A Cancelable Biometric Scheme Based on Multi-lead ECGs

Peng-Tzu Chen, Shun-Chi Wu* *Member, IEEE*, and Jui-Hsuan Hsieh

***Abstract*—Biometric technologies offer great advantages over other recognition methods, but there are concerns that they may compromise the privacy of individuals. In this paper, an electrocardiogram (ECG)-based cancelable biometric scheme is proposed to relieve such concerns. In this scheme, distinct biometric templates for a given beat bundle are constructed via "subspace collapsing." To determine the identity of any unknown beat bundle, the multiple signal classification (MUSIC) algorithm, incorporating a "suppression and poll" strategy, is adopted. Unlike the existing cancelable biometric schemes, knowledge of the distortion transform is not required for recognition. Experiments with real ECGs from 285 subjects are presented to illustrate the efficacy of the proposed scheme. The best recognition rate of 97.58 % was achieved under the test condition N_{train} = 10 and N_{test} = 10.**

I. Introduction

Biometric technologies directly utilize physiological or behavioral characteristics (i.e., biometrics) possessed by individuals to detect their identities. This alleviates the problems (e.g., losing keys or forgetting passwords) associated with the existing possession-based and knowledge-based approaches [1]. Propelled by the advent of low-cost, high-accuracy sensing and computing devices, these technologies are now deployed in various applications (e.g., access control and e-commerce [2]). However, with the convenience offered by these technologies, there are concerns about the compromise of the privacy of individuals [3-5]. The biometrics of an individual is uniquely and permanently associated with him/her. But, this property also makes it difficult for the biometrics to be revoked [3]. In addition, most of the biometrics (e.g., fingerprints, faces, and iris) currently in use are extrinsic, and could be easily recorded without an individual's consent [4]. As a result, compromised biometrics may lead not only to replay attacks (note that the biometrics is irreplaceable), but also to the disclosure of physiological and/or pathological medical conditions (e.g., retinal patterns may provide information about diabetes [1]) of the individual who possesses it. Moreover, biometrics compromised in one application may result in all other applications also being compromised (i.e., database cross-matching) because adoption of the same set of biometrics is hardly avoided, due to the limited number of biometrics [5].

Several attempts have been made to address these concerns, and cancelable biometrics is one approach that has drawn the most attention [3-5]. The concept of cancelable biometrics involves the enablement of a biometric template to be revocable like a password. Distinct templates associated with the same biometrics are generated by distorting the biometrics differently (through different distortion settings). This distortion transform is normally noninvertible so that reconstructing the original biometrics from the template is infeasible. Several approaches for cancelable biometric template generation have been proposed. Examples include the noninvertible geometric transforms [6], BioHashing [7], random projections [8] and cancelable biometric filters [9]. However, these are intended for the extrinsic biometrics mentioned above.

Even though miscellaneous biometrics schemes exist, the search for new ones continues. Recently, the use of electrocardiograms (ECGs) as a biometrics is gaining in increasing interest [10-12]. ECGs are recordings that are able to capture the cardiac electrical activity generated by repeated depolarization and repolarization of the atria and ventricles. Each ECG lead illustrates the morphological variations from one specific orientation in space [13]. Owing to the differences in individuals' pericardium and torso surface geometries as well as the conductivity distributions in between [14], these morphological variations exhibit dissimilarly from one individual to another, making the utilization of ECGs as a biometrics become feasible. Moreover, the extracted characteristics of ECGs have been shown to be insensitive to the electrode positions and states of anxiety [12]. Compared to the existing extrinsic biometrics, ECGs' intrinsic nature and inherent indication of "liveness" are even more appealing as these properties further increase the difficulty of falsification. In this paper, an ECG-based cancelable biometric scheme is proposed. Through "subspace collapsing," multiple revocable and noninvertible ECG templates can be constructed in order to avoid privacy invasion and cross-matching problems. By incorporating a strategy of "suppression and poll," the well-known multiple signal classification (MUSIC) method [15] can effectively determine the identity of a given unknown beat bundle. Unlike the existing cancelable schemes, the identity can be recognized without the knowledge of the distortion transform, which further increases the difficulty of recovering the original ECGs.

II. ECG-based Biometric Scheme

In this paper, we focus on the application of the proposed scheme to multi-lead ECGs. However, generalizing it to a single-lead ECG may still be possible. To begin, we assume that the R peaks have been detected on one of the ECG leads (e.g., lead I) with existing approaches (e.g., [16]), and that the multi-lead, time-aligned ECG data blocks (referred to as "beat bundle" hereafter) around each detected R peak are isolated. Assuming there are m leads and n samples per block, the data corresponding to the i^{th} detected R peak forms an $n\times m$ matrix $\mathbf{X}_i$. Normally, n is much larger than m.

This work was supported by the Ministry of Science and Technology of Taiwan, R.O.C., under the contract nos. MOST 103-2218-E-007-013 and MOST 105-2221-E-007-090.

P.-T. Chen (e-mail: libebc@hotmail.com.tw), S.-C. Wu (*corresponding author; tel: +886 3 5715131x34304; fax: +886 3 5720724; e-mail: shunchi.wu@mx.nthu.edu.tw), and J.-H. Hsieh (e-mail: jimmy51338@yahoo.com.tw) are with the Department of Engineering and System Science, National Tsing Hua University, Hsinchu, Taiwan 30013.

978-1-5090-2809-2/17/$31.00 ©2017 IEEE

A. *Signal and Noise Subspaces of a Beat Bundle*

Typically, as the depolarization and repolarization waves spread, the cardiac vector expands, contracts, and rotates, as a function of time [13-14]. Each lead of the ECG can be regarded as the response vector induced on the multi-lead ECG system by this cardiac vector, in the orientation of that lead. Since the lead placement related to the trajectory of the cardiac vector is different from one lead to another, each lead exhibits dissimilar waveform shapes. As a result, it is difficult to represent any lead of the ECG as a linear combination of the rest of the leads (especially when m is small) of the ECGs, and thus, any beat bundle $\mathbf{X}$ is of full rank, m. Assuming $n > m$, the singular value decomposition (SVD) of $\mathbf{X}$ will be given by

$$\mathbf{X} = \mathbf{V\Sigma U}^T = \left[\mathbf{V}_S\ \mathbf{V}_N\right]\mathbf{\Sigma U}^T, \tag{1}$$

where $\mathbf{V}_S = \mathbf{V}(:, 1{:}m)$ contains the m left singular vectors with non-zero singular values, and $\mathbf{V}_N = \mathbf{V}(:, m{+}1{:}n)$ contains the rest of the singular vectors whose singular values are zeros (because the energy in $\mathbf{X}$ is confined to an m dimensional subspace defined by the m-lead ECGs). We refer to the subspaces spanned by $\mathbf{V}_S$ and $\mathbf{V}_N$ as the signal and noise subspaces of $\mathbf{X}$, respectively, which are orthogonal complements.

B. *Construction of Cancelable Biometric Templates*

It is required that a cancelable biometric template is revocable, noninvertible and diverse; meanwhile, its formation should not deteriorate the recognition performance. In the discussion that follows, we describe how a cancelable biometric template is generated when the i^{th} subject's beat bundle, $\mathbf{X}_i$, is presented. To begin, a random matrix (the components therein are normal random variables)

$$\mathbf{\Theta}_i = [\boldsymbol{\theta}_1^{(i)}, \ldots, \boldsymbol{\theta}_d^{(i)}] \in \mathbb{R}^{m\times d}, \tag{2}$$

whose columns $\boldsymbol{\theta}_j^{(i)} \in \mathbb{R}^{m\times 1}$ are of unit length (i.e., $\left\|\boldsymbol{\theta}_j\right\| = 1$) is generated. Through $\mathbf{\Theta}_i$, the desired cancelable template $\mathbf{F}_i$ can be formed as

$$\mathbf{F}_i = \mathbf{X}_i\mathbf{\Theta}_i \in \mathbb{R}^{n\times d}. \tag{3}$$

To let the template $\mathbf{F}_i$ be noninvertible, d must be less than m. When multiple templates are needed for a given beat bundle $\mathbf{X}_i$, it is only required to substitute various random matrices into (3) in order to obtain them. As the templates are formed by linearly combining the columns (i.e., leads) of a beat bundle with $d < m$, they occupy different subspaces in $\mathbf{X}_i$'s signal subspace (on the contrary, this can be thought as that $\mathbf{X}_i$'s signal subspace collapses into different subspaces of lower dimension for various templates). Consequently, any two of these templates can be distinguished from one another if the corresponding random matrices are different.

C. *Identity Determination for an Unknown Beat Bundle*

Suppose that a number of N_S subjects are enrolled in the biometric system, whose biometric templates (generated using (3)) are expressed as $\mathbf{F}_i$, for $i = 1\ldots N_S$. Moreover, suppose that an unknown beat bundle $\mathbf{X} \in \mathbb{R}^{n\times m}$ is presented to the system, whose noise subspace vectors (i.e., the vectors span the noise subspace of $\mathbf{X}$) is $\mathbf{V}_N \in \mathbb{R}^{n\times n-m}$. To determine what subject this unknown beat bundle corresponds to, the well-known MUSIC method [15] is adopted:

$$\hat{i} = \arg\max_i P_{MUSIC}(i) = \arg\max_i \frac{\left\|\mathbf{F}_i^T\mathbf{F}_i\right\|_F}{\left\|\mathbf{F}_i^T\mathbf{V}_N\mathbf{V}_N^T\mathbf{F}_i\right\|_F}, \tag{4}$$

where $\|\cdot\|_F$ represents the Frobenius norm. As mentioned, a biometric template obtained using (3) remains in the signal subspace of its originating beat bundle, regardless of what the random matrix is. When a "matched" noise subspace is presented (i.e., $\mathbf{V}_N$ and $\mathbf{F}_i$ arise from the same beat bundle), the denominator of (4) will be zero. The identity of the unknown beat bundle is thus found by viewing the MUSIC spectrum, P_{MUSIC}, as a function of the enrolled subjects' indices, i, and searching for the index of infinite P_{MUSIC}. Since the beat bundles taken from time to time may not be exactly the same (but still very similar) as the one used to construct the template, the denominator is only approximately zero. However, a discernible peak can still be found at the correct index. Figure 1 (a) shows the MUSIC spectrum obtained with (4) when Subject 142's beat bundle is presented to the system. It can be seen that a clear peak in the MUSIC spectrum is found at i = 142, which indicates that the identity of the unknown beat bundle can be correctly identified using (4). In practice, the signal subspaces of different subjects' beat bundles may not be disjoint, meaning that they may partially overlap. This is especially true as the number of subjects increases. As a result, when a beat bundle that shares a common subspace with others is presented to the system, the resulting MUSIC spectrum can be confounding. This can be seen in Figure 1 (b). Even though the beat bundle substituted into (4) is from Subject 63, the maximum peak is clearly not at the index of 63.

As discussed in the previous section, the morphological variations in different ECG leads are exhibited dissimilarly from one individual to another, such that the signal subspaces of their beat bundles are not the same (this is why (4) works). However, these differences may only be partially retained, because these templates reside only in the collapsed subspaces of the original signal subspaces (since $d < m$). The contribution

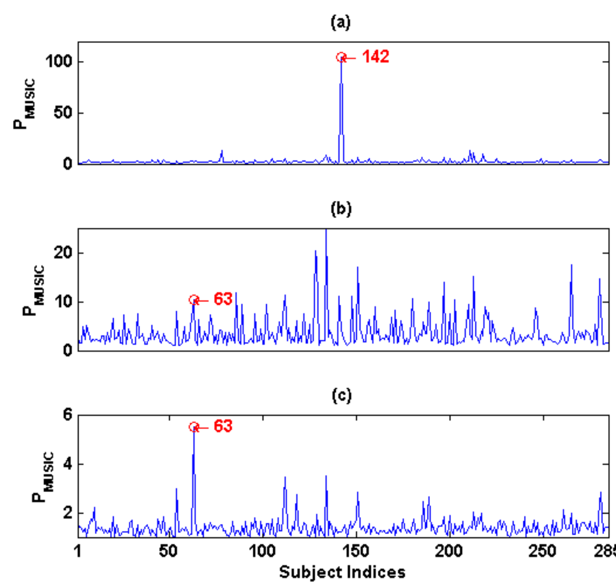

Fig. 1. The MUSIC spectra obtained using (4) and (6) when the beat bundles of Subjects 142 (a) and 63 (b, c) are presented to the system.

TABLE I. PLAUSIBLE SUBJECT INDICES IDENTIFIED USING (4) WHEN SUBJECT 63'S BEAT BUNDLE IS PRESENTED TO THE SYSTEM. THE CORRESPONDING INDICES DETERMINED BY (6) ARE LISTED AS WELL.

Plausible idx.	134	128	129	265	151	213	280	197
k_j identified using (6)	**63**	**63**	**63**	**63**	**63**	**63**	**63**	**63**
Plausible idx.	86	112	141	148	180	203	63	189
k_j identified using (6)	134	**63**	151	**63**	134	134	134	**63**

of the common subspace shared by the confounding subjects (the noise subspaces of their beat bundles are orthogonal to the common subspace) may conceal the differences, thus resulting in the confounding spectrum, which makes the situation even worse. If the shared common subspace can be removed prior to performing MUSIC, the subspace differences may be revealed for identity determination. Normally, this common subspace is not known a priori. However, a feasible estimate may be obtained as that spanned by a biometric template whose value of the MUSIC spectrum is large (i.e., such a biometric template may span the common subspace and its own distinct subspace). To mitigate the contribution of the common subspace, a "suppression and poll" strategy is utilized as follows. Suppose that the templates $\mathbf{F}_j$ for $j = 1 \ldots N_{peak}$ are those of the largest N_{peak} P_{MUSIC} values obtained with (4) (N_{peak} needs to be large enough to include the true subject index). The idea is to suppress the contribution of each $\mathbf{F}_j$ from $\mathbf{X}$ using

$$\mathbf{X}_j = (\mathbf{I}_n - \mathbf{P}_j)\mathbf{X} \in \mathbb{R}^{n\times m}, \quad (5)$$

where $\mathbf{P}_j = \mathbf{F}_j(\mathbf{F}_j^T\mathbf{F}_j)^{-1}\mathbf{F}_j^T \in \mathbb{R}^{n\times n}$ is the projection matrix onto the subspace spanned by $\mathbf{F}_j$. Note that not only the common subspace, but also the distinct subspace of $\mathbf{F}_j$ is suppressed in (5). Denoting the noise subspace vectors of $\mathbf{X}_j$ as $\mathbf{V}_{N,j} = \mathbf{V}_j(:, m+1:n)$ and substituting it into (4), we have

$$k_j = \arg\max_k \frac{\left\|\mathbf{F}_{j,k}^T\mathbf{F}_{j,k}\right\|_F}{\left\|\mathbf{F}_{j,k}^T\mathbf{V}_{N,j}\left(\mathbf{V}_{N,j}\right)^T\mathbf{F}_{j,k}\right\|_F}. \quad (6)$$

The index k_j represents the plausible subject index determined using the subspace spanned by $\mathbf{F}_j$ as the common subspace estimate. Notice that the projection in (5) also alters the signal subspace of the corresponding subject so that all the templates to be tested must be modified accordingly: $\mathbf{F}_{j,k} = (\mathbf{I}_n - \mathbf{P}_j)\mathbf{F}_k$. Figure 1 (c) is the MUSIC spectrum obtained with (6) when Subject 128's template is used to estimate the common subspace. As can be seen, a peak at index 63 can effectively be brought out. Finally, the same procedures are repeated until all the chosen templates have been used once in (6), and all the plausible indices are polled to determine what the unknown beat bundle should be classified as. Table I lists the 16 plausible subjects identified by the MUSIC spectrum of (4) when Subject 63's beat bundle is presented. The identified index, k_j, after suppressing the contribution of each plausible subject's template, is also provided below. As can be seen, the index of 63 appears more times than others, and thus the identity of this presented unknown beat bundle is decided to be 63.

III. EXPERIMENTS AND DISCUSSIONS

A. Datasets and Preprocessing

The Physikalisch-Technische Bundesanstalt (PTB) database from [17] is a public database contains records of the Frank-lead vectorcardiogram and the standard 12-lead ECGs, sampled at 1000 Hz. To evaluate the performance of the proposed scheme, recordings of leads I, II, and III (i.e., $m = 3$) from 285 subjects (205 men and 80 women, aged 17–87 with an average of 57.01). Before proceeding, each ECG lead was subject to the baseline wander removal using the approach of [18]. Finally, the bundles were cut with a fixed length of 240 ms and 420 ms before and after the R peaks, respectively, to fully enclose activity in a typical cardiac cycle, resulting in a sample number of $n = 661$.

B. Results and Discussions

Not only our proposed schemes (recognition with (4) and (6) are referred to as MUSIC and sp-MUSIC, respectively), but also two commonly referred non-cancelable ECG biometric recognition approaches were implemented for performance comparison: (1) a fiducial-based approach using the 21 morphological attributes [10] (only applied to the Lead-I recordings), and (2) multi-lead principal component analysis (PCA), a generalization of [11] to multi-lead ECGs, referred to as "mPCA" (for each subject, calculate the first few principal components (PCs) for each lead separately, and then combine the extracted PCs as a feature vector). The extracted features of these two methods were classified using the k-nearest neighbors algorithm with $k = 1$ [19]. Finally, d in (2) was 1, and N_{peak} were empirically assigned a value of 20.

In the first experiment, we studied the influence of the numbers of training (N_{train}) and testing (N_{test}) beat bundles on the recognition rate (the proportion of correctly identified heartbeats/beat bundles). Due to changes in physiological state and noise corruption, inter-beat morphological variations are inevitable, which can somehow be mitigated through averaging. Thus, for a given trial, we randomly selected N_{train} beat bundles from each subject for averaging, before template construction or feature extraction. Moreover, another N_{test} from each subject were chosen and averaged for testing. Five different combinations were evaluated: (1) $N_{\text{train}} = 1$ and $N_{\text{test}} = 1$, (2) $N_{\text{train}} = 5$ and $N_{\text{test}} = 1$, (3) $N_{\text{train}} = 5$ and $N_{\text{test}} = 5$, (4) $N_{\text{train}} = 10$ and $N_{\text{test}} = 5$, and (5) $N_{\text{train}} = 10$ and $N_{\text{test}} = 10$. To obtain statistically significant results, 100 trials were conducted under various conditions. The resulting mean recognition rates are depicted in Figure 2. As can be seen, with fewer training/testing beats, the performance of all the methods worsened, especially the fiducial-based approach. This was because of the difficulty in accurately determining the fiducial points under the influence of morphological variations. MUSIC gave worse recognition rates than those of sp-MUSIC, due to the problem of subspace overlapping. The ability of the PCA based approach to remove the fluctuating components (corresponding to the PCs with the smallest eigenvalues) allowed it to be robust against the morphological variations. The application of noise subspaces in (4) and (6) is in some sense to enhance the portion of $\mathbf{F}_i$ corresponding to the signal subspace of an unknown beat bundle, reducing the influence of the fluctuations in the signal subspace caused by inter-beat variations on recognition rates. As a result, mPCA and sp-MUSIC performed the best.

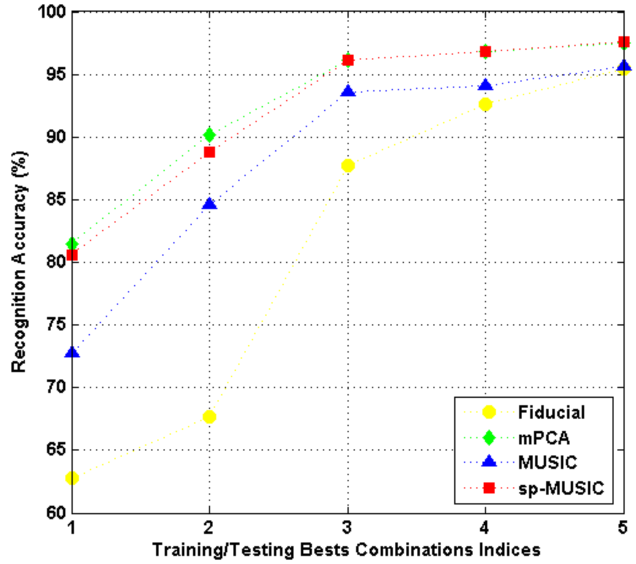

Fig. 2. Influence of the training/testing beat bundle combinations on the recognition rate.

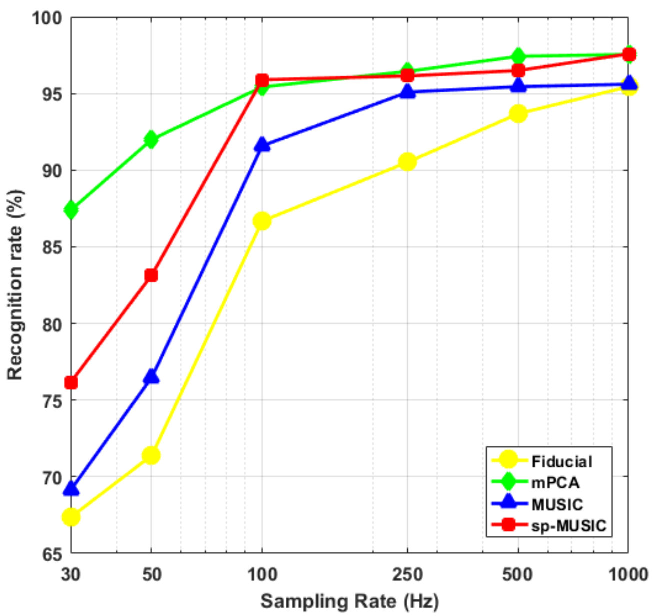

Fig. 3. Influence of the sampling rates on the recognition rate.

In the next example, the influence of the sampling rates on the recognition rate was studied. Different sampling rates were achieved by downsampling the original recordings. N_{train} and N_{test} were set to 10. A reduction in the sampling rate leads to a reduction in the details of ECG waveforms; thus, more errors occur. It can be seen in Figure 3 that the recognition rates decrease as the sampling rate decreases, in all the methods, especially those relying on the morphological information (i.e., the fiducial-based method). However, the MUSIC-based approaches still exhibited better performances.

IV. Conclusions

This paper presents a novel cancelable biometric scheme, based on multi-lead ECGs. Initially, the biometric template of each subject was constructed by randomly combining the columns (i.e., leads) of the corresponding beat bundle. The well-known MUSIC algorithm, in conjunction with a "suppression and poll" strategy, was then used to determine the identity of an unknown beat bundle, thus mitigating the problem of subspace overlapping. The performance of the proposed scheme was evaluated using the ECGs from 285 subjects. Compared with the existing non-cancelable approaches, our proposed scheme achieved relatively high recognition rates. Moreover, with the desirable properties of revocability, non-inevitability, and diversity, concerns regarding the privacy invasion can be addressed by the proposed scheme as well.

References

[1] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Trans. Circuits Syst. Video Technol.,* vol. 14, pp. 4-20, 2004.

[2] J. Unar, W. C. Seng, and A. Abbasi, "A review of biometric technology along with trends and prospects," *Pattern Recog.,* vol. 47, pp. 2673-2688, 2014.

[3] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Syst. J.,* vol. 40, pp. 614-634, 2001.

[4] V. M. Patel, N. K. Ratha, and R. Chellappa, "Cancelable biometrics: A review," *IEEE Signal Process. Mag.,* vol. 32, pp. 54-65, 2015.

[5] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security and privacy concerns," *IEEE Secur. Priv.,* 2003.

[6] R. M. Bolle, J. H. Connell, and N. K. Ratha, "Biometric perils and patches," *Pattern Recog.,* vol. 35, pp. 2727-2738, 2002.

[7] R. Belguechi, E. Cherrier, C. Rosenberger, and S. Ait-Aoudia, "An integrated framework combining Bio-Hashed minutiae template and PKCS15 compliant card for a better secure management of fingerprint cancelable templates," *Comput. Secur.,* vol. 39, pp. 325-339, 2013.

[8] J. K. Pillai, V. M. Patel, R. Chellappa, and N. K. Ratha, "Sectored random projections for cancelable iris biometrics," *Proc. IEEE Int. Conf. Acoust. Speech Signal Process*, pp. 1838-1841, 2010.

[9] M. Savvides, B. V. Kumar, and P. K. Khosla, "Cancelable biometric filters for face recognition," *Proc. Int. Conf. Pattern Recognition,* pp. 922-925, 2004.

[10] Y. Wang, F. Agrafioti, D. Hatzinakos, and K. N. Plataniotis, "Analysis of human electrocardiogram for biometric recognition," *EURASIP J. Adv. Signal Processing,* vol. 2008, pp. 1-11, 2008.

[11] J. M. Irvine, S. A. Israel, W. T. Scruggs, and W. J. Worek, "eigenPulse: Robust human identification from cardiovascular function," *Pattern Recog.,* vol. 41, pp. 3427-3435, 2008.

[12] S. A. Israel, J. M. Irvine, A. Cheng, M. D. Wiederhold, and B. K. Wiederhold, "ECG to identify individuals," *Pattern Recog*., vol. 41, pp. 3427-3435, 2005.

[13] L. Sörnmo and P. Laguna, *Bioelectrical signal processing in cardiac and neurological applications*, Academic Press, 2006.

[14] G. D. Clifford, F. Azuaje, and P. E. McSharry, *Advanced methods and tools for ECG data analysis*, Artech House, 2006.

[15] R. Schmidt, "Multiple emitter location and signal parameter estimation," *IEEE Trans. Antennas Propag.,* vol. 34, pp. 276-280, 1986.

[16] J. Pan and W. J. Tompkins, "A real-time QRS detection algorithm," *IEEE Trans. Biomed. Eng.,* pp. 230-236, 1985.

[17] A. L. Goldberger, L. A. N. Amaral, L. Glass, J. M. Hausdorff, P. C. H. Ivanov, R. G. Mark, J. E. Mietus, G. B. Moody, C.-K. Peng, H. E. Stanley, "Physiobank, physiotoolkit, and physionet: Components of a new research resource for complex physiologic signals," *Circulation*, vol. 101, pp. 215–220, 2000.

[18] P. D. Chazal, C. Heneghan, E. Sheridan, R. Reilly, P. Nolan, M. O'Malley, "Automated processing of the single-lead electrocardiogram for the detection of obstructive sleep apnoea," *IEEE Trans. Bio Med. Eng.* vol. 50, pp. 686-696, 2003.

[19] R. O. Duda, P. E. Hart, D. G. Stork, Pattern Classification, 2nd Edition, Wiley-Interscience, 2001.