HEARTID™ WHITE PAPER

07.27.2015

This document provides the reader with an overview of the Nymi Band’s proprietary biometric process: HeartID™.

HeartID can validate a user’s identity based on ECG sampling, and subsequently authenticate them in a secure and continuous manner.

Contents

The HeartID Technology

ECG Recognition

INTRODUCTION

A biometric is defined as a behavioural or physiological characteristic that is used to recognize a person's identity. In order for a biometric to be effective, it must be universal, unique for each individual in the population, and stable over time[1]. One of the earliest biometrics used were fingerprints because they were mostly universal, unique, permanent, and easy to capture. More recently, facial recognition has become common for applications ranging from access control to surveillance. One of the challenges with these biometrics is that they can often be lifted or captured without a person's consent (known as skimming).

Electrocardiograms (ECGs), by comparison, cannot easily be captured without cooperation from the person. ECG is the electrical signal generated by the heart. It requires direct or very close contact with the user, making it perfect for user-controlled biometric recognition systems. Unlike fingerprints, latent samples are not left behind on contact surfaces. Additionally, ECG can be captured in a way that is still very seamless and convenient for the user.

Standing research supports the use of ECG as a biometric to reliably distinguish people[2-8, 13-15]. The distinctive patterns present in an ECG signal are a result of several factors of the cardiac function that control how the wave is depicted. Electrophysiological variations of the heart muscle, such as its size and position, along with the timing of blood pumping in and out of the heart, add to the unique properties of every person's ECG waveforms[5].

Among the strengths of ECG in biometric recognition is its continuous property. Unlike iris or fingerprint images that can be scanned at a single point in time, the ECG signal has a constant flow that allows it to be continuously reassessed to identity a user. The inconvenience with traditional biometric systems, such as the fingerprint technologies, is that when the system rejects a user, the user has to swipe or scan their fingers again for their claim to be reconsidered. Using ECG eliminates this inconvenience by collecting the signal continuously until the device is confident it has a match, which also allows the system to opt for high accuracy and continuous authentication.

Leveraging these inherent benefits of the ECG signal, the HeartID technology employs cutting edge signal processing and machine learning algorithms to uniquely identify a person using their ECG biometric.

HISTORY OF ECG AS A BIOMETRIC

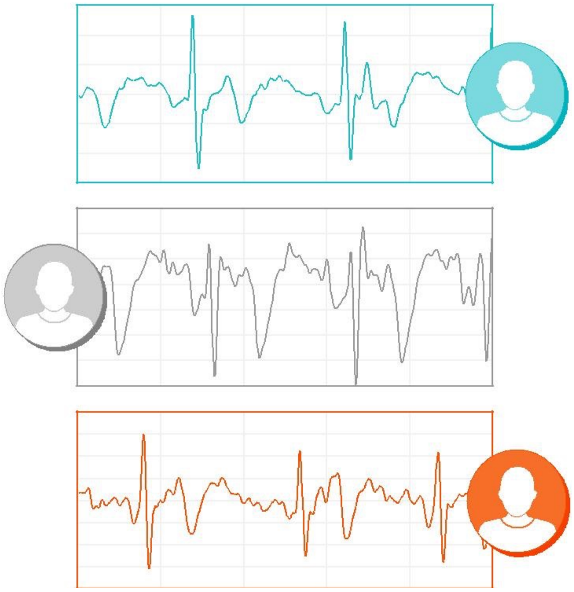
ECG has come a long way since its development by Nobel Prize winning physiologist Willem Einthoven in the early 20th century[10]. Since that time, it has become an indispensable tool in clinical cardiology and is one of the most widely used signals in healthcare. Recorded at the surface of the body, with electrodes attached in various configurations, the ECG signal is studied for diagnostics. In essence, this signal describes the electrical activity of the heart over time. The output is in the form of a wave that depicts an individual's unique internal heart rhythm.

The ECG signal is a relatively new addition to the biometric family. Interestingly, because different individual's ECGs vary with such significance, the medical community has had difficulty creating diagnostic standards for medical applications. Although the unique properties and characteristics of ECG signals had been observed before and ideas of biometric applications were discussed in 2001, the process of gathering data was complicated. Some of the earliest research in the field demonstrated the feasibility of using ECG signals from subjects of various ages and experimenting with electrode placement[9,11]. These early reports on ECG biometrics focused on the extraction of distinctive characteristics from ECG waves, without much consideration for how the technology could be practically applied.

Similar to facial recognition, early efforts in ECG technology were focused on creating points of reference for authentication (also known as the fiducial approach[13]). Like measuring the distance between a person's eyes or the length of their nose, ECG waves were analyzed in terms of the relative distances between points and the duration of inter-beat intervals. From 2007, systematic efforts from Professor Dimitrios Hatzinakos' group at the University of Toronto led the way to analyzing the overall ECG waveform instead of distinct points of reference for ECG recognition (also known as the non-fiducial approach[5]). Recently, both fiducial and non-fiducial approaches have been utilized for ECG biometric[14].

HeartID's ECG biometric originated from the extensive research conducted at the University of Toronto[5]. The original algorithm has been shown to outperform most contemporary ECG biometric systems[8,15]. Since its creation, the system has evolved significantly by deploying the latest advances in the fields of signal processing and machine learning. It has now matured to deliver the most robust and efficient commercially available ECG biometric authentication system.

ECG Verification and Pattern Recognition



While healthy ECG signals from different people conform to roughly the same repetitive pulse pattern, small differences in the overall shape of their waves reveal significant distinctions between individuals (as illustrated in the figure to the right). During the authentication process, HeartID is able to discard noise from recording artifacts that result from breathing, body movement or an inadequate connection and instead focuses on pattern recognition to either accept or reject the user. HeartID's pattern recognition engine uses a unique hybrid of fiducial and non-fiducial type features extracted from ECG. This allows the ECG wave to be analyzed for repeated unique patterns while factoring out artifacts and incidental forms. Following this, machine learning techniques are employed to improve detection of the user's unique ECG signature. During enrollment, HeartID extracts features which are persistent in an individual's ECG and at the same time distinguishable amongst a population.

Heart Conditions and Rate Fluctuations

Medical heart conditions such as cardiac arrhythmias, arterial fibrillations, or implants (e.g., pacemakers) do not impact HeartID's performance. Every heartbeat, even an irregular one, has a unique signature[4]. Because these conditions are persistent, HeartID's pattern recognition engine learns the condition and includes it as part of the user's biometric template[4].

In addition, mild variations in heart rate caused by activities such as moderate exercise, consuming caffeine or taking medication do not impact HeartID's ability to authenticate the user. During the authentication process, the system is able to ignore low frequency anomalies and can still correctly identify the enrolled user.

If an individual experiences a severe cardiac event that significantly alters their ECG, they can update their biometric template using a secure process. HeartID can use this updated template to recognize the individual.

WHY HEARTID IS NOT A MONITORING SYSTEM

The existing HeartID system is not a continuous heart monitoring or medical device, and cannot be used to diagnose medical conditions. The signal retrieved and processed by the HeartID system is customized for biometric purposes only. It is possible that future generations of HeartID could expand to include medical capabilities.

References

1. Jain, A. K., Bolle, R., Pankanti, S. “Biometrics: personal identification in networked society”. Kluwer Academic Publications. 1999.

2. Wang, Y., Agrafioti, F., Hatzinakos, D., Plataniotis, K. N. “Analysis of human electrocardiogram for biometric recognition”. In EURASIP Journal on Advances in Signal Processing. 2008.

3. Agrafioti, F., Hatzinakos, D. “Fusion of ECG sources for human identification”. In International Symposium on Communications, Control and Signal Processing: ISCCSP. 2008.

4. Agrafioti, F., Hatzinakos, D. “ECG biometric analysis in cardiac irregularity conditions”. In Signal, Image and Video Processing. 2009.

5. Agrafioti, F., ECG in Biometric Recognition: Time Dependency and Application Challenges, Doctoral Thesis, University of Toronto, 2011.

6. Sam Raj, P., ECG Biometrics using Intuitive Bases and Support Vector Machines, University of Toronto, 2014.

7. Pouryayevali, S., Wahabi, S. ; Hari, S. ; Hatzinakos, D. On establishing evaluation standards for ECG biometrics, in IEEE conference on Acoustics, Speech and Signal Processing, 2014.

8. Ikenna Odinaka, Po-Hsiang Lai, AlanD.Kaplan, Joseph A. O’Sullivan, Erik J. Sirevaag, and John W. Rohrbaugh. ECG. Biometric Recognition: A Comparative Analysis, IEEE Transactions on Information Forensics and Security, Vol. 7, No. 6, December 2012.

9. Van Oosterom, A., Hoekema, R., Uijen, G. J. “Geometrical factors affecting the interindividual variability of the ECG and the VCG”. In Journal of Electrocardiolgy.

2000.

10. Sornmo, L., Laguna, P. “Bioelectrical signal processing in cardiac and neurological applications”. Elsevier Academic Press. 2005.

11. Biel, L., Pettersson, O., Philipson, L., Wide, P. “ECG analysis: a new approach in human identification”. In IEEE Transactions on Instrumentation and Measurement. 2001.

12. Wübbeler, G., Stavridis, D., Kreiseler, R., Bousseljot, R., Elster, C. “Verification of humans using the electrocardiogram”. In Pattern Recognition Letters. 2007.

13. Israel, S. A., Irvine, J. M., Cheng, A., Wiederhold, M. D., Wiederhold, B. K. “ECG to identify individuals”. In Journal of Pattern Recognition. 2005.

14. Pereira Coutinho, D., Silva, H. ; Gamboa, H. ; Fred, A. ; Figueiredo, M., Novel fiducial and non-fiducial approaches to electrocardiogram-based biometric systems, in Biometrics, IET , 2013.

15. Carlos Carreiras, Andre Lourenc¸ Ana Fred, Rui Ferreira, “ECG Signals for Biometric Applications Are we there yet?”, in International Conference on Informatics in Control, Automation and Robotics, 2014.