IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 6, 2018, accepted December 28, 2018, date of publication January 9, 2019, date of current version January 29, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2891817

Cancelable ECG Biometrics Using Compressive Sensing-Generalized Likelihood Ratio Test

HANVIT KIM, (Student Member, IEEE), AND SE YOUNG CHUN, (Member, IEEE)
Department of Electrical Engineering, Ulsan National Institute of Science and Technology, Ulsan 44919, South Korea

Corresponding author: Se Young Chun (sychun@unist.ac.kr)

This work was supported in part by the Institute for Information and communications Technology Promotion grant funded by the Korean Government (MSIT) (Development of Personal Identification Technology based on Biomedical Signals to Avoid Identity Theft) under Grant R0190-15-2054, and in part by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education under Grant NRF-2017R1D1A1B05035810.

ABSTRACT Electrocardiogram (ECG) has been investigated as promising biometrics, but it cannot be canceled and re-used once compromised just like other biometrics. We propose methods to overcome the issue of irrevocability in ECG biometrics without compromising performance. Our proposed cancelable user authentication uses a generalized likelihood ratio test (GLRT) based on a composite hypothesis testing in compressive sensing (CS) domain. We also propose a permutation-based revocation method for CS-based cancelable biometrics so that it becomes resilient to record multiplicity attack. In addition, to compensate for inevitable performance degradation due to cancelable schemes, we also propose two performance improvement methods without undermining cancelable schemes: a self-guided ECG filtering and a T-wave shift model in our CS-GLRT. Finally, our proposed methods were evaluated for various cancelable biometrics criteria with the public ECG-ID data (89 subjects). Our cancelable ECG biometric methods yielded up to 93.0% detection probability at 2.0% false alarm ratio (PD*) and 3.8% equal error rate (EER), which are comparable to or even better than non-cancelable baseline with 93.2% PD* and 4.8% EER for challenging *single-pulse* ECG authentication, respectively. Our proposed methods met all cancelable biometrics criteria theoretically or empirically. Our cancelable secure user template with our novel revocation process is practically non-invertible and robust to record multiplicity attack.

INDEX TERMS Cancelable biometrics, ECG biometrics, generalized likelihood ratio test, compressive sensing, single pulse ECG.

I. INTRODUCTION

A. ELECTROCARDIOGRAM AS BIOMETRICS

Biometrics such as fingerprint, face, and iris provide convenient and powerful security tools to verify or identify individuals. Fingerprint recognition has been widely used in smart phone authentication, computer login, and access control system for buildings. Face recognition and iris-based user verification are often used in modern electronic devices. Biometrics are now combined with electronic passport for border control systems in many countries.[1] Combining more than one biometrics as multimodal biometrics has been widely investigated for high performance authentication [1]. A comprehensive review on recent biometrics research can be found in [2].

Electrocardiogram (ECG) has been investigated as a promising biometrics for authentication, identification and liveness validation [3]–[5]. One pulse of an ECG signal consists of P wave, QRS complex, and T wave that are from atrial depolarization, ventricular depolarization, and ventricular repolarization, respectively [6]. These characteristics depend on the structure and biological substrate of a heart which are known to be different on each person [7]. Previous studies have demonstrated that using ECG signals as a biometrics is a promising tool for authentication [3], [8]–[10].

It is worth noting that recent works on ECG biometrics have made significant progress so that ECG biometrics can be potentially used in various daily activities through wearable ECG sensors and devices. Wearable ECG sensors have been investigated for long-term health monitoring [11], [12] and have recently been commercialized such as Samsung

[1]International Civil Aviation Organization (ICAO) Doc 9303 Machine Readable Travel Documents Part 1

S-Patch and Apple Watch Series 4. There have been recent works on ECG biometrics for wearable devices in terms of wearable ECG band development [13], low power circuit design [14], and light-weight authentication algorithm [15]. ECG has also been investigated as part of multimodal biometric systems with fingerprint/face [16], voice [17] or sub-skin structure [18].

B. CANCELABLE ECG BIOMETRICS

Biometrics is a convenient and powerful tool, but one of the drawbacks is its irrevocability. If a password is compromised, this password can be immediately canceled and then a new password can be generated. However, once biometrics is compromised, it cannot be canceled and re-used since biometrics cannot be changed forever. Strengthening the security level of biometric systems can be one solution [19]. However, it is desirable to have cancelable schemes in biometrics.

Bolle *et al.* [20] proposed a concept of cancelable biometrics for protecting user-specific features. Teoh *et al.* [21] summarized four criteria that cancelable biometrics should satisfy based on the work of Maltoni *et al.* [22]:

1. **Efficiency:** cancelable biometrics should not deteriorate recognition performance.
2. **Re-usability:** there should be straightforward revocation and reissue procedures in the event of compromise.
3. **Diversity:** the same cancelable template should not be used in two different applications.
4. **Non-invertibility:** the recovery of the original biometric template from cancelable biometrics should be prevented.

Note that performance under lost key scenario is often separately considered for cancelable biometrics.

There have been several works on cancelable biometrics for fingerprint [23], [24], face [25], [26] and iris [27]. Cancelable multimodal biometrics have also been proposed and investigated recently [28]. These cancelable biometrics works are usually based on Johnson-Lindenstrauss (JL) lemma [29] or compressive sensing (CS) [30]. They both showed that the distance between two signals can be approximately preserved before and after random projections of them if the random projection matrix is properly designed. Thus, randomly projected biometric signals or features can be used for authentication or identification. Cancelable face biometrics was investigated based on JL lemma [21], [25]. Other works for cancelable biometrics were based on CS theory for iris [27]. There have been some works on cancelable biometrics using BioHash for face [26]. More comprehensive reviews on cancelable biometrics/multimodal biometrics are in [31]–[33].

Unfortunately, protecting biometric information with cancelable schemes often comes with the price of lowering authentication performance [31], [34], [35]. Even though compressed biometric signals may well-preserve the distance between signals based on JL lemma or CS theory, usual choice for distance metric is Euclidean distance or its variant, which may be sub-optimal. It is also important to note that CS theory has been developed for recovering the original unknown signal from compressed samples [30]. Thus, it is crucial to ensure that a CS based cancelable biometrics yields similar authentication performance, is almost non-invertible and is resilient to record multiplicity attack.

Unlike other biometrics, cancelable schemes for ECG have not been well-investigated. Dey *et al.* [36] investigated cancelable ECG biometrics using BioHash. Using highly compressed ECG using Hadamard transform yielded good identification performance [37], but this is invertible. Applications of CS theory for ECG have been investigated for compression or classification [38]–[40]. So far, there has been no prior work on cancelable ECG biometrics using CS theory that deals with the issue of performance degradation due to cancelable schemes, near-optimal distance metric for compressed samples, and validation for cancelable biometrics criteria altogether.

C. CONTRIBUTIONS AND ORGANIZATION

In this article, we propose a cancelable ECG biometrics by deriving a near-optimal generalized likelihood ratio test (GLRT) from a composite hypothesis testing in CS domain. Recently, CS was applied to conventional statistical signal processing such as detection and filtering and further it shows more efficient when the signals are processed under CS domain [41], [42]. Therefore, we conjecture that our proposed GLRT in CS domain is efficient, but not recoverable with appropriately small sample size. We also propose a novel revocation process for CS based cancelable biometrics that is robust to record multiplicity attack. Our proposed GLRT method was investigated for cancelable biometrics criteria (efficiency, re-usability, diversity and non-invertibility) [21]. To the authors' knowledge, this article is the first work of combining CS theory with ECG biometrics for cancelable ECG biometrics with near-optimal metric, of considering record multiplicity attack, and of evaluating the proposed method for cancelable biometrics criteria.

For performance degradation due to cancelable biometrics scheme, we developed two performance improvement methods by extending our previous performance boosting works [43], [44] that could potentially undermine our cancelable biometric schemes. Our newly developed methods yielded comparable performance to the previous works without compromising cancelable biometric scheme.

Part of the proposed works was presented at the 2017 IEEE EMBC [45]. In this article, we significantly extended our previous work by developing new revocation process for CS based biometrics to prevent record multiplicity attack, proposing two performance boosting tricks called self-guided filter and GLRT with T-wave shift model that can be used in cancelable ECG biometrics without compromising strong security level, and performing in-depth analyses for the cancelability of our proposed methods with extensive simulations.

Section II reviews backgrounds on ECG signal modeling and CS based statistical signal processing. Then, Section III describes our proposed methods: cancelable ECG based authentication method with GLRT in CS domain, permutation based revocation procedure for CS based cancelable biometrics, performance boost tricks for cancelable ECG biometrics, and cancelable biometrics criteria with analytical arguments. Section IV illustrates simulation results using the public ECG-ID data set [46] from the PhysioNet [47]. We also investigated if our proposed cancelable ECG biometric methods satisfy cancelable biometrics criteria and is robust to record multiplicity attack experimentally. Sections V and VI present discussion and conclusion for our proposed methods.

II. BACKGROUND

A. ECG SIGNAL MODELING AND AUTHENTICATION

An acquired ECG signal is usually contaminated by unwanted noise or artifacts such as baseline drift, power-line noise, and/or high frequency noise. Slowly varying baseline drift can be corrected by high-pass filtering or wavelet based drift correction. Power-line noise is on a specific frequency (50 or 60 Hz) that can be reduced by bandstop filters (see [48] for details). High frequency noise can be reduced by low-pass filtering, but this filtering could also remove some high frequency details of an original ECG signal. Thus, low-pass filtering should be used with care to preserve details, while to reduce noise. Then, for the pre-processed ECG signal, R-peak detection is performed using algorithms such as Pan-Tompkins method [49] so that R-peak aligned ECG pulses can be extracted. We model a pre-processed, R-peak aligned ECG pulse as $\mathbf{f} \in \mathbb{R}^K$ such that

$$\mathbf{f} = \mathbf{x} + \mathbf{n} \tag{1}$$

where $\mathbf{x} \in \mathbb{R}^K$ is an original ECG pulse, $\mathbf{n} \in \mathbb{R}^K$ is high frequency noise, and K is the length of a R-peak aligned, extracted ECG pulse.

A conventional user authentication is done by measuring the distance between an enrolled ECG signal or feature set $\{\mathbf{f}_1, \ldots, \mathbf{f}_N\}$ for N number of ECG pulses and an input ECG signal or feature set $\{\mathbf{s}_1, \ldots, \mathbf{s}_M\}$ for M number of ECG pulses as follows:

$$d(\{\mathbf{f}_1, \ldots, \mathbf{f}_N\}, \{\mathbf{s}_1, \ldots, \mathbf{s}_M\}) \underset{\text{accept}}{\overset{\text{reject}}{\gtrless}} \gamma \tag{2}$$

where d is a distance metric or classifier for two signals or feature sets and γ is a threshold. It has been shown that ECG user authentication methods can yield better performance with more ECG signals (or larger N, M) [9].

One of the ECG user authentication methods for limited memory and computation power is to use a single user template

$$\mathbf{t} = \frac{1}{N}\sum_{i=1}^{N} \mathbf{f}_i \in \mathbb{R}^K \tag{3}$$

and a single ECG pulse $\mathbf{s} = \mathbf{s_1}$ with a simple Euclidean distance:

$$d(\{\mathbf{t}\}, \{\mathbf{s}\}) = \sqrt{\sum_{j=1}^{K} (\mathbf{t}[j] - \mathbf{s}[j])^2} \underset{\text{accept}}{\overset{\text{reject}}{\gtrless}} \gamma' \tag{4}$$

where $\mathbf{t}[j]$ is the jth sample of the vector $\mathbf{t}$ and γ' is a threshold. It has been shown that this simple metric is actually a generalized likelihood ratio test (GLRT) if $\mathbf{n}$ follows an independent and identically distributed ($i.i.d.$) Gaussian distribution [44]. This method has been demonstrated to be effective for user authentication when proper performance improvement methods with mild computation increases are used together [43], [44].

B. SIGNAL PROCESSING WITH COMPRESSIVE MEASUREMENT

CS theory has been evolved from estimation based signal recovery with compressive measurement [50], [51] to other statistical signal processing problems such as filtering and signal detection [41], [42]. Davenport *et al.* [42] proposed a hypothesis testing for compressive measurement:

$$\begin{aligned} \mathcal{H}_0 &: \mathbf{y} = \Phi\mathbf{n} \sim p_0(\mathbf{y}) \\ \mathcal{H}_1 &: \mathbf{y} = \Phi(\mathbf{x} + \mathbf{n}) \sim p_1(\mathbf{y}) \end{aligned} \tag{5}$$

where $\mathbf{y} \in \mathbb{R}^L$ is a measured vector, $\mathbf{x} \in \mathbb{R}^K$ is a known, deterministic signal, $\mathbf{n} \sim \mathcal{N}(\mathbf{0}, \sigma^2\mathbf{I}_K) \in \mathbb{R}^K$ is an $i.i.d.$ Gaussian noise with σ^2 variance and a $K \times K$ identity matrix $\mathbf{I}_K$, and $\Phi \in \mathbb{R}^{L\times K}$ is a restricted isometry property (RIP) random matrix. The probability density functions for the hypothesis testing (5) can be derived:

$$p_0(\mathbf{y}) = \frac{\exp\left\{-\frac{1}{2}\mathbf{y}^T(\sigma^2\Phi\Phi^T)^{-1}\mathbf{y}\right\}}{(2\pi)^{L/2}\left|\sigma^2\Phi\Phi^T\right|^{1/2}} \tag{6}$$

$$p_1(\mathbf{y}) = \frac{\exp\left\{-\frac{1}{2}(\mathbf{y} - \Phi\mathbf{x})^T(\sigma^2\Phi\Phi^T)^{-1}(\mathbf{y} - \Phi\mathbf{x})\right\}}{(2\pi)^{L/2}\left|\sigma^2\Phi\Phi^T\right|^{1/2}} \tag{7}$$

where T is a transpose operator and $|\cdot|$ is a matrix determinant.

The optimal Neyman-Pearson (NP) detector for the hypothesis testing (5) is a likelihood ratio test:

$$\Lambda(\mathbf{y}) := \frac{p_1(\mathbf{y})}{p_0(\mathbf{y})} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \eta$$

where η is a threshold. By taking logarithm, the final detector in CS domain can be obtained as

$$\mathbf{y}^T(\Phi\Phi^T)^{-1}\Phi\mathbf{x} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \sigma^2\, log(\eta) + \frac{1}{2}\mathbf{x}^T\Phi^T(\Phi\Phi^T)^{-1}\Phi\mathbf{x}$$

where the right side can be treated as a constant that does not depend on the measurement $\mathbf{y}$. Direct detection method in CS domain yielded much better performance than indirect detection method in signal domain after CS reconstruction with sufficiently small amount of measurement [42]. This observation is potentially useful for cancelable biometrics.

III. METHODS

A. CANCELABLE ECG BIOMETRICS

Storing the enrolled ECG template $\mathbf{t}$ in (4) is necessary in conventional ECG based user authentication, but once compromised, the same template cannot be revoked and re-used. Inspired by [42], we propose a cancelable ECG biometrics with CS measurement based on the conjecture that our proposed method does have reasonably good authentication performance while does not have enough measurements for signal recovery. Note that Pillai *et al.* [27] proposed random projection based template protection for iris recognition with robust performance using sparse representation. This approach recovers biometric features from projected data while our proposed method performs user authentication in projection domain without recovering any feature.

A compressive measurement for ECG can be constructed using (1) as follows:

$$\mathbf{y} = \mathbf{H}\mathbf{f} = \mathbf{H}(\mathbf{x} + \mathbf{n}) \tag{8}$$

where $\mathbf{y} \in \mathbb{R}^L$ with $L \ll K$, $\mathbf{H}$ is a modified Bernoulli random matrix with the size of $L \times K$ with each element of either $1/\sqrt{K}$ or $-1/\sqrt{K}$ with probability 0.5, and $\mathbf{n} \sim \mathcal{N}(\mathbf{0}, \sigma^2\mathbf{I}_K)$ with $K \times K$ identity matrix for simplicity. It is worth noting that this particular random matrix $\mathbf{H}$ was chosen because it only requires $L(K-1)$ summations, L subtractions, and L divisions as well as a small storage of LK bits. These properties can potentially be advantageous for wearable bands with limited computing power and memory.

For the measurement model (8), we formulated a composite hypothesis test

$$\begin{aligned} \mathcal{H}_0 &: \mathbf{y} \sim p_0(\mathbf{y}; \mathbf{H}\mathbf{x}) \\ \mathcal{H}_1 &: \mathbf{y} \sim p_1(\mathbf{y}; \boldsymbol{\mu}), \quad \boldsymbol{\mu} \neq \mathbf{H}\mathbf{x} \end{aligned} \tag{9}$$

where $\mathbf{H}\mathbf{x} \in \mathbb{R}^L$, $\boldsymbol{\mu} \in \mathbb{R}^L$ is a vector, and each hypothesis probability density functions are

$$p_0(\mathbf{y}; \mathbf{H}\mathbf{x}) = \frac{\exp\left\{-\frac{1}{2}(\mathbf{y}-\mathbf{H}\mathbf{x})^T(\sigma^2\mathbf{H}\mathbf{H}^T)^{-1}(\mathbf{y}-\mathbf{H}\mathbf{x})\right\}}{(2\pi)^{L/2}\left|\sigma^2\mathbf{H}\mathbf{H}^T\right|^{1/2}}, \tag{10}$$

$$p_1(\mathbf{y}; \boldsymbol{\mu}) = \frac{\exp\left\{-\frac{1}{2}(\mathbf{y}-\boldsymbol{\mu})^T(\sigma^2\mathbf{H}\mathbf{H}^T)^{-1}(\mathbf{y}-\boldsymbol{\mu})\right\}}{(2\pi)^{L/2}\left|\sigma^2\mathbf{H}\mathbf{H}^T\right|^{1/2}}, \tag{11}$$

respectively. The nearly-optimal GLRT is

$$\Lambda(\mathbf{y}) = \frac{\max_{\boldsymbol{\mu}\neq\mathbf{H}\mathbf{x}} p_1(\mathbf{y}; \boldsymbol{\mu})}{p_0(\mathbf{y})} = \frac{p_1(\mathbf{y}; \hat{\boldsymbol{\mu}}_{\mathrm{ML}})}{p_0(\mathbf{y})} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \gamma \tag{12}$$

where $\hat{\boldsymbol{\mu}}_{\mathrm{ML}}$ is the maximum likelihood (ML) estimator for $p_1(\mathbf{y}; \boldsymbol{\mu})$ and γ is a threshold. Since $\hat{\boldsymbol{\mu}}_{\mathrm{ML}} = \mathbf{y}$, the numerator of (12) becomes a constant. Equation (12) can be further simplified to

$$(\mathbf{y} - \mathbf{H}\mathbf{x})^T(\mathbf{H}\mathbf{H}^T)^{-1}(\mathbf{y} - \mathbf{H}\mathbf{x}) \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \gamma' \tag{13}$$

where γ' determines the trade-off between detection probability and false alarm probability.

The ground truth ECG pulse $\mathbf{x}$ is not available, but the ECG user template (3) can be a good ML estimator for it. By using a 'plug-in' approach, the proposed CS-GLRT becomes

$$(\mathbf{y} - \mathbf{y}^{\mathbf{t}})^T(\mathbf{H}\mathbf{H}^T)^{-1}(\mathbf{y} - \mathbf{y}^{\mathbf{t}}) \gtrless \gamma''. \tag{14}$$

where our proposed secure user template $\mathbf{y}^{\mathbf{t}} := \mathbf{H}\mathbf{t}$ and γ'' is a threshold. Note that $\mathbf{y}^{\mathbf{t}}$ and $\mathbf{H}$ will be stored for authentication so that the user template $\mathbf{t}$ will be protected. Even though both $\mathbf{y}^{\mathbf{t}}$ and $\mathbf{H}$ are compromised, it will be challenging to recover the original signal $\mathbf{t}$ from them if the length of $\mathbf{y}^{\mathbf{t}}$ is small enough. We will further investigate this in the simulation.

B. PERMUTATION BASED REVOCATION PROCESS

Cancelable biometrics should provide a way to revoke current secure user template and to regenerate a new one when it is compromised. One naive approach is to regenerate a random projection matrix $\mathbf{H}$ and a secure template $\mathbf{y}^{\mathbf{t}} = \mathbf{H}\mathbf{t}$ as a revocation process [45]. However, this procedure is vulnerable to record multiplicity attack. Assume that both $\mathbf{H}_1$ and $\mathbf{H}_1\mathbf{t}$ are compromised. Then, a new random matrix and secure template can be generated again: $\mathbf{H}_2$ and $\mathbf{H}_2\mathbf{t}$. Assuming successful record multiplicity attack, an imposter may be able to obtain enough number of random matrices $\mathbf{H}_1, \ldots, \mathbf{H}_J$ and secure templates $\mathbf{H}_1\mathbf{t}, \ldots, \mathbf{H}_J\mathbf{t}$ to recover the original signal $\mathbf{t}$. This is possible because a stack of random matrices

$$\begin{bmatrix} \mathbf{H}_1^T & \cdots & \mathbf{H}_J^T \end{bmatrix}^T \tag{15}$$

still satisfies RIP condition and a stack of secure templates now provides enough number of measurements for excellent CS recovery. In practice, record multiplicity attack is quite challenging and secure templates may contain different T-waves due to heart beat rate changes and noise. However, with an extremely small probability, it is potentially possible to obtain important P-QRS complex information of the original user template $\mathbf{t}$ through record multiplicity attack.

Thus, we propose a permutation based revocation procedure for CS based cancelable biometrics. Our permutation process is purely random and it does not depend on any user specific information. Instead of generating a new random matrix $\mathbf{H}_2$ during the revocation process, we propose to randomly permute the original $\mathbf{H}_1$ matrix to generate a new $\tilde{\mathbf{H}}_1$. The matrix $\mathbf{H}_1$ can be represented as a stack of row vectors as:

$$\mathbf{H}_1 := \begin{bmatrix} \mathbf{h}_{11} & \cdots & \mathbf{h}_{1L} \end{bmatrix}^T \tag{16}$$

where $\mathbf{h}_{1i} \in \mathbb{R}^K$ for $i = 1, \ldots, L$. During the revocation process, a permutation function $\tau(i)$ can be randomly generated to construct a new random matrix

$$\tilde{\mathbf{H}}_1 = \begin{bmatrix} \mathbf{h}_{1\tau(1)} & \cdots & \mathbf{h}_{1\tau(L)} \end{bmatrix}^T. \tag{17}$$

Note that $L!$ (factorial) possible random permutation functions exist for $\tau(i)$.

This newly generated matrix $\tilde{\mathbf{H}}_1$ and new secure template $\tilde{\mathbf{H}}_1\mathbf{t}$ essentially does not provide any new information for CS

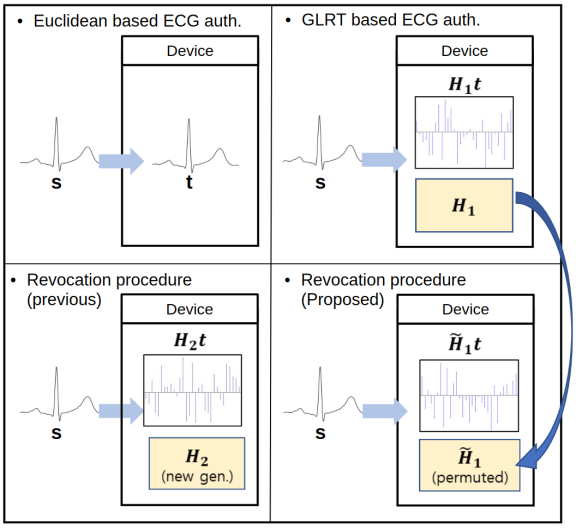


FIGURE 1. Illustrations for conventional Euclidean based ECG biometrics storing the original user template (top left), proposed GLRT based cancelable ECG biometrics storing secure template $\mathbf{H}_1\mathbf{t}$ and $\mathbf{H}_1$ (top right), previously proposed revocation process re-generating $\mathbf{H}_2$ and $\mathbf{H}_2\mathbf{t}$ [45] (bottom left), and newly proposed revocation process permuting the rows of $\mathbf{H}_1$ randomly to generate $\tilde{\mathbf{H}}_1$ and $\tilde{\mathbf{H}}_1\mathbf{t}$ to prevent record multiplicity attack (bottom right).

recovery when $\mathbf{H}_1$ and $\mathbf{H}_1\mathbf{t}$ are available. More specifically, $\mathbf{H}_1$ and $\mathbf{H}_1\mathbf{t}$ form a linear system of L equations with K unknowns, but adding $\tilde{\mathbf{H}}_1$ and $\tilde{\mathbf{H}}_1\mathbf{t}$ will provide the equivalent set of equations so that the problem remains as the same linear system of L equations with K unknowns. In addition, a stack of multiple randomly permuted matrices, similar to (15), won't be able to satisfy RIP condition for CS recovery. Therefore, record multiplicity attack won't be able to recover the original user template $\mathbf{t}$ as far as $L \ll K$ is small enough to ensure non-invertibility. Fig. 1 illustrates the differences among different revocation procedures.

C. SECURE PERFORMANCE BOOST I: SELF-GUIDED FILTERING

It is well known that the performance degradation in cancelable biometrics is inevitable [31], [35]. So, performance boost methods for cancelable biometrics are desirable. For improving performance in ECG biometrics, Chun proposed to use a 1D guided filter (GF) for ECG authentication using user template as a guide signal to yield improved performance [43]. User template guided filtering is denoted as:

$$\hat{\mathbf{s}} = GF(\mathbf{s}; \mathbf{t}) \tag{18}$$

where $\mathbf{t}$ is the user template as a guided signal, $\mathbf{s}$ is an noisy input signal for filtering, and $\hat{\mathbf{s}}$ is the output of the filter. Using $\hat{\mathbf{s}}$ instead of $\mathbf{s}$ substantially improved authentication performance in ECG biometrics [43]. This computation is fast due to low computation complexity $O(1)$ of GF since it is essentially local affine fitting with efficient analytical solution [52]. However, this scheme cannot be used for cancelable ECG biometrics since the user template $\mathbf{t}$ must be stored.

We designed an irreversible transformation for user template $\mathbf{t}$ for cancelable ECG biometrics [45] based on the following observations:

1. GF with both flat and user template guide signals yielded similarly good denoising results over P and T waves.
2. Having a good guide signal (*e.g.*, user template) is critical for good denoising performance in QRS complex.

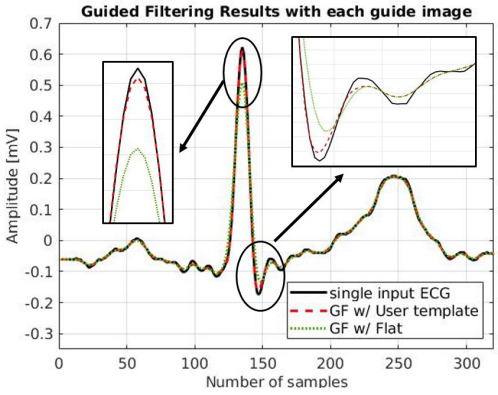


FIGURE 2. Observations of various ECG GF results with user template and flat signal. In P or T wave, GF with both guided signals achieved similar denoising performance. However, In QRS complex, GF with flat signal severely blurred the original ECG input signal, while user template based GF preserved details.

These observations are illustrated in Fig. 2. However, the output of the irreversible transformation still contains partial information about the user template, which can potentially weaken the security level of cancelable biometrics.

To eliminate partially stored user information for GF, we propose a self-GF, generating a guide signal by modifying the input ECG signal $\mathbf{s}$ based on this additional observation:

3. ECG QRS complex has high signal-to-noise ratio, so that a single pulse QRS complex can be used as a guide signal.

Note that the original GF also has self GF using input image by blurring it [52]. However, since GF transfers information in signals to the output, there will be a trade-off between powerful denoising performance and detail preservation. Our proposed self GF generates a guide signal for ECG denoising to preserve details in QRS complex and to yield strong denoising performance in P and T waves as illustrated in Fig. 3. A new guide signal $\mathbf{s}_{\text{crop}}$ contains QRS complex of input ECG signal based on the 2nd and 3rd observations and flat signal over P and T waves based on the 1st observation. Self-GF is denoted by

$$\hat{\mathbf{s}} = GF(\mathbf{s}; \mathbf{s}_{\text{crop}}). \tag{19}$$

Now no additional information about user template $\mathbf{t}$ is used for GF, but self-GF still yields comparable performance improvements to the original GF method with user template (see Section IV for the results).

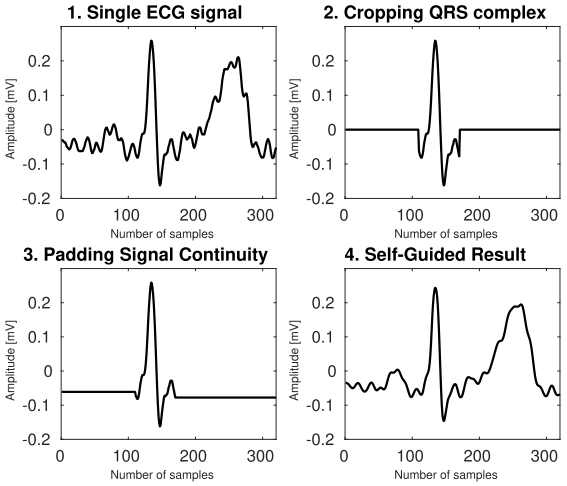


FIGURE 3. Steps for generating a guide signal for self-GF using a single pulse ECG: original input signal s (top left), cropping P and T wave areas (top right), padding to reduce sudden signal changes for cropping points (bottom left), and self-GF result (bottom right).

D. SECURE PERFORMANCE BOOST II: T-WAVE SHIFT MODEL IN GLRT

GLRT based ECG authentication method using T-wave circular shift model was proposed to improve the authentication performance for the case of having unknown heart rate variation [44]. This method also requires to use the original ECG template $\mathbf{t}$ to find the minimum distance between the template $\mathbf{t}$ and T-wave shifted ECG input $\mathbf{s}$ with unknown shift value so that it is not appropriate for cancelable biometrics. In here, we propose to incorporate T-wave shift model into the proposed CS-GLRT in (14).

We first modeled the input signal $\mathbf{s} \in \mathbb{R}^K$ to be separated into the PQRS segment $\mathbf{s}^F \in \mathbb{R}^{K_1}$ and T wave segment $\mathbf{s}^S \in \mathbb{R}^{K_2}$ where $K = K_1 + K_2$. T wave can be modeled to be shifted for different heart rate as follows:

$$\mathbf{s}_\alpha := \begin{bmatrix} \mathbf{s}^F \\ \mathbf{\Gamma}_\alpha \mathbf{s}^S \end{bmatrix} \tag{20}$$

where $\mathbf{\Gamma}_\alpha$ is a circular shift operator with a step size $\alpha \in \mathbb{Z}$. Then, a composite hypothesis testing to consider variable heart rate is constructed:

$$\begin{aligned} &\mathcal{H}_0 : \mathbf{y}_\alpha \sim p_0(\mathbf{y}; \mathbf{Hx}) \\ &\mathcal{H}_1 : \mathbf{y}_\alpha \sim p_1(\mathbf{y}; \boldsymbol{\mu}), \quad \boldsymbol{\mu} \neq \mathbf{Hx} \end{aligned} \tag{21}$$

where p_0, p_1 are defined in (9), $\boldsymbol{\mu}$ and α are unknown, and $\mathbf{y}_\alpha = \mathbf{Hs}_\alpha$. Finally, a near-optimal GLRT with T wave shift model is derived as follows:

$$\frac{\max\limits_{\boldsymbol{\mu} \neq \boldsymbol{\mu}_0, \alpha} \exp\left(-\frac{1}{2}(\mathbf{y}_\alpha - \boldsymbol{\mu})^T (\mathbf{HH}^T)^{-1} (\mathbf{y}_\alpha - \boldsymbol{\mu})\right)}{\max\limits_{\alpha} \exp\left(-\frac{1}{2}(\mathbf{y}_\alpha - \mathbf{Hx})^T (\mathbf{HH}^T)^{-1} (\mathbf{y}_\alpha - \mathbf{Hx})\right)}. \tag{22}$$

For the unknown $\mathbf{x}$, a 'plug-in' approach can be used to replace it by $\mathbf{t}$. Since the numerator of (22) becomes 1 due to the maximum likelihood estimator $\boldsymbol{\mu} = \mathbf{y}_\alpha$, our proposed GLRT can be simplified:

$$\min_{\alpha} \left\{ \left(\mathbf{y}_\alpha - \mathbf{y}^{\mathbf{t}}\right)^T (\mathbf{HH}^T)^{-1} \left(\mathbf{y}_\alpha - \mathbf{y}^{\mathbf{t}}\right) \right\} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \gamma \tag{23}$$

where γ is a threshold.

Equation (23) is computationally expensive due to brute-force search for α. We derived an equivalent operation for (23) using matrix-vector form to speed up computation:

$$\min \mathbf{D}\left\{ (\mathbf{H}\mathbf{\Gamma}^{\boldsymbol{s}} - \boldsymbol{Y}^{\boldsymbol{t}})^T (\mathbf{HH}^T)^{-1} (\mathbf{H}\mathbf{\Gamma}^{\boldsymbol{s}} - \boldsymbol{Y}^{\boldsymbol{t}}) \right\} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \gamma \tag{24}$$

where $\boldsymbol{Y}^{\boldsymbol{t}} = \left[\mathbf{y}^{\mathbf{t}} \cdots \mathbf{y}^{\mathbf{t}}\right] \in \mathbb{R}^{L \times K_2}$, $\mathbf{D}\{\cdot\}$ is an operator to extract diagonal elements to form a vector, and

$$\mathbf{\Gamma}^{\boldsymbol{s}} = \begin{bmatrix} \mathbf{s}^F & \cdots & \mathbf{s}^F \\ \mathbf{\Gamma}_1 \mathbf{s}^S & \cdots & \mathbf{\Gamma}_{K_2} \mathbf{s}^S \end{bmatrix} \in \mathbb{R}^{K \times K_2}. \tag{25}$$

Equation (24) implies that the comparison between T waves of input signal and enrolled user template is performed in CS domain. This is valid if $\mathbf{H}$ is a RIP operator to approximately preserve the distance between two signals after projection. The matrix-vector form (24) substantially reduced computation cost since (24) consists of a simple operator to find the minimum value in a vector and (25) can be generated quickly using pre-computed indices for a given input signal vector $\mathbf{s}$. Note that our proposed GLRT with T-wave shift model requires no additional enrolled user information unlike [44].

E. ANALYSES ON CANCELABLE BIOMETRICS CRITERIA

Here we analyzed our proposed CS-GLRT (14), revocation procedure (17) and performance boost methods (19), (24) for cancelable ECG biometrics to validate that they satisfy all cancelable biometrics criteria [25].

Efficiency Our proposed CS-GLRT (14) is based on a composite hypothesis testing in CS domain and on a nearly optimal GLRT detector for it to minimize performance degradation due to cancelable schemes. We also developed self-GF for effective denoising (19) and incorporated T-wave shift model into CS-GLRT (24) without compromising security and near-optimality. In Section IV-C, simulation results will support our argument by showing that the proposed cancelable CS-GLRT yielded performance comparable to or even better than the non-cancelable baseline.

Re-usability Our proposed revocation method (17) ensures robustness to record multiplicity attack as well as re-usability. Once a stored secure template $\mathbf{Ht}$ and/or a random matrix $\mathbf{H}$ are compromised, a new matrix $\tilde{\mathbf{H}}$ will be generated by randomly permuting the rows of the previous $\mathbf{H}$. Then, a new user template $\tilde{\mathbf{H}}t$ can also be generated with a new user template $\mathbf{t}$ and then $\mathbf{t}$ will be discarded. Finally, $\tilde{\mathbf{H}}t$ and $\tilde{\mathbf{H}}$ will be re-used for authentication. For example, if $L = 30$, then $L! \approx 2.65 \times 10^{32}$ different pairs can be generated, so this revocation process ensures re-usability.

Diversity In two different applications, two random matrices $\mathbf{H} \in \mathbb{R}^{L \times K}$'s can be generated and the probability that these two matrices are the same will be $1/2^{LK}$ where

$L \ll K$. With the proposed permutation based revocation procedure (17), the probability of having the same matrices up to random row permutation is

$$L!/2^{LK} \tag{26}$$

This is almost zero in our cancelable ECG biometrics. For example, our simulation used a random matrix $\mathbf{H} \in \mathbb{R}^{32\times 320}$ and (26) becomes about $1/(3.5 \times 10^{70}) \approx 0$.

Non-invertibility Cancelable ECG template must be obtained using non-invertible transformation to prevent the recovery of biometric data from secure template. In CS theory, the original signal can be recovered with a random matrix $\mathbf{H}$ if both $\mathbf{H}$ and $\mathbf{y^t}$ are available and the size of the vector $\mathbf{y^t}$ is large enough. Thus, the size of a CS measurement $\mathbf{y^t}$ should be determined to ensure efficiency (the larger, the better) as well as to ensure non-invertibility (the smaller, the better). Since CS signal recovery seems to require much larger measurements than CS signal detection does [42], it is possible to determine appropriate size of measurement for both efficiency and non-invertibility. We investigated this issue for our cancelable ECG biometrics (14) with simulation in Section IV-E for the worst case with compromised $\mathbf{H}$ and $\mathbf{y^t}$. Note that this case should rarely happen: FIDO2[2] allows biometrics to be only used locally for a variety of applications on the internet and a random matrix $\mathbf{H}$ can possibly be stored securely and used with hardware such as smart card. This worst case is considered as one of the strongest attacks [53].

Our revocation procedure (17) is also resilient to record multiplicity attack that multiple pairs of $\mathbf{H}$ and $\mathbf{y^t}$ are compromised. As discussed in Section III-B, a stack of 2 or more random matrices from our proposed permutation based revocation processes will compromise the RIP condition of the matrix stack. Moreover, multiple pairs of $\mathbf{H}$ and $\mathbf{y^t}$ won't provide additional information to a single pair of $\mathbf{H}$ and $\mathbf{y^t}$ due to row permutation of $\mathbf{H}$. We will study this worst case with simulations in Section IV-F.

IV. EXPERIMENTAL RESULTS

We investigated our proposed methods of cancelable ECG biometrics using CS-GLRT (14), self-GF (19), GLRT with T-wave shift model (24), and random permutation based revocation process (17) with the public ECG-ID dataset [46] from the PhysioNet [47]. MATLAB was used for all implementations (The Mathworks, Inc., MA, USA).

A. ECG DATA SET AND PRE-PROCESSING

The ECG-ID data set consists of ECG pulses from 90 subjects with recordings on the same or different days [46]. Each raw record was acquired for about 20 seconds with 500 Hz sampling rate, 12-bit resolution. This data set also provides pre-processed ECG signals reducing baseline draft, power-line noise, and high-frequency noise [46]. The pre-processed ECG data was used in our simulations.

[2]https://fidoalliance.org/

Two records per subject from ECG-ID were used in our simulations (89 subjects). Each record was processed using the Pan-Tompkins method for R-peak detection [49]. Then, each ECG record was segmented with the length of 320 samples (0.64 second), which are -134, $+185$ samples from the R-peak covering all P-QRS-T fragment. From selected 12 ECG pulses, an average ECG template was generated. One record was used for ECG template generation and the other record was used for user authentication test with cross validation. Compressive sensing random matrix for each person was generated where the numbers of CS measurements are 32, 96, and 160 samples.

For the performance evaluation, we adopt PD* and EER where PD* is detection probability at FAR $= 2\%$ and EER is a point where false rejection rate (FRR) $=$ FAR $=:$ EER.

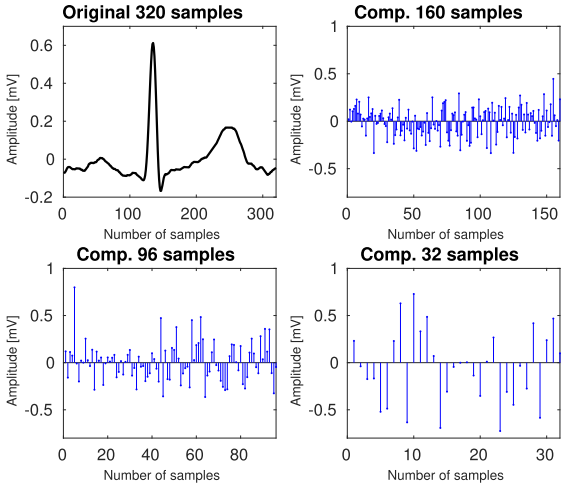


FIGURE 4. Examples of CS measurements of an ECG pulse (top left) for 160 (top right), 96 (bottom left), and 32 samples (bottom right).

TABLE 1. Performance summary of CS-GLRT. Cancelable biometrics yielded results comparable to non-cancelable baseline (Euclidean) with mild performance degradation.

Method	PD* (%)	EER (%)
Euclidean, signal domain	93.2	4.8
CS-Euclidean, 32 samples	89.2	5.5
CS-GLRT, 32 samples	89.8	5.4

B. CANCELABLE ECG BIOMETRICS USING CS-GLRT

Fig. 4 illustrates examples of CS measurements from a ECG pulse with 160, 96, and 32 samples. All CS measurements look like random noise, but they contain information about the original ECG pulse with 320 samples. We found experimentally that CS measurement with 32 samples yielded reasonable authentication performance while was practically non-invertible since CS recovered template yielded poor authentication performance. Table 1 summarizes authentication performance results for non-cancelable baseline (Euclidean distance in signal domain), CS-Euclidean with 32 samples (Euclidean distance in CS domain), and proposed CS-GLRT with 32 samples. Both CS-Euclidean and

CS-GLRT with 32 samples yielded performance comparable to the non-cancelable baseline with mild performance degradation. CS-GLRT yielded better performance than CS-Euclidean in both PD* and EER. However, the performance gap between them was slight since $\mathbf{H}\mathbf{H}^T$ in (14) is close to a diagonal matrix with a constant so that (14) becomes similar to CS-Euclidean.

C. SECURE PERFORMANCE IMPROVEMENTS IN CS DOMAIN

The guide signal for self-GF in (19) was generated as illustrated in Fig. 3. More specifically, QRS complex was extracted from 0.218 sec to 0.342 sec among 0.64 sec for each ECG pulse of all subjects and other intervals of (0 sec - 0.218 sec, 0.342 sec - 0.64 sec) were padded with values to ensure the continuity of the resulting signal so that sharp transitions are not transferred to the denoising output. For CS-GLRT with T-wave shift model (24), the length of the T-wave part was chosen to be $K_2 = 140$ samples (0.28 sec) for all subjects (the whole length of ECG pulse is $K = 320$ samples, 0.64 sec). The parameter α for circular shift operator sweeps from 0 to 140 samples with the step size of 2 samples.

TABLE 2. Performance summary when using performance boost methods. Proposed tricks significantly improved performance over CS-GLRT, yielded results comparable to the baseline.

Method	PD* (%)	EER (%)
CS-GLRT, 32 samples	89.8	5.4
CS-GLRT, 32 samples, GF w/ user template	92.0	4.8
CS-GLRT, 32 samples, self-GF	92.0	5.0
CS-GLRT, 32 samples, T-wave	90.5	4.4
CS-GLRT, 32 samples, self-GF , T-wave	93.0	3.8

Table 2 summarizes the results of the two proposed performance boost tricks for GLRT based cancelable ECG biometrics. When using GF with user template guide signal [43], significant performance increase was observed in terms of all performance metrics over the cancelable baseline, CS-GLRT with 32 samples. However, it does require storing the enrolled user template $\mathbf{t}$. Self-GF for CS-GLRT yielded comparable performance to CS-GLRT using GF with user template while it does not require storing additional enrolled user information. T-wave shift model in CS-GLRT yielded substantially better EER and better PD* than CS-GLRT. Lastly, using both performance boost methods yielded significantly improved performance over CS-GLRT. This method, CS-GLRT with 32 samples, self-GF and T-wave, yielded substantially better performance than the non-cancelable baseline in Table 1 in EER and also yielded comparable performance in PD*.

D. CANCELABLE BIOMETRICS CRITERIA: EFFICIENCY

Tables 1 and 2 demonstrated that the proposed cancelable biometrics methods are efficient since the authentication performance of them is comparable to or better than the non-cancelable baseline using Euclidean distance and user template. The RIP condition of a random matrix $\mathbf{H}$ theoretically guarantees that the distance between two signals can be well-preserved after projections using $\mathbf{H}$ so that the distance between secure user template $\mathbf{y^t}$ and projected input signal $\mathbf{Hs}$ can be well-evaluated [30], [50], [51]. In addition, nearly optimal CS-GLRT with two performance improvement methods (self-GF, T-wave model in CS-GLRT) enabled CS-GLRT to be efficient as a cancelable ECG biometrics.

E. CANCELABLE BIOMETRICS CRITERIA: NON-INVERTIBILITY

Non-invertibility of our proposed methods was evaluated using simulations with 89 subjects in ECG-ID data set. ECG signal recovery from CS measurement was performed by solving the following minimization problem:

$$\hat{\mathbf{t}} = \arg\min_{\mathbf{t}} \|\mathbf{y^t} - \mathbf{Ht}\|_2^2 + \beta\|\mathbf{Wt}\|_1 \tag{27}$$

using approximate message passing (AMP) with Daubechies wavelet transform $\mathbf{W}$ for promoting sparsity of the reconstructed signal [40]. However, any converged convex optimization can yield the same solution for (27).

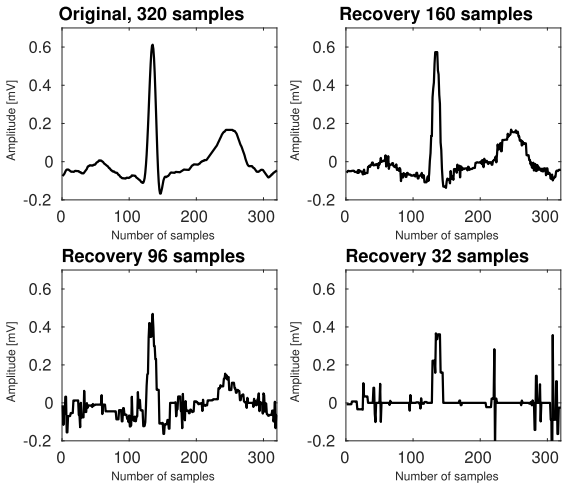


FIGURE 5. CS recovery results of ECG signals from CS measurements with 160 (top right), 96 (bottom left), and 32 samples (bottom right). CS recovered signals with 32 samples (bottom right) lost distinct shape information about the original signal (top left).

Fig. 5 illustrates the examples of recovered ECG signals from CS measurements with 160, 96, and 32 samples, respectively. The less CS measurements were used for recovery, the more distinct features of the original signal such as P, T waves are lost in the reconstructed signals. When 32 samples were used, almost no ECG figures were recovered from CS measurement visually. However, CS measurement with 32 samples was still able to achieve good hypothesis testing performance as shown in Tables 1 and 2.

Further simulation was performed for investigating the authentication performance of CS recovered signals. Fig. 6 illustrates the authentication performance changes for different CS sample numbers for an enrolled user (User) and for an imposter who reconstructed a signal from $\mathbf{H}$ and $\mathbf{y^t}$ and then used it for authentication (Imposter w/ recon signal).

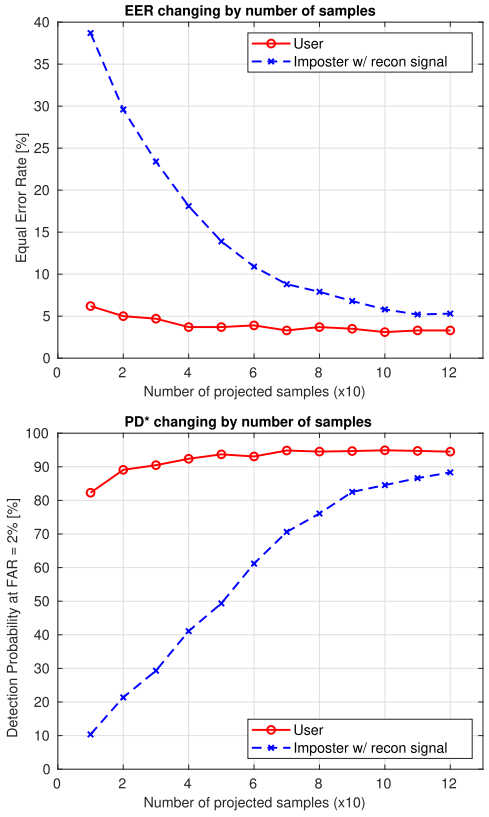


FIGURE 6. Plots of EER (top) and PD* (bottom) versus number of CS samples. Reconstructed signals from small number of CS samples (Imposter) yielded significantly worse authentication performance than the original signal (User) in both EER and PD*.

With large amount of CS samples, both User and Imposter achieved good authentication performance. However, with small amount of samples, User achieved significantly better performance in user authentication than Imposter. It looks infeasible for Imposter to be successful in authentication if there is a proper authentication lock (preventing multiple attempts).

F. RECORD MULTIPLICITY ATTACK

We also investigated record multiplicity attack with two different revocation procedures: random re-generation of $\mathbf{H}$ (randomly generated) [45] and our proposed random re-permutation of $\mathbf{H}$ (randomly permuted) in (17). Fig. 7 shows the plot of EER versus the number of successful attacks. F number of record multiplicity attacks for random re-generation based revocation process essentially allows imposter to recover the original signal using CS recovery algorithm with CS measurements F times more than the original CS samples. However, multiple times of record multiplicity attacks for our random row re-permutation based revocation process prevent Imposter achieving good authentication performance. This result shows that our proposed revocation process is resilient to record multiplicity attack.

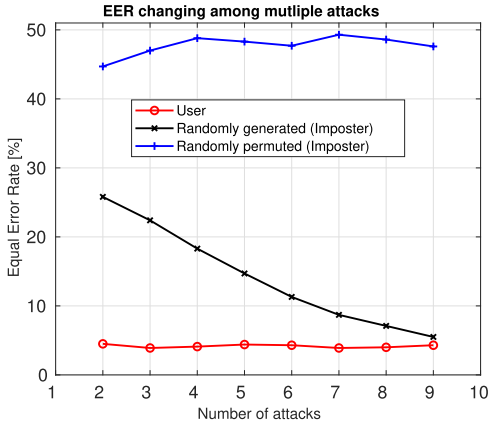


FIGURE 7. Simulation result of record multiplicity attack when using 32 compressive samples for authentication. As the number of attacks increases, EER for random re-generation based revocation decreases (Randomly generated - Imposter). However, EER for the proposed random re-permutation based revocation remains around poor EER (Randomly permuted - Imposter).

V. DISCUSSION

In this article, we proposed cancelable ECG biometrics methods using composite hypothesis testing in CS domain. We showed that these proposed methods yielded performance comparable to or better than the non-cancelable baseline with small amount of samples (10% in simulations) that were not enough for recovering the original signal properly. The proposed CS-GLRT detector in CS domain seems to use CS samples more efficiently than detectors with recovered signals from CS measurements. This is an important property for cancelable biometrics with efficiency and non-invertibility.

Even though the detection probability of imposter (PD*) was about 30% as shown in Fig. 6, it may be possible to try authentication multiple times to increase the chance of success. For that, it is possible to protect the system by limiting the number of tries, which is similar to 'password lock' that blocks an incoming user with several authentication failures. Another protection method is to use FIDO2[3] for biometrics. In this case, our proposed method can be used locally so that strong protection on cancelable user templates becomes possible while a variety of services on the internet can be used without revealing secure user template online.

Our proposed schemes could provide *secure* ECG biometrics to the cases with limited access to others' ECG data or with limited computation power and memory. Examples are low-cost wearable bands with ECG sensors such as [18] or other recently commercialized wearable bands/sensors. We, along with other researchers, have showed that it is possible to achieve state-of-the-art authentication performance (0.1% EER) with multimodal biometrics using ECG and MSP (multispectral skin photomatrix) by storing all user information [18]. Since our proposed methods yielded comparable performance to the baseline ECG

[3]https://fidoalliance.org/

biometrics, it seems possible for our proposed cancelable biometrics methods to achieve similar state-of-the-art authentication performance in a *secure* way.

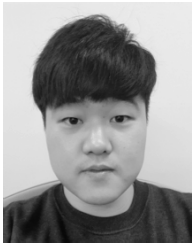
VI. CONCLUSION

We proposed a cancelable ECG biometric using CS based composite hypothesis testing (CS-GLRT), developed a novel random row permutation based revocation process for being resilient to record multiplicity attack, and investigated their cancelable biometrics properties. We further investigated two performance improvement methods to compensate for performance degradation due to the proposed cancelable biometric schemes. Our proposed methods were practically cancelable, but still yielded up to 93.0% PD* and 3.8% EER with the public ECG-ID data set (89 subjects) for challenging single pulse ECG, that is comparable to or better than non-cancelable baseline. Our proposed methods can provide a secure ECG biometrics to wearable bands / devices with ECG sensors or to multimodal biometrics for achieving state-of-the-art authentication performance.

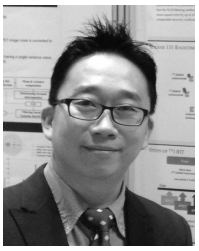
REFERENCES

[1] A. Ross and A. K. Jain, "Multimodal biometrics: An overview," in *Proc. 12th Eur. Signal Process. Conf.*, Sep. 2004, pp. 1221–1224.
[2] J. A. Unar, W. C. Seng, and A. Abbasi, "A review of biometric technology along with trends and prospects," *Pattern Recognit.*, vol. 47, no. 8, pp. 2673–2688, 2014.
[3] 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.
[4] J. M. Irvine, S. A. Israel, W. T. Scruggs, and W. J. Worek, "eigenPulse: Robust human identification from cardiovascular function," *Pattern Recognit.*, vol. 41, no. 11, pp. 3427–3435, Nov. 2008.
[5] M. Komeili, N. Armanfard, and D. Hatzinakos, "Liveness detection and automatic template updating using fusion of ECG and fingerprint," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 7, pp. 1810–1822, Jul. 2018.
[6] W. Einthoven, "The different forms of the human electrocardiogram and their signification," *Lancet*, vol. 179, no. 4622, pp. 853–861, Mar. 1912.
[7] 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.
[8] 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.
[9] I. Odinaka, P. Lai, A. D. Kaplan, J. A. O'Sullivan, E. J. Sirevaag, and J. W. Rohrbaugh, "ECG biometric recognition: A comparative analysis," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 6, pp. 1812–1824, Dec. 2012.
[10] M. Merone, P. Soda, M. Sansone, and C. Sansone, "ECG databases for biometric systems: A systematic review," *Expert Syst. Appl.*, vol. 67, pp. 189–202, Jan. 2017.
[11] E. Nemati, M. J. Deen, and T. Mondal, "A wireless wearable ECG sensor for long-term applications," *IEEE Commun. Mag.*, vol. 50, no. 1, pp. 36–43, Jan. 2012.
[12] M. Elgendi, B. Eskofier, S. Dokos, and D. Abbott, "Revisiting QRS detection methodologies for portable, wearable, battery-operated, and wireless ECG systems," *PLoS ONE*, vol. 9, no. 1, p. e84018, Jan. 2014.
[13] S. J. Kang, S. Y. Lee, H. I. Cho, and H. Park, "ECG authentication system design based on signal analysis in mobile and wearable devices," *IEEE Signal Process. Lett.*, vol. 23, no. 6, pp. 805–808, Jun. 2016.
[14] S. Yin *et al.*, "Low-power ECG biometric authentication for wearable systems featuring sparse memory compression," in *Proc. On-Device Intell. Workshop Int. Conf. Mach. Learn. (ICML)*, Jun. 2016.
[15] S. Y. Chun, J.-H. Kang, H. Kim, C. Lee, I. Oakley, and S.-P. Kim, "ECG based user authentication for wearable devices using short time Fourier transform," in *Proc. Int. Conf. Telecommun. Signal Process.*, Jun. 2016, pp. 656–659.
[16] Y. N. Singh, S. K. Singh, and P. Gupta, "Fusion of electrocardiogram with unobtrusive biometrics: An efficient individual authentication system," *Pattern Recognit. Lett.*, vol. 33, no. 14, pp. 1932–1941, 2012.
[17] M. D. Bugdol and A. W. Mitas, "Multimodal biometric system combining ECG and sound signals," *Pattern Recognit. Lett.*, vol. 38, pp. 107–112, Mar. 2014.
[18] H. Kim *et al.*, "A wearable wrist band-type system for multimodal biometrics integrated with multispectral skin photomatrix and electrocardiogram sensors," *Sensors*, vol. 18, no. 8, p. 2738, 2018.
[19] A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: A tool for information security," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 2, pp. 125–143, Jun. 2006.
[20] R. M. Bolle, J. H. Connell, and N. K. Ratha, "Biometric perils and patches," *Pattern Recognit.*, vol. 35, no. 12, pp. 2727–2738, 2002.
[21] A. B. J. Teoh, A. Goh, and D. C. L. Ngo, "Random multispace quantization as an analytic mechanism for BioHashing of biometric and random identity inputs," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 28, no. 12, pp. 1892–1901, Dec. 2006.
[22] D. Maltoni, D. Maio, A. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*. London, U.K.: Springer, 2009.
[23] N. Ratha, J. Connell, R. M. Bolle, and S. Chikkerur, "Cancelable biometrics: A case study in fingerprints," in *Proc. Int. Conf. Pattern Recognit.*, Aug. 2006, pp. 370–373.
[24] A. Othman and A. Ross, "On mixing fingerprints," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 1, pp. 260–267, Jan. 2013.
[25] A. Teoh and C. T. Yuang, "Cancelable biometrics realization with multispace random projections," *IEEE Trans. Syst., Man, Cybern. B, Cybern.*, vol. 37, no. 5, pp. 1096–1106, Oct. 2007.
[26] A. B. J. Teoh, Y. W. Kuan, and S. Lee, "Cancellable biometrics and annotations on BioHash," *Pattern Recognit.*, vol. 41, no. 6, pp. 2034–2044, Jun. 2008.
[27] J. K. Pillai, V. M. Patel, R. Chellappa, and N. K. Ratha, "Secure and robust iris recognition using random projections and sparse representations," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 33, no. 9, pp. 1877–1893, Sep. 2011.
[28] A. M. P. Canuto, F. Pintro, and J. C. Xavier-Junior, "Investigating fusion approaches in multi-biometric cancellable recognition," *Expert Syst. Appl.*, vol. 40, no. 6, pp. 1971–1980, 2013.
[29] W. B. Johnson and J. Lindenstrauss, "Extensions of Lipschitz mappings into a Hilbert space," *Contemp. Math.*, vol. 26, pp. 189–206, 1984.
[30] E. J. Candès, J. Romberg, and T. Tao, "Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information," *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 489–509, Feb. 2006.
[31] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP J. Inform. Secur.*, vol. 2011, no. 1, pp. 1–25, 2011.
[32] M. Gomez-Barrero, E. Maiorana, J. Galbally, P. Campisi, and J. Fierrez, "Multi-biometric template protection based on Homomorphic Encryption," *Pattern Recognit.*, vol. 67, pp. 149–163, Jul. 2017.
[33] V. M. Patel, N. K. Ratha, and R. Chellappa, "Cancelable biometrics: A review," *IEEE Signal Process. Mag.*, vol. 32, no. 5, pp. 54–65, Sep. 2015.
[34] T. Ignatenko and F. M. J. Willems, "Biometric systems: Privacy and secrecy aspects," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 4, pp. 956–973, Dec. 2009.
[35] S. Rane, Y. Wang, S. Drape, and P. Ishwar, "Secure biometrics: Concepts, authentication architectures, and challenges," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 51–64, Sep. 2013.
[36] M. Dey, N. Dey, S. K. Mahata, S. Chakraborty, S. Acharjee, and A. Das, "Electrocardiogram feature based inter-human biometric authentication system," in *Proc. Int. Conf. Electron. Syst., Signal Process. Comput. Technol. (ICESC)*, Jan. 2014, pp. 300–304.
[37] C. Camara, P. Peris-Lopez, and J. E. Tapiador, "Human identification using compressed ECG signals," *J. Med. Syst.*, vol. 39, no. 11, p. 148, 2015.
[38] C. M. Fira, L. Goras, C. Barabasa, and N. Cleju, "ECG compressed sensing based on classification in compressed space and specified dictionaries," in *Proc. Eur. Signal Process. Conf.*, Aug./Sep. 2011, pp. 1573–1577.
[39] D. Craven, B. McGinley, L. Kilmartin, M. Glavin, and E. Jones, "Adaptive dictionary reconstruction for compressed sensing of ECG signals," *IEEE J. Biomed. Health Inform.*, vol. 21, no. 3, pp. 645–654, May 2017.
[40] Y. V. Parkale and S. L. Nalbalwar, "Application of compressed sensing (CS) for ECG signal compression: A review," in *Proc. Int. Conf. Data Eng. Commun. Technol.*, 2017, pp. 53–65.

[41] J. Haupt and R. Nowak, "Compressive sampling for signal detection," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process.*, vol. 3, Apr. 2007, pp. III-1509–III-1512.
[42] M. A. Davenport, P. T. Boufounos, M. B. Wakin, and R. G. Baraniuk, "Signal processing with compressive measurements," *IEEE J. Sel. Topics Signal Process.*, vol. 4, no. 2, pp. 445–460, Apr. 2010.
[43] S. Y. Chun, "Single pulse ECG-based small scale user authentication using guided filtering," in *Proc. Int. Conf. Biometrics*, Jun. 2016, pp. 1–7.
[44] S. Y. Chun, "Small scale single pulse ECG-based authentication using GLRT that considers T wave shift and adaptive template update with prior information," in *Proc. 23rd Int. Conf. Pattern Recognit.*, Dec. 2016, pp. 3043–3048.
[45] H. Kim, M. P. Nguyen, and S. Y. Chun, "Cancelable ECG biometrics using GLRT and performance improvement using guided filter with irreversible guide signal," in *Proc. IEEE 39th Annu. Int. Conf. Eng. Med. Biol. Soc. (EMBC)*, Jul. 2017, pp. 454–457.
[46] T. S. Lugovaya, "Biometric human identification based on electrocardiogram," M.S. thesis, Dept. Fac. Comput. Technol. Inf., Saint Petersburg Electrotech. Univ., Saint Petersburg, Russia, Jun. 2005.
[47] 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, 2000.
[48] S. Luo and P. Johnston, "A review of electrocardiogram filtering," *J. Electrocardiol.*, vol. 43, no. 6, pp. 486–496, 2010.
[49] J. Pan and W. J. Tompkins, "A real-time QRS detection algorithm," *IEEE Trans. Biomed. Eng.*, vol. BME-32, no. 3, pp. 230–236, Mar. 1985.
[50] E. J. Candès and M. B. Wakin, "An introduction to compressive sampling," *IEEE Signal Process. Mag.*, vol. 25, no. 2, pp. 21–30, Mar. 2008.
[51] D. L. Donoho, "Compressed sensing," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1289–1306, Apr. 2006.
[52] K. He, J. Sun, and X. Tang, "Guided image filtering," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 35, no. 6, pp. 1397–1409, Jun. 2013.
[53] K. Simoens, J. Bringer, H. Chabanne, and S. Seys, "A framework for analyzing template security and privacy in biometric authentication systems," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 833–841, Apr. 2012.



HANVIT KIM received the B.S.E. degree from the School of Electrical Engineering, Ulsan National Institute of Science and Technology (UNIST), South Korea, in 2016, and the M.S.E. degree from the Department of Electrical Engineering, UNIST, in 2018. His research interests include image reconstruction and denoising, and statistical signal processing for biometrics. He is a Student Member of the IEEE.



SE YOUNG CHUN received the B.S.E. degree from the School of Electrical Engineering, Seoul National University, South Korea, in 1999, and the dual M.S.E./M.S. degrees in electrical engineering (systems/mathematics) and the Ph.D. degree in electrical engineering (systems) from the University of Michigan, Ann Arbor, MI, USA, in 2005 and 2009, respectively. From 2009 to 2011, he was a Research Fellow with Massachusetts General Hospital and Harvard Medical School, Boston, MA, USA, and from 2011 to 2013, he was a Research Fellow with the Departments of Electrical Engineering and Computer Science and Radiology, University of Michigan.

From 2013 to 2017, he was an Assistant Professor with the School of Electrical and Computer Engineering, Ulsan National Institute of Science and Technology, Ulsan, South Korea, where he is currently an Associate Professor. His research interests include modeling, algorithms, and analyses using statistical signal processing and machine learning for signal/image reconstruction, denoising, motion estimation and correction, detection and classification for the applications in ECG biometrics, computer vision for robotics, medical image reconstruction, and medical image analysis.

Dr. Chun is a member of the IEEE. He was a recipient of the 2010 Society of Nuclear Medicine Computer and Instrumentation Young Investigator Award (second place). He was also a recipient of the 2015 Bruce Hasegawa Young Investigator Medical Imaging Science Award from the IEEE Nuclear and Plasma Sciences Society. Recently, his group received the third place at the CVPR 2018 NTIRE Single Image Super Resolution Challenge (tracks 2, 3, 4: realistic). He has served as an Area Chair of the IEEE ICASSP, in 2018. He has been a member of the IEEE Computational Imaging Technical Committee, since 2016, an Associate Member of the IEEE Bio Imaging and Signal Processing Technical Committee, since 2018, and an Editorial Board Member of *Nuclear Medicine and Molecular Imaging* (Springer), since 2015.