Chapter 5
Behavioral Biometrics:
A Biosignal Based Approach

Kenneth Revett
University of Westminster, UK

ABSTRACT

Behavioral biometrics is a relatively new form of authentication mechanism which relies on the way a person interacts with an authentication device. Traditional instances of this approach include voice, signature, and keystroke dynamics. Novel approaches to behavioral biometrics include biosignals, such as the electroencephalogram and the electrocardiogram. The biosignal approach to user authentication has been shown to produce equal error rates on par with more traditional behavioral biometric approaches. In addition, through a process similar to biofeedback, users can be trained with minimal effort to produce computer-based input via the manipulations of endogenous biosignal patterns. This chapter discusses the use of biosignal based biometrics, highlighting key studies and how this approach can be integrated into a multibiometric user authentication system.

INTRODUCTION

Behavioral biometrics is an approach to user verification and/or identification based on the *way* a person interacts with the biometrics device. Some of the most prominent instantiations include keystroke dynamics, mouse dynamics, signature, voice, gait, and odor (Revett, 2008). In order to serve as a biometric, the input must not only be unique, but must be convenient, reliable, and difficult to replicate.

DOI: 10.4018/978-1-60566-725-6.ch005

The uniqueness of behavioral biometrics refers to individual differences in the way people interact with the verification device. With respect to signature verification as an example – how unique are our signatures? In part, this depends on how closely one looks at a signature. A clerk in a shop may provide a quick glance when comparing a signature to that written on the back of a credit card. At the other extreme, an off-line signature verification system may extract several features including pen pressure or wavelet transform of a digitized version when comparing a signature to a reference exemplar

(Coetzer et al., 2004). The question remains - are signatures sufficiently unique to provide unequivocal person authentication? The data suggests that error rates on the order of 5% or less - depending on the verification methodology employed (see Kholmatov, 2001 for a comprehensive discussion on this topic) are obtainable. Other behavioral biometrics produce similar error rates – though large variations have been published, depending on the exemplar matching approach employed, the quality of the data, and the features extracted (see Revett, 2008 for details).

Convenience in the context of biometrics is intimately related to familiarity in many respects – if we are used to entering a password/PIN, then this form of user verification in the stricter context of biometrics is not prohibitive. Typically, most behavioral based biometrics utilize familiar functions and hence convenience is not an issue. For instance, gait analysis can be performed in real-time – for example, while users are approaching a gate at an airport. In addition, convenience refers to the level of invasiveness of the biometric. One may consider a retinal scan as invasive – simply because we are not used to engaging in such activities – even though there is no inherent risk to the user. This sense of user acceptability/convenience is one of the key factors in the rapid deployment of behavioral based biometrics.

The reproducibility factor refers to the trial-to-trial variation produced by a user when entering their biometric verification details. Are signatures constant over time, do we type exactly the same way, does our voice change with our state of health? The obvious answer is that there are variations in these behaviors as they are influenced by our emotional and/or physical state – which in turn influences our physiology/behavior in non-linear and potentially complex ways. To date, there has been no systematic study within the field of behavioral or physiological based biometrics that has investigated the issue of inherent variability on the resulting accuracy of the biometric. On the contrary, most research focuses on trying to enhance accuracy by reducing data variability via filtering and deploying multiple machine learning techniques. Typically, the reproducibility is quantified by measuring the false acceptance rate (FAR) and the false rejection rate (FRR) has yet to be solved. Users wish to be authenticate without being rejected too frequently (thus minimizing FRR), while the possibility of a successful intruder is minimized (FAR). The cross-over error rate (CER) is defined as the intersection of the FAR/FRR, as a function of some authentication threshold. One can then equate reproducibility with the value of the CER – all other factors being held equal. The last factor to consider is the difficulty in replicating a user's authentication details – which is intimately related to uniqueness and reliability. For instance, a password that is drawn from a dictionary can easily be cracked using a dictionary based off-line attack. The information content of the biometric is critical in terms of discriminating the authentic owner from an impostor. The critical issue is the depth of the feature space of the biometric: how many features can be extracted from the authentication approach? In a noisy environment such as voice or signature – the cardinality of the feature space can compensate for the inherent noise levels. Clearly, enhancing the feature space of a biometric reduces the success rate of impostors (lowers FAR). One approach to augmenting the depth of the feature space is combining different authentication approaches – the multi-biometric approach. For instance, voice and signature, or password and voice can be employed together to enhance the degrees of freedom for classification purposes (see Ross & Jain, 2003). Again, there is a trade-off here – the richer the feature space – the more one has to remember – or at least the more one must practice their biometric details if they are behavioral.

In addition to the multi-biometric approach, one must consider whether we have exhausted the full spectrum of authentication approaches. In this chapter, the author proposes that there are additional biometric approaches that have not yet