Chapter 22
Identity Assurance through EEG Recordings

Massimiliano Zanin
Innaxis Foundation & Research Institute, Spain

David Papo
Universidad Politecnica de Madrid, Spain

ABSTRACT

The problem of identity assurance, i.e. determining if a claimed identity can be trusted, has been gaining relevance in the last decade, due to the increasing use of on-line services. While this trend can be seen for many biometric sensors, very few studies have considered the use of brain electric signals. This contribution proposes a first solution, based on the reconstruction of motifs (patterns of connectivity between three electroencephalographic sensors) and on the assessment of their stability across different trials for a single subject. Results indicate that, although computationally costly, this approach is promising in terms of the classification scores obtained.

INTRODUCTION

Identity assurance, i.e. the problem of determining if a claim of a particular identity can be trusted to actually be the claimant’s identity, has grown in importance in last years, especially with the increasing use of on-line services. Traditionally, this task has been performed through “something you know”, as for instance a secret password (Burr, Dodson & Polk, 2004). Due to the easiness in stealing such kind of information, it has been expanded to “something you have”, that is, relying on something the user has, e.g. a mobile phone, for a “two-factor” authentication. The final frontiers are called “something you are”, and is based on something intrinsic to the principal being authenticated. While this last option is the most secure of the three, as for instance it is relatively difficult to steal a fingerprint, it is still not widespread due to several problems: its complexity, the cost of associated measurement sensors, and the fact that not all people can interact with biometric devices (as some people do not have fingers or eyes).

Here we explore the use of brain dynamics to authenticate a person’s identity. This approach is based on the idea that, even if a given cognitive task is executed similarly by different subjects, each subject
Identity Assurance through EEG Recordings

displays some variability, which can be used as a univocal identifier. Because altering our brain activity on a very short time and spatial scale is an arduous task, it is impossible to impersonate another subject. This chapter first introduces the basics of functional brain networks, i.e. how the brain activity during the execution of a cognitive task can be mapped into a graph-like structure. The mathematical method for authentication is then discussed, and tested with a set of real brain recordings. Finally, some future lines of works are discussed, and conclusions are drawn.

BACKGROUND

The idea that the brain activity can be described through the electric (and magnetic) field it generates during a task is not new, and was proposed back in 1875 (Swartz, 1988). Electrophysiological techniques such as the ElectroEncephaloGraph (EEG) measure the voltage fluctuations generated by the ionic current within the neurons. More recently, it was recognized that coordination, e.g. synchronization, between electrical activity at different brain regions represent a basic modus operandi of brain information transfer and processing. However, only over the last fifteen years have such structures of interactions been described as networks, thanks to the raising field of complex networks analysis (Albert & Barabasi, 2002; Boccaletti, Latora, Moreno, Chavez & Hwang, 2006).

Network theory is a statistical mechanics understanding of an old branch of pure mathematics: graph theory. In order to represent a system by means of a network, all unnecessary details are deleted, to extract only its constituent parts and their interactions; these are then respectively represented by nodes and links. The structure created by such interactions is then called the network topology. Most social, biological, and technological networks (including, of course, the brain) display substantial non-trivial topological properties, i.e. patterns of connection between their elements are neither purely regular nor purely random (Costa et al., 2011). These properties can be thought of as features describing the network’s structure. The topological properties of a network can directly or indirectly be retrieved from the so-called adjacency matrix, which represents which nodes are connected to which other nodes in a network (Costa, Rodrigues, Travieso & Villas Boas, 2007).

The brain can be represented by at least two conceptually different types of networks. The first is obtained by mapping the physical connections between neurons or groups of them, thus representing their wiring diagram: this anatomical pattern of connectivity is called the connectome (Sporns, Tononi & Kötter, 2005). A second type of description, which will be used in this Chapter, disregards physical connections, and tries to determine if two regions are “functionally connected”, i.e. they are interacting in a given task to perform a function. These functional networks are obtained by (i) recording the brain activity, for instance by means of an EEG, at different locations; (ii) calculating some form of synchronization between the dynamics of pairs of regions (e.g. linear correlation, or more complex causality measures); (iii) creating a link between the corresponding nodes when the detected synchronization is statistically significant. A complete discussion of the use of functional networks, and of their pros and cons, can be found in (Bullmore & Sporns, 2009; Papo, Zanin, Pineda-Pardo, Boccaletti & Buldú, 2014).

Following the progressive decrease in their cost and complexity, EEG devices have increasingly been used in HMI applications (McFarland, Krusienski, Sarnacki & Wolpaw, 2008; Iturrate, Antelis, Kübler & Minguez, 2009). There is nevertheless one application for which they have largely been neglected: identity assurance, i.e. verifying the identity of the user of an information system. Even if very few examples of