Tampering Attack Detection in Analog to Feature Converter for Wearable Biosensor

Xiaochen Tang, Shanshan Liu, Wenjie Che and Wei Tang
Klipsch School of Electrical and Computer Engineering
New Mexico State University
Las Cruces, NM, USA
{hypnus, ssliu, wche, wtang}@nmsu.edu

2022 IEEE International Symposium on Circuits and Systems (ISCAS) | 978-1-6654-8485-5/22/$31.00 ©2022 IEEE | DOI: 10.1109/ISCAS48785.2022.9937707

***Abstract*—Wearable biosensors have been widely used to assist disease diagnosis or monitor health conditions, making the authorization to communicate with these biosensors very critical. The potential tampering attack may cause disasters that threaten human lives. In this paper, a tampering attack detection method is proposed for securing key parameters of a real-time ECG monitoring system. The detection method is based on a built-in triangle waveform and the corresponding extracted abnormal pattern vector examination. When the deviation of the pattern vector is above the defined attack detection threshold value, we could recognize that an attack occurs. Two representative records of ECG data are used to evaluate the different attack levels impact. The proposed tampering attack detection framework is implemented using 0.18 μm standard CMOS process and costs 41413 μm^2 chip area, with an estimated dynamic power consumption of 15 nW, which is very hardware-efficient and easy to be implemented.**

***Index Terms*—Biosensor, Electrocardiogram, Tampering attack, pattern vector examination**

I. Introduction

Wearable biosensors have been playing critical roles in monitoring human health conditions and diagnosing several types of diseases [1]. Cardiovascular disease (CVD), as the leading factor of death worldwide recognized by WHO [2], could also benefit from wearable biosensors. Real-time abnormal heartbeat rhythm detection and pre-diagnosis can lead to in-time treatment, which prevents high occupation of medical resources and long waiting time of patients. Such wearable biosensors usually grant access to adjusting key parameters of sensors to doctors or skilled technicians responsible for analyzing the ECG data, so that they can obtain detailed information of patients. However, this results in a potential backdoor that may be hacked to result in a malfunction in sensors to make them transmit false data. This attack may lead to accidents that miss important heartbeats information, thus missing the best timing window for treatment. In other cases, a healthy person may be diagnosed with a critical condition, thus wasting lots of medical resources. According to the American Heart Association report [3], the direct and indirect expenditures on CVD have reached $363.4 billion in the United States in 2016-2017.

The smarter and advanced medical devices/systems with more complex software and hardware components expose a broader attack surface for malicious attacks [4]. A rising number of security issues on medical devices have been reported in recent years. Researchers demonstrated cyber-attacks on commercial implantable medical devices (IMDs) where an implantable cardiac defibrillator (ICD) can be remotely disabled and reprogrammed with new therapies [5]. Moreover, medical devices have been shown vulnerable to eavesdropping attacks through the communication media [6] (Wi-Fi, Bluetooth, Zigbee, etc.) where adversaries can access the transmitted data [5]. Different security solutions have been proposed as countermeasures to malicious attacks, e.g., by limiting the range of communications via body-coupled communication protocols [7], using cryptographic authentications [8] or biometric-based authentications derived from the measured medical signal itself [9], or by introducing physical layer security along with cryptographic authentications [10], [11]. In this paper, we proposed a tampering detection mechanism to defend against malicious manipulations on the key parameters of a real-time ECG monitoring system.

We previously proposed a low-power real-time Arrhythmia detection system [12], [13] based on Delta Modulator circuits [14] and bit-stream signal processing algorithms [15]. In the proposed system, the threshold of DM2 as the key parameters is opened to specific terminals. Doctors can adjust the threshold remotely to check the details of ECG signals to obtain the information they need or improve the heartbeats detection accuracy. However, tampering attacks on the threshold may lead to severe issues, including detection failure of important fiducial points, adding false fiducial points due to noise, or completely messing up the bit-streams (output of DM2). All problems result in missing critical information. In this paper, we propose a tampering attack detection framework, which reuses several blocks of existing circuits to achieve hardware efficient design. The paper is organized as follows: Section II describes the DM2 based AFC and the system for real-time Arrhythmia classification. Section III presents the tampering attack model and our proposed method for detecting the attack. Section IV provides the evaluation of the performance of the proposed method. Finally, Section VI concludes the paper.

II. Circuits and Systems

As shown in Fig. 1, we propose an on-sensor Arrhythmia recognition system, which includes a parallel DM2 based AFC

This work was supported by the National Science Foundation Grants ECCS-1652944 and ECCS-2015573

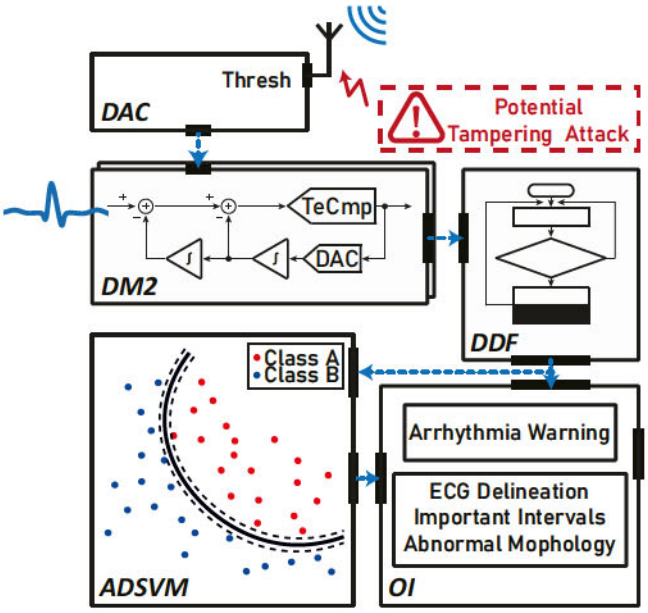

Fig. 1: The proposed wearable heartbeat monitor system includes the second-order Delta Modulator (DM2), ECG delineation algorithms (DDF), patient-dependant SVM classifier for arrhythmia recognition (ADSVM), and output interface (OI) for reporting warnings and fiducial points.

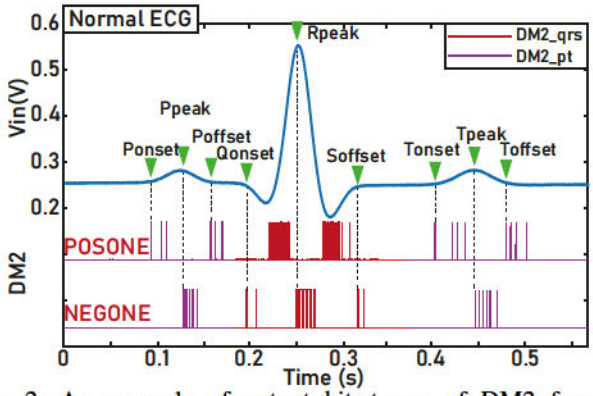

Fig. 2: An example of output bit-stream of DM2 from a conversion of a normal ECG signal, and the fiducial points detected from the corresponding delineation algorithm.

(DM2) [16], the corresponding heartbeats detection and ECG signal delineation algorithm implementation (DDF), and an Arrhythmia detection algorithm realized by a patient dependent rotated linear kernel SVM classifier (ADSVM) [17]. The system can report Arrhythmia detection results that include classifying Supraventricular ectopic beats (SVEB), Ventricular ectopic beats (VEB), and normal heartbeats through the output interface (OI). It can also report important ECG signal delineation information, including essential intervals (PR/RR/QT interval, ST segment, QRS duration), and abnormal morphology of P/T waves and QRS complexes.

The DM2 we reported previously in [16] is controlled by a non-overlap clock. In DM2, the two-stage switch-capacitor-based discrete-time integrators generate the feedback. The feedback is subtracted by input to compute the residue voltage. Then, through a ternary comparator (TeCmp), the residue voltage is compared with a threshold voltage pair. Threshold, as the key parameter, is introduced by a digital to analog converter (DAC). Thus, the output bit of the current clock can be generated. DM2 converts the analog input signal to digital bit-streams, in which the pulse density is proportional to the slope variation of the input. An example of the conversion with a standard ECG waveform input is shown in Fig. 2. At large slope varying points like Q/R/S wave peaks, pulses in the output bit-stream of DM2 are more intensive, and vice versa.

DDF delineates the ECG signal from the output bit-stream of DM2. It detects the QRS complexes first and searches back in the data cache to locate the P wave. Meantime, DDF keeps monitoring the T wave. With the corresponding ECG delineation algorithm, we can extract the timing information of these fiducial points. Thus, the feature vector for ADSVM to recognize Arrhythmia could be generated. An example of the delineation result could also be found in Fig. 2. The results show that the DM2 can detect all important fiducial points within the ECG signal. There are 22 features extracted from the DM2 in total. Most of the features are timing information from the delineation of the fiducial points and essential intervals. The previously proposed classifier [17] costs very low hardware overhead, making it suitable for low-power biosensor applications. The classifier is achieved as follows: (1) Training the global classifier using a public Arrhythmia database; (2) Training the local classifier using a certain amount of heartbeats from the patient; (3) Finding the intersection hyperplane between global and local classifier; (4) Rotating the global classifier to local classifier by a certain angle, though the intersection hyperplane. The proposed method aims at balancing the generalization performance and specificity.

The outputs of DM2 can be affected by tuning the threshold introduced by DAC through commands received wirelessly from a remote station. The permission to adjust this threshold value is left for doctors or skilled technicians. With different parameter values, DM2 could be sensitive to different levels of slope variation. Therefore, doctors can obtain more detailed information of the fiducial points they care for, and it is also why we used paralleled DM2 in the proposed system. $DM2_{qrs}$ is designed with a threshold value that only reacts to significant slope variations like QRS complexes, which are not easily contaminated by noise. On the other hand, $DM2_{pt}$ is designed to be sensitive to small waves but may confront saturation conditions. By optimizing the threshold values, we can achieve the timing error under 3 ms for detecting a turning point of the input signal.

III. Attack Model and The Proposed Frame work

A. Threat Model

As stated above, the sensitivity level of DM2 to different slope variations can be adjusted by remotely tuning the threshold in the DAC module. Such fine-tuning capability, initially designed for doctors' convenience of improving measurement accuracy, unfortunately, could be leveraged by adversaries for

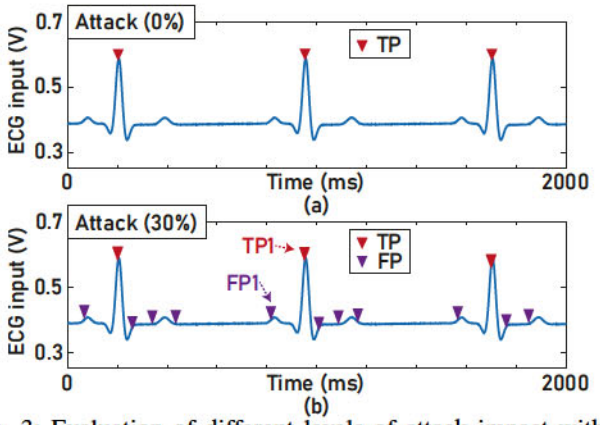

Fig. 3: Evaluation of different levels of attack impact with a standard ECG waveform input. Heartbeats detection with (a) no attack (Thresh as shown in Fig. 1 is set to 10 mV wirelessly by default, thus the DM2 has 500±10 mV threshold pair from the DAC), and (b) attack of threshold changing 30%.

malicious purposes. We have the following assumptions in our threat model: (1) adversary's goal is to mislead the recognition system to make false/inaccurate detection by attacking the analog-to-feature conversions module; (2) adversary's capability is that the attacker has the access to the threshold adjustment of DM2 to deviate it from its appropriate setting for inaccurate measurements. Specifically, we consider attack scenarios where adversaries can tune the threshold by deviating from appropriate settings in the form of adding a DC voltage bias. The attack could result in the removal/addition of important fiducial points or undesirable noise, further causing false detection by the recognition system.

An example of evaluating attack influence on detecting heartbeats through the above-mentioned system is shown in Fig. 3. It can be found that with a tampering attack on changing the threshold value by 20%, false positive (FP) beats appears. FP beats may influence the true positive (TP) detection accuracy. Because the ECG detection algorithm does not allow heartbeats detection within a very short time window, in Fig. 3 (d), the appearance of FP1 may eliminate the opportunity of expected detection of TP1. FP beats result in severe heartbeats detection accuracy decreasing and degrading the performance of the fiducial points delineation, feature extraction, and arrhythmia classification.

B. Proposed Tampering Detection Framework

Due to the potential attack targeting on the control of the DAC, which results in threshold variation and may malfunction the whole system, it is required to have a mechanism to form protection. We propose an attack detection framework that is capable to capture "abnormal" patterns in such malicious threshold adjustments. The proposed framework is designed to report an alarm if anomalies are detected so that either the patient or the doctor is alerted about the potential attack. In cases where the doctor is conducting a benign threshold adjustment, the patient (user of the device) will receive a prior notification about the upcoming adjustment so that the generated alert can be properly treated/ignored.

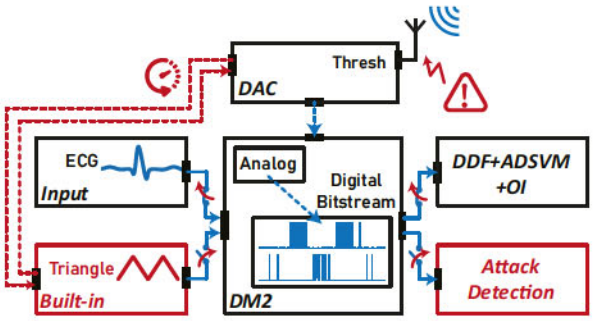

Fig. 4: The proposed attack detection framework, including the normal functional mode (NFM, black blocks) and attack examination mode (EM, red blocks).

A high-level overview of the proposed detection framework is illustrated in Fig. 4. Compared to the original system, the framework introduces two major components for tampering detection, i.e., a build-in triangle wave (BITrW) generator (with the help of the existing DAC, and with internal safe control) and an attack detection module (marked as red blocks in Fig. 4). The framework provides two modes that can be interchanged using a switch controlling the connection of the triangle generator. In the normal functional mode (NFM), the triangle generator is disconnected/disabled so that only the ECG input is fed into the AFC module. The DM2 output bit-stream is connected to the original DDF+ADSVM+OI modules for Arrhythmia recognition. In the examination mode (EM), the BITrW generator is enabled so that the triangle signal becomes the input signal instead, and the corresponding output bit-stream is connected to the attack detection module for attack detection. After the AFC conversion process, malicious threshold adjustment will be exposed and present as explicit abnormal patterns in the output bit-stream which is to be detected by the attack detection module.

Fig. 5 shows the output bit-stream converted from the built-in triangle waveform through DM2 (for saving space, DM2's output is represented in one ternary bit-stream instead of the actual two-channel pulses as shown in Fig. 2), and the corresponding output with different attack levels in the form of different DC bias. In this work, we mainly focus on a typical attack scenario where the malicious adjusting behaves in the form of a DC bias. It is shown that the number of pulses in DM2's output varies significantly associated with the change of threshold value. An 800 ms BITrW (with peak-to-peak amplitude of 0.2 V, and period of 200 ms) is used as the input. The middle 600 ms data is used for generating the detection data pattern, while the first 100 ms data is used to make the DM2 conversion stable. The 600 ms data includes six turning points, and the slope varies most at these points. The data is divided into twelve windows as shown in Fig. 5 (a). Within each window like w2, we count the number of '+1' bits and '-1' bits, respectively. Thus, a 24-dimension vector for standard threshold (NThVc) can be generated, i.e., the vector extracted from the attack-free bit-stream as shown in Fig. 5 (b). The NThVc data is stored on the sensor. Thus, we regularly switch the system from NFM to EM with the defined time setting

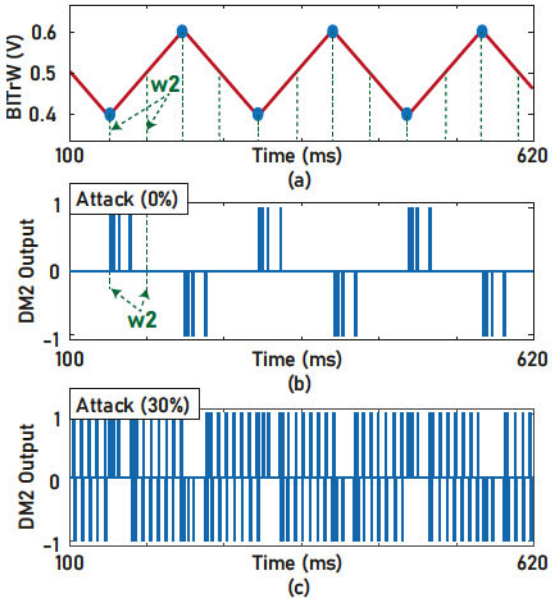

Fig. 5: Abnormal patterns check vector extraction for the built-in Triangle waveform based attack examination. (a) The middle 600 ms data of the built-in triangle waveform, (b) standard threshold vector extraction, and (c) abnormal pattern check vector extraction at attack level at 30%.

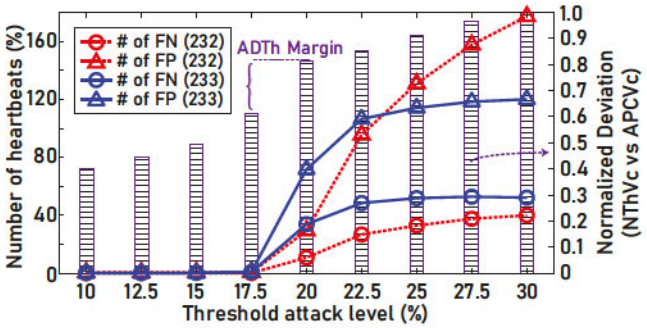

Fig. 6: The number of False positive and false negative heartbeats detected with different threshold attack levels in evaluating two representative records in MIT-BIH arrhythmia database.

and compute the abnormal patterns check vector (PCVc). Then, the PCVc and stored NThVc is compared to find if the system is under attack or not. The detection circuit is internally integrated with the DM2-based AFC circuit. Therefore, it is designed to be resilient to any physical removing/tampering attacks.

IV. Performance Evaluation

Two representative records data (232 includes VEB detection and 233 includes SVEB detection) in the MIT-BIH Arrhythmia Database are used to evaluate the attack effectiveness. With simulation of the two records data, the attack detection threshold (ADTh) is obtained. Then, ADTh is used to decide if the system is under attack. As shown in Fig. 6, the performance of the system in heartbeats detection drops dramatically when the attack level reaches 20%. The system

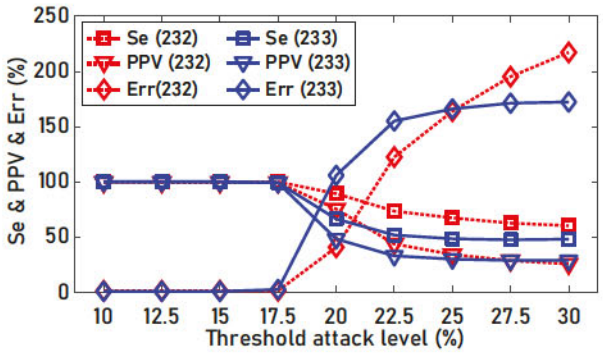

Fig. 7: Sensitivity and positive prediction value affected with different threshold attack levels in evaluating two representative records in MIT-BIH arrhythmia database.

becomes malfunctions ultimately when the attack level reaches 30%. The trends of FP and false negative (FN) beats curves associated with increasing attack levels are similar. Sensitivity, positive prediction value, and error rate are also used to evaluate the performance change as shown in Fig. 7, where the curves of the two records also show similar trends.

According to the evaluation results shown in Fig. 6 and Fig. 7, we define deviation between NThVc and PCVc at the attack level of 20% as the ADTh. The deviation is calculated by the summation elements of the absolute value of PCVc-NThVc. As shown in Fig. 6, the deviation between attack levels 17.5% and 20% is defined as the ADTh Margin, which shows no attack impact on heartbeats detection. If the deviation is over ADTh, we declare there is an attack. Detected deviation within ADTh Margin represents that there is a potential attack so that another examination is needed to confirm if it is an attack. Since we can calculate the ADTh by counting the difference of the number of pulses in all windows, the proposed attack detection method is very hardware-efficient.

To evaluate the compatibility with the ECG sensor chip [16], the framework is implemented using the same technology, the 0.18 μm standard CMOS process. The chip area (41413 μm^2) is obtained using Synopsys Design Compiler, with an estimated dynamic power consumption of 15 nW with the working clock of the sensor (1K Hz), and the estimated leakage power of 158 nW. The proposed tampering attack detection framework shows great potential for future low-power wearable biosensor applications.

V. Conclusion

In this paper, we presented a tampering attack examination mechanism for a previously proposed real-time wearable ECG monitoring sensor. By checking the 24-dimension abnormal pattern vector, we can detect if the system is under attack. The abnormal pattern vector is generated from the existing circuit with a built-in triangle waveform as input. The proposed method is validated with two records data from the MIT-BIH arrhythmia database. Thus, the attack detection threshold value is defined by evaluating the attack effectiveness at different levels. The proposed attack detection method is highly hardware friendly to be implemented. The methodology can be extended to other future biosensors for hardware security.

REFERENCES

[1] A. Pantelopoulos and N. G. Bourbakis, "A survey on wearable sensor-based systems for health monitoring and prognosis," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 40, no. 1, pp. 1–12, 2009.

[2] "New initiative launched to tackle cardiovascular disease, the world's number one killer." [Online]. Available: $http://www.who.int/cardiovascular_diseases/en/$

[3] S. S. Virani, A. Alonso, H. J. Aparicio, E. J. Benjamin, M. S. Bittencourt, C. W. Callaway, A. P. Carson, A. M. Chamberlain, S. Cheng, F. N. Delling *et al.*, "Heart disease and stroke statistics-2021 update: a report from the american heart association," *Circulation*, vol. 143, no. 8, pp. e254–e743, 2021.

[4] A. I. Newaz, A. K. Sikder, M. A. Rahman, and A. S. Uluagac, "A survey on security and privacy issues in modern healthcare systems: Attacks and defenses," *ACM Transactions on Computing for Healthcare*, vol. 2, no. 3, pp. 1–44, 2021.

[5] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in *2008 IEEE Symposium on Security and Privacy (sp 2008)*. IEEE, 2008, pp. 129–142.

[6] D. Benessa, M. Salajegheh, K. Fu, and S. Inoue, "Protecting global medical telemetry infrastructure," Tech. Rep.). Hanover, NH: Institute of Information Infrastructure Protection, Tech. Rep., 2008.

[7] W. J. Tomlinson, S. Banou, S. Blechinger-Slocum, C. Yu, and K. R. Chowdhury, "Body-guided galvanic coupling communication for secure biometric data," *IEEE Transactions on Wireless Communications*, vol. 18, no. 8, pp. 4143–4156, 2019.

[8] M. Alioto, "Trends in hardware security: From basics to asics," *IEEE Solid-State Circuits Magazine*, vol. 11, no. 3, pp. 56–74, 2019.

[9] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, "They can hear your heartbeats: Non-invasive security for implantable medical devices," in *Proceedings of the ACM SIGCOMM 2011 conference*, 2011, pp. 2–13.

[10] S. Maji, U. Banerjee, S. H. Fuller, M. R. Abdelhamid, P. M. Nadeau, R. T. Yazicigil, and A. P. Chandrakasan, "A low-power dual-factor authentication unit for secure implantable devices," in *2020 IEEE Custom Integrated Circuits Conference (CICC)*. IEEE, 2020, pp. 1–4.

[11] R. T. Yazicigil, P. M. Nadeau, D. D. Richman, C. Juvekar, S. Maji, U. Banerjee, S. H. Fuller, M. R. Abdelhamid, N. Desai, M. I. Ibrahim *et al.*, "Beyond crypto: Physical-layer security for internet of things devices," *IEEE Solid-State Circuits Magazine*, vol. 12, no. 4, pp. 66–78, 2020.

[12] X. Tang and W. Tang, "An ECG Delineation and Arrhythmia Classification System using Slope Variation Measurement by Ternary Second Order Delta Modulators for Wearable ECG Sensors," *IEEE Transactions on Biomedical Circuits and Systems*, vol. Early Access, pp. 1–14, 2021.

[13] X. Tang, Q. Hu, and W. Tang, "A Real-Time QRS Detection System With PR/RT Interval and ST Segment Measurements for Wearable ECG Sensors Using Parallel Delta Modulators," *IEEE Transactions on Biomedical Circuits and Systems*, vol. 12, no. 4, pp. 751–761, 2018.

[14] W. Tang and E. Culurciello, "A pulse-based amplifier and data converter for bio-potentials," in *2009 IEEE International Symposium on Circuits and Systems (ISCAS)*, 2009, pp. 337–340.

[15] Y. Liu, P. M. Furth, and W. Tang, "Hardware-efficient delta sigma-based digital signal processing circuits for the internet-of-things," *Journal of Low Power Electronics and Applications*, vol. 5, no. 4, p. 234, 2015. [Online]. Available: http://www.mdpi.com/2079-9268/5/4/234

[16] X. Tang and W. Tang, "A 151nW Second-Order Ternary Delta Modulator for ECG Slope Variation Measurement with Baseline Wandering Resilience," in *2020 IEEE Custom Integrated Circuits Conference (CICC)*. IEEE, 2020, pp. 1–4.

[17] X. Tang, Z. Ma, Q. Hu, and W. Tang, "A Real-time Arrhythmia Heartbeats Classification Algorithm using Parallel Delta Modulations and Rotated Linear-kernel Support Vector Machines," *IEEE Transactions on Biomedical Engineering*, vol. 67, no. 4, pp. 978–986, 2019.