ECG Authentication for Mobile Devices

Article *in* IEEE Transactions on Instrumentation and Measurement · December 2015

DOI: 10.1109/TIM.2015.2503863

CITATIONS
138

READS
2,997

3 authors:

Juan Arteaga-Falconi
University of Ottawa
6 PUBLICATIONS **272** CITATIONS
SEE PROFILE

Hussein Al Osman
University of Ottawa
66 PUBLICATIONS **910** CITATIONS
SEE PROFILE

Abdulmotaleb El Saddik
Mohamed bin Zayed University of Artificial Intelligence
742 PUBLICATIONS **11,816** CITATIONS
SEE PROFILE

ECG Authentication for Mobile Devices

Juan Sebastian Arteaga-Falconi, *Graduate Student Member, IEEE*, Hussein Al Osman, and Abdulmotaleb El Saddik, *Fellow, IEEE*

***Abstract*— Traditional mobile login methods, like numerical or graphical passwords, are vulnerable to passive attacks. It is common for intruders to gain access to personal information of their victims by watching them enter their passwords into their mobile screens from a close proximity. With this in mind, a mobile biometric authentication algorithm based on electrocardiogram (ECG) is proposed. With this algorithm, the user will only need to touch two ECG electrodes (lead I) of the mobile device to gain access. The algorithm was tested with a cell phone case heart monitor in a controlled laboratory experiment at different times and conditions with ten subjects and also with 73 records obtained from the Physionet database. The obtained results reveal that our algorithm has 1.41% false acceptance rate and 81.82% true acceptance rate with 4 s of signal acquisition. To the best of our knowledge, this is the first approach on mobile authentication that uses ECG biometric signals and it shows a promising future for this technology. Nonetheless, further improvements are still needed to optimize accuracy while maintaining a short acquisition time for authentication.**

***Index Terms*— Biometrics, electrocardiogram (ECG) authentication, electrocardiography, human identification, mobile authentication, mobile security, portable ECG.**

I. Introduction

MOBILE smart devices have become indispensable gadgets for numerous functions. Users are becoming more comfortable with the idea of storing highly private information such as e-mails, photos, and other sensitive documents on such devices. The popular mobile login methods rely on numerical or graphical passwords. These techniques are vulnerable to shoulder surfing attacks instigated by individuals with line-of-sight from a short distance [1] in order to see the phone screen or the movement of the fingers with the goal of stealing the password.

Biometric technologies offer better security mechanisms over traditional authentication methods [2], like password-based ones, given the fact that the biometric feature is a unique physiological characteristic that is always present and, depending on the method used, may not be visible to other people. However, one concern is that some biometric techniques have certain hardware and response time requirements that make them inappropriate for mobile devices (as we will discuss in Section II-B).

Manuscript received May 28, 2015; revised October 10, 2015; accepted October 11, 2015. This work was supported by the Ecuadorian Government under the 2013 SENESCYT Scholarship Program. The Associate Editor coordinating the review process was Dr. Kurt Barbe.

The authors are with the Multimedia Communications Research Laboratory, University of Ottawa, Ottawa, ON K1N 6N5, Canada (e-mail: jarte060@uottawa.ca; halosman@uottawa.ca; elsaddik@uottawa.ca).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIM.2015.2503863

Fingerprint is a popular biometric technique and has been used for over 100 years [3] in different applications, including authentication on mobile phones. But fingerprint authentication can fail if the fingerprint is damaged [4] or, in a worst case scenario, spoofed by an attacker that captures the prints left by users on objects [5]. This vulnerability has been demonstrated with commercial mobile phones that use fingerprint authentication [6].

Electrocardiogram (ECG) methods have the advantage of concealing the biometric features during authentication. However, complex hardware is required to acquire this signal, making it hard to implement in mobile devices. In spite of this, some companies have already developed ECG devices that work with mobile phones [7] for medical monitoring purposes. To the best of our knowledge, these devices have not been used for authentication in any commercial product or research study.

Current ECG authentication algorithms, such as the ones proposed in [8]–[18], show good results in validating users. Nonetheless, they are not designed to work in mobile environments given the fact that they require lengthy ECG signals or need to be combined with other biometric methods in order to achieve satisfactory results. This is not viable on mobile devices, where users cannot wait long periods of time to gain access.

Given the advantages of ECG biometric authentication, in this paper, we propose an ECG-based authentication algorithm that is specifically tailored for mobile devices, with two electrodes (lead I), and requires a short acquisition time. The rest of this paper is structured as follows. In Section II, we present some existing ECG authentication algorithms. In Section III, we describe our proposed ECG authentication algorithm. The evaluation of our algorithm is presented in Section IV, where we describe our experiment and analyze the obtained results. In Section V, we provide a brief summary of the contributions made and ideas for future work.

II. Background and Related Works

A. Biometrics and Mobile Phones

According to [19], biometrics is any human physiological (e.g., face [20], eyes [21], fingerprints-palm [22], or ECG [9]) or behavioral (e.g., signature [23], voice [24], gait [25], or keystroke pattern [26]) characteristic that is measurable and present in everybody and that has unique differences that will not change significantly over time. A biometric technique can work in two modes: authentication or identification [27]; and the reliability can be measured by the false

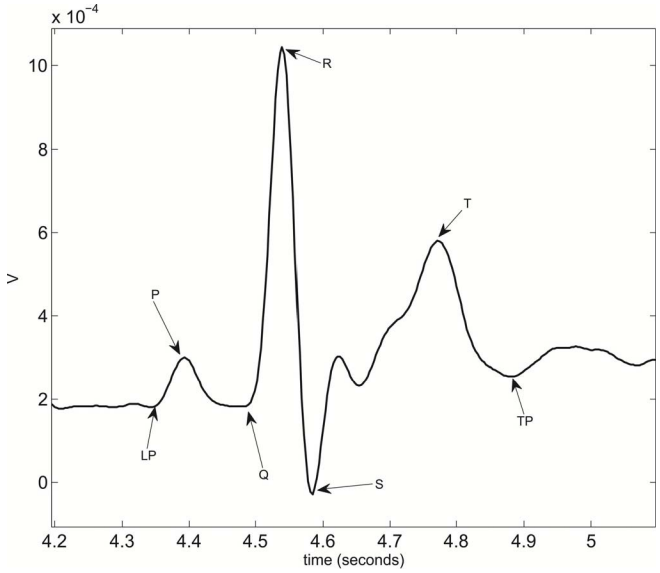

Fig. 1. Fiducial points of the ECG signal. Peaks are P, R, and T. Valleys are LP, Q, S, and TP.

acceptance rate (FAR) [28], false rejection rate [28], true rejection rate [27], and true acceptance rate (TAR) [27].

Existing approaches in biometric mobile access use the iris [29], voice [30], face [31], gesture [1], gait [32], or the fusion of different biometrics (e.g., voice, face, and signature) [33] for authentication. These technologies face challenges in terms of mobile phone deployment.

Iris biometric authentication is a reliable technology but depends heavily on the acquisition of good quality images with appropriate lightning condition [34]. The mobile access method through voice recognition is susceptible to environmental noise or can be tricked by audio records [35]. Mobile gait authentication is implemented using onboard accelerometer data [32]. Derawi *et al.* [32] suggest that validation rates are promising but are not reliable enough for practical use yet. According to [1], gesture-based authentication passwords can be stolen if attempts are not limited and with a properly trained attacker. Fingerprint authentication in mobiles is already available on the market by different companies; consequently it has been tested by consumers. The security vulnerabilities have been discussed in different publications and online articles. Many security experts have concluded that fingerprint authentication can be spoofed through the use of latex [6].

B. ECG as Biometric Authentication Technique

Electrocardiogram, better known as ECG, is a method used to measure and record the electrical potential generated by the heart on the skin. An ECG heartbeat is shown in Fig. 1 and has three main complexes: 1) P; 2) QRS; and 3) T. The sensor that measures this signal is called the electrocardiograph; it captures the information by means of conductive electrodes placed on the surface of the arms, legs, and chest wall [36]. In ECG, the term lead is commonly used and it refers to virtual vectors along which the electrical depolarization of the heart is measured. The medical community has defined 12 possible vectors known as lead: I, II, III, aVR, aVL, aVF, V_1, V_2, V_3, V_4, V_5, and V_6 [36]. For instance, lead I refer to the measurement of the depolarization across a lateral vector going from left to right across the chest (or from the right hand to the left hand). Therefore, only two electrodes are required to register a lead I signal.

An ECG signal is distinct for every individual. Its uniqueness is a result of gender, heart mass orientation, conductivity, and order of activation of cardiac muscles [37]–[39]. Traditional medicine has made efforts to universalize this signal to produce a general diagnostic method applicable to most people [40], but the distinctiveness of ECG among individuals, a challenge in medicine, is an advantage in biometrics [18].

Numerous studies have demonstrated ECG-based authentication to be a robust biometric method. To prove that it is possible to identify people using ECG, Biel *et al.* [9] used a method based on the shape of the signal. They extracted time-based, amplitude-based, and slope features for classification. Their results show that it is possible to identify a person from a predefined group of people using ECG. They also conclude that it is not necessary to use a 12-lead configuration with a 10-electrode ECG sensor nor it is imperative; one lead—three electrodes—is enough to achieve good results [9].

Another ECG biometric approach is presented by Singh and Singh [16], where they extract 20 features from each heartbeat, including those based on time, amplitude, and angles. They calculate the Euclidean distance between each feature from the enrollment template and authentication template. The experiment was done with records from 73 subjects obtained from the MIT/BIH Physionet database [41], with a sample duration of at least 3 min. The results obtained are 82.00% TAR with a 7.00% FAR. These rates are further improved when they combined ECG biometrics with fingerprint authentication and face recognition. The resultant multimodal system produced a 99.00% TAR.

A physiological analysis of ECG and its relation to the features extracted to apply ECG identification is presented by Israel *et al.* [11]. In this work, they analyze how time ECG features (e.g., R–P distance, R–T distance, R–LP distance, R–Q distance, R–S distance, R–TP distance, P width, T width, S–T distance, P–Q distance, P–T distance, LP–Q distance, and S–TP distance) are affected by heart rate changes. They conclude that linear normalization can be applied to eliminate the effects of heart rate changes on such features. The normalization is done by dividing the length of each affected feature by the total length of the correspondent ECG beat. Amplitudes are not considered since a change in the placement of the electrodes directly affects these values. The experiment was performed with 29 subjects with samples of 20 s at different states of anxieties and with different electrode placement positions. The analytic classification was performed based on a linear discriminant analysis of the features, and the results obtained conclude that a correct classification can be performed even if the heart rate is affected by different states of anxiety and independent of the placement of electrodes.

One concern for ECG biometrics is the length of time that a record can remain valid. To address this concern,

Wübbeler *et al.* [12] performed ECG verification based on a database of 74 subjects, where the data were collected with a time difference ranging from months to years. To produce an enrollment or authentication templates, they combine, through the Euclidean norm, three ECG recordings of 10 s that correspond to lead I, lead II and lead III signals. The authentication is performed by applying the standard nearest neighbor algorithm. They achieved a TAR of 98.10%. Therefore, they state that ECG biometrics is still applicable several years after the generation of an enrollment template.

C. Conclusion

Given the works presented Sections II-A and II-B, we conclude that ECG can be used as a biometric technique [38]. If we consider FAR and TAR rates as the measuring factors for the quality of an ECG biometric algorithm, some of the referenced works present good results, with TAR above 95.00% and FAR between 3.00% and 5.00%.

In order to apply ECG authentication to mobile phones, a number of factors need to be considered, namely, the number of electrodes, quality of mobile ECG sensors, time required to gain access to the phone, FAR, and TAR. None of the algorithms in the presented studies are tailored for mobile authentication. Specifically, [8] uses a nonmobile friendly 12-lead sensor, and [11] and [15] require the capture of lengthy ECG signals (10 and 180 s, respectively).

In this paper, we present our ECG authentication algorithm that uses signals captured via a lead I sensor (left arm–right arm). This allows users to input their biometric data by touching two electrodes with their fingers. The employed ECG sensor is a practical mobile phone heart monitor that produces a somewhat modest quality signal. Furthermore, we have set a short time limit for the length of the ECG authentication. Since the algorithm execution time (order of milliseconds) is negligible compared with the signal capture time, the overall authentication time must remain short.

III. Design of an ECG Authentication Algorithm for Mobiles

An ECG signal $\mathbf{E}[n]$, shown in (1), with a length of N, has to be treated before applying our authentication algorithm. The steps involved in the enrollment and authentication are shown in Fig. 2. In the first stage, peaks and valleys (fiducial points) from the ECG signal are detected. This allows us to align and normalize the signal in order to avoid the effects of changes in heart rate. Once the signal is normalized, we proceed to extract the features. If we are enrolling a new user, the extracted features allow us to create an enrollment template to be stored in memory. If we are authenticating a user, the extracted features generate an authentication template. This authentication template is used by the algorithm to authenticate a user against an enrollment template (stored in memory). The following section explains these steps and also the main contribution of this work, which is our ECG authentication algorithm:

$$\mathbf{E}[e_1, e_2, \ldots, e_{N-1}, e_N]. \tag{1}$$

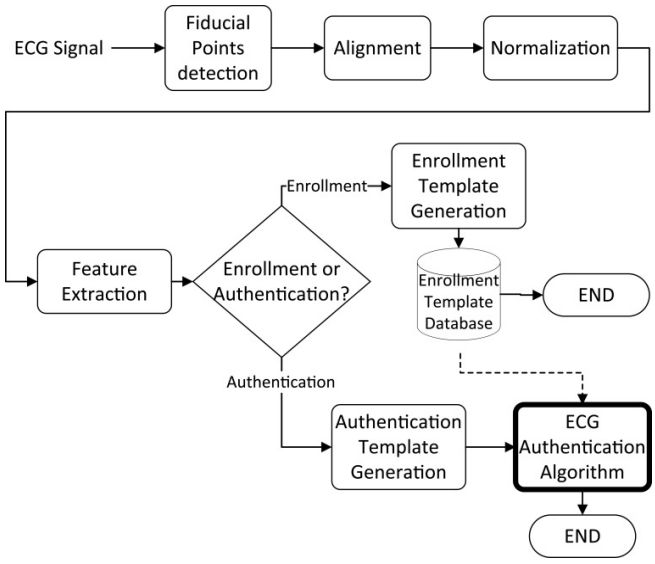

Fig. 2. Preprocessing stages for the ECG signal before applying the ECG authentication algorithm.

A. Fiducial Point Detection

The fiducial points used in this algorithm are shown in Fig. 1, and they are LP, P, Q, R, S, T, and TP. There are many good techniques to detect these fiducial points, in this paper, we use the techniques presented in [42] and [43] that are based on differentiation. We use these techniques because our algorithm is aimed for mobile phones, where processing resources are potentially scarce. Arzeno *et al.* [44] have shown that fiducial point detection methods based on differentiation are computationally more efficient than their counterpart.

After the fiducial point detection, we create the vectors shown in (2). These vectors contain the indices of the R, S, Q, P, T, LP, and TP fiducial points, respectively, found in vector $\mathbf{E}$

$$\begin{aligned}
&\mathbf{R}[r_1, r_2, \ldots, r_{B-1}, r_B]\\
&\mathbf{S}[s_1, s_2, \ldots, s_{B-1}, s_B]\\
&\mathbf{Q}[q_1, q_2, \ldots, q_{B-1}, q_B]\\
&\mathbf{P}[p_1, p_2, \ldots, p_{B-1}, p_B]\\
&\mathbf{T}[t_1, t_2, \ldots, t_{B-1}, t_B]\\
&\mathbf{LP}[lp_1, lp_2, \ldots, lp_{B-1}, lp_B]\\
&\mathbf{TP}[tp_1, tp_2, \ldots, tp_{B-1}, tp_B].
\end{aligned} \tag{2}$$

In other words, vector $\mathbf{R}[b]$ is the series of indices of R peaks found in $\mathbf{E}[i]$; where $1 \leq b \leq B$ and B is the number of heartbeats present in $\mathbf{E}[i]$; each heartbeat is delimited by the LP and TP valleys (see Fig. 3). The same applies for vector $\mathbf{S}[b]$ that stores the series of indices of the S valleys found in $\mathbf{E}$ and so forth repeats for the rest of the fiducial points.

The amplitudes $\mathbf{RA}[b]$, $\mathbf{SA}[b]$, and $\mathbf{QA}[b]$ of the fiducial points $\mathbf{R}[b]$, $\mathbf{S}[b]$, and $\mathbf{Q}[b]$ are the values of $\mathbf{E}[i]$ corresponding to the indices of the fiducial points $\mathbf{R}[b]$, $\mathbf{S}[b]$, and $\mathbf{Q}[b]$.

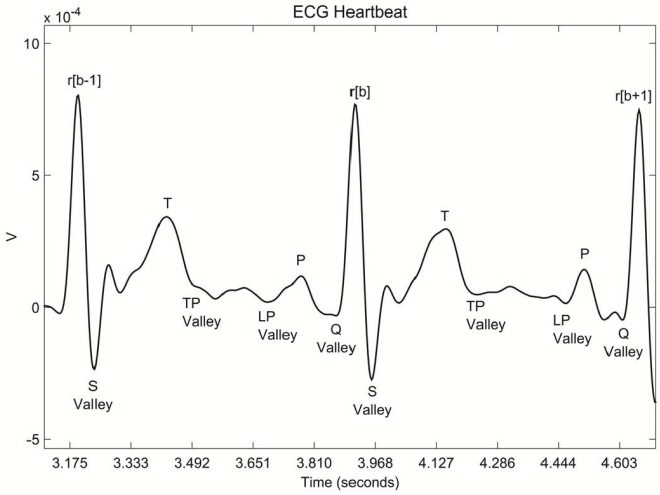

Fig. 3. Detection of Q, S, LP, and TP valleys and P, R, and T peaks. A heartbeat is limited by LP and TP valleys.

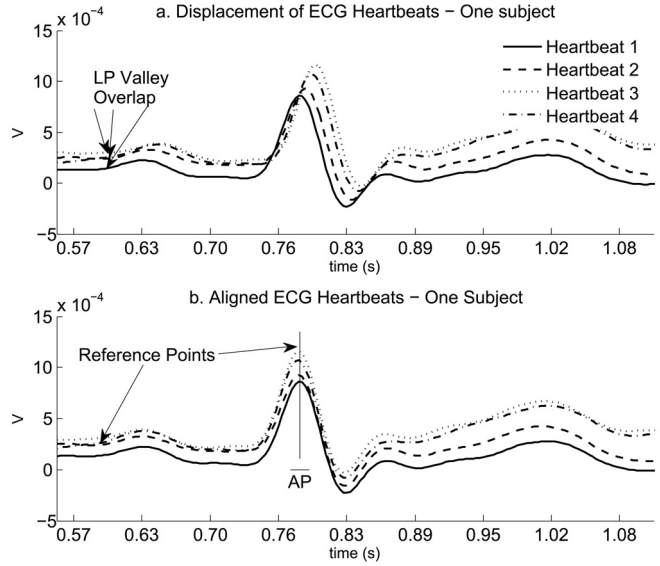

Fig. 4. Alignment of the ECG heartbeats. (a) R peaks are grouped in the same time reference. (b) ECG signals after alignment to the mean of R peaks as reference point.

This is shown in

$$\begin{aligned}\mathbf{RA}[b] &= \mathbf{E}[\mathbf{R}[b]]\\ \mathbf{SA}[b] &= \mathbf{E}[\mathbf{S}[b]]\\ \mathbf{QA}[b] &= \mathbf{E}[\mathbf{Q}[b]], \quad 1 \le b \le B\end{aligned} \tag{3}$$

where B is the total number of heartbeats present in $\mathbf{E}[i]$.

B. Alignment

This process consists of shifting all the ECG heartbeats to align them around a reference point (see Fig. 4). Since R is the fiducial point less affected by noise (due to its distinguishable form), we use it to align all ECG heartbeats. Hence, first, we need to shift all the ECG heartbeats so that their starting points, in this case the LP valley, overlap [see Fig. 4(a)]. Then, with all the ECG heartbeats starting at the same point, we calculate the median of the indices values of the R peaks. This median value is our alignment point $\overline{AP}$ that is used as a reference to align the rest of the fiducial points using (4). The aligned heartbeats are shown in Fig. 4(b)

$$\begin{aligned}\mathbf{RL}[b] &= \overline{AP}\\ \mathbf{SL}[b] &= \mathbf{S}[b] - \mathbf{R}[b] + \overline{AP}\\ \mathbf{QL}[b] &= \mathbf{Q}[b] - \mathbf{R}[b] + \overline{AP}\\ \mathbf{PL}[b] &= \mathbf{P}[b] - \mathbf{R}[b] + \overline{AP}\\ \mathbf{TL}[b] &= \mathbf{T}[b] - \mathbf{R}[b] + \overline{AP}\\ \mathbf{LPL}[b] &= \mathbf{LP}[b] - \mathbf{R}[b] + \overline{AP}\\ \mathbf{TPL}[b] &= \mathbf{TP}[b] - \mathbf{R}[b] + \overline{AP}, \quad 1 \le b \le B.\end{aligned} \tag{4}$$

At this stage, the R peaks of all the heartbeats overlap. But we have not yet taken into account the changes in the heart rate; this will be done through the normalization process.

C. Normalization

Different heuristic studies show that changes in the heart rate are linear [9], [11]. Therefore, a linear normalization process of the signal is applied to match the ECG of a subject despite any changes in the rate of their heartbeats. In this paper, we are using a normalization that is based on a unitary system [11] where the duration of each feature is divided by the total length of a heartbeat.

The normalization of the fiducial points (necessary to extract the features) is stored in vectors

$$\begin{aligned}&\mathbf{SN}[b]\\ &\mathbf{QN}[b]\\ &\mathbf{PN}[b]\\ &\mathbf{TN}[b]\\ &\mathbf{LPN}[b]\\ &\mathbf{TPN}[b].\end{aligned} \tag{5}$$

As previously mentioned, the ECG amplitude with respect to 0 V changes constantly, but the amplitude relative to the R peak depends on the placement of the electrodes. Since for this study all ECG records are taken through the same setup, there is no need to normalize the amplitudes; the relative amplitudes remain the same [11]. In the case of the ECG records from the mobile devices, the signal always comes from the fingers. For the case of the ECG records from Physionet [41], the ECG signal comes from lead I sensor.

D. Feature Extraction

With all the heartbeats of the ECG signal aligned and normalized, the next step is to extract the unique features of the ECG by which a person can be identified. In Fig. 5, the eight features extracted are shown. After preliminary experiments, these features were selected since they tend to remain identifiable in the presence of noise. These features are the same as in [9] and [16]; they came from the fiducial points previously indicated in (2). It is important to mention that those studies extract more features than the ones indicated

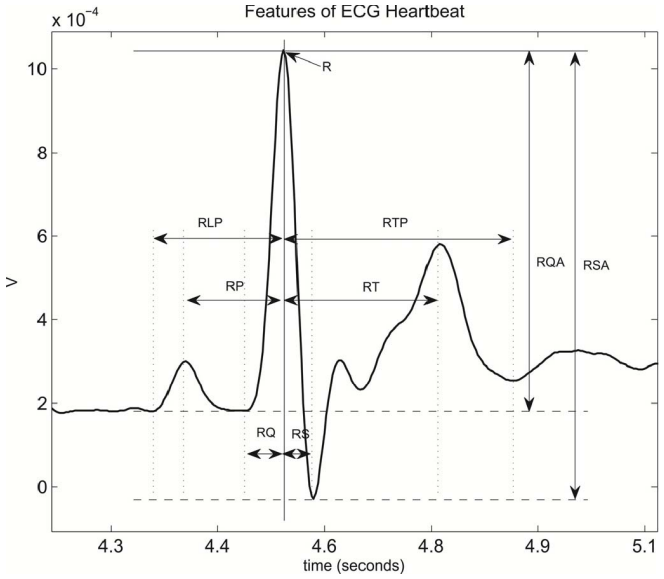

Fig. 5. ECG features that are used in our ECG authentication algorithm. There are six time and two amplitude-based features.

here, and this is due to the quality of ECG signal in the mobile; some of the features are not possible to get.

The process of extracting the features requires the use of $\overline{\mathbf{AP}}$ as a reference for subtraction of the normalized vectors. This is done using

$$\begin{aligned}
\mathbf{RLP}[b] &= \overline{\mathbf{AP}} - \mathbf{lpn}[b] \\
\mathbf{RP}[b] &= \overline{\mathbf{AP}} - \mathbf{pn}[b] \\
\mathbf{RQ}[b] &= \overline{\mathbf{AP}} - \mathbf{qn}[b] \\
\mathbf{RS}[b] &= \mathbf{sn}[b] - \overline{\mathbf{AP}} \\
\mathbf{RT}[b] &= \mathbf{tn}[b] - \overline{\mathbf{AP}} \\
\mathbf{RTP}[b] &= \mathbf{tpn}[b] - \overline{\mathbf{AP}}, \quad 1 \leq b \leq B. \qquad (6)
\end{aligned}$$

The amplitude difference of the Q and S valleys with respect to the R peak is calculated in $\mathbf{RQA}[b]$ and $\mathbf{RSA}[b]$ vectors as presented in

$$\begin{aligned}
\mathbf{RQA}[b] &= \mathbf{ra}[b] - \mathbf{qa}[b] \\
\mathbf{RSA}[b] &= \mathbf{ra}[b] - \mathbf{sa}[b], \quad 1 \leq b \leq B. \qquad (7)
\end{aligned}$$

E. Template Generation

ECG features in every heartbeat vary slightly, even for the same person. This is a common phenomenon for any biological signal. Nonetheless, in order to create a template, a median of all the extracted features is calculated.

Two types of templates are required: 1) enrollment template and 2) authentication template. The enrollment template is generated when a user registers for the first time. The authentication template is generated every time a user tries to gain access.

1) Enrollment Template: The enrollment template is generated with an ECG signal longer than the authentication template. The amount of time that a template remains valid has not been determined and can be analyzed in a future study.

The template is expressed by ten vectors: 1) $\overline{\mathrm{RLP}_T}$; 2) $\overline{\mathrm{RP}_T}$; 3) $\overline{\mathrm{RQ}_T}$; 4) $\overline{\mathrm{RS}_T}$; 5) $\overline{\mathrm{RT}_T}$; 6) $\overline{\mathrm{RTP}_T}$; 7) $\overline{\mathrm{RQA}_T}$; 8) $\overline{\mathrm{RSA}_T}$; 9) $\overline{\mathrm{AP}}$; and 10) $\overline{\mathrm{TPL}}$. The value of each vector corresponds to the median value of the extracted features.

The template information must be encrypted and stored in a secure location. It can be the phone memory, smart card, or a central database. The storage security details of the template are beyond the scope of this work.

2) Authentication Template: Once we have an enrollment template, we can generate the authentication template. This template is generated every time a user tries to gain access, then the authentication template requires a shorter ECG signal; which gives a faster access time to the mobile device.

The generation of the authentication template is similar to the enrollment template, except that for the alignment and the normalization we do not calculate $\overline{\mathbf{AP}}$ and $\overline{\mathbf{TPL}}$, but we use the values obtained at the enrollment template stage (see Fig. 2). After this, we extract the features as previously indicated.

With the features extracted, we calculate the median of all the features: $\overline{\mathrm{RLP}_A}$, $\overline{\mathrm{RP}_A}$, $\overline{\mathrm{RQ}_A}$, $\overline{\mathrm{RS}_A}$, $\overline{\mathrm{RT}_A}$, $\overline{\mathrm{RTP}_A}$, $\overline{\mathrm{RQA}_A}$, and $\overline{\mathrm{RSA}_A}$.

With this information, the authentication algorithm will compare the authentication template against the enrollment template to conclude whether the user should be given access (see Fig. 2).

F. Authentication Algorithm

The proposed authentication algorithm is shown in Fig. 6 and differs from previous ECG authentication algorithms in two aspects: 1) the use of feature specific percentage of tolerance (i.e., each ECG feature has its own threshold) and 2) the adoption of a *hierarchical validation scheme*.

All the time-based features, except RTP (because R and TP, which are used for normalization, are equivalent during enrollment and authentication), are evaluated individually, and if they fall in the accepted range of tolerance, a counter is increased. Once this process is completed, if the value of the counter reaches an established score, the time-based features are considered valid.

Once the time-based features are validated, then the algorithm proceeds to check the RS amplitude. If the RS amplitude falls into the accepted range, the RQ amplitude will then be verified. If it is within an accepted threshold, then the system will validate the user. If any check of these amplitude features fails, then the algorithm concludes that the authentication template is a nonmatch.

In this scheme, amplitude features are given more prominence than the other features. If all the time-based feature checks pass and the amplitudes checks do not, then a nonmatch conclusion is reached. In our preliminary experiments, we analyzed ECG signals from 73 subjects and after the calculation of the feature variance across subjects, we observed that the highest deviations occur on the amplitude features. Therefore, we concluded that these features tend to be more disparate across subjects than the time-based features. Therefore, they are given more prominence in our hierarchical validation scheme.

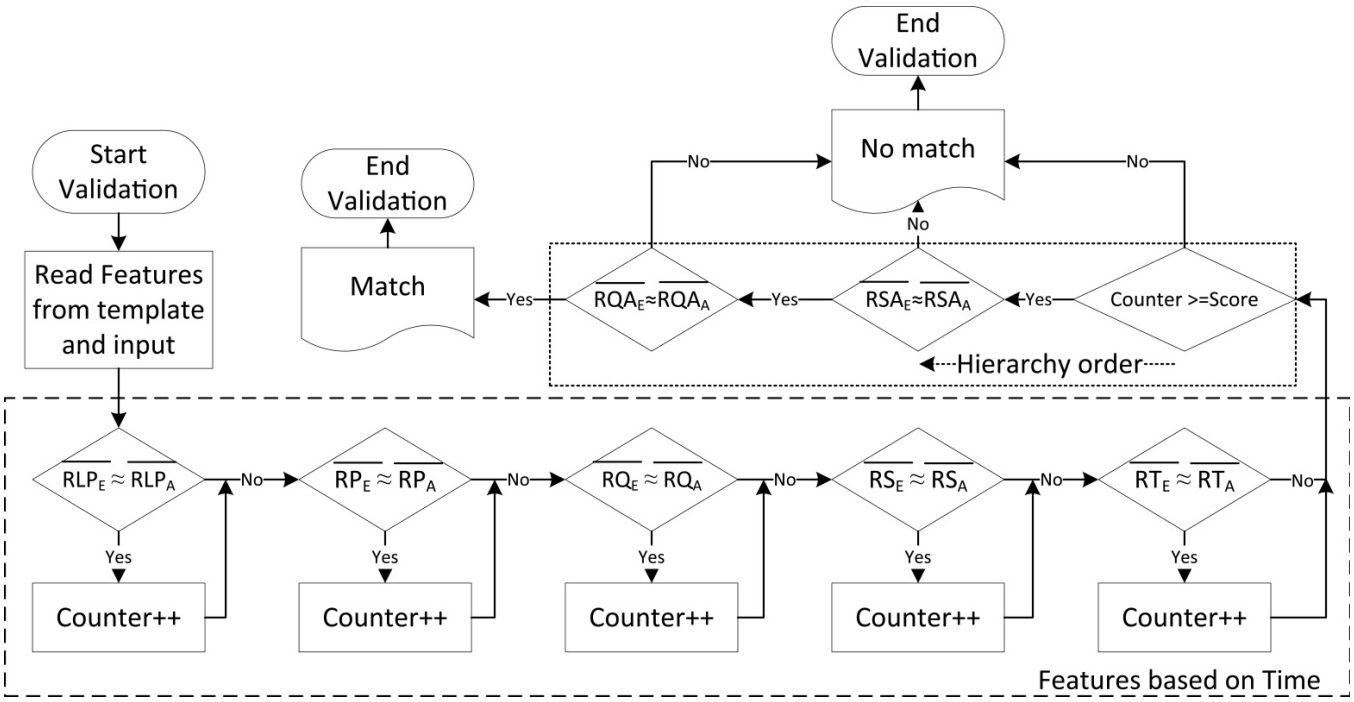

Fig. 6. ECG authentication algorithm. Each feature from the enrollment template E is compared against each feature from the authentication template A. The time-based features generate a score. If the score reaches the minimum value, then it goes to validate the features based on the amplitudes. The amplitude validation follows a hierarchy order, $\overline{RSA}$ is first and then $\overline{RQA}$.

The advantage of this hierarchical algorithm is that it takes each feature individually. It is the result of a standard deviation analysis of each feature. In this way, we know which features are more likely to be similar between other users and which ones are more different. In another works, we say that some features are more important to distinguish than others. The algorithm is built on this basis; then it helps to achieve better results than other process that takes all the features with the same degree of importance. The outcome under the same conditions without the hierarchical algorithm would be 0.21% FAR and 50.41% TAR. These results are very impressive in terms of FAR but not in terms of TAR, because a TAR of 50.41% means that a genuine user will be rejected almost half of the attempts to access the system.

IV. Evaluation of the Algorithm

The algorithm was tested in three stages. The first stage is to find the threshold values that will be used in the authentication evaluation. The second stage is to assess the authentication accuracy of the algorithm using 73 ECG records corresponding to 73 subjects from the Physionet database [41]. The third stage is to assess the authentication accuracy of the algorithm through an evaluation performed at the MCRLab at the University of Ottawa with ECG data collected from ten subjects using a mobile phone-based ECG sensor. In this paper, we will refer to the term subject to the ECG data extracted from people at the laboratory and the term record will refer to the data extracted from the Physionet database.

To establish an appropriate time for authentication, we estimated the time required for the users to input their traditional passwords in their phones. It was found that it takes them an average time of 4 s from ten users in the laboratory.

A. Finding of Thresholds

Our algorithm uses independent threshold values for each one of the extracted ECG features. This section explains the procedure to obtain these values.

1) ECG Data: To search for the most appropriate thresholds, we used 73 different records from four Physionet [41] databases: 1) European ST–T database [45]; 2) MIT-BIH Normal Sinus Rhythm database [46]; 3) MIT–BIH Arrhythmia database [47]; and 4) QT database [48].

2) Threshold Search: The search for threshold values was conducted using a batch process. Each feature has a corresponding threshold value. For each feature, the process initially sets the corresponding threshold at 100.00% of that feature's value in the enrollment template. The thresholds are then decreased by steps of 1.00%, one at a time, until they all reach 0.00% of their corresponding features. Therefore, the process performs a brute force search for optimal thresholds by testing all possible combinations of threshold values (within a 1.00% precision). For each combination of threshold values, the process calculates the FAR and TAR. The best results in terms of the difference between TAR and FAR, qualify for a second and more sensitive threshold search.

The second threshold search is localized around $\pm 1.00\%$ of the best results previously identified and uses steps of 0.01%.

3) Results: The evaluation of different combinations of the threshold values is shown in Fig. 7, where combination 5 is the one that achieves the best results. We can observe that FAR reaches 1.41% and TAR 81.82%. Threshold values of combination 5 are indicated in Table I.

Table I shows the threshold values in which the algorithm was tested. Each combination has a set of eight numbers.

TABLE I
SYSTEM RESPONSE BY DIFFERENT THRESHOLD VALUES

FEATURE	Comb.1	Comb.2	Comb.3	Comb.4	Comb. 5
RS	12.60 %	12.60 %	12.90 %	12.90 %	12.90 %
RT	11.30 %	11.30 %	11.30 %	11.30 %	11.30 %
RQ	17.09 %	17.09 %	17.09 %	17.09 %	17.09 %
RP	18.80 %	18.80 %	18.80 %	18.80 %	18.80 %
RLP	13.20 %	13.20 %	13.20 %	10.00 %	10.00 %
RQA	45.00 %	30.00 %	26.00 %	25.90 %	22.00 %
RSA	26.00 %	26.00 %	16.50 %	11.00 %	17.00%
score	5	4	4	4	4

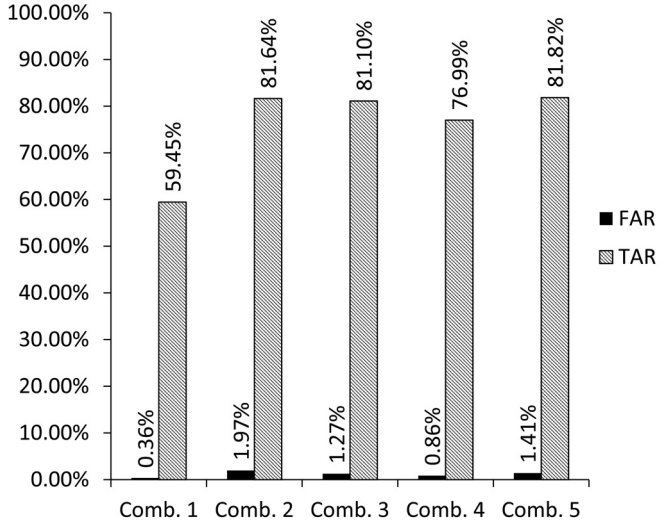

Fig. 7. FAR and TAR results for combinations of threshold values. Only one portion of all the combinations is shown.

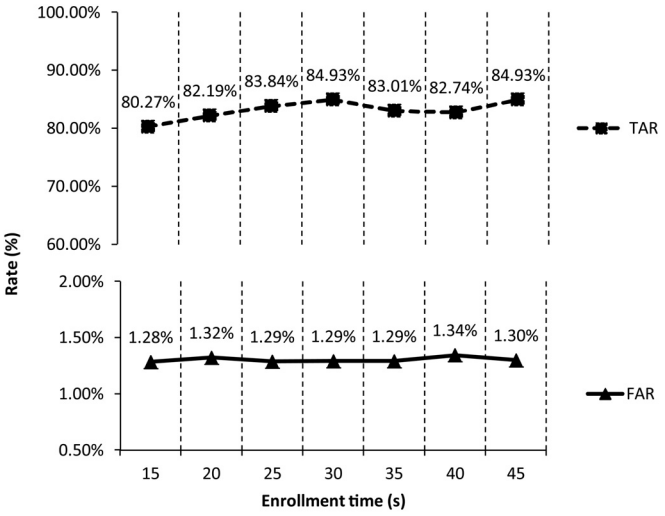

Fig. 8. Algorithm response to changes in the enrollment time length.

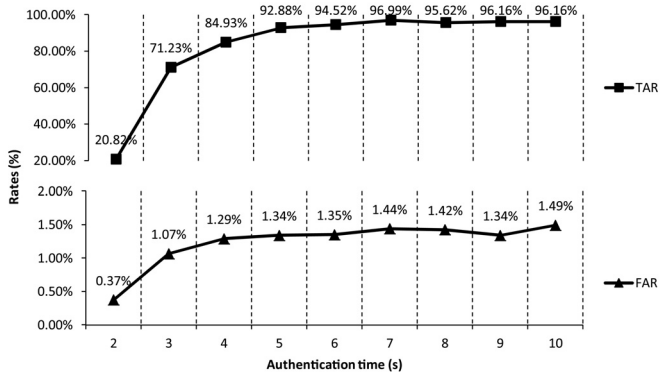

Fig. 9. Algorithm response to changes in the authentication time length.

These numbers represent the seven features and a value for score (refer to Fig. 6 for score). The results of each combination datum from Table I are presented in Fig. 7.

B. Experiment Using Physionet ECG Records

We ran our algorithm using comparable ECG data to similar studies such as [12], [16], and [17]. These studies use 73 or 74 records from the Physionet databases to validate their algorithms. In our experiment, we therefore used 73 records from the same Physionet databases as [16] and [17]. This allowed us to compare our experimental results with those of these studies and simultaneously validate the results obtained in the laboratory experiment.

The 73 records were obtained from the same databases used for the threshold search (see Section IV-A1, but from records that belongs to different subjects than the ones used in the threshold search. The time length for the ECG records of the database varies from 30 min to up to 24 h. These signals have been previously analyzed by physicians and are part of different research projects in the medical and electrical field. Each record belongs to different patients, but there is only one acquisition session per patient. From each ECG record, we extracted four continuous and nonoverlapping sections at random starting points. The first section was used for enrollment and the other sections were used for authentication.

The test was performed using MATLAB to extract data from Physionet [41]. Each time a new user was enrolled, the algorithm was executed with the authentication templates of all users, one at a time. Only a single user was enrolled at any point of time. In other words, at any point of time, we had one client and 72 imposters.

The algorithm was evaluated with enrollment times of 15, 20, 25, 30, 35, 40, and 45 s. The experiments were performed on the 73 records from Physionet database. The algorithm response in terms of FAR and TAR is presented in Fig. 8.

To evaluate the effects of an increase or decrease in the authentication time, we tested the algorithm with records of 2–10 s in time length. The TAR and FAR recorded for these various record lengths are shown in Fig. 9. This is the result of the 73 records from Physionet database at different authentication times.

Based on the results shown in Fig. 8, we see that the best enrollment time is achieved at 30 s. After that, it gets stable. For authentication time, we can see in Fig. 9 that at 4 s the TAR is 84.93% and FAR is 1.29%. The results at 5 s and later are better and become more stable. We refer to the value of 4 seconds for the laboratory experiment because it is the

Fig. 10. ECG mobile sensor used in the laboratory experimentation from AliveCore [7].

average time that a user takes to input a traditional password on their phones.

C. Laboratory Experiment

A laboratory experiment was conducted using a lead I ECG sensor from AliveCor [7] with two electrodes. The sensor can be fitted onto a mobile phone's case. It has two electrodes with an analog-to-digital converter of 16-bit resolution and a sampling frequency of 300 Hz [7]. This sensor transmits data over an audible band at 20 KHz using FM modulation with bandwidth of 0.62–40 Hz. The input dynamic range is 10 mV peak-to-peak and an input impedance of 100 MΩ. A desktop computer with MATLAB was used to receive the ECG signal, to perform the calculations, and to test the algorithm.

Ten individuals from the MCRLab at the University of Ottawa participated in the test. Seven males and three females with an average age of 28 years and a standard deviation of 2.86. The participants were either standing or sitting on a chair depending on their preference, but none of them were moving during data collection.

The ECG acquisition was conducted in two sessions, where in each session, 2-min-long ECG records were collected using the AliveCor device (shown in Fig. 10). During each session, the subjects were simply asked to hold the sensor for the 2-min period while avoiding any sudden hand movement.

The sessions were conducted on different days and at different times of the day. Given the difference of time between the sessions, it is assumed that during each session, the subject was in at least a slightly different physiological and psychological situation. During the second session, two male participants explicitly stated that they have just completed a physical exercise and one expressed that he is a bit stressed. According to [11], these conditions are corrected by the normalization process.

From the ECG record of the first session, we extracted 30 s worth of data for enrollment (starting at a random point). From the ECG signal of the second session, we extracted three continuous and nonoverlapping sections at random starting points. Each section is 4 s long and is used for authentication.

The evaluation of TAR and FAR was performed for each user; this means that after enrolling a user, the authentication templates of all users were employed, one at a time, to run the authentication algorithm. Only a single user was enrolled at any point of time. With this, in each evaluation, we had one client and nine imposters. The user that was a client at the first evaluation will become an imposter for the rest of the evaluations. With this, we evaluated all the users against all the users.

With the data of the ten subjects previously described, our proposed ECG authentication rendered an FAR of 1.41% and a TAR of 81.82%. These results are almost similar to the results obtained with the database. This is shown in Table II.

TABLE II
RESULTS OF THE ALGORITHMS

Algorithm	No. Subjects	TAR	FAR	Authent. length	Enroll length
Singh et al. [16]	73	82.00%	7.00%	½ of record	½ of record
Wübbeler et al. [12]	74	97.00%	3.00%	10 s.	10 s.
Singh et al. [17]	73	95.55%	4.45%	10 heart beats	10 heart beats
Proposed Algorithm (Laboratory Experiment)	10	81.82%	1.41%	4 s.	30 s.
Proposed Algorithm (Database)	73	84.93%	1.29%	4 s.	30 s.

D. Discussion

In Table II, the results of this presented work and previous works on ECG authentication are presented. Each of the referenced works uses a different approach to measure the time required for the enrollment and the authentication process. Singh and Singh [16] indicate that they used one half of each record for enrollment and the other half for authentication. They used four databases and the time length of each record is different; it can be 15 min [48], 30 min [47], 2 h [45], or even 25 h [46]. In any of these scenarios, the length of the enrollment and authentication templates is larger than the ones used in our study. In [17], they measure the length of the authentication and enrollment templates by number of heartbeats. They are using ten heartbeats; therefore, the length of the record used varies depending on the heart rate. According to [17], an ECG beat can have up to 1040 ms; therefore, we approximate the length of the templates to 10.4 s.

The proposed algorithm reduces the FAR by over 5.00% and increases the TAR by almost 3.00% in comparison with [16]. The TAR we obtained (84.93%) is lower than the one presented in [12] and [17]; but the FAR we attained (1.29%) is also lower than any of these works, with the advantage that the required time to perform the authentication with our proposed algorithm is 4 s only.

The mobile ECG sensor used in this study does not allow us to extract other features (i.e., features based on peak and valley angles, length of valleys, or data combination with other leads)

used in other works such as [9], [11], [12], [16], and [17]; because, as mentioned previously, this device is not sensitive enough to pick up these subtle features. Consequently, good results obtained in previous works are inapplicable in a mobile authentication setup.

The state of anxiety of the user for the laboratory experiments was not formally asked; some of them stated this aspect. We are considering that these conditions are corrected by the normalization process [11].

From our preliminary tests, we found that the best performance could be obtained with an enrolment template of 30 s. We noticed that if the enrollment template length is increased, the performance of the algorithm does not improve significantly; when it reaches 30 seconds, TAR and FAR fluctuates around the same value. These minorfluctuations show that the results at this point become almost the same. Therefore, we picked 30 seconds for our training time because is the shortest time where the results does not change significantly.

Note that we had set at the beginning of the study the authentication template length to 4 s as part of our requirements for an acceptable mobile phone access experience. In Fig. 9, we can observe that we can get better results with a longer authentication time, but we estimated that 4 s is the limit for a user comfort. If we sacrifice 1 s in the user comfort, we will have better results. We can observe that for 5 s we achieve a TAR of 92.88% and an FAR of 1.34%. After 5 s, it keeps improving the results but without a big difference.

The TAR and FAR achieved by the proposed mobile ECG biometric method are inferior to the ones typically attained by fingerprint biometric systems, where Cappelli *et al.* [49] obtained an FAR of 2.07% and a TAR of 97.93%. However, the vulnerability of fingerprint authentication technologies (i.e., failure to authenticate when the prints are damaged [4] or to be spoofed by capturing the prints left on objects [5]) motivates the study of alternative methods that do not suffer from the same weaknesses, such as ECG authentication. ECG authentication methods are relatively new; hence, we foresee an increase in their accuracy as sensory technologies improve.

ECG authentication can be applied to nonmobile applications such as room access control, forensics, and identification or in a multimodal biometric scheme. In the latter, an increased level of accuracy can be attained if ECG authentication is used in combination with other biometric technologies (e.g., fingerprint authentication).

V. Conclusion

In this paper, we have proposed a new ECG authentication algorithm that can be used in mobile devices. The algorithm was tested with a sensor designed for a mobile environment. The obtained results show that the algorithm is suitable to work with mobiles and with other sensors; as it was tested also with Physionet database. To the best of our knowledge, this is the first ECG authentication approach designed exclusively for mobile phones. The proposed algorithm uses a hierarchal scheme that reduces the acquisition time of ECG signals to 4 s for authentication. We evaluated our algorithm with ten subjects using a mobile phone ECG sensor. We obtained an 81.82% TAR and a 1.41% FAR. Furthermore, we also evaluated the algorithm using ECG records from the Physionet database. We obtained 84.93% TAR and 1.29% FAR. We have compared our results with those of three existing algorithms; the comparison accounted for authentication time, FAR, and TAR. We have shown that the proposed algorithm can be as reliable as other existing ones (in terms of FAR and TAR) with the advantage of a supporting shorter acquisition time (4 s). Our future works will aim to improve the TAR and FAR using machine learning algorithms, such as support vector machines.

References

[1] G. D. Clark and J. Lindqvist, "Engineering gesture-based authentication systems," *IEEE Pervasive Comput.*, vol. 14, no. 1, pp. 18–25, Jan./Mar. 2015.

[2] R. W. Frischholz and U. Dieckmann, "BiolD: A multimodal biometric identification system," *Computer*, vol. 33, no. 2, pp. 64–68, Feb. 2000.

[3] E. H. Holder, Jr., L. O. Robinson, and J. H. Laub, "The fingerprint sourcebook," Dept. Justice, Office Justice Programs, Nat. Inst. Justice, Office Justice Programs, Washington, DC, USA, Tech. Rep. NCJ 225321, 2011.

[4] P. J. Phillips, A. Martin, C. L. Wilson, and M. Przybocki, "An introduction evaluating biometric systems," *Computer*, vol. 33, no. 2, pp. 56–63, Feb. 2000.

[5] M. Espinoza, C. Champod, and P. Margot, "Vulnerabilities of fingerprint reader to fake fingerprints attacks," *Forensic Sci. Int.*, vol. 204, nos. 1–3, pp. 41–49, Jan. 2011.

[6] (2013). *Chaos Computer Club breaks Apple TouchID*. [Online]. Available: http://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid

[7] *Heart Monitor AC-002 User Manual*, AliveCor, Inc., San Francisco, CA, USA, Apr. 2015.

[8] Y. Wang, K. N. Plataniotis, and D. Hatzinakos, "Integrating analytic and appearance attributes for human identification from ECG signals," in *Proc. Biometrics Symp., Special Session Res. Biometric Consortium Conf.*, Sep./Aug. 2006, pp. 1–6.

[9] L. Biel, O. Pettersson, L. Philipson, and P. Wide, "ECG analysis: A new approach in human identification," *IEEE Trans. Instrum. Meas.*, vol. 50, no. 3, pp. 808–812, Jun. 2001.

[10] T. W. Shen, W. J. Tompkins, and Y. H. Hu, "One-lead ECG for identity verification," in *Proc. 24th Annu. Conf. Annu. Fall Meeting Biomed. Eng. Soc. EMBS/BMES Conf. Eng. Med. Biol.*, 2002, pp. 62–63.

[11] S. A. Israel, J. M. Irvine, A. Cheng, M. D. Wiederhold, and B. K. Wiederhold, "ECG to identify individuals," *Pattern Recognit.*, vol. 38, no. 1, pp. 133–142, Jan. 2005.

[12] G. Wübbeler, M. Stavridis, D. Kreiseler, R.-D. Bousseljot, and C. Elster, "Verification of humans using the electrocardiogram," *Pattern Recognit. Lett.*, vol. 28, no. 10, pp. 1172–1175, Jul. 2007.

[13] F. Sufi, I. Khalil, and I. Habib, "Polynomial distance measurement for ECG based biometric authentication," *Secur. Commun. Netw.*, vol. 3, no. 4, pp. 303–319, Jul./Aug. 2010.

[14] F. Sufi and I. Khalil, "An automated patient authentication system for remote telecardiology," in *Proc. Int. Conf. Intell. Sensors, Sensor Netw. Inf. Process. (ISSNIP)*, Dec. 2008, pp. 279–284.

[15] S. Z. Fatemian, F. Agrafioti, and D. Hatzinakos, "HeartID: Cardiac biometric recognition," in *Proc. 4th IEEE Int. Conf. Biometrics, Theory Appl. Syst. (BTAS)*, Sep. 2010, pp. 1–5.

[16] Y. N. Singh and S. K. Singh, "Evaluation of electrocardiogram for biometric authentication," *J. Inf. Secur.*, vol. 3, no. 1, pp. 39–48, Jan. 2012.

[17] Y. N. Singh and S. K. Singh, "Identifying individuals using eigenbeat features of electrocardiogram," *J. Eng.*, vol. 2013, Feb. 2013, Art. ID 539284.

[18] A. D. C. Chan, M. M. Hamdy, A. Badre, and V. Badee, "Wavelet distance measure for person identification using electrocardiograms," *IEEE Trans. Instrum. Meas.*, vol. 57, no. 2, pp. 248–253, Feb. 2008.

[19] F. Agrafioti, F. M. Bui, and D. Hatzinakos, "Medical biometrics: The perils of ignoring time dependency," in *Proc. IEEE 3rd Int. Conf. Biometrics, Theory, Appl., Syst. (BTAS)*, Sep. 2009, pp. 1–6.

[20] H. Sellahewa and S. A. Jassim, "Image-quality-based adaptive face recognition," *IEEE Trans. Instrum. Meas.*, vol. 59, no. 4, pp. 805–813, Apr. 2010.

[21] M. S. Hosseini, B. N. Araabi, and H. Soltanian-Zadeh, "Pigment melanin: Pattern for iris recognition," *IEEE Trans. Instrum. Meas.*, vol. 59, no. 4, pp. 792–804, Apr. 2010.

[22] J. Doi and M. Yamanaka, "Discrete finger and palmar feature extraction for personal authentication," *IEEE Trans. Instrum. Meas.*, vol. 54, no. 6, pp. 2213–2219, Dec. 2005.

[23] D. Wang, Y. Zhang, C. Yao, J. Wu, H. Jiao, and M. Liu, "Toward force-based signature verification: A pen-type sensor and preliminary validation," *IEEE Trans. Instrum. Meas.*, vol. 59, no. 4, pp. 752–762, Apr. 2010.

[24] S. Engelberg, Y. Saidoff, and Y. Israeli, "Voice identification through spectral analysis," *IEEE Instrum. Meas. Mag.*, vol. 9, no. 5, pp. 52–55, Oct. 2006.

[25] A. Kale *et al.*, "Identification of humans using gait," *IEEE Trans. Image Process.*, vol. 13, no. 9, pp. 1163–1173, Sep. 2004.

[26] S. Liu and M. Silverman, "A practical guide to biometric security technology," *IT Prof.*, vol. 3, no. 1, pp. 27–32, Jan. 2001.

[27] S. R. M. Prasanna, S. K. Sahoo, and T. Choubisa, "Multimodal biometric person authentication: A review," *IETE Tech. Rev.*, vol. 29, no. 1, pp. 54–75, 2012.

[28] S. K. Dahel and Q. Xiao, "Accuracy performance analysis of multimodal biometrics," in *Proc. IEEE Syst., Man Cybern. Soc. Inf. Assurance Workshop*, Jun. 2003, pp. 170–173.

[29] D.-H. Cho, K. R. Park, D. W. Rhee, Y. Kim, and J. Yang, "Pupil and iris localization for iris recognition in mobile phones," in *Proc. 7th ACIS Int. Conf. Softw. Eng., Artif. Intell., Netw., Parallel/Distrib. Comput. (SNPD)*, Jun. 2006, pp. 197–201.

[30] W.-S. Chen and J.-F. Huang, "Speaker recognition using spectral dimension features," in *Proc. 4th Int. Multi-Conf. Comput. Global Inf. Technol. (ICCGI)*, Aug. 2009, pp. 132–137.

[31] Q. Tao and R. Veldhuis, "Biometric authentication system on mobile personal devices," *IEEE Trans. Instrum. Meas.*, vol. 59, no. 4, pp. 763–773, Apr. 2010.

[32] M. O. Derawi, C. Nickel, P. Bours, and C. Busch, "Unobtrusive user-authentication on mobile phones using biometric gait recognition," in *Proc. 6th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process. (IIH-MSP)*, Oct. 2010, pp. 306–311.

[33] L. Allano *et al.*, "Nonintrusive multibiometrics on a mobile device: A comparison of fusion techniques," *Proc. SPIE*, vol. 6202, p. 62020P, Apr. 2006.

[34] F. Scotti and V. Piuri, "Adaptive reflection detection and location in iris biometric images by using computational intelligence techniques," *IEEE Trans. Instrum. Meas.*, vol. 59, no. 7, pp. 1825–1833, Jul. 2010.

[35] S. Wang and J. Liu, "Biometrics on mobile phone," in *Recent Application in Biometrics*. Rijeka, Croatia: InTech, Jul. 2011, pp. 3–22, doi: 10.5772/17151.

[36] A. L. Goldberger, *Clinical Electrocardiography: A Simplified Approach*, 8th ed. Amsterdam, The Netherlands: Elsevier, 2012.

[37] R. Hoekema, G. J. H. Uijen, and A. van Oosterom, "Geometrical aspects of the interindividual variability of multilead ECG recordings," *IEEE Trans. Biomed. Eng.*, vol. 48, no. 5, pp. 551–559, May 2001.

[38] A. van Oosterom, R. Hoekema, and G. J. Uijen, "Geometrical factors affecting the interindividual variability of the ECG and the VCG," in *Proc. 25th Annu. ISCE Conf. Res. Technol. Transf. Comput. Electrocardiol.*, Tenaya Lodge, CA, USA, Apr./May 2000, vol. 33. no. 2000, pp. 219–227.

[39] B. P. Simon and C. Eswaran, "An ECG classifier designed using modified decision based neural networks," *Comput. Biomed. Res.*, vol. 30, no. 4, pp. 257–272, Aug. 1997.

[40] H. W. Draper, C. J. Peffer, F. W. Stallmann, D. Littmann, and H. V. Pipberger, "The corrected orthogonal electrocardiogram and vectorcardiogram in 510 normal men (Frank lead system)," *Circulation*, vol. 30, no. 6, pp. 853–864, 1964.

[41] A. L. Goldberger *et al.*, "PhysioBank, PhysioToolkit, and PhysioNet: Components of a new research resource for complex physiologic signals," *Circulation*, vol. 101, no. 23, pp. e215–e220, Jun. 2000.

[42] B.-U. Kohler, C. Hennig, and R. Orglmeister, "The principles of software QRS detection," *IEEE Eng. Med. Biol. Mag.*, vol. 21, no. 1, pp. 42–57, Jan./Feb. 2002.

[43] J. S. Arteaga-Falconi, H. Al Osman, and A. El Saddik, "R-peak detection algorithm based on differentiation," in *Proc. IEEE 9th Int. Symp. Intell. Signal Process. (WISP)*, May 2015, pp. 1–4.

[44] N. M. Arzeno, Z.-D. Deng, and C.-S. Poon, "Analysis of first-derivative based QRS detection algorithms," *IEEE Trans. Biomed. Eng.*, vol. 55, no. 2, pp. 478–484, Feb. 2008.

[45] A. Taddei *et al.*, "The European ST-T database: Standard for evaluating systems for the analysis of ST-T changes in ambulatory electrocardiography," *Eur. Heart J.*, vol. 13, no. 9, pp. 1164–1172, 1992.

[46] Beth Israel Deaconess Medical Center. *MIT-BIH Normal Sinus Rhythm Database*. [Online]. Available: http://physionet.org/physiobank/database/nsrdb/, accessed 2015.

[47] G. B. Moody and R. G. Mark, "The impact of the MIT-BIH arrhythmia database," *IEEE Eng. Med. Biol. Mag.*, vol. 20, no. 3, pp. 45–50, May/Jun. 2001.

[48] P. Laguna, R. G. Mark, A. Goldberg, and G. B. Moody, "A database for evaluation of algorithms for measurement of QT and other waveform intervals in the ECG," in *Proc. Comput. Cardiol.*, Sep. 1997, pp. 673–676.

[49] R. Cappelli, D. Maio, D. Maltoni, J. L. Wayman, and A. K. Jain, "Performance evaluation of fingerprint verification systems," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 28, no. 1, pp. 3–18, Jan. 2006.

Juan Sebastian Arteaga-Falconi (S'06–M'09–GSM'12) received the Engineering degree in electronics from Politecnica Salesiana University, Cuenca, Ecuador, in 2008, and the M.A.Sc. degree in electrical and computer engineering from the University of Ottawa, Ottawa, ON, Canada, in 2013, where he is currently pursuing the Ph.D. degree in electrical and computer engineering.

He was with SODETEL Company Ltd., Cuenca, from 2008 to 2011, where he was the Co-Founder and served as the General Manager. He joined the Multimedia Communications Research Laboratory, University of Ottawa, in 2012, where he is currently a Teaching Assistant. His current research interests include biometrics, signal processing, system security, and machine learning.

Mr. Arteaga-Falconi received the 2011 and 2013 SENESCYT Ecuadorian Scholarship for graduate studies. He served as a Treasurer in the IEEE ExCom of the Ecuadorian Section from 2010 to 2012.

Hussein Al Osman received the B.A.Sc. (*summa cum laude*) (Hons.) degree in computer engineering, the M.A.Sc. degree in electrical engineering, and the Ph.D. degree in electrical engineering from the University of Ottawa, Ottawa, ON, Canada, in 2007, 2009, and 2014, respectively.

He is currently an Assistant Professor of Software Engineering with the School of Electrical Engineering and Computer Science, University of Ottawa. His current research interests include health informatics, serious games for health, affective computing, human–computer interaction, and active biometrics.

Dr. Al Osman has received numerous scholarships and awards, including 3X NSERC Scholarships, the Queen Elizabeth II Graduate Scholarship, the best paper award at the 2008 Distributed Simulation and Real Time Applications Conference, and the Part Time Professor Award, over the course of his academic journey.

Abdulmotaleb El Saddik (M'01–SM'04–F'09) is currently a Distinguished University Professor and University Research Chair with the School of Electrical Engineering and Computer Science, University of Ottawa, Ottawa, ON, Canada. He is an Internationally Recognized Scholar who has made strong contributions to the knowledge and understanding of multimedia computing, communications, and applications. He has authored or co-authored four books and over 500 publications. He has supervised more than 100 researchers.

Dr. El Saddik was an ACM Distinguished Scientist and a fellow of the Engineering Institute of Canada and the Canadian Academy of Engineers, and received several international awards, such as the IEEE Canada Computer Medal. He was the Chair of more than 40 conferences and workshops, and has received research grants and contracts totaling more than $18 Mio.