Chapter 6
Cognitive Biometrics: A Novel Approach to Continuous Person Authentication

Kenneth Revett
British University in Egypt, Egypt

ABSTRACT

Cognitive biometrics is a new authentication scheme that utilises the cognitive, emotional, and conative state of an individual as the basis of user authentication and/or identification. These states of mind (and their derivatives) are extracted by recording various biosignals such as the EEG, ECG, and electrodermal response (EDR) of the individual in response to the presentation of the authentication stimulus. Stimuli are selected which elicit characteristic changes within the acquired biosignal(s) that represent unique responses from the individual. These characteristic changes are processed using a variety of machine learning algorithms, resulting in a unique signature that identifies or authenticates the individual. This approach can be applied in both static mode (single point of authentication), or in continuous mode, either alone, or in a multi-modal approach. The data suggest that the classification accuracy can reach 100% in many scenarios, providing support for the efficacy of this new approach to both static and continuous biometrics.

INTRODUCTION

Cognitive biometrics is a novel approach to user authentication and/or identification that utilises the response(s) of nervous tissue. The approach relies on the presentation of one or more stimuli, and the subsequent response(s) are acquired and used for authentication – a typical stimulus-response paradigm. The stimulus could be the presentation of a familiar photograph, song, or a Rorschach ink blot, either singly or in various combinations.

DOI: 10.4018/978-1-61350-129-0.ch006

This feature alone clearly distinguishes cognitive biometrics from traditional physiological biometrics, which relies on acquiring a fixed input-output relationship (i.e. a fingerprint).

The approach deployed by cognitive biometrics is to extract a unique signature from the user – but one based not on a constant physiological trait such as their iris or retina – but rather on the cognitive, affective, and conative state of the individual – either alone or more typically in various combinations. The motivation for this approach is to provide a more intuitive, potentially more robust and user-friendly authentication protocol that is also cost effective for both static and continuous authentication requirements. In addition, the cognitive approach can be combined with physiological approaches such as keystroke/mouse dynamics for example, augmenting the feature space and providing a truly multi-modal approach. Moreover, the authentication modality (visual, auditory, olfactory, or any combination) can provide a significant range of possible inputs that can be deployed for authentication purposes. For instance, a user can be authenticated while playing a game for a short interval as opposed to entering their user ID and password. Likewise, in a continuous authentication scheme, users can periodically be monitored, with or without their knowledge – simply by examining their responses to particular sets of stimuli at any point in time. The stimulus presented to the user is typically in video and/or auditory format – which can be provided by any standard mobile phone, notebook, or desktop computing device. What is required is the production of the stimulus and a way to record the response – this can be accomplished through a software only mechanism in some cases, or typically through a biosignal collection device (as discussed in detail in later sections). In addition, this approach may be considered to be less offensive to the user community relative to iris or retinal scanners – user acceptability and obtrusiveness is a critical design issue when developing a biometric.

Cognitive biometrics must in a sense compete against more traditional forms of biometrics, such as anatomical and even more recently, behavioural (physiological) approaches. Anatomical biometrics, such as fingerprint or iris scans have been deployed for over several decades, yielding very low classification errors (on the order 10^9). Typically, anatomical biometrics is deployed in a static fashion, providing a single access protection protocol. The continued deployment of a retinal scan for instance may be perceived as too invasive. The issues of usability, user perception, cost, and convenience are probably the limiting factors to their widespread distribution. Behavioural and physiological biometrics have provided a lightweight alternative in terms of the required hardware and user perception/convenience issues. Signature verification, gait analysis and keystroke dynamics provide a very acceptable mechanism for extracting authenticity information from an individual that is steeped in a long standing tradition (e.g., signature verification). In terms of deployment, keystroke dynamics could be deployed in both a static and continuous fashion, acquiring samples from the user during their interaction with a word processor, would be a very natural approach. The issue with respect to the widespread deployment of behavioural biometrics is probably based on the perception that the approach is not 'high-tech' enough. In part, it is human nature to believe that if something is going to work, it must be constructed from 'solid' materials – 'medicine must taste bad to be good' mentality. Research has demonstrated that the approach is sound, producing classification accuracies (sometimes reported as the equal error rates) approaching 95+% in many cases (Revett, 2009a, Revett 2009b, Nixon & Carter, 2004, Jain et al., 2002). The potential difficulty with behavioural biometrics is the inability of humans to perform repetitive motoric tasks in a reliable fashion. Our signatures are never the same: our typing cadence can vary based on mood or the input device type (e.g. laptop versus a desktop