



저작자표시-비영리-변경금지 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.

다음과 같은 조건을 따라야 합니다:



저작자표시. 귀하는 원저작자를 표시하여야 합니다.



비영리. 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.



변경금지. 귀하는 이 저작물을 개작, 변형 또는 가공할 수 없습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 [이용허락규약\(Legal Code\)](#)을 이해하기 쉽게 요약한 것입니다.

[Disclaimer](#)

Master's Thesis

Towards multi-modal Biometrics for Wearable devices

Hanvit Kim

Department of Electrical Engineering

Graduate School of UNIST

2018

Towards multi-modal Biometrics for Wearable devices

Hanvit Kim

Department of Electrical Engineering

Graduate School of UNIST


Towards multi-modal Biometrics for Wearable devices

A thesis/dissertation
submitted to the Graduate School of UNIST
in partial fulfillment of the
requirements for the degree of
Master of Science

Hanvit Kim

12 / 06 / 2017

Approved by



Advisor

Se Young Chun

Thesis/Dissertation Title

Hanvit Kim

This certifies that the thesis/dissertation of Hanvit Kim is approved.

06 December 2017



Advisor: Se Young Chun



Jae-Young Sim: Thesis Committee Member #1



Sung-Phil Kim: Thesis Committee Member #2

Abstract

Biometrics such as fingerprint, iris, face, and electrocardiogram (ECG) have been investigated as convenient and powerful security tools that can potentially replace or supplement current possession or knowledge based authentication schemes. Recently, multi-spectral skin photomatrix (MSP) has been newly found as one of the biometrics. Moreover, since the interest of usage and security for wearable devices have been increasing, multi-modal biometrics authentication which is combining more than two modalities such as (iris + face) or (iris + fingerprint) for powerful and convenience authentication is widely proposed.

However, one practical drawback of biometrics is irrevocability. Unlike password, biometrics can not be canceled and re-used once compromised since they are not changed forever. There have been several works on cancelable biometrics to overcome this drawback. ECG has been investigated as a promising biometrics, but there are few research on cancelable ECG biometrics.

As we aim to study a way for multi-modal biometric scheme for wearable devices that is assumed circumstance under some limitations such as relatively high performance, low computing power, and limited information (not sharing users information to the public), in this study, we proposed a multi-modal biometrics authentication by combining ECG and MSP. For investigating the performances versus level of fusions, Adaboost algorithm was studied as a score level fusion method, and Majority Voting was studied as a decision level fusion method. Due to ECG signal is 1 dimensional, it provides benefits in wearable devices for overcoming the computing memory limitation. The reasons that we select MSP combination with ECG are it can be collected by measuring on inner-wrist of human body and it also can be considered as hardly stolen modality in remote ways.

For proposed multi-modal biometrics, We evaluate our methods using collected data by Brain-Computer-Interface lab with 63 subjects. Our Adaboost based proposed multi modal biometrics method with performance boost yielded 99.7% detection probability at 0.1% false alarm ratio ($PD^{0.1}$) and 0.3% equal error rate

(EER), which are far better than simply combining by Majority Voting algorithm with 21.5% $PD^{0.1}$ and 1.6% EER. Note that for training the Adaboost algorithm, we used only 9 people dataset which is assumed as public data and not included for testing data set, against for knowledge limitation as the other constraint.

As initial step for user template protection, We proposed a cancelable ECG based user authentication using a composite hypothesis testing in compressive sensing domain by deriving a generalized likelihood ratio test (GLRT) detector. We also proposed two performance boost tricks in compressive sensing domain to compensate for performance degradation due to cancelable schemes: user template guided filtering and T-wave shift model based GLRT detector for random projection domain. To verify our proposed method, we investigated cancelable biometrics criteria for the proposed methods to confirm that the proposed algorithms are indeed cancelable.

For proposed cancelable ECG authentication, We evaluated our proposed methods using ECG data with 147 subjects from three public ECG data sets (ECG-ID, MIT-BIH Normal / Arrhythmia). Our proposed cancelable ECG authentication method is practically cancelable by satisfying all cancelable biometrics criteria. Moreover, our proposed method with performance boost tricks achieved 97.1% detection probability at 1% false alarm ratio (PD^1) and 1.9% equal error rate (EER), which are even better than non-cancelable baseline with 94.4% PD^1 and 3.1% EER for single pulse ECG authentication.

Contents

Contents	iii
List of Figures	v
List of Tables	vi
I. Introduction	1
1.1 Aim of the Research	1
1.2 Biometrics Authentication	1
1.3 Contribution of This Thesis	2
1.4 Organization of This Thesis	3
II. Multimodal Biometrics Authentication by Combining ECG and MSP	4
2.1 Background and Related Works	4
2.1.1 Electrocardiogram as Biometrics	4
2.1.2 ECG signal modeling and authentication	5
2.1.3 Multi-spectral Skin Photomatrix	6
2.1.4 Distance Measurements	6
2.1.5 Fusion Methods	7
2.2 Simulation Settings	9
2.2.1 Data Pre-processing	9
2.2.2 Performance Evaluation	9
2.2.3 Distance Normalization.	9
2.2.4 Method Description	10
2.3 Results	10
2.3.1 Uni-Modal Authentication	10
2.3.2 Multi-Modal Authentication	11
2.4 Discussion	11
III. Authentication Scheme by Using Protected User Template	13

3.1	Background and Related Works	13
3.1.1	Cancelable Biometrics	13
3.1.2	Compressive sensing and restricted isometry property	14
3.1.3	Signal processing with compressive measurement	15
3.2	Methods	16
3.2.1	Cancelable ECG biometrics using composite hypothesis testing with com- pressive measurement	16
3.2.2	Performance boost trick I: Guided filtering in CS domain	18
3.2.3	Performance boost trick II: T-wave shift in CS domain	19
3.2.4	Cancelability criteria evaluation	21
3.3	Simulation Results	22
3.3.1	Public ECG databases and data normalization	22
3.3.2	Data pre-processing	23
3.3.3	Proposed GLRT based cancelable ECG biometrics	24
3.3.4	Proposed performance boost tricks in CS domain	24
3.3.5	Cancelable biometrics: efficiency and non-invertibility	25
3.4	Discussion	27
IV.	Conclusion	29
	References	30

List of Figures

1.1	Examples of biometric characteristics: (a) face, (b) fingerprint, (c) hand geometry, (d) iris, (e) keystroke, (f) signature, and (g) voice [1]	2
2.1	Electrocardiogram (ECG) signal, consists of P wave, QRS complex, and T wave .	4
2.2	Anatomical structure of human skin with penetration depths of light [2].	6
2.3	Types of fusion level: Feature, Score, and Decision.	7
2.4	Potentially useful observation:threshold determination.	12
3.1	Examples of GF results with different guide signals (user template, the proposed irreversible guide signal, and flat signal) and their zoomed plots.	18
3.2	Steps for generating an irreversible guide signal from ECG template: cropping, padding, and random scaling.	19
3.3	Schematic diagram for the summary of enrollment and authentication procedures.	21
3.4	Data normalization across different ECG databases. Top and bottom figures show histograms of three public ECG databases for the amplitude of ECG signals before and after data normalization, respectively.	22
3.5	Examples of compressed samples from ECG signals with different compression ratio.	24
3.6	Examples of CS recovery results of ECG signals from samples with different compression ratios (50%, 30% and 10%).	26
3.7	Performance plots of EER (top) and PD^1 (bottom) versus number of compressed samples. For imposter cases with small number of samples, low authentication performances were achieved.	27

List of Tables

2.1	Performance results for all experiments about uni-modal authentication	10
2.2	Performance results for all experiments about multi-modal authentication versus proposed methods	11
3.1	Performance summary for GLRT. Cancelable biometrics yielded comparable results to conventional ECG biometrics.	25
3.2	Performance summary for performance boost tricks. Proposed tricks significantly improved authentication over baseline.	25
3.3	Performance table for non-invertibility evaluation	26

Acknowledgement

I cannot believe that it has been already 2 years since I study for a master degree. Without so many people around me, this thesis may not have been completed. First of all, I would like to thank my supervisor Professor Se Young Chun for his guidance and teaching for overall of my study and research. If he did not offer me as a master student with this research, I may not achieve this great work and experiences. I also want to express my sincere thanks to my defense committee members: Professor Sung-Phil Kim, for providing the story line comments and encouraging me to understand the level of fusion for multimodal biometrics, and Professor Jae-Young Sim for his comments about experimental results description. I would also like to acknowledge lab mates: Thanh Quoc Phan, Dong-Won Park, Magauyiya Zhussip, Shakarim Soltanayev, Ji-Soo Kim, Kwan-Young Kim, Jae-Euen Seo, and Byung-Hyun Lee. And many thanks to my best friends: An-Jung Lee, Jong-Hyeok Park, Kyu-Bin Kwon, Woo-Suck Choi, Woo-Young Choi, Eun-Ku Park, Su-Jeong Back, Gu-Tack Kim, Daniel Song, Jun-Mo Kang, and Kang-Taek Lee. Thank you to Dong-Young Kim for encouraging me whenever I met a hard task. Lastly, I would like to give my very special thanks to my family for always believing in me, especially my parents, who always encouraged me whenever I was down.

Introduction

1.1 Aim of the Research

The aim of this research is to investigate a way of using biometrics as alternative of knowledge based authentication methods for computationally constrained and data limited circumstance such as wearable devices. The detail aims of the study are (1) to investigate a combining methods of uni-modal biometrics (in this study we used electrocardiogram (ECG) and multi-spectral skin photomatrix (MSP)) for multi-modal biometrics authentication, (2) to overcome the practical drawback of biometrics by investigating of user template protection methods which is called as cancelable biometrics, and (3) to compensate the performance degradation which is commonly observed by protecting user templates, we finally studied the ways of performance boosting while practically keeping the cancelability of authentication system.

1.2 Biometrics Authentication

Biometrics such as fingerprint, face, and iris provide convenient and powerful security tools to verify or identify individuals. A biometric system is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a set of features from the acquired data, and comparing this feature set to the enrolled feature set [3].

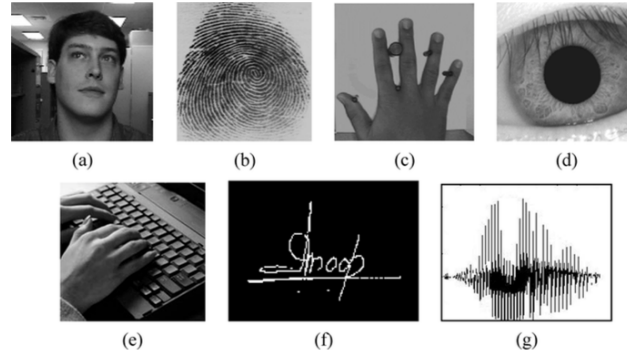


Figure 1.1: Examples of biometric characteristics: (a) face, (b) fingerprint, (c) hand geometry, (d) iris, (e) keystroke, (f) signature, and (g) voice [1]

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 [4]. Combining more than one biometrics as a multimodal biometrics has been widely investigated for strong security [5, 6]. A comprehensive review on recent biometrics research can be found in [7].

1.3 Contribution of This Thesis

In this study, We investigate the potential of MSP which is recently proposed, as biometrics material for wearable devices. And also, by performing various simulations for observation of the modality combination effect, we propose an Adaboost algorithm for multi-modal authentication method for ECG and MSP with 63 subjects provided by BCI labs. Since ECG is 1-dimensional signal, and by vectorizing the feature of MSP that may simultaneously measured with ECG, it against the low computing power that is one of constraint on wearable devices. We tried to overcome the limitation, due to wearable device implementation, for every proposed methods in this study.

Furthermore, we propose a cancelable ECG biometrics by deriving a near-optimal generalized likelihood ratio test (GLRT) detector from a composite hypothesis testing in compressed sensing (CS) domain. The CS theory was about recovering the original signal from undersampled data [8] when enough samples are acquired. Recently, CS was applied to conventional statistical signal processing tools such as detection and filtering [9, 10]. One of the results in [10] showed that statistical signal processing tools in CS domain is more efficient than using CS recovery and signal processing tools separately in terms of sampling size. Therefore, we conjecture

that our new GLRT detector in CS domain is efficient, but not recoverable with appropriately small sample size. Our proposed GLRT method was investigated to see if it satisfied cancelable biometrics criteria (efficiency, re-usability, diversity and non-invertibility) [11]. 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 and of evaluating the proposed method for cancelable biometrics criteria. Fira *et al.* proposed to use a random matrix of normal distribution for ECG signals using CS theory, but their work focused on efficient data compression for different pathological classes [12].

For performance degradation due to cancelable biometrics scheme, we also propose to use two performance improvement tricks called user template guided filtering [13] and T-wave circular shift model [14] that were shown to be effective in performance boosting in ECG biometrics. For user template guided filtering, it is required to store an original user template information [13], but in cancelable ECG biometrics, it should not be stored. In this article, we propose an irreversible guide signal construction method to resolve this conflict so that user template guided filtering can be used for detectors in CS domain. For T-wave shift model, we also propose an efficient algorithm to use T-wave shift model in CS domain.

Part of the works here was presented at the 2017 IEEE EMBC [15]. Its extended version was submitted to IEEE T-IFS including more detailed descriptions, more ECG data to all simulations (MIT-BIH Normal / Arrhythmia data sets [16, 17] were added to ECG-ID [18] with signal normalization additionally), investigating cancelable biometrics criteria with more simulation results, and proposing a new T-wave shift method in CS domain (related to Chapter III). For the other part related to Chapter II of the works here is in preparation for submission to IEEE T-IFS. We are going to propose an Adaboost based multimodal authentication method with combination of ECG and MSP with 63 subjects while overcoming the circumstance limitation in wearable devices.

1.4 Organization of This Thesis

This thesis is organized as follows. Chapter II describes some works on authentication method for uni-modal each, and its combination effect, and proposes a Adaboost algorithm for multi-modal authentication by using ECG and MSP. Chapter III reviews some previous works on cancelable biometrics, and proposes a cancelable ECG biometrics by deriving the generalized likelihood ratio test (GLRT) in compressed sensing (CS) domain with two performance boost tricks. Finally, in chapter IV concludes this thesis with a summary and future works.

Multimodal Biometrics Authentication by Combining ECG and MSP

2.1 Background and Related Works

2.1.1 Electrocardiogram as Biometrics

Electrocardiogram (ECG) has been investigated as a promising biometrics for authentication, identification and liveness validation [19–21]. One pulse of an ECG signal consists of P wave, QRS complex, and T wave (in Figure.2.1) that are from atrial depolarization, ventricular depolarization, and ventricular repolarization, respectively [22]. These characteristics depend on the structure and biological substrate of a heart which are known to be different on each person [23].

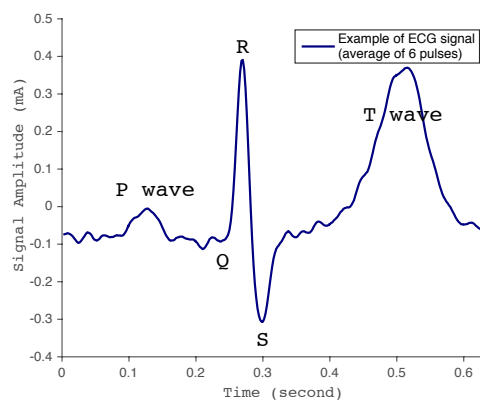


Figure 2.1: Electrocardiogram (ECG) signal, consists of P wave, QRS complex, and T wave

There have been many works on ECG biometrics since early 2000's. Biel *et al.* was one of the first works on ECG biometrics using fiducial features such as amplitude, duration, and deflection of QRS complex [24]. Since then, fiducial and non-fiducial features of ECG have been investigated for biometrics such as using durations / intervals of ECG waves [25], using intervals, amplitude and angles [26], autocorrelation and discrete cosine transform [27] and wavelet transform [28]. Various classification / authentication algorithms have also been applied for ECG biometrics such as decision based neural network [29], linear discriminant analysis (LDA) with PCA [18], dynamic time warping (DTW) and Fisher's LDA [30], various distance metrics such as DTW, earth mover's distance, Frechet distance and Hausdorff distance [31] and Euclidean distance variants [20,32,33]. For more comprehensive reviews on ECG biometrics, we refer readers to [34,35].

It is worth noting that recent works on ECG biometrics have made significant progresses 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 [36,37]. There have been recent works on ECG biometrics for wearable devices in terms of wearable ECG band development [38], low power circuit design [39], and light-weight authentication algorithm [40]. ECG has also been investigated as part of multimodal biometrics systems with fingerprint / face [41], voice [42] or palmprint [43]. ECG has a great potential as a biometrics.

2.1.2 ECG signal modeling and authentication

The acquired ECG signal f' can be modeled as:

$$f' = x + n + r + p \quad (\text{II.1})$$

where x is an original ECG signal (length K), n is high frequency noise, r is baseline drift and p is power-line noise. Usually, preprocessing of f' can reduce unwanted noise or artifacts. Slowly varying baseline drift r can be corrected by high-pass filtering or wavelet based drift correction. Power-line noise p is on specific frequency such as 50Hz or 60 Hz it can be reduced by bandstop filters (see [44] for details). High frequency noise n can be reduced by low-pass filtering, but this filtering could also remove some high frequency details of x . Thus, low-pass filtering should be used with care to preserve details, while to reduce noise. Here we assume that low-pass filtering is not applied. Then, the pre-processed ECG signal f can be modeled as:

$$f \approx x + n. \quad (\text{II.2})$$

2.1.3 Multi-spectral Skin Photomatrix

The multi-spectral skin photomatrix (MSP) is recently investigated as a biometrics [2]. According to this research, due to optical patterns of their inner-wrist skin tissue is unique, it can be used as potential identification tools. For MSP data acquisition, optical patterns are measured by 2×8 photodiode channel with selective wavelength (called IR and Yellow) which is positioned on the inner-wrist skin. Despite it is initial study as biometrics, they achieve moderately high performance (FAR 0.3% and FRR 0%) with 21 subjects by using linear discriminant analysis (LDA) for IR + Yellow feature case.

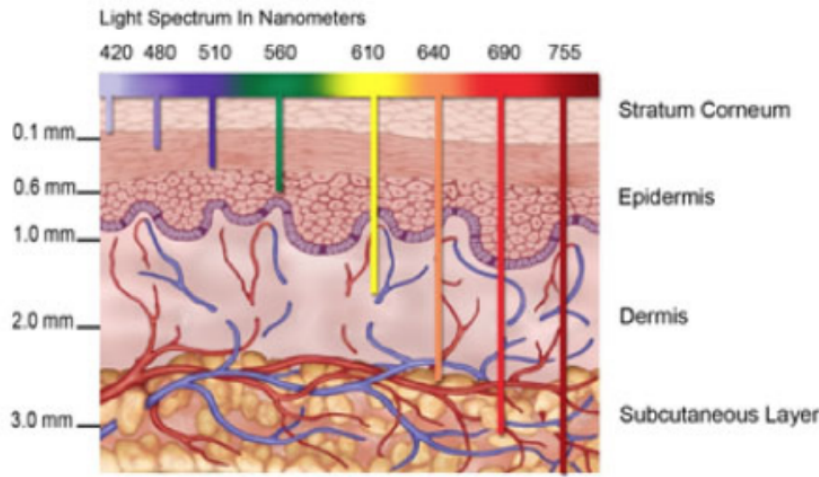


Figure 2.2: Anatomical structure of human skin with penetration depths of light [2].

2.1.4 Distance Measurements

The conventional user authentication is done by measuring the distance between enrolled template signals f_1, \dots, f_N and current input signals s_1, \dots, s_M as follows:

$$d(\{f_1, \dots, f_N\}, \{s_1, \dots, s_M\}) \underset{\text{accept}}{\overset{\text{reject}}{\geq}} \gamma \quad (\text{II.3})$$

where d is a distance metric or classifier and γ is a threshold. Especially in case of ECG user authentication, It has been shown that this can yield better performance with more ECG signals (or larger N, M) [34].

One of the conventional user authentication methods for limited memory and computation power is to use a single user template t and a single biometrics feature s such that $t = \sum_{i=1}^N f_i / N$

and $s = s_1$ with a simple Euclidean distance as follows:

$$d(t, s) = \sqrt{\sum_{j=1}^K (t[j] - s[j])^2} \begin{matrix} \text{reject} \\ \geq \\ \text{accept} \end{matrix} \gamma' \quad (\text{II.4})$$

where γ' is a threshold. It has been shown that this simple detector is actually a generalized likelihood ratio test (GLRT) detector if n follows an independent and identically distributed (*i.i.d.*) Gaussian noise [14]. This method has been demonstrated to be effective for user authentication when proper performance improvement methods with mild computation increases are used together [13, 14]. As we described in section. 2.1.1, there are various studies for signal similarity or distance measuring not only for using Euclidean distance.

2.1.5 Fusion Methods

According to the Sarhan et al, There are four standard fusion types including feature level fusion, score level fusion, decision level fusion, and sensor level fusion. Comparative performance evaluation is here [6].

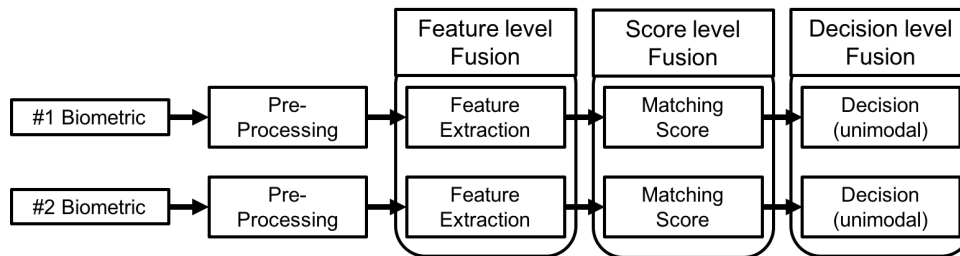


Figure 2.3: Types of fusion level: Feature, Score, and Decision.

In this study, we concentrated on two methods: Majority Voting (Algorithm 1 [45, 46]), and Adaboost (Algorithm 2 [47]) which are two different methods of decision level fusion. Majority Voting method can be simply described that acceptance is decided when the sum of every voting is over half of number of classifiers by assuming every uni-modal decision as one voting. Adaboost algorithm can be explained as finding appropriate coefficients between weak classifiers by updating the observation weight based on classification error. Shortly, MV means all sum of decision without any weighting while the Adaboost method implies the weighted sum of each classifiers. Since decision level fusion is relatively simple to implement when the device already store the classifiers, we choose that decision level fusion may be more suitable for multimodal biometrics on wearable devices than other fusion on different stages. Comprehensive information of other methods for decision level fusion is here [48].

Algorithm 1 Majority voting [45, 46]

1: For the given threshold, th and number of classifier, M .

$$G(x) = \sum_{i=1}^M g_m(x) > \lfloor M/2 \rfloor$$

where x is input score, and the classifier,

$$g_m(x) = \begin{cases} 1, & x > th \\ 0, & x < th \end{cases}$$

Algorithm 2 Adaboost.M1 for multi-modal biometrics [47]

1: Initialize the observation weight

2: $w_i = 1/N, i = 1, 2, \dots, N$. and $y_i \in [-1, 1]$.

3: **for** $m = 1$ to M **do**

4: Thresholding the distances with given threshold, th .

5:

$$f_m(x_i) = \begin{cases} 1, & x_i > th \\ -1, & x_i < th \end{cases}$$

6: Compute an error.

$$err_m = \frac{\sum_{i=1}^N w_i I(y_i \neq f_m(x_i))}{\sum_{i=1}^N w_i}$$

where $I(\cdot)$ is an indicator function.

7: Compute weight, α for individual classifier

8:

$$\alpha_m = \log((1 - err_m)/err_m)$$

9: Update the weights

10:

$$w_i \leftarrow w_i \cdot \exp[\alpha_m \cdot I(y_i \neq f_m(x_i))], \forall i$$

11: Weight normalization such that

$$\sum_{i=1}^N w_i = 1$$

12: **end for**

13: Final Decision,

$$F(x) = \text{sign}\left[\sum_{m=1}^M \alpha_m f_m(x)\right]$$

2.2 Simulation Settings

2.2.1 Data Pre-processing

In this experience, we divided a measured ECG and MSP data set into 6 records regarding 3 pulses and 3 feature respectively. For the measured few-minute ECG records per one subject, to segment into single pulses with regarding to R-peak, Pan-Tompkins method for R-peak detection was applied [49] after base-line correction by band-pass filtering. Due to its sampling rate is 250 Hz, single pulse, which cover P-QRS-T fragment, can be achieved by cut with length 160 samples or 0.64 seconds, which are $-67,+92$ samples from the R-peak.

For the case of MSP data per one subject, 4×32 feature (Red, Yellow, IR, IY and 32 channels) vectors were collected. Two features (R+Y) were used for authentication method by linearly combining. Thus, for each subject, MSP feature matrix transformed into one vector with 64 lengths.

Totally, 111 subjects participated for measuring the data. After pre-process step, we divided a data set into 'Experiment' and 'Public'. The 'Experiment' set which is composed with the 63 subjects who have both ECG and MSP features. The other, 'Public', data set is composed with the 39 subjects have only ECG pulses and 9 subjects have only MSP features. The 'Public' data set was used for AdaBoost training.

2.2.2 Performance Evaluation

For evaluating the performance, we used EER , PD^1 , and $PD^{0.1}$. EER can be obtained by the finding the point where $FRR = FAR := EER$. PD^1 and $PD^{0.1}$ are detection probability at FAR is same as 1% and 0.1% respectively. Since the performance evaluation should be done under fixed FAR value, we assume that by setting the fixed threshold is means fixed FAR value. Thus, in under fixed threshold which is under same situation, the better detection probability is the better performance. Also FRR^0 means FRR value at FAR equals to 0 value which means relatively hard thresholding situation.

2.2.3 Distance Normalization.

Our proposed authentication system is based on the Euclidean distance between 'Enrolled' and 'Authenticate' features. However, since the range of ECG pulses and MSP features are different, the distance normalization was necessary for using the same classifier. Max distance normalization was used by computing all the distances between subjects.

2.2.4 Method Description

1. **Thresholding (TH)** based on distance between enrolled and 1 single feature or pulse then simple thresholding with given threshold.
2. **Averaging (AVG)** based on distance between enrolled and averaged of more than 2 features or pulses then simple thresholding with given threshold.
3. **Majority Voting (MV)** based on distance between enrolled and more than 2 features or pulses each then classify with majority voting that composed of simple thresholdings with given threshold.
4. **Ada.MV** based on distance between enrolled and more than 2 pulses and feature each then classify with one single classifier which is weighted sum of classifier. In this exp, 4 classifier was used (3 ECG pulses and 1 MSP feature).
5. **Ada.AVG** based on distance between enrolled and averaged of more than 2 pulses and feature then classify with one single classifier which is weighted sum of classifier. In this exp, 2 classifier was used (averaging of 3 ECG pulses and 1 MSP feature).

2.3 Results

2.3.1 Uni-Modal Authentication

Table 2.1: Performance results for all experiments about uni-modal authentication

ECG Only					MSP Only				
Method	#Feature vectors	EER	$PD^{0.1}$	FRR^0	Method	#Feature vectors	EER	$PD^{0.1}$	FRR^0
TH	1	1.7	47.0	3.42	TH	1	1.2	90.8	3.33
AVG	2	1.3	95.4	9.23	AVG	2	1.2	90.8	3.10
	3	1.0	97.3	4.76		3	1.2	93.3	3.10
MV	2	1.8	87.6	29.1	MV	2	1.2	95.1	2.99
	3	1.8	87.6	29.1		3	1.2	93.8	3.10
Ada.MV	2	1.8	87.6	29.1	Ada.MV	2	1.2	95.1	2.99
	3	1.7	87.2	28.9		3	1.2	95.1	2.99

Table. 2.3.1 is the result of ROC curve for uni-modal authentication comparison. The best performance was yielded by using averaged 3 ECG pulses case. That method was even better than using majority voting or adaboost based majority voting. Note that here, under extremely low FAR case, using MSP feature was better than ECG pulses overall.

2.3.2 Multi-Modal Authentication

Table 2.2: Performance results for all experiments about multi-modal authentication versus proposed methods

#Feature vectors	MV			Ada.MV			Ada.AVG		
	EER	$PD^{0.1}$	FRR^0	EER	$PD^{0.1}$	FRR^0	EER	$PD^{0.1}$	FRR^0
1,1	0.5	44.1	2.91	0.1	99.86	4.13	0.1	99.86	4.13
2,2	0.5	94.9	2.86	0.1	99.85	2.99	0.1	99.99	0.61
3,3	0.5	99.3	2.75	0.1	99.80	2.94	0.1	1.00	0.03

Table 2.2 summarizes all experiment results for multi-modal authentication. By simply combining two modality with majority voting, we achieved far better results than using uni-modal based authentication. Furthermore, by using adaboost to performance enhancing, it showed that was effective way. And also, it is observed that the best performance was adaboost with 3 features and pulses each (0.03%, FRR^0)

2.4 Discussion

In this chapter, we investigated the ways of combining two modality, ECG and MSP. We showed that our final proposed methods (Ada.AVG) yielded the best result. It is far better than other uni-modal based authentication. By observing the performance difference between averaging 3 pulses of ECG and combining 3 pulses of ECG and 3 MSP feature by majority voting method, One more interesting point was averaging effect was more stronger than we expected. Furthermore, since this Adaboost coefficients are trained by public data only (not including the test data), it means that we may can find an appropriate weight distribution between ECG modality and MSP modality.

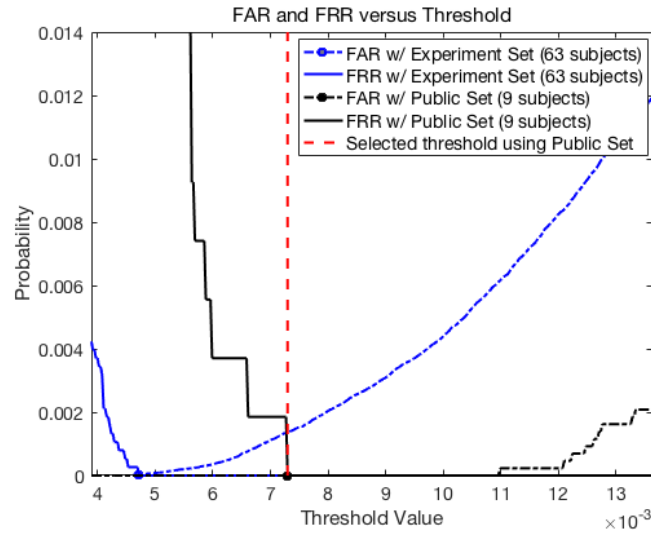


Figure 2.4: Potentially useful observation:threshold determination.

Finally, with this proposed combination methods, we showed powerful performance while overcoming given constrained comes from using wearable devices as following: knowledge limitation by Adaboost training with only public data set, low computing power by using ECG and MSP in the shape of 1-dimensional signal, and with relatively high performance.

As a future work, we aim to investigate the threshold determination. It is commonly known that determining appropriate thresholds without any other dataset except the user information is challenging problem. Based on interesting observation in Figure 2.4, it is observed that performance with experiment data set (63 subjects) on the threshold which is determined by minimizing the error on public data set (9 subjects) showed appropriate results. That performance has only 0.001 difference with optimal EER point of experiment data set.

Authentication Scheme by Using Protected User Template

3.1 Background and Related Works

3.1.1 Cancelable Biometrics

Biometrics is a convenient and powerful security tool, but one of the drawbacks is its irrevocability. If one password is compromised, this password can be immediately canceled and then a new password can be generated and used. However, once biometrics is compromised, it can not be canceled and re-used. Biometrics can not be changed forever.

Jain *et al.* emphasized strengthening the security of biometric system in [1]. Bolle *et al.* proposed the concept of cancelable biometrics for protecting user-specific features [50]. Maltoni *et al.* summarizes four criteria that cancelable biometrics must satisfy as follows [51, 52]:

- 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.

There have been several works on cancelable biometrics for fingerprint [53, 54], face [55, 56] and iris [57]. Cancelable multimodal biometrics have also been proposed and investigated recently [58, 59]. These cancelable biometrics works are usually based on Johnson-Lindenstrauss(JL) lemma [60] or compressive sensing (CS) [8]. 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 [52, 61]. Other works for cancelable biometrics were based on CS theory for iris [57]. There has been some works on cancelable biometrics using BioHash for face [56]. For more comprehensive reviews on cancelable biometrics and cancelable multimodal biometrics, we refer readers to [62–64].

Recently, cancelable ECG biometrics have been investigated based on BioHash [65] and CS theory [12, 66]. It has been shown that highly compressed ECG yielded reasonable authentication performance [12, 66]. Applications of CS theory for ECG have been investigated for compression or classification [67, 68].

Unfortunately, it has been observed that protecting biometrics information comes with the price of lowering authentication or identification performance [69, 70]. Moreover, compressed biometric signals may preserve the distance between signals well based on JL lemma or CS theory, but the usual choice for distance metric for compressed biometric signals is Euclidean distance or its variant, which may be sub-optimal. Originally, CS theory has been developed to recover the original signal from compressed samples [8]. Therefore, it is critical to check the method based on CS theory has non-invertibility. There has been no prior work on cancelable ECG biometrics 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.

3.1.2 Compressive sensing and restricted isometry property

Compressive sampling (CS) theory models that the measurement $y \in \mathbb{R}^L$ for the original signal $x \in \mathbb{R}^K$ is

$$y = \Phi x \tag{III.1}$$

where Φ is an $L \times K$ sensing matrix. The matrix Φ satisfies restricted isometry property (RIP) of order P if there exists a constant $\delta \in (0, 1)$ such that

$$(1 - \delta) \|x\|_2^2 \leq \|\Phi x\|_2^2 \leq (1 + \delta) \|x\|_2^2 \tag{III.2}$$

holds for all $x \in \Sigma_P$ where the set Σ_P is all P -sparse signals such that

$$\Sigma_P = \{x \in \mathbb{R}^K : \|x\|_0 \leq P\}.$$

The RIP condition implies that some matrices with very small δ can approximately preserve the l_2 norm of a signal. Examples are Gaussian random matrix and modified Bernoulli random matrix [8]. This condition also implies that the distance between two P -sparse signals is approximately preserved after applying Φ to these signals.

The CS theory also provided a way of reconstruct the original signal from the measurement using a computationally efficient l_1 minimization as follows [8]:

$$\min_{\tilde{x} \in \mathbb{R}^K} \|\tilde{x}\|_{l_1} \quad s.t. \quad \Phi \tilde{x} = y. \quad (\text{III.3})$$

It has been shown that the recovery in (III.3) is exact for P -sparse signals and is reasonably good for non P -sparse signals with the measurement size L that is larger than a certain number, but is much smaller than K [71, 72].

3.1.3 Signal processing with compressive measurement

The conventional CS theory focused on estimation problems in signal processing [71, 72]. The CS theory has been extended to other signal processing problems such as filtering and signal detection [9, 10]. We review the signal detection in CS domain.

Davenport *et al.* proposed a hypothesis testing [10]:

$$\begin{cases} H_0 & : & \Phi n \\ H_1 & : & \Phi (x + n) \end{cases} \quad (\text{III.4})$$

where $x \in \mathbb{R}^K$ is a known signal, $n \sim N(0, \sigma^2 I_K) \in \mathbb{R}^K$ is an *i.i.d.* Gaussian noise and Φ is a random matrix. Then, the probability density functions for the hypothesis testing (III.4) can be derived as follows:

$$\begin{aligned} f_0(y) &= \frac{\exp\{-\frac{1}{2}y^T(\sigma^2\Phi\Phi^T)^{-1}y\}}{|\sigma^2\Phi\Phi^T|^{1/2}(2\pi)^{L/2}} \\ f_1(y) &= \frac{\exp\{-\frac{1}{2}(y-\Phi x)^T(\sigma^2\Phi\Phi^T)^{-1}(y-\Phi x)\}}{|\sigma^2\Phi\Phi^T|^{1/2}(2\pi)^{L/2}} \end{aligned}$$

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

The optimal Neyman-Pearson(NP) detector for the hypothesis testing (III.4) is a likelihood ratio test as follows:

$$\Lambda(y) = \frac{f_1(y)}{f_0(y)} \underset{H_0}{\overset{H_1}{\geq}} \eta$$

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

$$y^T (\Phi \Phi^T)^{-1} \Phi x \underset{H_0}{\overset{H_1}{\geq}} \sigma^2 \log(\eta) + \frac{1}{2} x^T \Phi^T (\Phi \Phi^T)^{-1} \Phi x := \gamma.$$

One interesting result in signal detection in CS domain is that Detection in CS domain yielded much better performance than detection in signal domain after CS reconstruction with very small measurement size [10], which can be potentially useful for cancelable biometrics.

3.2 Methods

3.2.1 Cancelable ECG biometrics using composite hypothesis testing with compressive measurement

Storing the enrolled ECG template t in (II.4) is necessary in conventional ECG based user authentication, but once compromised, the same template can not be revoked and re-used. Inspired by [10], here we propose a new detector with compressive sensing measurement based on the conjecture that this new detector does have reasonably good authentication performance while does not have enough measurements for good signal recovery.

The compressive measurement for ECG can be defined as follows:

$$y = Hf \approx H(x + n) \tag{III.5}$$

where $n \sim N(0, C_K)$, C_K is a $K \times K$ covariance matrix, and H is a modified Bernoulli random matrix with the size of $L \times K$ with the element of either $1/\sqrt{K}$ or $-1/\sqrt{K}$ with probability 0.5. We chose this particular random matrix because this random matrix H only requires $L(K - 1)$ summations, L subtractions, and L divisions as well as a small storage of LK bits. These properties of H can potentially be appropriate for low cost wearable bands with limited computing power and memory.

We formulated a composite hypothesis test as follows:

$$\begin{cases} H_0 & : & \mu = \mu_0 := Hx \\ H_1 & : & \mu \neq \mu_0 \end{cases} \tag{III.6}$$

where their probability density functions are

$$f_0(y) = \frac{\exp\left\{-\frac{1}{2}(y - \mu_0)^T(\sigma^2 HC_K H^T)^{-1}(y - \mu_0)\right\}}{|\sigma^2 HC_K H^T|^{1/2} (2\pi)^{L/2}},$$

$$f_1(y; \mu) = \frac{\exp\left\{-\frac{1}{2}(y - \mu)^T(\sigma^2 HC_K H^T)^{-1}(y - \mu)\right\}}{|\sigma^2 HC_K H^T|^{1/2} (2\pi)^{L/2}},$$

respectively. The nearly-optimal GLRT detector is

$$\Lambda(y) = \frac{\max_{\mu \neq \mu_0} f_1(y; \mu)}{f_0(y)} = \frac{f_1(y; \hat{\mu}_{ML})}{f_0(y)} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\geq}} \gamma \quad (\text{III.7})$$

where $\hat{\mu}_{ML}$ is the maximum likelihood estimator using $f_1(y; \mu)$. In this case, $\hat{\mu}_{ML}$ is the sample y so that the numerator of (III.7) becomes a constant. Further simplification of (III.7) leads to

$$(y - \mu_0)^T (HC_K H^T)^{-1} (y - \mu_0) \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\geq}} \gamma' \quad (\text{III.8})$$

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

The original randomly projected ECG signal $\mu_0 = Hx$ is usually not available. However, for the case where a low noise user template t and a single ECG pulse input s are available, it is reasonable to assume that $Hx \approx Ht$. By using a ‘plug-in’ approach, the proposed GLRT detector becomes

$$(Hs - Ht)^T (HC_K H^T)^{-1} (Hs - Ht) \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\geq}} \gamma' \quad (\text{III.9})$$

The noise covariance matrix C_K can be estimated from the data. However, for simplicity, in this paper we further simplified this by assuming *i.i.d.* Gaussian noise n so that the proposed GLRT detector becomes

$$(Hs - Ht)^T (HH^T)^{-1} (Hs - Ht) \geq \gamma''. \quad (\text{III.10})$$

where γ'' is a threshold.

Note that (Ht) and H will be stored for authentication so that the user template t will be protected unless both (Ht) and H are compromised and the original signal can be recovered from them. We will investigate the possibility of recovering the original user template from (Ht) and H in the simulation.

3.2.2 Performance boost trick I: Guided filtering in CS domain

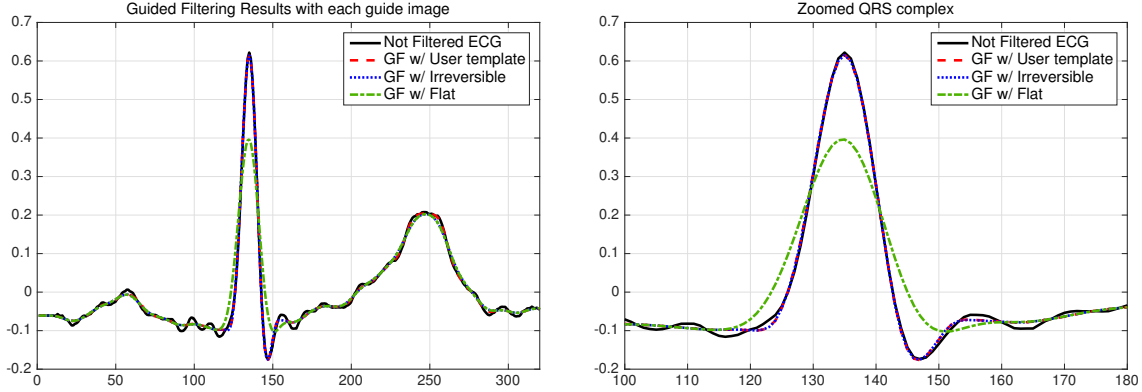


Figure 3.1: Examples of GF results with different guide signals (user template, the proposed irreversible guide signal, and flat signal) and their zoomed plots.

It is well known that the performance degradation in cancelable biometrics is inevitable [69, 70]. Therefore, using performance boost tricks for cancelable biometrics is desirable.

Guided image filter (GF) was originally proposed in computer vision and has yielded excellent performance in various applications such as denoising, artifact removal and upsampling [73]. Recently, Chun proposed to use a 1D GF for ECG authentication to yield improved performance [13]. This user template guided filter utilized the enrolled ECG template t as a guide signal to denoise the single pulse ECG input signal s . Since GF is essentially the local affine fitting of a guide image (or signal in 1D) to a noisy image (or signal) within moving local windows, this operation requires very low computation complexity $O(1)$ [73]. We denote this GF procedure as:

$$\hat{s} = GF(s; t). \quad (\text{III.11})$$

Then t and \hat{s} are used for authentication instead of t and s .

Unfortunately, user template guided filtering for ECG authentication [13] can not be used in cancelable ECG authentication schemes since it requires storing the original user template t . In here, we propose a method to use this user template GF for cancelable biometrics.

Here are a few observations on the user template GF for ECG based authentication as also shown in Fig. 3.1:

1. When using GF with a flat signal, good denoising results were obtained for P and T waves.
2. Having a good guide signal for denoising QRS complex is critical for good performance.
3. A scaled version of a guide signal still yields good denoising results.

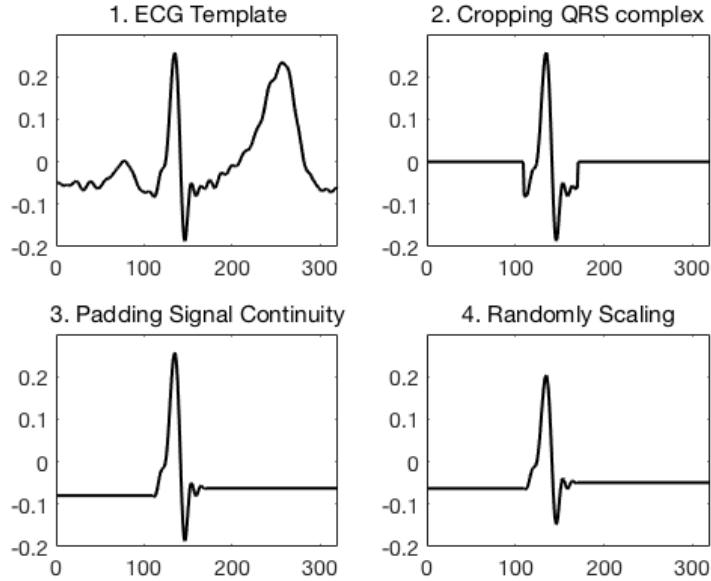


Figure 3.2: Steps for generating an irreversible guide signal from ECG template: cropping, padding, and random scaling.

Based on them, we propose a guide construction method, called irreversible guide signal for GF, to process the original ECG template t using a couple of consecutive irreversible operations such as cropping P / W waves and random scaling with unknown scaling factor as illustrated in Fig. 3.2. The resulting signal, t_{ir} , can be stored and used as an irreversible guide signal:

$$\hat{s} = GF(s; t_{ir}). \quad (\text{III.12})$$

It is expected that

$$GF(s; t_{ir}) \approx GF(s; t)$$

as demonstrated in Fig. 3.1. Recovering t_{ir} from t is infeasible due to two irreversible operators used to create t_{ir} . Note that the scaling factor should not be stored.

3.2.3 Performance boost trick II: T-wave shift in CS domain

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 [14]. This method also requires to use the original ECG template t to find the minimum distance between the template t and T-wave shifted ECG input s with unknown shift value. In here, we propose a new T-wave shift model to use it in CS domain.

We first modeled the input signal s to be separated into the PQRS segment s^F and T wave segment s^S as also used in [14]. Then, the T wave can be modeled to be shifted for different heart rate as follows:

$$\begin{bmatrix} s^F \\ \Gamma_\alpha s^S \end{bmatrix} \quad (\text{III.13})$$

where Γ_α is a circular shift operator with an integer step size α . Then, we construct a composite hypothesis testing to consider variable heart rate as follows:

$$\begin{aligned} H_0 &: y_\alpha \sim N(\mu_0, C_K) \\ H_1 &: y_\alpha \sim N(\mu, C_K), \mu \neq \mu_0 \end{aligned} \quad (\text{III.14})$$

where μ, α are unknown and

$$y_\alpha := H \begin{bmatrix} s^F \\ \Gamma_\alpha s^S \end{bmatrix}.$$

Then, we derived a GLRT detector with T wave shift model as follows:

$$\frac{\max_{\mu \neq \mu_0, \alpha} \exp\left(-\frac{1}{2}(y_\alpha - \mu)^T (HC_K H^T)^{-1} (y_\alpha - \mu)\right)}{\max_{\alpha} \exp\left(-\frac{1}{2}(y_\alpha - \mu_0)^T (HC_K H^T)^{-1} (y_\alpha - \mu_0)\right)}. \quad (\text{III.15})$$

For the unknown μ_0 , a ‘plug-in’ approach can be used to replace it by Ht . Since the numerator of (III.15) becomes 1 for the maximum likelihood estimator for μ , the GLRT detector can be simplified as follows:

$$\min_{\alpha} \left\{ (y_\alpha - \beta)^T (HC_K H^T)^{-1} (y_\alpha - \beta) \right\} \underset{H_0}{\overset{H_1}{\geq}} \gamma \quad (\text{III.16})$$

where $\beta = Ht$ and γ is a threshold.

Equation (III.16) is computationally expensive due to brute-force search for α . We derived an equivalent operation for (III.16) using matrix-vector form to speed up computation as follows:

$$\min_{\alpha} \mathbf{D} \left\{ (H\Gamma - X)^T (HC_K H^T)^{-1} (H\Gamma - X) \right\} \underset{H_0}{\overset{H_1}{\geq}} \gamma \quad (\text{III.17})$$

where $X = [\dots \beta \dots] \in \mathcal{R}^{L \times K'}$, K' is the length of the T wave segment (s^S), \mathbf{D} is an operator to extract diagonal elements to form a vector, and

$$\Gamma = \begin{bmatrix} s^F & \dots & s^F \\ \Gamma_1 s^S & \dots & \Gamma_{K'} s^S \end{bmatrix} \in \mathcal{R}^{K \times K'}.$$

Note that K' is about the half of K . This result implies that since H is a RIP operator to

approximately preserve the distance between two signals, the comparison that has been done in signal domain for T wave shift model can be approximately done in CS domain.

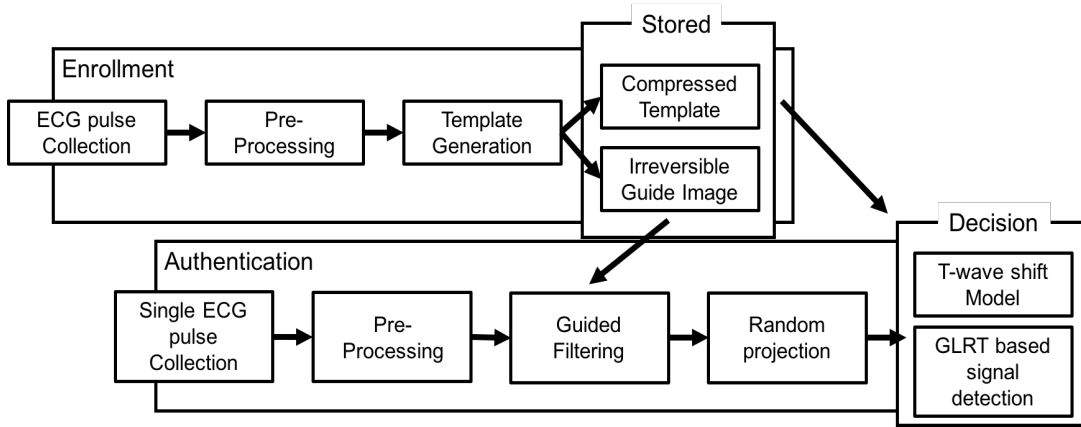


Figure 3.3: Schematic diagram for the summary of enrollment and authentication procedures.

3.2.4 Cancelability criteria evaluation

Cancelable biometrics methods should be evaluated in terms of different aspects. Here we investigated our proposed GLRT method (III.10) for cancelable ECG biometrics. to validate that the proposed method satisfies all cancelable biometrics criteria that we discussed in [11, 61, 74].

Efficiency Our proposed GLRT method is based on the CS theory and signal processing detection theory in CS measurement with appropriate random matrix H . Therefore, our detector will be effective in CS domain. In addition, two performance boost tricks in CS domain will help having efficient authentication. Simulation results will also support this aspect of our proposed methods.

Re-usability Our proposed method has straightforward revocation and reissue procedures. Once compromised, a new random matrix H will be generated and through the new enrollment step, new user template t will be obtained. Both H and Ht will be stored and re-used, but t will be discarded.

Diversity In two different applications, two random matrices H 's can be generated. However, the probability that these two random matrices are the same will be almost 0. For example, our simulation used a random matrix H with the size of 32×320 . Then, the probability that two random matrices are the same is $(1/2)^{32 \times 320} \approx 0$.

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 H if both H and Ht are available and the size of the compressive sensing measurement is large enough.

We conjecture that our GLRT detector in CS domain requires much smaller amount of samples than the CS recovery does for good reconstruction. We will extensively investigate this issue with simulations in Section 3.3.5 for the worst case (Considered as one of the strongest attack by the Simoens *et al.* [75]): compromised H and Ht .

Note that a random matrix H can be securely stored and used using hardwares such as smart card. If there is no H available, then our proposed scheme is simply non-invertible.

3.3 Simulation Results

We investigated our proposed methods of cancelable ECG biometrics detector using GLRT (III.10), performance boost tricks in CS domain such as user template GF (III.11), (III.12) and T wave shift model (III.17) with a few public ECG databases. MATLAB was used for all implementations (The Mathwork, Inc., MA, USA). Fig. 3.3 illustrates enrollment and authentication procedures of our proposed methods. All the details will be described in the following sub-sections.

3.3.1 Public ECG databases and data normalization

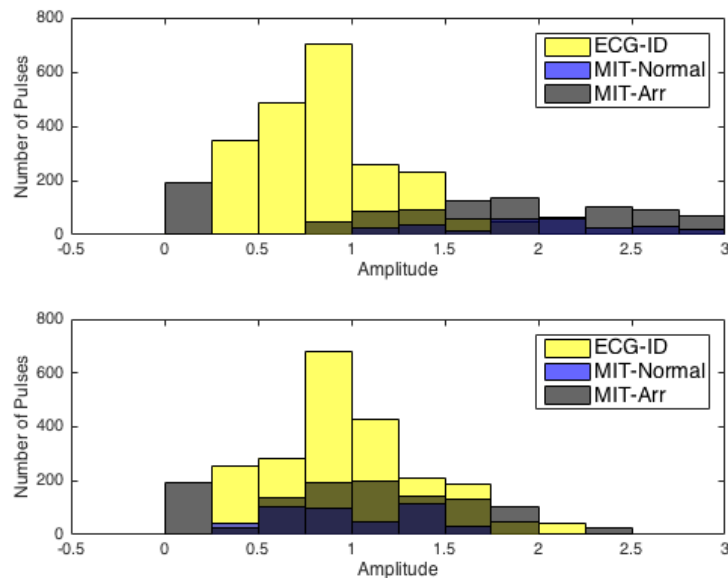


Figure 3.4: Data normalization across different ECG databases. Top and bottom figures show histograms of three public ECG databases for the amplitude of ECG signals before and after data normalization, respectively.

Three public ECG databases from the PhysioNet were combined and used in simulations [17] including subjects with normal heart condition as well as arrhythmia. The ECG-ID database consists of ECG data from 89 healthy subjects with recordings from the same or different days [18]. Each raw ECG record was acquired for about 20 seconds with the 500 Hz sampling rate, 12-bit resolution. The ECG-ID database provides pre-processed ECG signals for baseline draft, power-line noise, and high-frequency noise. The MIT-BIH Normal Sinus Rhythm database contains ECG data from 18 healthy subjects for about one day (24 hours) with 128 Hz sampling rate [16]. Five records were extracted per subject data. Lastly, ECG data from 40 subjects with arrhythmia in the MIT-BIH Arrhythmia database were used in our simulation. These consist of 48 half-hour excerpts of two-channel ambulatory with 360 Hz sampling rate, 11-bit resolution. Five records were extracted per subject data. ECG signals from both MIT-BIH Normal Sinus Rhythm and MIT-BIH Arrhythmia databases were resampled with 500 Hz sampling rate, which is the same as ECG signals in ECG-ID. Since three public ECG databases used different sensors with different sensitivity, all three databases were normalized according to their amplitude histograms as shown in Fig. 3.4. Before data normalization, amplitude histograms of different databases were not matched well, but after normalizing the maximum amplitude of each database, amplitude histograms were now matched approximately.

3.3.2 Data pre-processing

Two records per subject from three public ECG databases were used in our simulations. Each record was processed using Pan-Tompkins method for R-peak detection [76]. 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 projected samples are 32, 96, 160, respectively. We denote these cases as ‘compressed to 10%, 30%, 50%, respectively.

For irreversible guide signal generation, QRS complex part was extracted from from 0.218s to 0.342s among 0.64s for each ECG pulse. Then, other parts of the extracted QRS complex (0s - 0.218s, 0.342s - 0.64s) were padded with values to ensure the continuity of the resulting signal. Then, finally, a random number was chosen from [0.5, 0.8] and then was multiplied to the padded QRS complex to yield an irreversible guide signal.

For the performance evaluation, we adopt AUC, PD^1 and EER where AUC can be obtained by numerical integration of ROC curve, PD^1 is detection probability at FAR = 1%, ROC curve

is a plot of false alarm probability P_F or FAR vs. detection probability P_D , and EER is a point where $FRR = FAR =: EER$.

3.3.3 Proposed GLRT based cancelable ECG biometrics

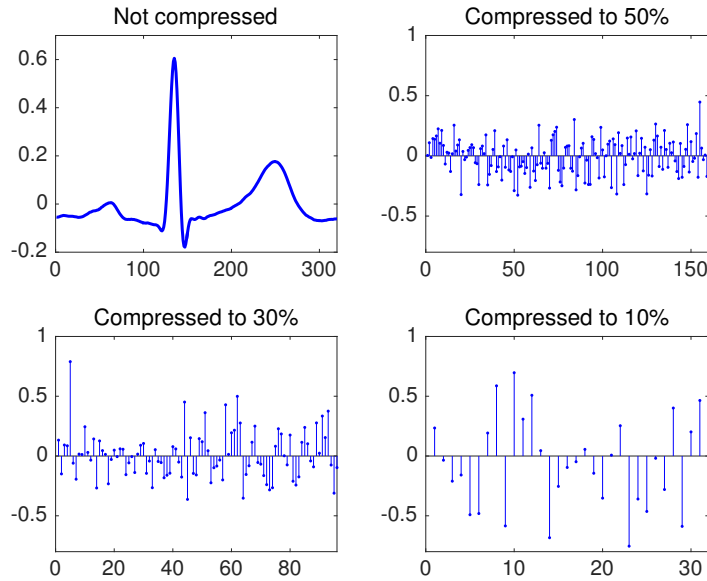


Figure 3.5: Examples of compressed samples from ECG signals with different compression ratio.

Fig. 3.5 illustrates examples of compressed samples from a ECG signal (shown in the top-left figure of Fig. 3.5) with different compression ratio. Other compressed signals in Fig. 3.5 did not shown any visually meaningful interpretation since they are randomly projected. Table 3.1 presents the results of authentication performance for Conventional, not projected (Euclidean distance in signal domain, baseline), Conventional, compressed to 10% (Euclidean distance in CS domain) and GLRT, compressed to 10% (proposed GLRT in CS domain). Note that the proposed GLRT with compressed to 10% yielded comparable results to the baseline. However, mild performance degradation was observed in cancelable biometrics methods. Proposed GLRT method yielded better PD^1 and EER than conventional method with the same measurement (compressed to 10%) even though performance gap was marginal.

3.3.4 Proposed performance boost tricks in CS domain

Table 3.2 summarizes the results of the two proposed performance boost tricks for GLRT based cancelable ECG biometrics. When using GF with user template guide signal, significant performance increase was observed in terms of all performance metrics over GLRT, compressed

Table 3.1: Performance summary for GLRT. Cancelable biometrics yielded comparable results to conventional ECG biometrics.

Method	PD ¹ (%)	AUC	EER (%)
Conventional, not projected	94.4	0.996	3.1
Conventional, compressed to 10 %	92.0	0.995	3.6
GLRT, compressed to 10 %	92.2	0.995	3.5

to 10%. Using GF enabled the proposed cancelable ECG biometrics method to yield better performance than baseline (Euclidean in signal domain). GF with irreversible guide signal yielded comparable performance to GF with original user template. T-wave model in CS domain yielded better EER than the original GLRT, but yielded worse PD^1 than that. Finally, using both tricks yielded significantly improved performance over GLRT, compressed to 10% as well as baseline in signal domain.

3.3.5 Cancelable biometrics: efficiency and non-invertibility

Tables 3.1 and 3.2 demonstrated that the proposed cancelable biometrics methods are efficient so that they satisfy one of the cancelable biometrics criteria since the authentication performance of them is comparable to or better than the baseline using user template.

For non-invertibility of cancelable biometrics criteria, firstly, CS recoveries from compressed ECG samples with different compression ratios were performed. Fig. 3.6 illustrates examples of recovered ECG signals from the compressed samples with 50%, 30% and 10%. For compressed to 50%, recovered ECG signal is visually similar to the original ECG pulse. For compressed to 30%, recovered signal still contains part of the shapes of the original signal. However, some details such as P wave, S wave are contaminated by artifacts. For compressed to 10%, almost no details were recovered. Therefore, with the compressed to 10% cancelable ECG samples, we were able to achieve good performance as shown in Tables 3.1 and 3.2, but we were not able to recover the original signal if the random matrix H and the secure user template Ht are given.

Table 3.2: Performance summary for performance boost tricks. Proposed tricks significantly improved authentication over baseline.

Method	PD ¹ (%)	AUC	EER (%)
GLRT, 10 %	92.2	0.995	3.5
GLRT, 10 %, GF	95.9	0.996	3.0
GLRT, 10 %, GF irreversible	96.1	0.996	2.9
GLRT, 10 %, T-wave	91.6	0.996	3.3
GLRT, 10 %, GF irreversible, T-wave	97.1	0.998	1.9

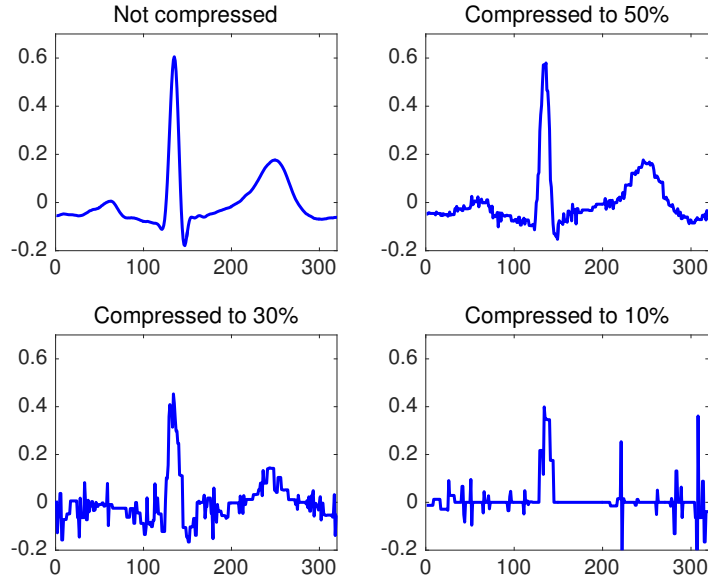


Figure 3.6: Examples of CS recovery results of ECG signals from samples with different compression ratios (50%, 30% and 10%).

We further simulated cases to examine that this recovered ECG data from compressed to 10% samples can be potentially used for authentication. One case is where an imposter stole the cancelable ECG template Ht with the random matrix H , recovered ECG signal using CS recovery, and then tried to intrude into the authentication system having the same random matrix H (called C1). The other case is almost the same as C1, but now the imposter tried to intrude into the system having different random matrix (H') that was re-generated after revocation and having a new secure user template (called C2). We also simulated a baseline case where the true user is using this new system with re-generated random matrix H' as well as re-issued secure template $H't$ (called P).

Fig. 3.7 shows plots of performance metrics (EER, PD^1) versus the number of compressed

Table 3.3: Performance table for non-invertibility evaluation

Compressed to	Cases	PD^1 (%)	AUC	EER (%)
10 %	P	93.5	0.996	2.8
	C1	19.1	0.863	22.0
	C2	17.7	0.880	20.6
30 %	P	95.7	0.997	2.1
	C1	74.9	0.985	6.3
	C2	54.0	0.965	10.4
50 %	P	96.2	0.997	2.0
	C1	92.7	0.996	2.6
	C2	91.2	0.996	3.0

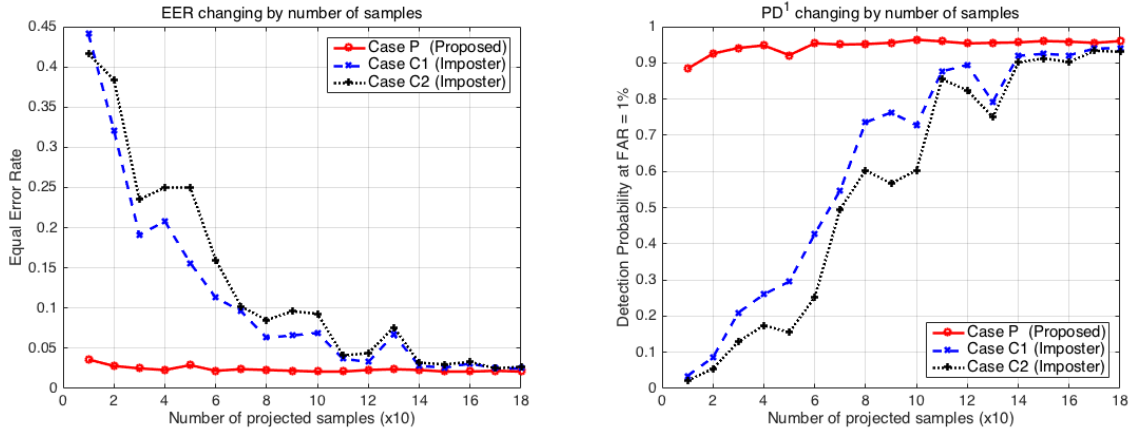


Figure 3.7: Performance plots of EER (top) and PD^1 (bottom) versus number of compressed samples. For imposter cases with small number of samples, low authentication performances were achieved.

samples. For very small number of compressed samples such as 10 or 20 samples, the proposed GLRT based detector yielded good performance. However, for more than 30% compression ratio, the imposters were able to achieve good authentication with recovered ECG signal from a random matrix as well as secure ECG template. Table 3.3 also shows quantitatively that the imposters with recovered signal from compressed to 10% secure template and random matrix was not able to achieve good authentication performance.

3.4 Discussion

In this article, we proposed cancelable ECG biometrics methods using composite hypothesis testing in CS domain. We showed that these proposed methods yielded comparable to or better than the baseline method of using original ECG user template with the small amount of samples (10% in simulations) that were not enough for recovering the original signal. The proposed detectors in CS domain seem to use samples more efficiently than detectors in signal domain using 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 cases were about 19.1 and 17.7 % for non-invertibility evaluation, the system can be protected well against these imposters using a scheme similar to ‘password lock’ that blocks an incoming user with several consecutive authentication fails. Therefore, the argument for non-invertibility of the proposed methods is still valid.

We also proposed two performance boost tricks that can be used in CS domain. Note that user template guided filtering for ECG biometrics has shown that GF was useful to improve the

performance of simple algorithms such as Euclidean metric or dynamic time warping (DTW), but was not improving performance for more sophisticated algorithms such as principle component (PCA) based authentication, which already is robust to noise [13]. We expect that the proposed tricks can be useful for the cases with limited access to others' ECG data or with limited computation power and memory (*e.g.*, low cost wearable band).

Having the irreversible guide signal for GF may potentially decrease the security level of cancelable biometrics. However, note that GF is not the only method to increase the security level of the system. For systems that require strong security level, one may consider using multimodal biometrics including our proposed ECG biometrics without GF. Locally different random scaling can potentially increase the security level of irreversible guide signal. Further studies may be interesting for this issue.

CHAPTER IV

Conclusion

In this study, we investigated an ability of combining ECG and MSP as a biometrics ingredients. By training Adaboost algorithm on each thresholds with 9 subjects of public data, outperform authentication results (which are 99.7% $PD^{0.1}$ and 0.2 % EER) was yielded with 63 subjects. Further investigation for the method of fusion will be performed in various way such as feature level or score level not only decision level fusion.

We proposed a cancelable ECG biometric using compressive sensing based composite hypothesis testing (GLRT) and investigated its cancelable biometrics properties. We further investigated a couple of tricks to compensate for performance degradation due to proposed cancelable biometric scheme. Our proposed method yielded up to 97.1% PD^1 and 1.9% EER with the integrated public ECG database with 147 subjects. As a future works, proposed method can be extended by investigation of cancelability of MSP biometrics and it further includes the fusion for cancelable multi-modal biometrics combined of ECG and MSP.

This study may contribute for development a powerful multi-modal biometrics based authentication for wearable devices, while they are computationally low cost, preventing the directing and indirecting spoofing, and potentially simple to implement.

References

- [1] A. K. Jain, A. Ross, and S. Pankanti, “Biometrics: a tool for information security,” *IEEE transactions on information forensics and security*, vol. 1, no. 2, pp. 125–143, 2006. [v, 2, 13](#)
- [2] Y. C. Jo, H. N. Kim, J. H. Kang, H. K. Hong, Y. S. Choi, S. W. Jung, and S. P. Kim, “Novel wearable-type biometric devices based on skin tissue optics with multispectral led–photodiode matrix,” *Japanese Journal of Applied Physics*, vol. 56, no. 4S, pp. 04CM01, 2017. [v, 6](#)
- [3] A. K. Jain, A. Ross, and S. Prabhakar, “An Introduction to Biometric Recognition,” *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4–20, Jan. 2004. [1](#)
- [4] “International Civil Aviation Organization (ICAO) Doc 9303 Machine Readable Travel Documents Part 1,” Accessed: 2016-04-20. [2](#)
- [5] A. Ross and A. K. Jain, “Multimodal biometrics: An overview,” in *Signal Processing Conference, 2004 12th European*. IEEE, 2004, pp. 1221–1224. [2](#)
- [6] S. Sarhan, S. Alhassan, and S. Elmougy, “Multimodal biometric systems: A comparative study,” *Arabian Journal for Science and Engineering*, vol. 42, no. 2, pp. 443–457, 2017. [2, 7](#)

REFERENCES

- [7] J. A. Unar, W. C. Seng, and A. Abbasi, “A review of biometric technology along with trends and prospects,” *Pattern recognition*, vol. 47, no. 8, pp. 2673–2688, 2014. [2](#)
- [8] E. J. Candès, J. Romberg, and T. Tao, “Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information,” *IEEE Transactions on information theory*, vol. 52, no. 2, pp. 489–509, 2006. [2](#), [14](#), [15](#)
- [9] J. Haupt and R. Nowak, “Compressive sampling for signal detection,” in *Acoustics, Speech and Signal Processing, 2007. ICASSP 2007. IEEE International Conference on*. IEEE, 2007, vol. 3, pp. III–1509. [2](#), [15](#)
- [10] M. A. Davenport, P. T. Boufounos, M. B. Wakin, and R. G. Baraniuk, “Signal processing with compressive measurements,” *IEEE Journal of Selected Topics in Signal Processing*, vol. 4, no. 2, pp. 445–460, 2010. [2](#), [15](#), [16](#)
- [11] R. Belguechi, E. Cherrier, A. M. El, and C. Rosenberger, “Evaluation of cancelable biometric systems: Application to finger-knuckle-prints,” in *Hand-Based Biometrics (ICHB), 2011 International Conference on*. IEEE, 2011, pp. 1–6. [3](#), [21](#)
- [12] C. M. Fira, L. Goras, C. Barabasa, and N. Cleju, “ECG compressed sensing based on classification in compressed space and specified dictionaries,” in *Signal Processing Conference, 2011 19th European*. IEEE, 2011, pp. 1573–1577. [3](#), [14](#)
- [13] S. Y. Chun, “Single pulse ECG-based small scale user authentication using guided filtering,” in *Biometrics (ICB), 2016 International Conference on*. IEEE, 2016, pp. 1–7. [3](#), [7](#), [18](#), [28](#)
- [14] 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 *Pattern Recognition (ICPR), 2016 23rd International Conference on*. IEEE, 2016, pp. 3043–3048. [3](#), [7](#), [19](#), [20](#)
- [15] 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 *Engineering in Medicine and Biology Society (EMBC), 2017 39th Annual International Conference of the IEEE*. IEEE, 2017, pp. 454–457. [3](#)
- [16] G. B. Moody and R. G. Mark, “The impact of the mit-bih arrhythmia database,” *IEEE Engineering in Medicine and Biology Magazine*, vol. 20, no. 3, pp. 45–50, 2001. [3](#), [23](#)
- [17] A. L. Goldberger, L. A. N. Amaral, L. Glass, J. M. Hausdorff, P. Ch. Ivanov, R. G. Mark, J. E. Mietus, C. K. Moody, G. B. Peng, H. E. Stanley, PhysioBank, PhysioToolkit, and

REFERENCES

- PhysioNet, “Components of a New Research Resource for Complex Physiologic Signals.,” *Circulation*, vol. 101, no. 23, pp. e215–e220, June 2000. [3](#), [23](#)
- [18] Lugovaya T. S., “Biometric human identification based on electrocardiogram,” M.S. thesis, Faculty of Computing Technologies and Informatics, Electrotechnical University ”LETI”, Saint-Petersburg, Russian Federation, June 2005. [3](#), [5](#), [23](#)
- [19] S. A. Israel, J. M. Irvine, A. Cheng, M. D. Wiederhold, and B. K. Wiederhold, “ECG to identify individuals,” *Pattern Recognition*, vol. 38, no. 1, pp. 133–142, Jan. 2005. [4](#)
- [20] J. M. Irvine, S. A. Israel, W. Todd S., and W. J. Worek, “eigenPulse: Robust human identification from cardiovascular function,” *Pattern Recognition*, vol. 41, no. 11, pp. 3427–3435, Nov. 2008. [4](#), [5](#)
- [21] F. Sufi, I. Khalil, and J. Hu, “ECG-Based Authentication,” in *Handbook of Information and Communication Security*, Peter Stavroulakis and Mark Stamp, Eds., pp. 309–331. Springer Berlin Heidelberg, 2010. [4](#)
- [22] W. Einthoven, “The Different Forms of the Human Electrocardiogram and Their Signification,” *The Lancet*, vol. 179, no. 4622, pp. 853–861, Mar. 1912. [4](#)
- [23] R. Hoekema, G. J. Uijen, and A. van Oosterom, “Geometrical aspects of the interindividual variability of multilead ECG recordings.,” *IEEE Transactions on Biomedical Engineering*, vol. 48, no. 5, pp. 551–559, May 2001. [4](#)
- [24] L. Biel, O. Pettersson, L. Philipson, and P. Wide, “ECG analysis: a new approach in human identification,” *IEEE Transactions on Instrumentation and Measurement*, vol. 50, no. 3, pp. 808–812, June 2001. [5](#)
- [25] M. Kyoso and A. Uchiyama, “Development of an ECG identification system,” in *Proceedings of the 23rd Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, Istanbul, 2001, pp. 3721–3723. [5](#)
- [26] Y. N. Singh and P. Gupta, “Biometrics Method for Human Identification Using Electrocardiogram,” in *International Conference on Biometrics*, M Tistarelli and M S Nixon, Eds., 2009, pp. 1270–1279. [5](#)
- [27] B. Vuksanovic and M. Alhamdi, “Analysis of Human Electrocardiogram for Biometric Recognition Using Analytic and AR Modeling Extracted Parameters,” *International Journal of Biometrics and Bioinformatics*, vol. 9-42, no. 3, pp. 25–25, 2015. [5](#)

REFERENCES

-
- [28] R. J. Martis, C. Chakraborty, and A. K. Ray, “Wavelet-based Machine Learning Techniques for ECG Signal Analysis,” in *Machine Learning in Healthcare Informatics*, pp. 25–45. Springer Berlin Heidelberg, Dec. 2013. [5](#)
 - [29] T. W. Shen, W. J. Tompkins, and Y. H. Hu, “One-lead ECG for identity verification,” in *Proceedings of the 2nd Joint EMBS/BMES Conference*. 2002, pp. 62–63, IEEE. [5](#)
 - [30] N. Venkatesh and S. Jayaraman, “Human electrocardiogram for biometrics using DTW and FLDA,” in *20th International Conference on Pattern Recognition (ICPR)*, Aug 2010, pp. 3838–3841. [5](#)
 - [31] P. Sung, Z. Syed, and J. Guttag, “Quantifying morphology changes in time series data with skew,” in *Proceedings of the 2009 IEEE International Conference on Acoustics, Speech and Signal Processing*, Taipei, Mar. 2009, pp. 477–480. [5](#)
 - [32] C. C. Chiu, C. M. Chuang, and C. Y. Hsu, “A Novel Personal Identity Verification Approach Using a Discrete Wavelet Transform of the ECG Signal,” in *Proceedings of International Conference on Multimedia and Ubiquitous Engineering*, 2008, pp. 201–206. [5](#)
 - [33] G. Wübbeler, M. Stavridis, Di. Kreiseler, R. D. Bousseljot, and C. Elster, “Verification of humans using the electrocardiogram,” *Pattern Recognition Letters*, vol. 28, no. 10, pp. 1172–1175, July 2007. [5](#)
 - [34] I. Odinaka, P. H. Lai, A. D. Kaplan, J. A. O’Sullivan, E. J. Sirevaag, and J. W. Rohrbaugh, “ECG Biometric Recognition: A Comparative Analysis,” *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 6, pp. 1812–1824, Nov. 2012. [5](#), [6](#)
 - [35] M. Merone, P. Soda, M. Sansone, and C. Sansone, “ECG databases for biometric systems: A systematic review,” *Expert Systems with Applications*, vol. 67, pp. 189–202, 2017. [5](#)
 - [36] E. Nemati, M. J. Deen, and T. Mondal, “A wireless wearable ECG sensor for long-term applications,” in *IEEE Communications Magazine*. McMaster University, Hamilton, Canada, Jan. 2012, pp. 36–43. [5](#)
 - [37] 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, pp. e84018–18, Jan. 2014. [5](#)
 - [38] 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 Processing Letters*, vol. 23, no. 6, pp. 805–808, 2016. [5](#)

REFERENCES

-
- [39] S. Yin, Y. Ma, Y. Liu, C. Bae, S. Kim, J. He, Y. Cao, and J. Seo, “Low-Power ECG Biometric Authentication for Wearable Systems Featuring Sparse Memory Compression,” in *On-Device Intelligence Workshop at ICML International Conference on Machine Learning*, June 2016. [5](#)
- [40] 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 *2016 39th International Conference on Telecommunications and Signal Processing, TSP 2016*. Ulsan National Institute of Science and Technology, Ulsan, South Korea, 2016, pp. 656–659, IEEE. [5](#)
- [41] Y. N. Singh, S. K. Singh, and P. Gupta, “Fusion of electrocardiogram with unobtrusive biometrics: An efficient individual authentication system,” *Pattern Recognition Letters*, vol. 33, no. 14, pp. 1932–1941, 2012. [5](#)
- [42] M. D. Bugdol and A. W. Mitas, “Multimodal biometric system combining ECG and sound signals,” *Pattern Recognition Letters*, vol. 38, pp. 107–112, 2014. [5](#)
- [43] S. Zokaei and K. Faez, “Human identification based on ECG and palmprint,” *International Journal of Electrical and Computer Engineering*, vol. 2, no. 2, pp. 261, 2012. [5](#)
- [44] S. Luo and P. Johnston, “A review of electrocardiogram filtering,” *Journal of electrocardiology*, vol. 43, no. 6, pp. 486–496, 2010. [5](#)
- [45] Robert S Boyer and J Strother Moore, “Mjrtj—a fast majority vote algorithm,” pp. 105–117, 1991. [7](#), [8](#)
- [46] Laurent Alonso and Edward M Reingold, “Analysis of boyer and moores mjrtj algorithm,” *Information Processing Letters*, vol. 113, no. 13, pp. 495–497, 2013. [7](#), [8](#)
- [47] Jerome Friedman, Trevor Hastie, and Robert Tibshirani, *The elements of statistical learning*, vol. 1, Springer series in statistics New York, 2001. [7](#), [8](#)
- [48] Vassilios Chatzis, Adrian G Bors, and Ioannis Pitas, “Multimodal decision-level fusion for person authentication,” *IEEE transactions on systems, man, and cybernetics-part a: systems and humans*, vol. 29, no. 6, pp. 674–680, 1999. [7](#)
- [49] Jiapu Pan and Willis J Tompkins, “A real-time qrs detection algorithm,” *IEEE transactions on biomedical engineering*, , no. 3, pp. 230–236, 1985. [9](#)
- [50] R. M. Bolle, J. H. Connell, and N. K. Ratha, “Biometric perils and patches,” *Pattern Recognition*, vol. 35, no. 12, pp. 2727–2738, 2002. [13](#)

REFERENCES

- [51] D. Maltoni, D. Maio, A. Jain, and S. Prabhakar, *Handbook of fingerprint recognition*, Springer Science & Business Media, 2009. [13](#)
- [52] A. B. Teoh, A. Goh, and D. C. L. Ngo, “Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 28, no. 12, pp. 1892–1901, 2006. [13](#), [14](#)
- [53] J. Ratha, N. and Connell, R. M. Bolle, and S. Chikkerur, “Cancelable Biometrics: A Case Study in Fingerprints,” vol. 4, pp. 370–373, 2006. [14](#)
- [54] A. Othman and A. Ross, “On mixing fingerprints,” *IEEE Transactions on Information Forensics and security*, vol. 8, no. 1, pp. 260–267, 2013. [14](#)
- [55] A. B. J. Teoh and C. T. Yuang, “Cancelable Biometrics Realization With Multispace Random Projections,” *IEEE Transactions on Systems, Man and Cybernetics, Part B (Cybernetics)*, vol. 37, no. 5, pp. 1096–1106, Sept. 2007. [14](#)
- [56] A. B. J. Teoh, Y. W. Kuan, and S. Lee, “Cancellable biometrics and annotations on BioHash,” *Pattern Recognition*, vol. 41, no. 6, pp. 2034–2044, June 2008. [14](#)
- [57] J. K. Pillai, V. M. Patel, R. Chellappa, and N. K. Ratha, “Secure and robust iris recognition using random projections and sparse representations,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 33, no. 9, pp. 1877–1893, Sept. 2011. [14](#)
- [58] A. M. P. Canuto, F. Pintro, and J. C. Xavier-Junior, “Investigating fusion approaches in multi-biometric cancellable recognition,” *Expert Systems with Applications*, vol. 40, no. 6, pp. 1971–1980, 2013. [14](#)
- [59] H. Kaur and P. Khanna, “Biometric template protection using cancelable biometrics and visual cryptography techniques,” *Multimedia Tools and Applications*, vol. 75, no. 23, pp. 16333–16361, 2016. [14](#)
- [60] W. B. Johnson and J. Lindenstrauss, “Extensions of lipschitz mappings into a hilbert space,” *Contemporary mathematics*, vol. 26, no. 189-206, pp. 1, 1984. [14](#)
- [61] A. B. J. Teoh and C. T. Yuang, “Cancelable biometrics realization with multispace random projections,” *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol. 37, no. 5, pp. 1096–1106, 2007. [14](#), [21](#)
- [62] C. Rathgeb and A. Uhl, “A survey on biometric cryptosystems and cancelable biometrics,” *EURASIP Journal on Information Security*, vol. 2011, no. 1, pp. 3, 2011. [14](#)

REFERENCES

- [63] M. Gomez-Barrero, E. Maiorana, J. Galbally, P. Campisi, and J. Fierrez, “Multi-biometric template protection based on homomorphic encryption,” *Pattern Recognition*, vol. 67, pp. 149–163, 2017. [14](#)
- [64] V. M. Patel, N. K. Ratha, and R. Chellappa, “Cancelable biometrics: A review,” *IEEE Signal Processing Magazine*, vol. 32, no. 5, pp. 54–65, 2015. [14](#)
- [65] M. Dey, N. Dey, S. K. Mahata, S. Chakraborty, S. Acharjee, and A. Das, “Electrocardiogram Feature based Inter-human Biometric Authentication System,” vol. 2014, pp. 300–304, 2014. [14](#)
- [66] C. Camara, P. Peris-Lopez, and J. E. Tapiador, “Human identification using compressed ECG signals,” *Journal of medical systems*, vol. 39, no. 11, pp. 1–10, 2015. [14](#)
- [67] D. Craven, B. McGinley, L. Kilmartin, and E. Glavin, M.and Jones, “Adaptive dictionary reconstruction for compressed sensing of ECG signals,” *IEEE journal of biomedical and health informatics*, vol. 21, no. 3, pp. 645–654, 2017. [14](#)
- [68] S. L. Parkale, Y. V .and Nalbalwar, “Application of compressed sensing (CS) for ECG signal compression: A review,” in *Proceedings of the International Conference on Data Engineering and Communication Technology*. Springer, 2017, pp. 53–65. [14](#)
- [69] C. Rathgeb and A. Uhl, “A survey on biometric cryptosystems and cancelable biometrics,” *EURASIP Journal on Information Security*, vol. 2011, no. 1, pp. 1–25, 2011. [14](#), [18](#)
- [70] S. Rane, Y. Wang, S. C. Draper, and P. Ishwar, “Secure biometrics: concepts, authentication architectures, and challenges,” *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 51–64, 2013. [14](#), [18](#)
- [71] E. J. Candès and M. B. Wakin, “An introduction to compressive sampling,” *IEEE signal processing magazine*, vol. 25, no. 2, pp. 21–30, 2008. [15](#)
- [72] D. L. Donoho, “Compressed sensing,” *IEEE Transactions on information theory*, vol. 52, no. 4, pp. 1289–1306, 2006. [15](#)
- [73] K. He, J. Sun, and X. Tang, “Guided image filtering,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 35, no. 6, pp. 1397–1409, June 2013. [18](#)
- [74] A. K. Jain, K. Nandakumar, and A. Nagar, “Biometric template security,” *EURASIP Journal on advances in signal processing*, vol. 2008, pp. 113, 2008. [21](#)

REFERENCES

- [75] K. Simoens, J. Bringer, H. Chabanne, and S. Seys, “A framework for analyzing template security and privacy in biometric authentication systems,” *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 833–841, 2012. [22](#)
- [76] J. Pan and W. J. Tompkins, “A real-time QRS detection algorithm,” *IEEE Transactions on Biomedical Engineering*, vol. 32, no. 3, pp. 230–236, Mar. 1985. [23](#)