ECG Authentication System Design Based on Signal Analysis in Mobile and Wearable Devices

Shin Jae Kang, Seung Yong Lee, Hyo Il Cho, and Hyunggon Park, *Senior Member, IEEE*

***Abstract*—We propose a practical system design for biometrics authentication based on electrocardiogram (ECG) signals collected from mobile or wearable devices. The ECG signals from such devices can be corrupted by noise as a result of movement, signal acquisition type, etc. This leads to a tradeoff between captured signal quality and ease of use. We propose the use of cross correlation of the templates extracted during the registration and authentication stages. The proposed approach can reduce the time required to achieve the target false acceptance rate (FAR) and false rejection rate (FRR). The proposed algorithms are implemented in a wearable watch for verification of feasibility. In the experiment results, the FAR and FRR are 5.2% and 1.9%, respectively, at approximately 3 s of authentication and 30 s of registration.**

***Index Terms*—Authentication, biometrics, electrocardiogram (ECG), mobile and wearable environments, signal analysis.**

I. Introduction

BIOMETRICS has been a useful security tool in recent decades because of its effectiveness for identifying and authenticating desired users versus potential intruders [1]–[3]. It has recently been adopted for smartphone unlock and mobile payment technologies in mobile and wearable environments.

In particular, fingerprint, iris, face, and voice recognition techniques have been implemented, showing good error performance (e.g., low error rates) with acceptable registration and authentication speeds. For example, fingerprint recognition shows approximately 2% false rejection rat (FRR) and 2% false acceptance rate (FAR), where FRR and FAR are well-known measures for biometric authentication error performance. The error performances have been shown to be 0.99% FRR and 0.94% FAR for iris recognition, 10% FRR and 1% FAR for face recognition, and 10% FRR and 5% FAR for voice recognition [4]. The time required for fingerprint authentication is approximately 1 s for devices such as the Apple iPhone and Samsung Galaxy S6. The registration times of these products are in general 10–30 s. In addition to the biometrics, electrocardiogram (ECG) has also been used in personal authentication systems [5]. Prior works involving ECG can be categorized into either ECG with the fiducial features of segmented heartbeats [6]–[13] or ECG with nonfiducial features, such as an ECG waveform [14]–[19].

Although these works have shown potential advantages for the fundamentals of ECG signal analysis and authentication, it has been developed based on the assumption that only low levels of noise are included in the ECG signals. However, ECG signals captured and collected by mobile or wearable devices include significantly higher levels of noise [20], [21]. This is because dry-type electrodes, in contrast to wet- or clamp-type electrodes, are equipped on the devices, and the users are often in motion. Fast authentication is also an important requirement for such devices. In [22], [23], ECG signals with high levels of noise and fast authentication speeds were considered, and the ECG authentication products were based on nonfiducial features commercialized as wearable watches [22]. Although a faster authentication is achieved in [23], it is not clearly addressed as to why employing the average ECG beat improves the authentication speed.

In this letter, we propose algorithms that can be employed in wearable-type ECG registration and authentication systems, where the requirements are high ease of use, fast authentication speed, and acceptable error rate. We show that the algorithms effective in the presence of high levels of noise in the ECG signals while also guaranteeing fast authentication speeds and acceptable error rates. The algorithms were implemented in a wearable watch. The experiment results for our prototype implementation show that the proposed approach achieved 3-s authentication speed with 5.2% FAR with 1.9% FRR.

II. System Setup and Problem Formulation

The conventional framework of ECG authentication consists of four blocks: sensing, preprocessing, feature extraction, and matching for authentication, as shown in Fig. 1.

The sensing block (Block I) captures the ECG signals from two dry lead-I-type electrodes, which can be installed at the back or front of mobile and wearable devices (e.g., smart phones and watches). The preprocessing block (Block II) removes the noise in the captured ECG signals via bandpass filtering or wavelet denoising and smoothing. Then, the denoised ECG waveform segmentation based on R-peak detection and normalization is performed [9], [23]–[25]. The feature extraction block (Block III) extracts a nonfiducial feature from the input ECG sequences. More details for this process are discussed in Section III. Finally, the matching block (Block IV) makes decisions of "authenticated" or "denied" based on the degree of similarity among the extracted features in the registration and authentication processes. In the proposed approach,

Manuscript received December 04, 2015; revised February 14, 2016; accepted February 17, 2016. Date of publication February 18, 2016; date of current version April 28, 2016. This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea Government (MSIP) (No. NRF-2014R1A2A1A11051257) and by the MSIP, South Korea, under the Information Technology Research Center (ITRC) support program (IITP-2015-H8501-15-1007) supervised by the Institute for Information & Communications Technology Promotion (IITP). The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Mehdi Moradi.

S. J. Kang, S. Y. Lee, and H. I. Cho are with the Advanced Research Institute Technology of LG Electronics, 06763 Seoul, South Korea (e-mail: shinjae.kang@lge.com; syong.lee@lge.com; henry.cho@lge.com).

H. Park is with the Department of Electronics Engineering, Ewha Womans University, 03760 Seoul, South Korea (e-mail: hyunggon.park@ewha.ac.kr).

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

Digital Object Identifier 10.1109/LSP.2016.2531996

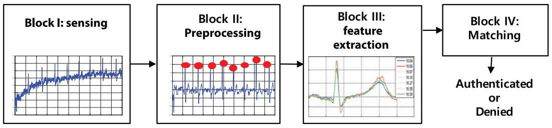

Fig. 1. Conventional framework of ECG authentication systems.

the similarity is measured by the cross correlation because it is well known for representing the similarity between two signals or waveforms.

Because the ECG signals captured by mobile or wearable devices include high levels of noise, the output signal of Block II may include high levels of noise in the features extracted for decisions. An example comparing the ECG signals captured from a conventional medical device (called a baseline device) with an implemented wearable-type device (called a target device) is shown in Fig. 2. Clearly, the ECG waveforms from the target device are significantly noisier than those from the baseline device. Therefore, it is essential to develop an algorithm that can explicitly overcome the noise in the ECG signals while achieving the required error performance and authentication speed.

III. Proposed Algorithms for Registration and Authentication

A. Filtered and Normalized ECG Beats

Let x and y each be one ECG beat in a sequence of ECG beats, which is the output of Block II. They are discrete ECG signals of length N, i.e., $x = [x(1), \ldots, x(N)]$ and $y = [y(1), \ldots, y(N)]$. Then, the normalized cross-correlation function $r_{xy}(d)$ can be expressed as

$$r_{xy}(d) = \frac{\sum_{n=1}^{N} x(n)y(n+d)}{\sqrt{\sum_{n=1}^{N} x^2(n)}\sqrt{\sum_{n=1}^{N} y^2(n)}}. \tag{1}$$

In this letter, we assume that the ECG signals x and y have unit energy, i.e.,

$$\sum_{n=1}^{N} x^2(n) = 1 \text{ and } \sum_{n=1}^{N} y^2(n) = 1 \tag{2}$$

which can easily be controlled by appropriately setting the system parameters. Because x and y are aligned, we set $d = 0$ in (1), leading to

$$r_{xy}(0) = \sum_{n=1}^{N} x(n)y(n).$$

Let $t(n)$ and $f(n)$ be the *template* and *feature*, defined as

$$t(n) = \frac{1}{M}\sum_{m=1}^{M} x_m(n) \text{ and } f(n) = \frac{1}{P}\sum_{p=1}^{P} y_p(n)$$

where $t(n)$ is the average of M ECG waveforms in the *registration* stage and $f(n)$ is the average of P ECG waveforms in the *authentication* stage.

The cross correlation $r_{tf}(0)$ of $t(n)$ with $f(n)$ can be reformulated as in (3), shown at the bottom of this page. If the values of the cross correlations between the ECG beats in the registration stage are approximately equal to α and those in the authentication stage are approximately equal to β, then (3) can be expressed as

$$\begin{aligned} r_{tf}(0) &= \frac{\sum_{m=1}^{M}\sum_{p=1}^{P}\sum_{n=1}^{N} x_m(n)y_p(n)}{\sqrt{MN + M(M-1)\alpha N}\sqrt{PN + P(P-1)\beta N}} \\ &= \frac{\sum_{m=1}^{M}\sum_{p=1}^{P}\sum_{n=1}^{N} x_m(n)y_p(n)}{\sqrt{\frac{N(1+\alpha(M-1))}{M}}\sqrt{\frac{N(1+\beta(P-1))}{P}} \cdot M \cdot P} \\ &= C \cdot \sum_{m=1}^{M}\sum_{p=1}^{P} r_{mp}(0)/MP \end{aligned} \tag{4}$$

where $C = \frac{\sqrt{M}}{\sqrt{N(1+\alpha(M-1))}} \frac{\sqrt{P}}{\sqrt{N(1+\beta(P-1))}}$. The expression in (4) means that the cross correlation of $t(n)$ with $f(n)$ is simply the average of the cross correlations of all possible MP pairs of ECG beats in $t(n)$ and $f(n)$ scaled by a constant C. Note that $C \leq 1$ because the sampling rate N is generally greater than several hundred, M and P are generally in the range from 2 to 50, and $-1 \leq \alpha, \beta \leq 1$.

We now generalize the above analysis by considering every element in each discrete ECG waveform to be a random variable, so that the ECG waveform is considered to be a random vector. Then, the cross correlation R_{mp} of random vectors $\mathbf{X}_m = [X_m(1), \ldots, X_m(N)]$ with $\mathbf{Y}_p = [Y_p(1), \ldots, Y_p(N)]$ in the ECG waveforms is a random variable given by

$$R_{mp} = \sum_{n=1}^{N} X_m(n)Y_p(n).$$

The corresponding cross correlation between the template of the registration stage and the feature of the authentication stage is given by

$$R_{tf} = C \cdot \sum_{m=1}^{M}\sum_{p=1}^{P} R_{mp}/MP. \tag{5}$$

By assuming that the mean and the variance of R_{mp} are μ and σ_0^2, respectively, the variance of R_{tf}, denoted by $V[R_{tf}]$, is given by

$$\begin{aligned} V[R_{tf}] &= C^2 \cdot \frac{1}{(MP)^2} V\left[\sum_{m=1}^{M}\sum_{p=1}^{P} R_{mp}\right] \\ &= \frac{C^2}{(MP)^2}\left(\sum_{m=1}^{M}\sum_{p=1}^{P} V[R_{mp}] \right. \\ &\quad \left. + \sum_{m=1}^{M}\sum_{p=1}^{P}\sum_{m'\neq m}\sum_{p'\neq p} \mathrm{cov}(R_{mp}, R_{m'p'})\right) \end{aligned}$$

$$\begin{aligned} r_{tf}(0) &= \frac{\sum_{n=1}^{N} t(n)f(n)}{\sqrt{\sum_{n=1}^{N} t^2(n)}\sqrt{\sum_{n=1}^{N} f^2(n)}} = \frac{\sum_{n=1}^{N}[\frac{1}{M}\sum_{m=1}^{M} x_m(n)][\frac{1}{P}\sum_{p=1}^{P} y_p(n)]}{\sqrt{\sum_{n=1}^{N}(\frac{1}{M}\sum_{m=1}^{M} x_m(n))^2}\sqrt{\sum_{n=1}^{N}(\frac{1}{P}\sum_{p=1}^{P} y_p(n))^2}} \\ &= \frac{\frac{1}{M}\frac{1}{P}\sum_{m=1}^{M}\sum_{p=1}^{P}\sum_{n=1}^{N} x_m(n)y_p(n)}{\frac{1}{M}\frac{1}{P}\sqrt{\sum_{m=1}^{M}\sum_{n=1}^{N} x_m^2(n) + \sum_{i\neq m}\sum_{n=1}^{N} x_i(n)x_m(n)}\sqrt{\sum_{p=1}^{P}\sum_{n=1}^{N} y_p^2(n) + \sum_{j\neq p}\sum_{n=1}^{N} y_p(n)y_j(n)}} \end{aligned} \tag{3}$$

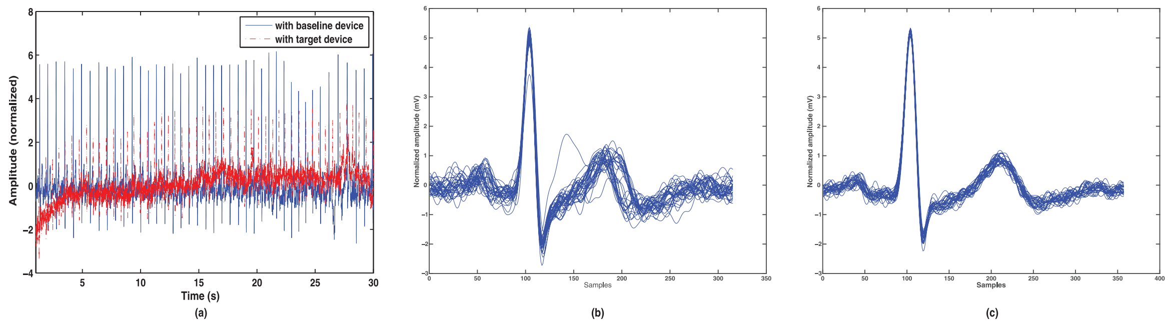

Fig. 2. Comparison of ECG signals with input devices.

$$\leq \frac{C^2\sigma_0^2}{MP} + \frac{C^2}{(MP)^2}\sum_{m=1}^{M}\sum_{p=1}^{P}\sum_{m'\neq m}\sum_{p'\neq p}\mathrm{cov}(R_{mp}, R_{m'p'})$$

$$\leq \frac{C^2\sigma_0^2}{MP} + \frac{C^2}{(MP)^2}((MP)^2 - MP)\sigma_0^2 = C^2 \cdot \sigma_0^2$$

where cov denotes the covariance. Since $C \leq 1$, it is clear that $V[R_{tf}] \leq V[R_{mp}]$, meaning that the correlation of the averages of multiple ECG beats provides a better estimate than the correlation of two ECG beats (any possible pairs of a beat from the template and a beat from the feature).

B. Design of ECG Authentication Systems

In this section, we propose a design of an ECG authentication system in which the proposed approach discussed in Section III-A is feasible for a real target system. The proposed design can be implemented in Block III, as shown in Fig. 1.

Recall that the proposed approach requires that all ECG signals 1) are aligned in time; 2) have equal duration of N samples; 3) have unit energy; and 4) have a cross correlation between ECG beats satisfying (4). For requirements 1), 2), and 3), the peak of the QRS complex in each ECG beat segment should be detected. Then, the left and right parts of the peaks are appropriately resampled so that every ECG beat has the same length N and is aligned at the peak of the QRS complex. Finally, the resampled ECG beats are normalized to have unit energy.

We propose Algorithms 1 and 2 to meet requirement 4) in the registration stage and the authentication stage, respectively. In the registration, ECG beats with cross-correlation values approximately at a predetermined level can be chosen based on Algorithm 1. In the authentication stage, Algorithm 2 is employed, which uses both coarse search and fine search. In this way, the desired ECG beats can be selected in real time, leading to expedited authentication.

IV. Experiment Results

In this section, we evaluate the effectiveness of the proposed ECG authentication design in actual physical implementation. The prototype was a wearable watch based on ARM Cortex-M MCU with a 168-MHz CPU and electrodes, as shown in Fig. 3. The electrodes were located on the front and back sides of the watch. The common electrode (ground) was at the bracelet buckle of the watch. When a participant wearing the watch touched his or her hand to the front of the watch, ECG signals were detected.

In order to highlight the effectiveness of the proposed algorithms for noise-corrupted ECG signals, 28 individuals (18% female, age range 25–45 years) who were calmly seated or slowly walking in comfortable environments participated in our experiment. The individuals register their own ECG beats in 30 s. The sampling frequency of input data was set by 512 Hz, and the number of samples in one ECG beat was 350 ($N = 350$). The numbers of ECG beats in registration and authentication were 25 and 5, respectively ($M = 25, P = 5$).

Algorithm 1. ECG Beat Selection for Registration

Require: Resampled, aligned, and normalized ECG beats $x_m(n), \theta, \alpha, \epsilon, C = \{m | 1 \leq m \leq M\}$.
1: **while** $\alpha - \epsilon \leq x_m(n) * x_{m'}(n) \leq \alpha + \epsilon$ for all $m, m' \in C, m \neq m'$
2: $C' \leftarrow \emptyset, t(n) = 1/|C| \cdot \sum_{m \in C} x_m(n)$
3: **repeat** for each $m \in C$
4: compute $r_{tm}(0) = t(n) * x_m(n)$
5: **if** $\theta \leq r_{tm}(0) \leq 1$ **then** $C' \leftarrow C' \cup \{m\}$
6: **until**
7: $C \leftarrow C'$
8: **until**

Algorithm 2. ECG Beat Selection for Authentication

Require: Resampled, aligned, and normalized ECG beat $y_p(n)$, template $t(n), \theta_1, \beta, P = 0$
1: **repeat**
2: compute $r_{tp}(0) = t(n) * y_p(n)$
3: **if** $r_{tp}(0) \geq \theta_1$ **then** $f(n) \leftarrow f(n) + y_p(n)$ and $P \leftarrow P + 1$
4: **if** $P \geq N_{target}$ **then** compute $r_{tf}(0) = \frac{1}{P} t(n) * f(n)$
5: **if** $r_{tf}(0) \geq \beta$ **then** stop
6: **else** $P \leftarrow 0$ and go to step 1 with new $y_p(n)$
7: **else** go to step 1 with new $y_p(n)$
8: **else** go to step 1 with new $y_p(n)$
9: **until**

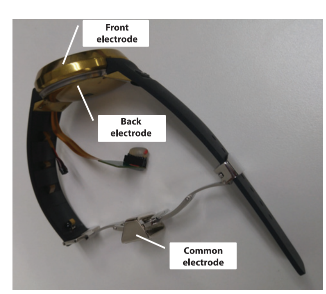

Fig. 3. Watch-type implementation for ECG authentication system.

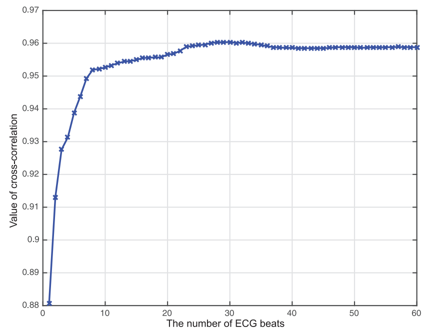

Fig. 4. Impact of the number of ECG beats on the cross correlation in the registration stage.

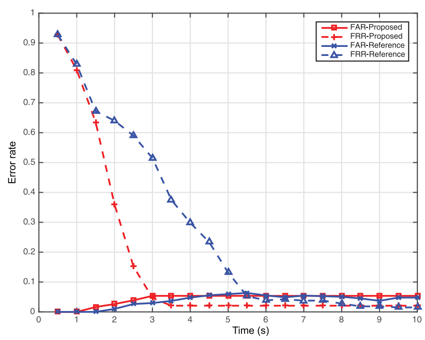

Fig. 5. FAR and FRR performances with authentication speed.

The proposed Algorithms I and II were employed with the parameters' set to $\alpha = 0.93$, $\epsilon = 0.03$, $0.85 \leq \theta \leq 0.97$ for different users in Algorithm I, and $\theta_1 = 0.7$ and $0.89 \leq \beta \leq 0.95$ for different users in Algorithm II.

Fig. 4 shows the impact of the number of ECG beats on the cross-correlation values for all trials (averaged over all participants) in the registration stage. As clearly shown, the cross-correlation values generally increased (performance improves) as more ECG beats were included. However, the cross-correlation values became saturated if enough ECG beats were included. This result confirms the analytical conclusions of Section III-A.

Fig. 5 shows the performance in terms of average FAR and FRR according to authentication speed, comparing the proposed algorithm with the approach in [23]. In the experiment, all the participants' templates in the registration stage were used. It is clearly observed that the proposed approach can reduce the time required to achieve a target FRR while the FAR remains at a similar error rate compared to the algorithm in [23]. For example, it took approximately 3 s to achieve 1.9% FRR, which is twice as fast as the approach in [23]. Therefore, the proposed algorithm would be suitable to equip on commercial products.

We have proposed an authentication system design using ECG signals captured by wearable and mobile devices. Considering the ease-of-use desirable for such devices, as well as acceptable error performance and authentication speed, our approach uses a set of average ECG beats and the corresponding cross-correlation values. We analytically show that the proposed approach improves system performance, and we implement the proposed algorithms in a watch-type prototype. Our experiment results show that the proposed system achieved 5.2% FAR with 1.9% FRR on average, with approximately 3 s for the authentication.

REFERENCES

[1] G. Kaur, G. Singh, and V. Kumar, "A review on biometric recognition," *Int. J. Bio-Sci. Bio-Technol.*, vol. 6, no. 4, pp. 69–76, 2014.

[2] A. R. M. Bolle, J. H. Connell, S. Pankanti, N. K. Ratha, and A. W. Senior, *Guide to Biometrics*. Berlin, Germany: Springer-Verlag, 2003.

[3] B. J. Chirillo and S. Blaul, *Implementing Biometric Security*. Hoboken, NJ, USA: Wiley, 2003.

[4] A. Ross and A. K. Jain, "Human recognition using biometrics: An overview," *Ann. Télécommun.*, vol. 62, no. 1, pp. 11–35, 2007.

[5] 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.

[6] M. Malik, "Heart rate variability: Standards of measurement, physiological interpretation, and clinical use," *Circulation*, vol. 93, no. 5, pp. 1043–1065, 1996.

[7] A. Sandryhaila, M. Puschel, and J. Kovacevic, "Efficient compression of QRS complexes using hermite expansion," *IEEE Trans. Signal Process.*, vol. 60, no. 2, pp. 947–955, Feb. 2012.

[8] H. Baali, R. Akmeliawati, M. J. E. Salami, A. Khorshidtalab, and E. Lim, "ECG parametric modeling based on signal dependent orthogonal transform," *IEEE Signal Process. Lett.*, vol. 21, no. 10, pp. 1293–1297, Oct. 2014.

[9] C. Li, C. Zheng, and C. Tai, "Detection of ECG characteristic points using wavelet transforms," *IEEE Trans. Biomed. Eng.*, vol. 42, no. 1, pp. 21–28, Jan. 1995.

[10] Y. Zou, J. Han, X. Weng, and X. Zeng, "An ultra-low power QRS complex detection algorithm based on down-sampling wavelet transform," *IEEE Signal Process. Lett.*, vol. 20, no. 5, pp. 515–518, May 2013.

[11] D. Thanapatay, C. Suwansaroj, and C. Thanawattano, "ECG beat classification method for ECG printout with principle components analysis and support vector machines," in *Proc. Int. Conf. Electron. Inf. Eng. (ICEIE'10)*, Aug. 2010, pp. 72–75.

[12] A. Page, A. Kulkarni, and T. Mohsenin, "Utilizing deep neural nets for an embedded ECG-based biometric authentication system," in *Proc. IEEE Biomed. Circuits Syst. Conf. (BioCAS'15)*, Oct. 2015, pp. 1–4.

[13] S. Keshishzadeh and S. Rashidi, "Single lead electrocardiogram feature extraction for the human verification," in *Proc. Int. Conf. Comput. Knowl. Eng. (lCCKE'15)*, Oct. 2015, pp. 118–122.

[14] J. Wang, M. She, S. Nahavandi, and A. Kouzani, "Human identification from ECG signals via sparse representation of local segments," *IEEE Signal Process. Lett.*, vol. 20, no. 10, pp. 937–940, Oct. 2013.

[15] K. Plataniotis, D. Hatzinakos, and J. Lee, "ECG biometric recognition without fiducial detection," in *Proc. IEEE Biom. Consortium Conf. (BCC)*, 2006, pp. 1–6.

[16] G. B. Moody, R. G. Mark, and A. L. Goldberger, "PhysioNet: A web-based resource for study of physiologic signals," *IEEE Eng. Med. Biol. Mag.*, vol. 20, no. 3, pp. 70–75, 2001.

[17] I. Odinaka, P. Lai, A. Kaplan, J. A. O'Sullivan, E. J. Sirevaag, and J. W. Rohrbaugh, "ECG biometric recognition: A comparative analysis," *IEEE Trans. Inf. Forensics Secur.*, vol. 7, no. 6, pp. 1812–1824, Dec. 2012.

[18] T. Choudhary and M. S. Manikandan, "A novel unified framework for noise-robust ECG-based biometric authentication," in *Proc. Int. Conf. Signal Process. Integr. Netw. (SPIN'15)*, Feb. 2015, pp. 186–191.

[19] F. Porée, G. Kervio, and G. Carrault, "ECG biometric analysis in different physiological recording conditions," *Signal Image Video Process.*, vol. 10, no. 2, pp. 267–276, Feb. 2016.

[20] K. Singh, A. Singhvi, and V. Pathangay, "Dry contact fingertip ECG-based authentication system using time, frequency domain feature and support vector machine," in *Proc. IEEE Int. Conf. Eng. Med. Biol. Soc. (EMBC'15)*, Aug. 2015, pp. 526–529.

[21] J. B. Fernando and K. Morikawa, "Improvement of human identification accuracy by wavelet of peak-aligned ECG," in *Proc. IEEE Int. Conf. Identity Secur. Behav. Anal. (ISBA'15)*, Mar. 2015, pp. 1–6.

[22] "Overview of Nymi Band," Nymi Inc., White Paper, Aug. 2015. [Online]. Available: https://www.nymi.com/wp-content/uploads/2013/11/NymiWhitePaper-1.pdf.

[23] S. Z. Fatemian, F. Agrafioti, and D. Hatzinakos, "Heartid: Cardiac biometric recognition," in *Proc. IEEE Int. Conf. Biom.: Theory Appl. Syst. (BTAS'10)*, Sep. 2010, pp. 1–5.

[24] P. S. Hamilton and W. J. Tompkins, "Quantitative investigation of QRS detection rules using the MIT/BIH arrhythmia database," *IEEE Trans. Biomed. Eng.*, vol. BE-33, no. 12, pp. 1157–1165, Dec. 1986.

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