpf	Loss	Accuracy %	FAR (%)	FRR(%)
Test 01	7	0.0176	99.44	0.03	0.06
Test 02	5	0.0270	99.47	0.03	0.06
Test 03	3	0.0179	99.53	0.02	0.05

costly than locking out a legitimate user (i.e. $K \times FAR = FRR$). The parameter K is equal to 2.5 for $bpf = \{5\}$ and is 2 for $bpf = \{3, 7\}$. Since the differences are minimal between the three alternatives examined, as a trade-off between usability and performance, we consider setting the bpf parameter to 5 (Test 02) as a fair value, and this is the value assumed in the subsequent experiments.

4.2. BPF Influence over User Identification with MIT-BIHDB

In order to test our model with other databases, we have performed the same experiment as the one above in Section 4.1. The MIT-BIHDB database (explained in Section 3.1) has been tested with different number of bpf to evaluate the performance of our model.

To do so, we first need to obtain the heatmap or EKM database of the MIT-BIHDB for every bpf (being 3, 5 or 7bpf). This dataset, as we have commented on Section 3.4.1, is different from the NSRDB on how it is built due to shorter EKG recordings. Consequently, as not all recordings have the same duration for each subject, we can not obtain the same number of EKMs for each subject. In fact, due to that, also different number of images are obtained for each experiment when talking about the bpf number because the total number of R-peaks from the EKG signal must be divided into the number of bpfs to obtain the number of images collected (i.e. $R-peaks_{total}$ / bpf = *Number of EKMs obtained for* $bpf = 3, 5, 7$). In conclusion, due to shorter EKG recordings, we are going to have unbalanced datasets of EKMs for each subject and bpf parameter –the higher is the number of bpf chosen, the fewer images are obtained for that dataset.

Once we have the EKG dataset, we should separate it into the training and testing sets as explained in Section 3.4.1. Due to shorter datasets, for the MIT-BIHDB we have done a split of 90% and 10% for training and testing, respectively. This way, more images are used in the training phase, and better results can be acquired. The rest of the experiment is developed following the same procedure described in Section 4.1.

Consequently, according to what we can see in Table 3 our method obtains similar results regarding the experiments performed with the NSRDB. We have moved from 54000 images in each experiment with the NSRDB database to 35949, 21149, and 15119 images for 3, 5, and 7 bpfs, respectively, with this database. Meaning that even we have reduced the pool of EKM images drastically, our method can achieve high performance. We can explain the slight decrease of some metrics such as the False Rejection Rate (FRR) because the fewer images that we have to train our model, the more difficult is the building of a model capable of generalizing for all subjects.

This also affects the difference in results between the number of bpf chosen because as higher is the bpf number, the lower amount of images we have to train and test the model.

4.3. BPF Influence over User Identification with PTBDB

Following the same line as the one in the previous experiment in Section 4.2 we have tested the PTBDB with 3, 5, and 7 bpfs to evaluate our approach with a different database.

As we have done with the two previous databases, we need to obtain a dataset of heatmaps or EKMs to perform the user classification. Again, this dataset is going to be an unbalanced one due to the length of each EKG recording. All EKG recordings from this dataset are even shorter than the ones in the MIT-BIHDB. The total number of images that we have to train this model is 9854, 5891, and 4180 for 3, 5, and 7 bpf, respectively.

Obtaining the heatmap dataset and performing the training and the testing phase of the experiments have been developed similarly to for the MIT-BIHDB database in Section 4.2, resulting in what we can see in Table 4.

Considering the fewer number of images that we dispose of for the training and testing of our model, our results seen in Table 4 are pretty good. As we have explained before and as a rule of thumb, the smaller is the number of images we have, the worst results we get. It also explains why we get a much better result when we evaluate our model with 3 bpf than when we are doing it with 7 bpf. Notably, we have approximately 2,3 times more images for the dataset with 3 bpf in comparison with the dataset with 7 bpf. Nevertheless, the results are competitive for all the experiments, even in the worst scenario with fewer images. What is remarkable is that even with a dataset of fewer than 10,000 images, we are can train and test a model which is good enough to classify and identify users with an accuracy of almost 90% using a simple CNN with only 1 Convolutional layer. Table 5.

4.4. Time Costs of Convergence

In this experiment, we aim to reduce the computational costs of our system. To do so, we train the model from Test 02 (i.e., bpf= 5) using the same parameters except for the number of epochs. We perform a decrease of 20% (from 50 to 30 epochs). Fig. 7 illustrates both models' performance during training and validation in terms of accuracy and loss.

As shown in Fig. 7, both configurations are feasible and work accurately. They achieve almost identical results in terms of classification success (a difference less than 10^{-2}). Concerning errors, the FRR is higher than FAR in both cases. The parameter K (i.e. $K \times FAR = FRR$) is equal to 2 and 2.2 for 50 and 30 epoch respectively. Therefore, if we can afford to have a slightly high *FRR* (legitimate users may attempt two times to get access to the system), the use of 30 epoch is appropriated. If that *FRR* is excessively high for the target application, it is better to use 50 epoch in which both *FAR* and *FRR* are at a low level.

4.5. One-vs-the-rest (OvR) Classifier

As an additional experiment, we test the system using the One-vs-the-rest (OvR) approach. For instance, we can use this solution for building the ID identification system of our smartphone. To make the system more resistant to attacks (e.g., replay or impersonation attacks), we use two classes (i.e., the samples of the target user and the rest).

We compute a new database following the approach described below. We randomly chose N EKM images of a user-q for building the target class. Next, we choose the same number of randomly sampled images for the resting users (i.e., user-p where

Table 3
Metrics obtained with the CNN over the MIT-BIHDB when varying the number of bpf into 3, 5 or 7.

Tests	bpf	Loss	Accuracy (%)	FAR (%)	FRR(%)
MITDB-01	7	0.0818	98.33	0.04	1.75
MITDB-02	5	0.0542	98.84	0.03	1.17
MITDB-03	3	0.0566	98.26	0.04	1.67

Table 4
Metrics obtained with the CNN over the PTBDB when varying the number of bpf into 3, 5 or 7.

Tests	bpf	Loss	Accuracy (%)	FAR (%)	FRR(%)
PTBDB-01	7	0.9239	79.12	0,01	0,05
PTBDB-02	5	0.512	87.27	0,06	0,48
PTBDB-03	3	0.4214	89.8	0,05	0,45

Table 5
Metrics obtained with the CNN for training the model with 50 or 30 epochs

Tests	Epochs	Loss	Accuracy (%)	FAR (%)	FRR(%)
Test 02	50 epochs	0.027	99.47	0.03	0.06
Test 04	30 epochs	0.0374	98.94	0.05	0.11

$p \in \{0, 1, \ldots 17\}$ and $p \neq q$). We use 2400 EKMs for the training and 600 EKMs for the testing datasets ($N = 3000$ in our experiments), as in other experiments.

Concerning the CNN model, we maintain many of the model's parameters (e.g., epochs or dropout) introduced in Section 3.4.2, but we make some modifications due to the problem nature. The changes consist of using a Sigmoid for the activation function and a Binary Cross-Entropy for the loss function.

In Table 6 we compare the results of this binary classification with Test 02 (multi-class classifier). In terms of accuracy, the differences are meaningless (a decrease of less than 0.2%). We observe a worsening of the results concerning errors, although the system works in the EER point (i.e., $FRR = FAR$). This result is still appropriate for a biometrics system since we are still below a 1% [60]. In Table 7, we observe the normalised confusion table of this experiment, which clearly shows a tiny misclassification rate.

4.6. Classification of a non-seen user

In this experiment, we assess the performance of our system against illegitimate samples. In cybersecurity, this kind of attack represents an impersonation attack.

Similarly than in Section 4.5, we build a OvR classifier for each of the eighteen users in the NSRDB. For testing these models against impersonation, we randomly choose a user of the BUTQDB[7]. We generate 3000 EKM images for this user, using the procedure explained in Section 3.4.1. Note that there is no bias between users from the same database or between both databases since no significant heart diseases were discovered in any subjects.

After that, we test each of the models with a set of illegitimate EKMs (i.e., 3000 EKMs of user 111001). We measure how many times each of the images are misclassified as a legitimate user. Next, we compute the average value of these eighteen experiments, representing the probability of success for an adversary to conduct an impersonation attack. Mathematically, assuming a target *user-p* that belongs to the *class-p* and an EKM^q sample of a *user-q* with $q \neq p$:

$$p(\mathscr{A}_I) = p(y = class - p | x = EKM^q) < \alpha \quad (2)$$

In our experiments, the average α value is 0.077. It is a reasonable value for many applications. Note that it implies that the adversary, on average, only bypasses the system one in ten times. A reader can consider that this value is high but likely, many systems are blocked after a much lower number of attempts (e.g., ATM cards are blocked after three attempts[8]).

4.7. Classification of a Noisy User

As a final experiment, we evaluate our system performance when dealing with noisy samples. We randomly choose a user from the NSRDB (e.g., the user-12) and add Gaussian Noise ($\mathcal{N}(0, 0.05)$) to its EKG record. Next, we process this noisy EKG obtaining its R-peaks (see Section 3.2) and computing the EKM images (see Section 3.3).

Once generated these EKMs, we evaluate these new instances with the CNN network of Test 02 (see Section 4.1 for details). After testing 2400 EKMs of the randomly chosen user, the classification accuracy is 99.083%. The above result implies that our proposed system maintains its workability with noisy signals. Note that noisy signals are widespread when the EKG records are captured with low-cost EKG sensors [61].

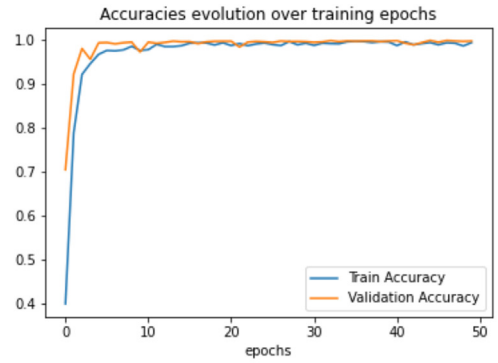
5. Discussion & conclusions

This work proposes a cutting-edge biometric identification technique based on the novel representation of an EKG trace named Electrocardiomatrix (ECM or EKM). Recall that EKMs are a heatmap representation of several aligned peaks of an EKG composed within a matrix. To show our identification proposal's feasibility, we use a simple CNN showing that our approach is enough to identify each user with just one convolutional layer.

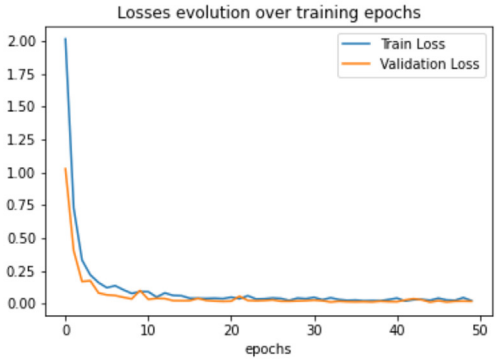
In our approach, the fiducial points (R-peaks) are needed to build the EKM heatmaps, but from this point, we build the identification system based on images, and fiducial points are not involved at all in this part (identification system). This property is in line with some works, such as [17] or [62], that claims that we can achieve better results when the identification avoids the fiducial points (non–handcrafted identification solutions [63]). Nevertheless, other works such as [45] use fiducial points to iden-

[7] In our experiments, the user *111001*.

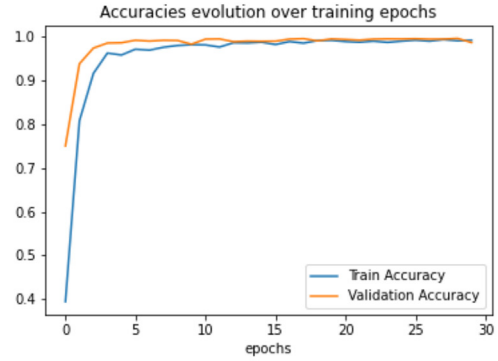
[8] e.g.,https://www.barclays.co.uk/help/cards/debit-card/wrong-pin/



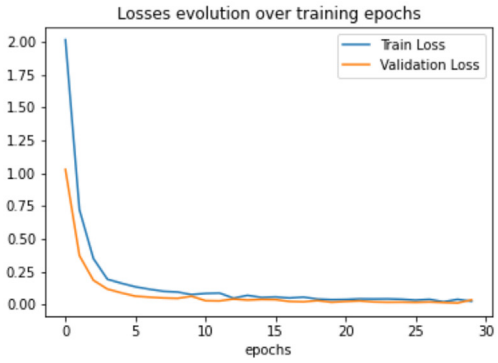
(a) Accuracy during training and validation for **50** epochs with 5bpf over the NSRDB.



(b) Loss during training and validation for **50** epochs with 5bpf over the NSRDB.



(c) Accuracy during training and validation for **30** epochs with 5bpf over the NSRDB.



(d) Loss during training and validation for **30** epochs with 5bpf over the NSRDB.

Fig. 7. Accuracy and Loss during training and validation for 50 and 30 epochs for heatmaps with 5bpf over the NSRDB.

tify users. This approach's main drawback is that detecting all fiducial points on an EKG has a high computational cost. Back to our proposal, there is a handcrafted step in which R-peaks are detected to generate the EKM inputs to the CNN network. Note that this fiducial point is easy to detect (e.g., peaks with higher amplitude), and we employ a well-known and efficient algorithm for getting these peaks (i.e., Pan-Tomkins algorithm).

Table 8 shows a comparison between proposals whose primary goal is to identify individuals through their EKG by applying many different techniques. In the wave mentioned previously, if we compare our solution to [45] based on fiducial points, we can observe that FAR (unauthorised persons are incorrectly accepted) is one magnitude lower in our proposal. Concerning experiment reproducibility, some works (e.g., [16] or [38]) use private databases, which hinder their repeatability. We avoid this critical issue, using NSRDB, MIT-BIHDB, PTBDB and BUTQDB, which all of them are freely available databases at Physionet, as explained in Section 3.1.

Apart from using public datasets, we consider it mandatory to explore the possibility of studying control users without mixing them with patients with CVD, as shown in the experiments with the NSRDB database. We use control users in all the experiments done with the NSRDB motivated by this fact. An opposite example is [49], in which the authors test their solution using the DiSciRi DB. Although the results are very positive, we consider that the authors primarily identify cardiac diseases instead of features that unequivocally identity users.

Regarding our model's efficiency, our EKM images, used to feed the CNN, are heatmaps of an EKG matrix. That is, all the information contained inside each pixel of the picture is meaningful (e.g., there are not black spaces or axis in the image). Contrary to that, in [44], the authors use images with blank spaces, which has consequences on the errors that are a bit high. In detail, abstracting from the used dataset, the errors (FAR and FRR) in our proposal are two magnitudes lower than in [44].

Apart from efficiency, system usability is another critical aspect in the design of a proposal. Our proposal shows its workability using 3, 5 or a maximum of 7 *R*-peaks, which is a low value and demands between 7 and 5 s for acquiring a sample (assuming a subject beating between 60 and 80 heartbeats per second). On the other end, we find solutions such as the one presented in [40]. In this approach, the authors achieve good results but require 20 beats per sample which may render the system unusable for many practical applications.

In line with the user identification using CNNs, we can find the work presented in [64] where their EKG segments are transformed to the wavelet domain to set them as the input of a 1-D CNN. The authors test it over eight different databases with control users and users with CVD, but their results in terms of the Identification Rate (IR) are not as accurate as ours. As we can see in Table 8 their accuracy is very high (99%) as in our proposal (99.98%.)

Cascaded-CNN is the Neural Network technique applied to the work done in [65]. In the presented work two CNNs are used: a first CNN for the feature extraction and a second CNN for User Identification. Their work is tested over different databases as we can see in Table 8 but again, in terms of the IR they can not achieve a high performance as we do. In fact, with the NSRDB they obtain an IR of 93.1% while we obtain a 99.95% with the same database.

Many works that use CNNs as the identification method for EKG signals, use a 1D-CNN instead of the usual 2D-CNN to set as the input of the NN a single vector. This approach is the case of [66] where they use four uni-dimensional convolutional layers together with the euclidian distance for the user identification. Over the

Table 6
Metrics obtained with the OvR experiment with user *14*

Tests	Classification	Loss	Accuracy (%)	FAR (%)	FRR(%)
Test 02	Categorical	0.027	99.47	0.03	0.06
OvR	Binary	0.023	99.33	0.67	0.67

Table 7
Normalised Confusion Matrix from the OvR experiment.

0	**0.987**	**0.013**
1	**0**	**1**
	0	1

PTBDB they obtain a 9.03% of Equal Error Rate (EER) which is a much higher rate than the one we obtain with the same database. Our worst result is a 0.27% of EER with the PTBDB.

Nowadays, the trend for designing identification system is to use Deep Learning approaches. An example of that is [42], in which high-performance metrics concerning the accuracy are obtained.

Table 8
Comparative analysis of ECG-based identification proposals.

Proposal	Year	Database	Subjects	Metric	Identification Method	Result
					DBNN	80
One-lead ECG for identity verification [40]	2002	MITDB	47	Acc (%)	Template Matching	95
				Acc (%)		99
ECG Biometrics: A robust short-time frequency analysis [16]	2010	Ad-hoc	269	EER (%)	MLE	0.37
				FAR (%)		$3.3 \cdot 10^{-5}$
Data improvement model based on ECG biometric for userauthentication and identification [45]	2020	"You snooze you win"	1985	FRR (%)	Feature Extraction + RF Classifier	0.64003
					RNN	93.3
					GRU	96.7
		ECG-ID	90		LSTM	100
					RNN	93.6
					GRU	96.8
ECG-based biometrics using Recurrent Neural Networks [42]	2017	MITDB	47	Acc (%)	LSTM	100
		PTB	290			1.63
Deep-ecg: Convolutional Neural Networks for ECG biometric Recognition [44]	2019	E-HOL-03–0202-003	202	EER (%)	CNN	4.47
		DiSciRi DB	51		MLP	99.3
		SVDB	67		RBF	96.4
ECG biometric with abnormal cardiac conditions in remote monitoring systems [49]	2014	MITDB	46	Acc (%)	NCN kNN	96.7
				IR (%)		98.07
ECG biometric recognition: Template-free approaches based on Deep Learning [43]	2019	PTB		FPIR (%)	Transfer Learning + MLP	13.36
		MITDB	47			99.73
ECG Identification For Personal Authentication UsingLSTM-Based Deep Recurrent NN [51]	2020	NSRDB	18	Acc (%)	Bidireccional LSTM	100
		ECG-ID	90			91.96
		NSRDB	18			99.86
ECG based human identification using Second Order Difference Plots [52]	2019	MITDB	47	Acc (%)	Feature Extraction with SODP + kNN	95.12
HeartID: A Multiresolution Convoltuional Neural Network for ECG-Based Biometric Human Identification in Smart Health Applications [64]	2017	CEBSDB	20	IR (%)	1D-CNN	99.0
		WECG	22			94.5
		FANTASIA	40			97.2
		NSRDB	18			95.1
		STDB	28			90.3
		MITDB	47			91.1
		AFDB	23			93.9
		VFDB	22			86.6
Toward improving ECG biometric identification using cascaded convolutional neural networks [65]	2020	CEBSDB	20	IR (%)	Cascaded-CNN	93.1
		NSRDB	18			91.4
		STDB	28			92.7
		AFDB	23			89.7
An End-to-End Convolutional Neural Network for ECG-Based Biometric	2019	PTBDB	232	EER (%)	1D-CNN	9.06

Table 8 (*continued*)

Proposal	Year	Database	Subjects	Metric	Identification Method		Result
Authentication [66]							
						3 bpf	**99.53**
						5 bpf	99.44
				Acc (%)		7 bpf	99.47
						3 bpf	**0.02**
						5 bpf	0.03
				FAR (%)		7 bpf	0.03
						3 bpf	**0.05**
						5 bpf	0.06
				FRR (%)		7 bpf	0.06
						3 bpf	0.04
						5 bpf	**0.04**
				EER (%)		7 bpf	0.04
						3 bpf	**99.95**
						5 bpf	99.94
				IR (%)		7 bpf	99.94
						3 bpf	**0.02**
						5 bpf	0.03
		NSRDB	18	FPIR (%)	EKM + CNN	7 bpf	0.03
						3 bpf	98.26
						5 bpf	**98.84**
				Acc (%)		7 bpf	98.33
						3 bpf	**0.04**
						5 bpf	**0.02**
				FAR (%)		7 bpf	0.03
						3 bpf	**2.08**
						5 bpf	2.08
				FRR (%)		7 bpf	2.08
						3 bpf	1.06
						5 bpf	**1.05**
				EER (%)		7 bpf	1.06
						3 bpf	**99.93**
						5 bpf	99.95
				IR (%)		7 bpf	99.93
						3 bpf	0.04
						5 bpf	**0.02**
Our Approach	Present	MITDB	48	FPIR (%)	EKM + CNN	7 bpf	0.04
						3 bpf	**89.8**
						5 bpf	87.27
				Acc (%)		7 bpf	79.12
						3 bpf	0.05
						5 bpf	0.06
				FAR (%)		7 bpf	**0.01**
						3 bpf	0.45
						5 bpf	0.48
				FRR (%)		7 bpf	**0.05**
						3 bpf	0.25
						5 bpf	0.27
				EER (%)		7 bpf	**0.03**
						3 bpf	99.91
						5 bpf	99.88
				IR (%)		7 bpf	**99.98**
						3 bpf	0.05
						5 bpf	0.06
		PTBDB	232	FPIR (%)	EKM + CNN	7 bpf	**0.01**

†Notation: Acc (Accuracy); FAR (False Acceptance Rate); FRR (False Rejection Rate); EER (Equal Error Rate); IR (Identification Rate); FPIR (False Positive Identification Error Rate)

These results are achieved as the penalty of using both complex Recurrent Neural Networks (LSTM or GRU) and a higher number of beats (9) per instance. In [43], Hong et al. propose a solution based on Transfer Learning. Interestingly in this proposal, the input images to the network are computed using Pearson's correlation coefficients. The results are slightly lower in terms of accuracy, and errors (FPR) are a magnitude higher than our proposal.

In terms of complexity, we put special attention on simplifying the network while maintaining high performance. In [51], Kim and Pyun obtain almost perfect results as expenses of requiring a complex bidirectional LSTM network, getting the best results with 250 hidden units and three hidden layers. Altan et al. propose a simple K-Nearest Neighbor algorithm as the core of its identification system. Although this approach is more straightforward than our CNN architecture, this proposal's main drawback is that it requires the extraction of features using a Second-Order Difference Plot (SODP), which is more complex than our EKM generation.

All in all, our proposal is competitive in comparison with state of the art. We have proposed a novel biometrics system based on EKG. The use of the EKG guarantees the universality (everyone alive is beating) and permanence (cardiac signals are stable during at least five years [67]) of our system. Collectibility is also satisfied even via low-cost EKG sensors, and the reproducibility is assured by using exclusively public datasets. We show how 3, 5 or 7 heartbeats are enough to generate the input images (EKMs), which guarantees system usability. Also, we can forecast the system

acceptability due to the possibility of acquiring an EKG through non-invasive devices such as a smartwatch and the widespread adoption of these devices [68]. Concerning workability, we achieve almost a perfect accuracy of 99.53% identifying the 18 users of NSRDB. The errors are also at a very level, with a False Acceptance Rate (FAR) and FRR of 0.02% and 0.05%, respectively. We have also tested how our system remains working accurately with noisy EKG inputs. Regarding the resistance to circumvention, the probability of conducting an impersonation is low (i.e., $p(\mathscr{A}_I) =< 0.077$). Therefore, we conclude that EKMs are both an effective technique to help cardiologists diagnose and an effective tool to build an identification system, as explained in this article.

CRediT authorship contribution statement

Caterina Fuster-Barceló: Conceptualization, Methodology, Supervision, Writing - original draft, Writing - review & editing, Validation. **Pedro Peris-Lopez:** Conceptualization, Methodology, Supervision, Writing - review & editing, Funding acquisition, Validation. **Carmen Camara:** Conceptualization, Methodology, Supervision, Writing - review & editing, Validation.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

This work was supported by Leonardo Grant for Researchers and Cultural Creators, BBVA Foundation (P2019-CARDIOSEC); by the Spanish Ministry of Science, Innovation and Universities grant PID2019-111429RBC21(ODIO); and by the Comunidad de Madrid (Spain) under the projects PUCFA (PUCFA-CM-UC3M) and CYNAMON (P2018/TCS-4566)–cofinanced by European Structural Funds (ESF and FEDER).

The authors gratefully acknowledge the computer resources at Artemisa and the technical support provided by the Instituto de Física Corpuscular IFIC (CSIC-UV). The European Union co-founds Artemisa through the 2014-2020 ERDF Operative Programme of Comunitat Valenciana, project IDIFEDER/2018/048.

References

[1] M. Taskiran, N. Kahraman, C.E. Erdem, Face recognition: Past, present and future (a review), Digital Signal Processing vol. 106 (2020), Available: URL: https://www.sciencedirect.com/science/article/pii/S1051200420301548 102809.
[2] N. Senthilkumar et al., Comprehensive review of fingerprint based biometric systems, Journal of Critical Reviews 7 (4) (2020) 1532–1542.
[3] N. Singla, M. Kaur, S. Sofat, Automated latent fingerprint identification system: A review, Forensic Science International vol. 309 (2020), Available: URL: https://www.sciencedirect.com/science/article/pii/S0379073820300499 110187.
[4] M. Al Rousan, B. Intrigila, A Comparative Analysis of Biometrics Types: Literature Review, Journal of Computer Science 16 (12) (2020) 1778–1788.
[5] E. Alajrami, B.A.M. Ashqar, B.S. Abu-Nasser, A.J. Khalil, M.M. Musleh, A.M. Barhoom, S.S. Abu-Naser, Handwritten signature verification using deep learning, International Journal of Academic Multidisciplinary Research (IJAMR) 3 (12) (2020) 39–44.
[6] K. Aizat, O. Mohamed, M. Orken, A. Ainur, and B. Zhumazhanov, "Identification and authentication of user voice using dnn features and i-vector," Cogent Engineering, vol. 7, no. 1, p. 1751557, 2020. [Online]. Available: doi: 10.1080/23311916.2020.1751557.
[7] B. Bhana and S. Flowerday, "Passphrase and keystroke dynamics authentication: Usable security," Computers & Security, vol. 96, p. 101925, 2020. [Online]. Available: URL:https://www.sciencedirect.com/science/article/pii/S0167404820302017.
[8] E. Ellavarason, R. Guest, F. Deravi, R. Sanchez-Riello, and B. Corsetti, "Touch-dynamics based behavioural biometrics on mobile devices - a review from a usability and performance perspective," ACM Comput. Surv., vol. 53, no. 6, Dec. 2020. [Online]. Available: doi: 10.1145/3394713.
[9] S. Adamovic, V. Mišković, N. Macek, M. Milosavljevic, M. Šarac, M. Saracevic, and M. Gnjatovic, "An efficient novel approach for iris recognition based on stylometric features and machine learning techniques," Future Generation Computer Systems, vol. 107, pp. 144–157, 2020. [Online]. Available: URL: https://www.sciencedirect.com/science/article/pii/S0167739X19314463.
[10] P. Kaur, K. Krishan, S.K. Sharma, and T. Kanchan, "Facial-recognition algorithms: A literature review," Medicine, Science and the Law, vol. 60, no. 2, pp. 131–139, 2020, pMID: 31964224. [Online]. Available: doi: 10.1177/0025802419893168.
[11] L.T. Nguyen, H.T. Nguyen, A.D. Afanasiev, and T.V. Nguyen, "Automatic Identification Fingerprint Based on Machine Learning Method," Journal of the Operations Research Society of China, 2021. [Online]. Available: doi: 10.1007/s40305-020-00332-7.
[12] D.P. Wagh, H.S. Fadewar, G.N. Shinde, Biometric finger vein recognition methods for authentication, in: B. Iyer, P.S. Deshpande, S.C. Sharma, U. Shiurkar (Eds.), Computing in Engineering and Technology, Springer Singapore, Singapore, 2020, pp. 45–53.
[13] L. Olanrewaju, O. Oyebiyi, S. Misra, R. Maskeliunas, and R. Damasevicius, "Secure ear biometrics using circular kernel principal component analysis, Chebyshev transform hashing and Bose-Chaudhuri-Hocquenghem error-correcting codes," Signal, Image and Video Processing, vol. 14, no. 5, pp. 847–855, 2020. [Online]. Available: doi: 10.1007/s11760-019-01609-y.
[14] R. Kushwaha and N. Nain, "Person identification using footprint minutiae," in Proceedings of 3rd International Conference on Computer Vision and Image Processing, B.B. Chaudhuri, M. Nakagawa, P. Khanna, and S. Kumar, Eds. Singapore: Springer Singapore, 2020, pp. 285–299.
[15] S. Khan, S. Parkinson, L. Grant, N. Liu, S. Mcguire, Biometric systems utilising health data from wearable devices: applications and future challenges in computer security, ACM Computing Surveys (CSUR) 53 (4) (2020) 1–29.
[16] I. Odinaka, P. Lai, A.D. Kaplan, J.A. O'Sullivan, E.J. Sirevaag, S.D. Kristjansson, A. K. Sheffield, and J.W. Rohrbaugh, "Ecg biometrics: A robust short-time frequency analysis," in 2010 IEEE International Workshop on Information Forensics and Security, 2010, pp. 1–6.
[17] I. Odinaka, P.-H. Lai, A.D. Kaplan, J.A. O'Sullivan, E.J. Sirevaag, J.W. Rohrbaugh, Ecg biometric recognition: A comparative analysis, IEEE Transactions on Information Forensics and Security 7 (6) (2012) 1812–1824.
[18] A.N. Uwaechia and D.A. Ramli, "A comprehensive survey on ecg signals as new biometric modality for human authentication: Recent advances and future challenges," IEEE Access, vol. 9, pp. 97 760–97 802, 2021.
[19] K.N. Plataniotis, D. Hatzinakos, and J.K.M. Lee, "Ecg biometric recognition without fiducial detection," in 2006 Biometrics Symposium: Special Session on Research at the Biometric Consortium Conference, 2006, pp. 1–6.
[20] M. Li, S. Narayanan, Robust ecg biometrics by fusing temporal and cepstral information, in: 2010 20th International Conference on Pattern Recognition, 2010, pp. 1326–1329.
[21] J.M. Irvine, S.A. Israel, M.D. Wiederhold, and B.K. Wiederhold, "A new biometric: human identification from circulatory function," in Joint Statistical Meetings of the American Statistical Association, San Francisco, 2003, pp. 1957–1963.
[22] K.A. Sidek, I. Khalil, and M. Smolen, "Ecg biometric recognition in different physiological conditions using robust normalized qrs complexes," in 2012 Computing in Cardiology, 2012, pp. 97–100.
[23] Y. Zhang, Z. Zhao, Y. Deng, X. Zhang, Y. Zhang, Human identification driven by deep cnn and transfer learning based on multiview feature representations of ecg, Biomedical Signal Processing and Control 68 (2021) 102689.
[24] D. Li, F. Tian, S. Rengifo, G. Xu, M.M. Wang, J. Borjigin, Electrocardiomatrix: A new method for beat-by-beat visualization and inspection of cardiac signals, J. Integr. Cardiol. 1 (5) (2015) 124–128.
[25] V. Lee, G. Xu, V. Liu, P. Farrehi, J. Borjigin, Accurate detection of atrial fibrillation and atrial flutter using the electrocardiomatrix technique, Journal of Electrocardiology 51 (6) (Nov 2018) S121–S125.
[26] D.L. Brown, G. Xu, A.M. Belinky Krzyske, N.C. Buhay, M. Blaha, M.M. Wang, P. Farrehi, and J. Borjigin, "Electrocardiomatrix Facilitates Accurate Detection of Atrial Fibrillation in Stroke Patients," Stroke, vol. 50, no. 7, pp. 1676–1681, Jul 2019. [Online]. Available: URL:https://www.ahajournals.org/journal/str.
[27] G. Xu, S. Dodaballapur, T. Mihaylova, J. Borjigin, Electrocardiomatrix facilitates qualitative identification of diminished heart rate variability in critically ill patients shortly before cardiac arrest, Journal of electrocardiology 51 (6) (2018) 955–961.
[28] R. Salinas-Martínez, J. De Bie, N. Marzocchi, and F. Sandberg, "Automatic detection of atrial fibrillation using electrocardiomatrix and convolutional neural network," in 2020 Computing in Cardiology, 2020, pp. 1–4.
[29] "A review on deep learning methods for ecg arrhythmia classification," Expert Systems with Applications: X, vol. 7, p. 100033, 2020. [Online]. Available: URL: http://www.sciencedirect.com/science/article/pii/S2590188520300123.
[30] F. Gargiulo, A. Fratini, M. Sansone, and C. Sansone, "Subject identification via ecg fiducial-based systems: Influence of the type of qt interval correction," Computer Methods and Programs in Biomedicine, vol. 121, no. 3, pp. 127–136, 2015. [Online]. Available: URL:http://www.sciencedirect.com/science/article/pii/S0169260715001625.
[31] W.-H. Jung and S.-G. Lee, "Ecg identification based on non-fiducial feature extraction using window removal method," Applied Sciences, vol. 7, no. 11, p. 1205, Nov 2017. [Online]. Available: URL:https://doi.org/10.3390/app7111205.

[32] "Toward improving ecg biometric identification using cascaded convolutional neural networks," Neurocomputing, vol. 391, pp. 83–95, 2020. [Online]. Available: URL:http://www.sciencedirect.com/science/article/pii/S0925231220300485.
[33] B. Pourbabaee, M. Howe-Patterson, E. Reiher, and F. Benard, "Deep convolutional neural network for ecg-based human identification," CMBES Proceedings, vol. 41, May 2018. [Online]. Available: URL:https://proceedings.cmbes.ca/index.php/proceedings/article/view/684.
[34] J. Pan and W.J. Tompkins, "A real-time qrs detection algorithm," IEEE Transactions on Biomedical Engineering, vol. BME-32, no. 3, pp. 230–236, 1985.
[35] M. Manikandan and K. Soman, "A novel method for detecting r-peaks in electrocardiogram (ecg) signal," Biomedical Signal Processing and Control, vol. 7, no. 2, pp. 118–128, 2012. [Online]. Available: URL:http://www.sciencedirect.com/science/article/pii/S1746809411000292.
[36] A. Kumar, M. Kumar, R. Komaragiri, Design of a biorthogonal wavelet transform based r-peak detection and data compression scheme for implantable cardiac pacemaker systems, Journal of Medical Systems 42 (6) (2018) 102.
[37] P. Jafari Moghadam Fard, M. Moradi, and M. Tajvidi, "A novel approach in r peak detection using hybrid complex wavelet (hcw)," International Journal of Cardiology, vol. 124, no. 2, pp. 250–253, 2008. [Online]. Available: URL:http://www.sciencedirect.com/science/article/pii/S0167527307002719.
[38] L. Biel, O. Pettersson, L. Philipson, P. Wide, Ecg analysis: a new approach in human identification, IEEE Transactions on Instrumentation and Measurement 50 (3) (2001) 808–812.
[39] H. Silva, A. Lourenço, F. Canento, A.L. Fred, N. Raposo, Ecg biometrics: Principles and applications, Biosignals (2013) 215–220.
[40] T.-W. Shen, W. Tompkins, and Y. Hu, "One-lead ecg for identity verification," in Proceedings of the Second Joint 24th Annual Conference and the Annual Fall Meeting of the Biomedical Engineering Society][Engineering in Medicine and Biology, vol. 1. IEEE, 2002, pp. 62–63.
[41] G.B. Moody, R.G. Mark, The impact of the mit-bih arrhythmia database, IEEE Engineering in Medicine and Biology Magazine 20 (3) (2001) 45–50.
[42] R. Salloum and C. J. Kuo, "Ecg-based biometrics using recurrent neural networks," in 2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2017, pp. 2062–2066.
[43] P.L. Hong, J.Y. Hsiao, C.H. Chung, Y.M. Feng, S.C. Wu, Ecg biometric recognition: Template-free approaches based on deep learning, in: in 2019 41st Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), 2019, pp. 2633–2636.
[44] R.D. Labati, E. Muñoz, V. Piuri, R. Sassi, F. Scotti, Deep-ecg: convolutional neural networks for ecg biometric recognition, Pattern Recognition Letters 126 (2019) 78–85.
[45] A. Barros, P. Resque, J. Almeida, R. Mota, H. Oliveira, D. Rosário, E. Cerqueira, Data improvement model based on ecg biometric for user authentication and identification, Sensors 20 (10) (2020) 2920.
[46] M. Ghassemi, B. Moody, L.-W. Lehman, C. Song, Q. Li, H. Sun, M.B. Westover, and G. Clifford, "You snooze, you win: The physionet/computing in cardiology challenge 2018," 12 2018.
[47] A. Goldberg, "Ecg-id database," March 2014. [Online]. Available: doi: 10.13026/C2J01F
[48] A.L. Goldberger, L.A.N. Amaral, L. Glass, J.M. Hausdorff, P.C. Ivanov, R.G. Mark, J. E. Mietus, G.B. Moody, C.-K. Peng, and H.E. Stanley, "PhysioBank, PhysioToolkit, and PhysioNet: Components of a new research resource for complex physiologic signals," Circulation, vol. 101, no. 23, pp. e215–e220, 2000 (June 13), circulation Electronic Pages: http://circ.ahajournals.org/content/101/23/e215.full PMID:1085218; doi: 10.1161/01.CIR.101.23.e215.
[49] K.A. Sidek, I. Khalil, H.F. Jelinek, Ecg biometric with abnormal cardiac conditions in remote monitoring system, IEEE Transactions on Systems, Man, and Cybernetics: Systems 44 (11) (2014) 1498–1509.
[50] M.O. Diab, A. Seif, M. Sabbah, M. El-Abed, and N. Aloulou, A Review on ECG-Based Biometric Authentication Systems. Singapore: Springer Singapore, 2020, pp. 17–44. [Online]. Available: doi: 10.1007/978-981-13-0956-4_2.
[51] B.-H. Kim and J.-Y. Pyun, "Ecg identification for personal authentication using lstm-based deep recurrent neural networks," Sensors, vol. 20, no. 11, 2020. [Online]. Available: URL:https://www.mdpi.com/1424-8220/20/11/3069.
[52] G. Altan, Y. Kutlu, and M. Yeniad, "Ecg based human identification using second order difference plots," Computer Methods and Programs in Biomedicine, vol. 170, pp. 81–93, 2019. [Online]. Available: URL:https://www.sciencedirect.com/science/article/pii/S0169260717301530.
[53] A. Goldberg, "Physiobank, physiotoolkit, and physionet: Components of a new research resource for complex physiologic signals. circulation [online]. 101 (23), pp. e215–e220," Aug 1999. [Online]. Available: doi: 10.13026/C2NK5R.
[54] R. Bousseljot, D. Kreiseler, and A. Schnabel, "Nutzung der ekg-signaldatenbank cardiodat der ptb über das internet," 1995.
[55] L. Smital, C.R. Haider, M. Vitek, P. Leinveber, P. Jurak, A. Nemcova, R. Smisek, L. Marsanova, I. Provaznik, C.L. Felton, B.K. Gilbert, D.R. Holmes, Real-Time Quality Assessment of Long-Term ECG Signals Recorded by Wearables in Free-Living Conditions, IEEE Transactions on Biomedical Engineering 67 (10) (Oct 2020) 2721–2734.
[56] A. Krizhevsky, I. Sutskever, G.E. Hinton, Imagenet classification with deep convolutional neural networks, in: Advances in neural information processing systems, 2012, pp. 1097–1105.
[57] Y. LeCun, B.E. Boser, J.S. Denker, D. Henderson, R.E. Howard, W.E. Hubbard, L.D. Jackel, Handwritten digit recognition with a back-propagation network, in: Advances in neural information processing systems, 1990, pp. 396–404.
[58] A. Krizhevsky and G. Hinton, "Convolutional deep belief networks on cifar-10," Unpublished manuscript, vol. 40, no. 7, pp. 1–9, 2010.
[59] D.P. Kingma and J. Ba, "Adam: A method for stochastic optimization," arXiv preprint arXiv:1412.6980, 2014.
[60] R. Srivastva, A. Singh, and Y.N. Singh, "Plexnet: A fast and robust ecg biometric system for human recognition," Information Sciences, vol. 558, pp. 208–228, 2021. [Online]. Available: URL:https://www.sciencedirect.com/science/article/pii/S0020025521000025.
[61] V. Ponciano, I.M. Pires, F.R. Ribeiro, and N.M. Garcia, "Data acquisition of timed-up and go test with older adults: accelerometer, magnetometer, electrocardiography and electroencephalography sensors' data", Data in Brief, vol. 32, p. 106306, 2020. [Online]. Available: URL:https://www.sciencedirect.com/science/article/pii/S2352340920312002.
[62] M. Ingale, R. Cordeiro, S. Thentu, Y. Park, and N. Karimian, "Ecg biometric authentication: A comparative analysis," IEEE Access, vol. 8, pp. 117 853–117 866, 2020.
[63] A.S. Rathore, Z. Li, W. Zhu, Z. Jin, and W. Xu, "A survey on heart biometrics," ACM Comput. Surv., vol. 53, no. 6, Dec. 2020. [Online]. Available: doi: 10.1145/3410158.
[64] Q. Zhang, D. Zhou, and X. Zeng, "Heartid: A multiresolution convolutional neural network for ecg-based biometric human identification in smart health applications," IEEE Access, vol. 5, pp. 11 805–11 816, 2017.
[65] Y. Li, Y. Pang, K. Wang, X. Li, Toward improving ecg biometric identification using cascaded convolutional neural networks, Neurocomputing 391 (2020) 01.
[66] J.R. Pinto and J.S. Cardoso, "An end-to-end convolutional neural network for ecg-based biometric authentication," in 2019 IEEE 10th International Conference on Biometrics Theory, Applications and Systems (BTAS), 2019, pp. 1–8.
[67] C. Camara, P. Peris-Lopez, and J.E. Tapiador, "Human identification using compressed ecg signals," Journal of Medical Systems, vol. 39, no. 11, p. 148, Sep 2015. [Online]. Available: doi: 10.1007/s10916-015-0323-2.
[68] B. Reeder and A. David, "Health at hand: A systematic review of smart watch uses for health and wellness," Journal of Biomedical Informatics, vol. 63, pp. 269–276, 2016. [Online]. Available: URL:https://www.sciencedirect.com/science/article/pii/S1532046416301137.

Caterina Fuster-Barceló received the B.S. degree of Telematics Engineering from Universitat de les Illes Balears, Spain, in 2019. She is currently pursuing a PhD degree at Universidad Carlos III de Madrid, Madrid, Spain. Her research interests include Biometrics techniques based in Deep Neural Networks usage focusing on Computer Vision.

Pedro Peris-Lopez received the M.Sc. degree in telecommunications engineering and the PhD degree in computer science from the Carlos III University of Madrid, Spain, in 2004 and 2008, respectively. He is currently an Associate Professor with the Department of Computer Science, Carlos III University of Madrid. His research interests are in the field of cybersecurity and e-health, digital forensics and hardware security. He has published a large number of articles in specialized journals (62) and conference proceedings (45). His works have more than 5200 citations, and his h-index is 33. For additional information, see https://www.-lightweightcryptography.com/.

Carmen Camara received a PhD degree in computer science and a PhD in biomedical engineering. She is currently an Assistant Professor with the Computer Security Laboratory, Carlos III University of Madrid, Spain. Her research interests are in the fields of cybersecurity in e-Health, bioengineering, and data science. Her webpage is https://carmen-camara.com.