Description of the problem

A biometric system is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database. Depending on the application context, a biometric system may operate either in authentication mode or in identiﬁcation mode:

The perfect biometric trait should have the following characteristics: very low intra-subject variability, very high inter-subject variability, very high stability over time, and universality. Typical biometric traits, such as ﬁngerprint, voice, and retina, are not universal and can be subject to physical damage (dry skin, scars, loss of voice, etc.). In fact, it is estimated that 2–3% of the population is missing the feature that is required for authentication, or that the provided biometric sample is of poor quality. Furthermore, these systems are subject to attacks such as presenting a registered deceased person, presenting a dismembered body part, or introduction of fake biometric samples. Since every living and functional person has a recordable EEG/ECG signal, the EEG/ECG feature is universal. Moreover, brain or heart damage is something that rarely occurs. Finally, it is very hard to fake an EEG/ECG signature or to attack an EEG/ECG biometric system.

This modality has several advantages: (1) it is conﬁdential (as it corresponds to a mental task), (2) it is very difﬁcult to mimic (as similar mental tasks are person dependent)and (3) it is almost impossible to steal (as the brain activity is sensitive to the stress and the mood of the person, an aggressor cannot force the person to reproduce his/her mental pass-phrase).

Major research efforts in recent years were directed towards application of brain waves as a biometric characteristic that is unique and inherent in every person. The main challenge of this research is recreating the brainwave. EEG as a biometric characteristic lacks constancy which depends on stress, fatigue, medication, environment (electrical equipment) etc. To cope with this, researchers often use some kind of stimuli to help in recreating the valid authentication EEG pattern [5], e.g. visualization of 3D object manipulation, counting, imagining letters and texts [4] etc.

EEGs are impossible to forge because they reflect the inner self of a person, and they are likely to be different from person to person when performing similar mental activities.

This is interesting as the EEG parameters are highly personal-dependent [1,2];

Methods are required that are both effective in combating impostors and acceptable to legitimate users. Although traditional methods such as passwords can be argued to succeed in the latter respect, this is often a factor of the inappropriate ways in which they are used, with many studies over the years having suggested that end-user practices serve to compromise security in favour of convenience (Morris R, Thompson K. Password security: a case history. Commun ACM 1979;22(11):594–7. , Klein D. Foiling the cracker: a survey of, and improvements to, password security. In: Proceedings of the Second USENIX Security Workshop, Portland, Oregon; August 1990. p. 5–14., Sasse MA, Brostoff S, Weirich D. Transforming the ‘‘weakest link’’: a human–computer interaction approach to usable and effective security. BT Technol J 2001;19(3):122–31).

It can be observed from the above definition that biometrics are grouped into two distinct categories, according to the factors that they attempt to measure. Specifically, they can be based upon physiological characteristics or behavioural traits of the user – i.e. how they are, and how they do things. Physiological approaches (such as fingerprint, facerecognition or hand-geometry) still account for the majority of current commercial biometric systems, representing the more mature technologies. They are also more invariant and discriminative techniques in comparison to the more transient behavioural approaches (Woodward et al., 2003, pp. 45–100). However, in both cases the related technologies range from the relatively mainstream to rather more obscure approaches that are still predominantly within the realms of research.

The EEG signals can be easily affected and governed by the user but they cannot be easily reproduced under conditions of stress, anxiety, drowsiness, effects of alcohol or drugs, etc. This way, the user has some control on the condition in which he can authenticate.

However, the changes of EEG patterns over longer periods of time need to be investigated.

The advantage of the method compared with others is that it is difficult to be forged it i.e. the possibility of illegal identification is low. However, it is true that VEP preparation might take longer than other biometric techniques such as fingerprints. For example, in this work, it was decided to use 61 active channels to examine the success/failure of the method. Although there are electrode caps available nowadays, using a high number of channels may be cumbersome in some applications. However, this is a price for added security. Therefore, the method may prove to be more suitable where security is a very important issue as in military applications. Currently, work to determine the success of the method using a smaller number of channels has been initiated to reduce the computational cost and complexity of the design.