# A REVIEW OF ECG BASED BIOMETRIC SYSTEMS

Liliana IVANCIU[1], Paul FARAGO[1], Sorin HINTEA[1]
[1]*Technical University of Cluj-Napoca, Romania*
*G. Baritiu Street, liliana.toma@bel.utcluj.ro*

**Abstract: In the past years many studies suggested the use of electrocardiogram (ECG) for biometrics. Its unique properties make it particularly interesting for both soft applications as a standalone authentication method and for hard applications as a security enhancement layer. Compared to existing biometric identification systems, ECG is difficult to counterfeit and also provides aliveness indication. This paper presents an overview of the methods used for ECG based biometric systems and discusses the applications and security concerns.**

***Keywords:*** *biometrics, ECG, fiducial methods, identification, non-fiducial methods*

## I. INTRODUCTION

Biometric recognition can be defined as a pattern recognition problem: the user that needs to be authenticated must provide a set of physiological and/or behavioral characteristics which match a previously registered signature. Biometric recognition relies on the natural diversity of humans and the fact that certain traits are unique for each individual [1].

The global biometric systems market is constantly growing. Demand mostly comes from areas such as: government, military and defense, transport and logistics, commercial safety and security, healthcare and recently banking and finance. The adoption of biometrics in smartphones, PCs, passport offices and banks means that in the not so distant future nearly everyone will use some kind of biometric system. There are however some factors negatively influencing the growth of this market: security concerns, the lack of cohesive support from governments and no strict regulations. With this in mind, the biometric systems market is predicted to have a 16.3% Compound Annual Growth Rate (CAGR) to 2023 [2].

Traditional strategies for automatic identity recognition include items such as PIN numbers, tokens, passwords and ID cards. While widely deployed, these techniques are either entity-based or knowledge-based and raise the serious concern of identity theft. On the other hand, biometric modalities are more difficult to steal or counterfeit when compared to PIN numbers or passwords. Moreover, since one does not have to carry a token or an ID card, they may prove more accessible and easier to use.

A comparison of different biometrics in terms of uniqueness, performance and measurability is provided in Table 1.

When it comes to user authentication and wellness, few technologies match ECG with respect to the amount of time and resources invested in the last few years. ECG (also known as EKG) stands for electrocardiogram. The electrocardiogram (ECG) is a well-known and studied biomedical signal, characterized by a high degree of inter-variability. In clinical practice this inter-variability is reduced as much as possible in order to better understand pathological characteristics. Biometric systems on the other hand take advantage of it, using the fact that ECG can provide intrinsic liveliness detection. Other characteristics of ECG include: universality, uniqueness, measurability, circumvention avoidance and most important, the fact that it can be continuously acquired with minimal intrusiveness, all of which make it particularly suitable for biometric identification [3].

Table 1. Comparison of different biometrics [4]

| Biometrics | Uniqueness | Performance | Measurability |
|---|---|---|---|
| Face recognition | High | Medium | High |
| Iris recognition | High | High | Medium |
| ECG recognition | High | High | Medium |
| Voice recognition | Low | Low | Medium |
| Palm Recognition | **M**edium | Medium | High |

The paper is structured as follows: Section II presents the ECG fundamentals; Section III describes the main methods used for ECG based biometric systems. The main applications and security concerns are discussed in Section IV while conclusions and future work end the paper.

## II ECG Fundamentals

*Morphology of the ECG signal*

The ECG signal measures the change in electrical potential over time. The trace of each heartbeat consists of three complexes: P, R, and T, defined by the peak of each complex, called the fiducial (Figure 1). The labels in the figure document the commonly used medical science ECG fiducials [5].

The ECG signal is composed of three waves [6]:

**The P wave:** The heartbeat is initiated by the sinoatrial node which spontaneously generates an electrical impulse. Upon propagation through the heart, this impulse causes the cardiac contraction. The P wave typically has a duration of less than 120 ms and a spectrum of 10 Hz to 15 Hz.

*Manuscript received October 31, 2018; revised December 5, 2018*

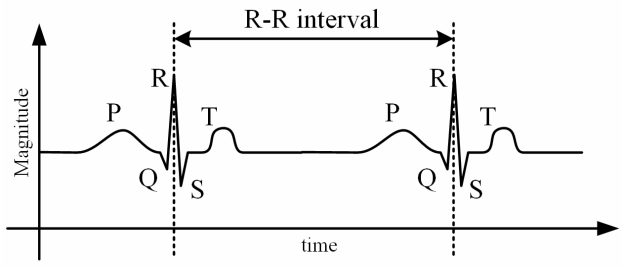


*Figure 1. Ideal ECG signal: This figure depicts two idealized heartbeats. The R–R interval indicates the duration of a heartbeat. The major ECG complexes comprising one heartbeat are indicated by P, QRS, and T*

**The QRS complex:** After the P wave, usually three consecutive peaks can be observed. These are the Q, R and S waves and correspond to the depolarization of the ventricles initiating the contraction of the heart. As shown in Figure 1, the downward Q wave is followed by the upward R wave. Next comes the downward S wave within about 100 ms. The QRS complex has a spectrum of 10 Hz to 40 Hz.

**The T wave** corresponds to the repolarization of the left and right ventricles. It has a duration of about 160 ms and is generated 80 ms to 120 ms after the QRS complex, depending on the heart rate: the ST segment gets shorter as the heart rate increases. The normal resting adult human heart rate typically ranges from 60-100 beats/minute. A slow heart rate (below 60 beats/minute) is called bradycardia while a fast heart rate (above 100 beats/minute at rest) is called tachycardia.

*ECG variability*

While healthy ECG signals from different people conform to roughly the same repetitive pulse pattern, each contains notably unique trends, depicting the various electrophysiological properties of the cardiac muscle. Many factors contribute to this significant variability among individuals: position, size and anatomy of the heart, age, sex, body weight, chest geometry, physical conditions, etc. Moreover, the timing of depolarization and repolarization and lead placement may also affect the ECG signal [7].

The ECG signal can also differ for the same individual. This variability may come from many sources but only few of them play an important role in routine situations if a standard protocol for ECG recording is used. Factors such as temperature, altitude, and pregnancy are either rare or can easily be detected and taken into account. Some sources including emotional status, physical fitness, weight, and age can also be taken into account, but are not so easily detected nor controlled. By far, the most difficult sources to deal with are the ones that vary in a random fashion, like chest electrode positioning or ones that are not controlled in routine situations, like breathing [8]. The adult ECG waveform varies very little with age, since only the amplitude of the waves decreases. Interestingly enough, the heart rate itself mainly affects the intervals between subsequent heartbeats thus making ECG authentication robust to its changes. There are, however, other cardiovascular conditions which can cause drastic and unpredictable changes in the ECG signal, as described in Table 2.

Table 2. Variability of the ECG signal: factors and effects (adapted from [9])

| Factor | Effect |
|---|---|
| Exercise | Affects the heart rate and alters the frequency content of the ECG signal. |
| Cardiac disorders | The geometrical characteristics of the ECG signal are modified. |
| Body posture | The electrical heart vector changes in relation to the body position. |
| Emotions of a person | Variations in the rhythm at which the muscle pumps blood. |

*ECG Biometric Systems*

Figure 2 illustrates the typical block diagram of a fiducial, or partially fiducial biometric system. These systems rely on the detection of notable ECG complexes (mainly QRS) for segmentation and extraction of a sequence of individual heartbeats [10].

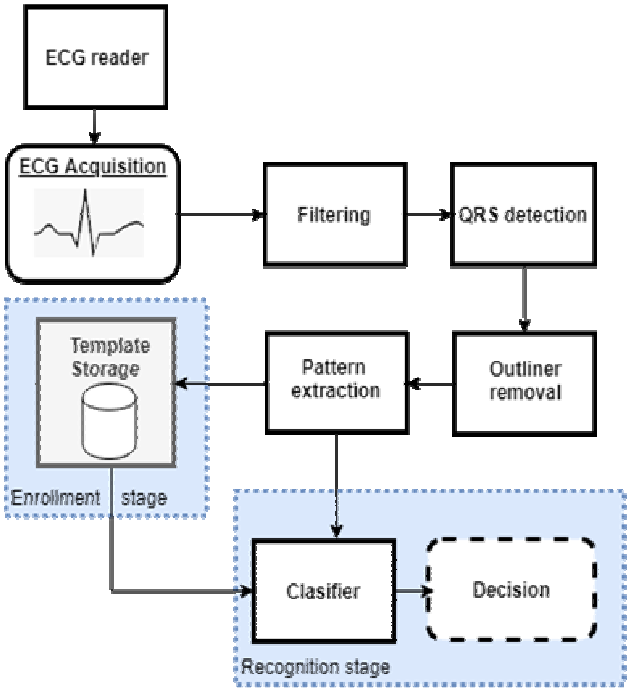


*Figure 2. Block diagram of a typical ECG biometric system [10]*

## III. METHODS USED FOR ECG BASED AUTHENTICATION

ECG biometric identification implies the collection of ECG data each time the person needs authentication. Therefore, the ECG signal is more prone to external variability conditions like circadian cycle, or particular circumstances affecting its rhythm and/or amplitude. As such, the methods used for ECG based authentication should be robust and immune to fluctuations and different sources of noise: muscle, movement, electrodes placement or pathologies [11].

ECG based identification\verification systems can be divided into two main categories: **fiducial** or **non-fiducial**. Fiducial systems use five categories of fiducial features: temporal, amplitude, area, angle and dynamic (across heartbeats, such as RR interval). They require the detection

of 11 fiducial points from the P, QRS and T waves of each heartbeat: three peak points (P, R and T), two valleys (Q and S) and the six onsets & offsets for the three waves. However, the fiducial detection process poses a particularly difficult challenge, especially for the onsets and the offsets of the three waves which are susceptible to noise. Even a slight error in wave detection or alignment can lead to misclassification but there is no universally acknowledged rule for defining the exact position of the wave boundaries [12]. Also, fiducial detectors rely on a healthy ECG and it is unclear how these algorithms would perform on patients with irregular cardiac conditions, such as premature ventricular contraction under heavy stress which causes superimposition of consecutive beats [13]. A possible solution [7] is to reject the heartbeat and ask for another reading instead of risking the accuracy of the decision.

On the other hand, non-fiducial systems usually investigate the ECG frequency content, by splitting the ECG sample into overlapping or non-overlapping windows. Features such as wavelet coefficients or discrete cosine transform coefficient are then extracted from those windows [13]. The main advantage of non-fiducial methods is that only the R peak (which is considered the easiest to spot due to its strong sharpness) must be detected and as such the preprocessing error is reduced. For some approaches, for example methods based on autocorrelation function, no detection is even needed at all [12].

Many of the methods currently found in the ECG biometric literature can be categorized as fiducial techniques. Several studies were conducted to test their efficiency. For example, Biel et al.'s [14] proposal for a fiducial feature extraction algorithm demonstrated the feasibility for using ECG signals in human identification with a 100% subject identification rate. Israel et al. [5] introduced an ECG-based identification system for temporal features extraction. The system achieved 100% subject and 81% heartbeat recognition rate for 29 subjects.
Shen et al [15] used a decision-based neural network (DBNN) for identity verification using one-lead ECG signals on 168 healthy subjects. The highest identification rate achieved in that work was 95.3%. Wübbeler et al. [16] addressed the issue of fluctuating anxiety states that affected the heart rate. The morphology of the *QRS* complex is utilized for feature extraction as this complex is less susceptible to rhythm variance. The method was tested on ECGs from 74 subjects and a 99% identification rate was achieved.

Plataniotis et al. [17] were among the earliest to report a non-fiducial technique for extracting feature from ECG segments. They used the autocorrelation of non-overlapping ECG windows as a source of discriminative information, followed by the discrete cosine transform for dimensionality reduction. The method was tested on 14 subjects; and 100% subject and window recognition rates were achieved.

Chiu et al. [18] proposed the use of Discrete Wavelet Transform (DWT) on heuristically isolated pulses. The DWT was used for feature extraction and the Euclidean distance as the similarity measure. The proposed method was applied to a database of 35 healthy subjects and a 100% verification rate was reported.

## IV. APPLICATIONS AND PRIVACY CONCERNS

The applications of ECG are numerous, the most obvious being in biometric technologies: physical access control, time and attendance monitoring, prison visitor systems, payment systems, border control systems, etc. [19]. This is mainly due to the fact that heartbeat data is difficult to counterfeit thus reducing the likelihood of falsifying credentials. Another use of ECG concerns traffic security: the vital details of the driver's wellness and readiness to drive could be evaluated before starting the vehicle. This evaluation includes stress, drowsiness or intoxication levels, if present. Furthermore, accidents may be prevented by detecting heart anomalies in mid traffic and allowing the vehicle to take over the controls. Other, less conventional ideas refer to using the ECG signal as an input for gaming devices. Such a system is described in [20].

As with other biometric modalities, using ECG data for personal identification poses considerable security and privacy concerns. First of all, when collecting ECG signals, a large amount of sensitive information is inevitably collected as well. This may reveal current and past medical conditions and even hints about the emotional state of the monitored individual. Once this information is compromised, the results are catastrophic for the subject's integrity. Second, once compromised, biometrics cannot easily be changed since they depend on the physiological and behavioral characteristics of the individual.

Traditional biometric techniques involving the face, iris or fingerprint recognition are prone to circumvention, obfuscation and replay attacks. Although unique, these features may be produced by impostors during enrollment. Fingerprints can be imitated with silicone or even photographs. As for the iris and face, these can be forged by using high definition printing technology. Moreover, noise in the user's features can cause an increase in false

Table 3. Results from selected studies on ECG based biometric systems.

| Study | Subjects | Technique | Identification Results |
|---|---|---|---|
| Biel et al. [14] | 20 | Fiducial | 100% |
| Israel et al. [5] | 29 | Fiducial: detect the peaks in the time domain by finding local maxima in regions surrounding each of the *P*, *R*, and *T* complexes | 100% |
| Shen et al [15] | 168 | Fiducial: decision-based neural network | 95.3% |
| Wübbeler et al [16] | 74 | Fiducial: morphology of QRS complex | 99% |
| Plataniotis et al. [17] | 14 | Non-fiducial: Discrete Cosine Transform (DCT) of the Autocorrelation (AC) sequence of ECG data segments | 100% |
| Chiu et al. [18] | 35 | Non-fiducial: Discrete Wavelet Transform on heuristically isolated pulses | 100% |

acceptance rates (zero-effort attacks) [21]. Unfortunately, this is also the case for ECG based biometrics. One solution to this problem is biometric encryption in which the biometric modality is encrypted with keys that are provided by the biometric itself and can only be unlocked when the same biometric is presented again. However, the time-dependent nature of the ECG poses a great challenge to biometric encryption on this signal due to the need of optimizing the feature space first [7]. At the same time, there is very little research into extracting features from ECG signals, thus preventing spoofing attacks.

The most common ways for compromising an ECG recording are either stealing the records from a medical institution or performing a social engineering attack on the victim to obtain their ECG. The next step is to digitalize the recording (if it is on paper) and fake the voltage levels at the electrodes of an ECG sensor using a waveform generator. This attack was demonstrated in [22]. A simple way to counter such presentation attacks is by using liveness detection, which aims to detect if the biometric was presented by a living individual. However, this method does not solve the issue of presentation attacks via signal injection. More work in this area is required to establish a viable defense against ECG data compromise [23].

## V. CONCLUSIONS

The unique properties of ECG signals make it particularly interesting in biometric systems. Low security and low user throughput soft applications may employ it as a standalone authentication method. On the other hand, for hard multi-biometric systems it can add a security enhancement layer. More importantly, as it can be continuously measured, it enables a new class of applications that benefit from the continuous biometric perspective. Existing biometric identification systems all use external features that can easily be stolen or counterfeited. By comparison, the ECG is difficult to steal, and when combined with an existing authentication mechanism such as a password, it can provide a highly secure way to provide user authentication. Considering its low cost, the difficulty of being falsified or spoofed and its ability to provide aliveness indication, the ECG is a very suitable candidate for biometric systems.

## REFERENCES

[1] A Survey of Wearable Biometric Recognition Systems ACM Computing Surveys, Vol. 49, No. 3, Article 43, 2016.
[2]***, https://www.marketwatch.com/press-release/global-biometric-systems-market-2018-industry-trend-and-forecast-2023-2018-06-18
[3] J.M. Carvalho, S. Brás, A. J. Pinho, "Compression-Based ECG Biometric Identification Using a Non-fiducial Approach", submitted Mar 2018
[4] G. Kaur , G. Singh, V. Kumar, "A Review on Biometric Recognition", International Journal of Bio-Science and Bio-Technology Vol.6, No.4, 2014, pp.69-76
[5] S.A. Israel, J. M. Irvine, A. Cheng, M. D. Wiederhold, & B. K Wiederhold, "ECG to identify individuals. Pattern recognition", 2005, 38(1), 133-142.
[6] F. Agrafioti and D. Hatzinakos, "ECG Based Recognition Using Second Order Statistics", Communication Networks and Services Research Conference, 2008, pp. 82– 87
[7] F. Agrafioti, "ECG in Biometric Recognition: Time Dependency and Application Challenges", Ph.D. thesis, University of Toronto, 2011
[8] B. J.A. Schijvenaars, "Intra-individual Variability of the Electrocardiogram", University of Rotterdam, 2000
[9] S. Wahabi, "Variability in ECG biometrics: state of the art and subspace methods", MSc thesis, University of Toronto, 2015
[10] C. Carreiras, A.Lourenço, A. Fred, R. Ferreira, "Ecg signals for biometric applications-are we there yet?", Informatics in Control, Automation and Robotics, 2014 11th International Conference on (Vol. 2, pp. 765-772), IEEE.
[11]F. Agrafioti, D. Hatzinakos, "ECG biometric analysis in cardiac irregularity conditions. Signal, Image and Video Processing", 2009, 3(4), 329.
[12] F. Agrafioti, J. Gao, D. Hatzinakos, "Heart Biometrics: Theory, Methods and Applications, In Biometrics", Book 3, J. Yang, Eds. Intech., 2011, pp.199-216.
[13] C. Pummer, "Continuous Biometric Authentication using Electrocardiographic (ECG) Data", MSc thesis, 2016, Hagenberg
[14] L. Biel, O. Pettersson, L. Philipson, P. Wide, "ECG analysis: A new approach in human identification", 2001, IEEE Trans. Instrume. Meas., 50(3):808–812
[15] T. W. Shen, "Biometric Identity Verification Based on Electrocardiogram (ECG)", Ph.D. thesis, University of Wisconsin, Madison, 2005.
[16] G. Wübbeler, M. Stavridis, D. Kreiseler, R. Bousseljot, C. Elster, "Verification of humans using the electrocardiogram, Pattern Recognit.", 2007, Lett., 28:1172–1175
[17] K. N. Plataniotis, D. Hatzinakos, J. K. M. Lee, "ECG biometric recognition without fiducial detection", Proceedings of Biometrics Symposiums, 2006, Baltimore
[18] C. C. Chiu, C. Chuang, C. Hsu, "A novel personal identity verification approach using a discrete wavelet transform of the ECG signal", Proceedings of International Conference on Multimedia and Ubiquitous Engineering, April 2008, pp. 201 –206.
[19] W. Tompkins, "The ECG as a Biometric for Human Identity Verification", [Online].Available: https://ay1214.moodle.wisc.edu/prod/...php/.../ECG_Biometric-last_lecture.pdf
[20] A. Chęć, D. Olczak, T. Fernandes, H.A. Ferreira, Physiological Computing Gaming, 2015
[21] T. Bhattasali, K. Saeed, N. Chaki, R. Chaki. "A Survey of Security and Privacy Issues for Biometrics Based Remote Authentication in Cloud", 13th IFIP International Conference on Computer Information Systems and Industrial Management, 2014, Ho Chi Minh City
Springer, Lecture Notes in Computer Science, LNCS- 8838, pp.112-121, 2014, Computer Information Systems and Industrial Management.
[22] Simon Eberz, Nicola Paoletti, Marc Roeschlin, Andrea Patan´e, Marta Z. Kwiatkowska, and Ivan Martinovic. Broken hearted: How to attack ECG biometrics. In NDSS, 2017.
[23] N. Samarin, "A Key to Your Heart: Biometric Authentication Based on ECG Signals", Project Report, Computer Science School of Informatics University of Edinburgh, 2018