Brain Waves

Science Fiction or Biometric of the Future

BY RAMASWAMY PALANIAPPAN, IAN SILLITOE

It is not science fiction! Just THINK about your PIN to get money out of ATM machine!

What you will learn…

- Introduction to biometrics using brain and heart signals
- Possible approaches to use these methods to identify or authenticate a person's individuality
- Challenging issues in using these approaches

What you should know…

- Basics of biometrics technology

This article will discuss the use of brain waves for both biometric authentication and identification while touching lightly on heart wave biometrics for individual identification purposes.

Biometrics Using Brain Waves

Biometrics is the intrinsic physical or behavioral traits of a person that can be used to identify or authenticate a person's identity. It is becoming important especially in ensuring security not only for high security applications but also for everyday transactions such as internet banking. The standard biometric approach is using fingerprints and many fingerprint biometric applications can be seen, for example, in ensuring secure door access and computer logins. Various ID-card government databases have also started using fingerprints. However, there are also another two other trends in the biometrics field. One is where research has focused on alternative biometrics such as those based on signature, face features, palm-print, hand geometry, iris and voice [1]. The second trend, which is more recent is to use signals from brain [2] (known as electroencephalogram, EEG) and heart [3] (known as electrocardiogram, ECG) as biometrics. Traditionally, such signals from the brain and heart have been used for medical diagnosis but the advantage of using such biological signal based biometric compared to other biometrics is its distinctiveness, for example it is difficult to be duplicated by someone else, therefore not easily forged or stolen. The storage is not a problem as the feature vector is of a small size compared to other biometric features (such as those based on images). Though data collection is cumbersome, the future improvements will reduce the unwieldiness and that the distinctiveness outweighs this difficulty especially for high security applications.

Biometrics can be divided into two categories: verification (authentication) and identification. For verification, user declares his or her identity and the system then searches its stored database for the person's information. If matching template information is obtained, the output is seen as positive, for example the person is verified but else it is negative and the person is classified as impostor and rejected. For identification, the system has to match the user to the stored databases of a pool of users. This is normally more difficult as this means matching against numerous user databases instead of one as in the case of verification.

Authentication Using Brain Responses During Mental Thoughts

Figure 1 shows a basic block diagram of how brain waves (signals) could be used to identify a person. An EEG cap, which normally consists of 16, 32 or 64 (though 128 or 256 is also possible) electrodes is used to record the brain signals when the user is either thinking of a particular task or when the user is perceiving a visual or auditory stimulus. Figure 2 shows possible electrode locations where the ear lobes are commonly used as reference channels while the next figure gives an example of a typical recorded EEG signal. To increase the conductance between the scalp and the electrodes, water based gel is commonly used. The EEG signals are in the microVolts range (for example very small amplitude) and hence they are amplified and an analogue to digital converter (ADC) converts the signals to digital. These digital signals are then passed to the preprocessing module that reduces noise by performing frequency specific filtering and the feature extraction module uses mathematical modeling to extract features representative of the signal.

Theses extracted features are then classified using an intelligent classifier such as an artificial neural network that recognizes the person's identity. In some scenarios, there is a feedback, obviously if there is an error – perhaps the system suggests the person is an impostor and a second attempt is performed by the user. Rather than a clean trial, the data from the first attempt is also used for the repeat attempts. This will ensure a higher security should an impostor continually tries to forge his identity.

After identifying himself/herself correctly, the user can then be allowed to proceed to the application stage, for example perhaps open a secured door, access confidential files etc.

What mental thoughts?

Obviously, the question is on what are the suitable mental thoughts that are sufficiently distinct between each individual. In the approach proposed in [4], users perceive a commonly encountered black and white line image such as cup, pencil, book etc and the brain starts to process the images. There are many processes involved in the brain such as recognizing that a picture is being perceived, extracting details of the picture and matching to memory in order to decide the name of the object. Such brain processes involve higher order functions that can be detected in gamma band frequency range of EEG.

What is gamma band EEG?

Gamma band denotes frequency range above 30 Hz. Frequency is a measure on the number of cycles and EEG has components in many frequency ranges. Delta band (below 3 Hz) EEG is usually prominent in deep sleep and meditative stages while theta rhythms (4-7 Hz) stage can normally be seen in EEG during drowsiness and sleep-onset. Alpha range (8-12 Hz) is normally encountered during relaxed conditions but also when performing concentrated mental tasks and beta (13-30 Hz) usually correlates with tensed situations. Gamma band on the other hand appears frequency in EEG and is involved whenever the brain does complex processing and is absent when there is no deep

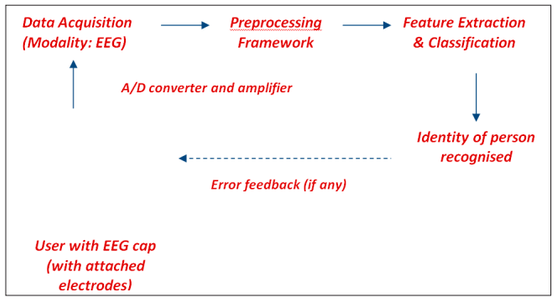

Figure 1. *Basic layout of a brain biometric system for individual identification*

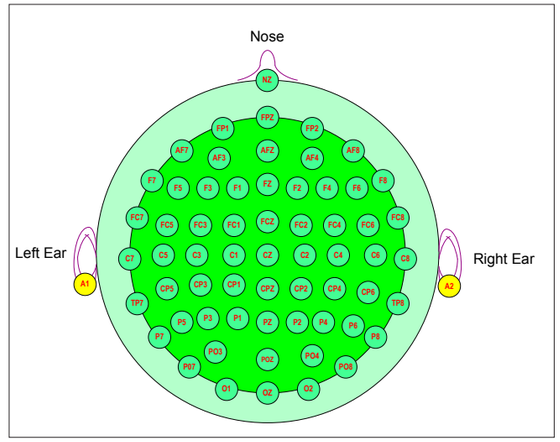

Figure 2. *EEG electrode location on the scalp (64 channel system is shown here as an example)*

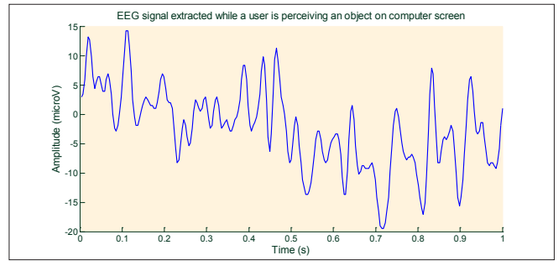

Figure 3. *A typical example of recorded EEG signal*

processing involved. For example, coma patients would not have EEG in gamma band range, though they may have EEG in other frequency ranges.

Accuracy?
A framework comprising of several advanced signal processing algorithms were employed in [4] and the accuracy of 98.12 was obtained when tested on 102 users. The overall high classification results indicated that the object recognition process has different properties for different individuals. The authors also speculated that this process could have a relation to genetic material though obviously only clinical trials would give conclusive results. Nevertheless, this accuracy is not high enough for practical applications but sufficient to show the promise behind the method.

Verification of Individuals Using Brain Waves

Verification of identity is where the system either accepts the user claiming a given identity or rejects his or her claim. The user is called as client in the former case and as impostor as in the latter case. In such systems, there will be two types of errors: *false accept error* (FAE) or *false reject error* (FRE). The former is the error made by the system when wrongly accepting an impostor while the latter is the error made when wrongly rejecting the client.

Obviously, the use of electrode caps causes some cumbersomeness and such applications would be more useful for verifying small groups of people, where the security would be an utmost important issue such as access to classified confidential documents or entry to restricted areas. Other biometric modalities such as fingerprints could be easily forged. This is also the case with most of the other biometrics like palm-print, face, and iris etc. But the thought processes in the brain are difficult to be duplicated and this EEG biometric will have higher fraud resistance. Nevertheless, this discussion applies to fraud in the data collection (sensor level) step and not fraud in the other parts of the system for example extracted features, decision etc, which has the possibility of fraud for any biometric.

The study in [5] have applied a two stage biometric verification using EEG signals that are extracted while the user is thinking of different mental tasks. As different individuals have different thought processes, this idea is appropriate for individual authentication. Description of the used mental tasks follows:

- *Baseline task*. Users are asked to relax and think of nothing in particular.
- *Non-trivial mathematical task*. Users are given nontrivial multiplication problems, such as 32 times 46, and are asked to solve them without vocalising or making any other physical movements. The tasks are non-repeating and designed so that an immediate answer is not apparent.
- *Geometric figure rotation task*. Users are given 30 seconds to study a particular three-dimensional block object, after which the drawing is removed and users are asked to visualise the object being rotated about an axis. The EEG signals are recorded during the mental object rotation period.
- *Mental letter composing task*. Users are asked to mentally compose a letter to a relative or a friend without vocalizing.
- *Visual counting task*. In this task, users imagine a blackboard and to visualize numbers being written on the board sequentially, with the previous number being erased before the next number is written. The subjects are instructed not to verbalize the numbers but to visualize them.

Only data from six channels (electrodes) were used: C3, C4, P3, P4, O1 and O2 (C stands for central location, P for parietal location and O for occipitial location) with reference electrodes A1 and A2 (located in the mastoids – just behind the ear). Several mathematical tools such as auto-regressive coefficients, channel spectral powers, inter-hemispheric channel spectral power differences, inter-hemispheric channel linear complexity and non-linear complexity (approximate entropy) were used as EEG features and cross validated using Manhattan distance measures. The authentication approach was based on a novel two-stage method where both FAE and FRE rates were minimized. Usually, most biometric methods are able to only minimize either one at the expense of the other. However, in this approach, different thresholds were used for FAE and FRE unlike a single FAE-FRE threshold (commonly known as equal error threshold) in the conventional biometric methods. Perfect accuracy was obtained, for example the FRE and FAE were both zero when the proposed method was tested on five subjects using a combination of the above thought activities.

Pass Code Generation with Brain Responses

Instead of identifying or authentication a person's identity, brain responses can also be used to generate a pass code or *personal identification number* (PIN) – for example to be used in *automated teller* (ATM) machines. Such methods are largely based on *brain-computer interface* (BCI) paradigms such as P300 BCI [6].

The study in [7] has explored the use of colors on screen as pass code. The user will focus on colors that randomly flash on screen. The objective would be to form a color coded pass code generated by thought alone. For example, a passcode could be in the form of RED, GREEN, BLUE, BLACK, BLUE (Figure 5 shows an example) – the sequence is obviously of paramount importance and the length can be increased for added security. The color flashes in the study lasted 100 ms, with an inter-stimulus interval (ISI) of 300 ms. During the ISI, there would be no flashes. The ISI is defined as the end of the flash to the start of the next flash. The brain responses (specifically known as P300) are obtained when the flashed color is part of the password thought by the user and this component is absent when non pass codes colors (for example non-focused target) flash on screen. Through frequency specific filtering and classification algorithms, the presence of P300 component can be detected and hence, the colour that is focused in the mind of the user can be recognized. The detections will be repeated, for example, until a sequence of colors is obtained. Such approaches share the similar problem to other password mechanisms where one could *steal* the password through force (perhaps by threatening with a knife pointed at the user) and get through the system. However, the main advantage of using brain waves is that *shoulder surfing* problem will be avoided, so one need not worry about people peeping over the shoulder to steal the password or PIN.

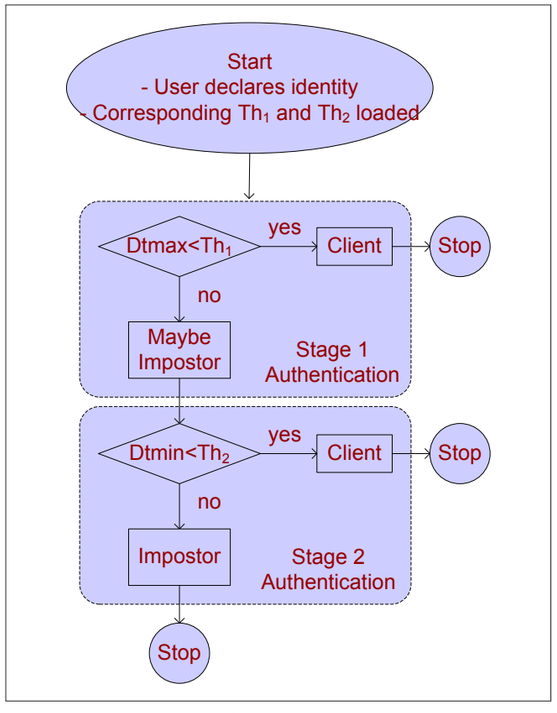

Figure 4. *Two-stage verification system [5] where different thresholds (Th1 and Th2) are used to decrease the FAE rate while also minimizing FRE rate*

Similar study in [8] explored the use of alphanumeric characters and obviously this would be useful for password generation using thoughts. Perfect accuracies were obtained for most of the users tested though some users required several trials before achieving good accuracy. Instead of using visual objects, it is also possible to use audio tones in a similar fashion. This was explored in [9] where brain responses were used to decide the tones focused by the user. Obviously, such audio based system would prove to be more fraud resistant than visual based systems. However, the performance of using audio tones were reported to be lower than visual stimulus – likely as it is more difficult for the user to concentrate on specific audio tones as compared to focusing on visual objects.

Challenges in Brain Wave Biometric

Biometrics based on brain waves is relatively new and there are still many challenges that need to be addressed before the technology can be used commercially. The main issue is the requirement of wet gel based electrode technology that is necessary to increase the conductance between the electrode and scalp. EEG signals are generated in the brain and passes through skull and scalp, which further attenuates the signal and hence sufficient *contact* is necessary to obtain good quality signal. Recent electrodes use active amplifier technology where some signal conditioning (for example noise reduction) is done on the electrode itself but such electrodes still require gel. The dry electrode technology based on capacitance has started emerging but the performance of such electrodes is questionable. Most of the brain wave biometric technology requires at least a few channels to achieve good accuracy and this can results in set-

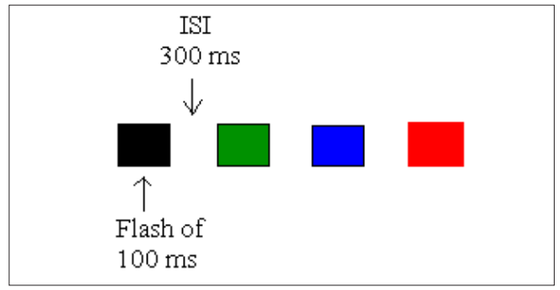

Figure 5. *A color block illustrating a sequence of flashes. Note that only one block flashed on screen at a time. ISI represents the inter-stimulus interval (for example time between the color flashes) while flash time is the time each color block stays on screen*

up time of a few minutes. Obviously with the signal processing advances seen in recent times, it could be possible to obtain sufficient accuracy with just a single channel thereby reducing the set-up time to seconds (with dry electrode technology, it could be just a matter of placing the cap/hat on the head).

The studies in this area have clearly shown that EEG waveforms are distinct between individuals and hence can serve as a good biometric. However, stability of such waveforms over time need to be studied – the brain is constantly evolving by acquiring new knowledge and this could affect the user templates generated from the brain responses. Hence, forms of normalization factor have to be developed to avoid genuine users from being rejected by the system after a lapse of time.

References

[1] J. Wayman, A. Jain, D. Maltoni, and D. Maio (eds.), Biometrics Systems: Technology, Design and Performance Evaluation, Springer-Verlag, New York, 2004.

[2] R. Palaniappan, Electroencephalogram signals from imagined activities: A novel biometric identifier for a small population, published in E. Corchado et al. (eds): Intelligent Data Engineering and Automated Learning – IDEAL 2006, Lecture Notes in Computer Science, vol. 4224, pp. 604-611, Springer-Verlag, Berlin Heidelberg, 2006.

[3] R. Palaniappan, and S. M. Krishnan, Identifying individuals using ECG signals, Proceedings of International Conference on Signal Processing and Communications, Bangalore, India, pp.569-572, 11-14 December, 2004.

[4] R. Palaniappan, and D. P. Mandic, Biometric from the brain electrical activity: A machine learning approach, IEEE Transactions on Pattern Analysis and Machine Intelligence (special issue on biometrics), vol. 29, no. 4, April 2007, pp. 738-742.

[4] R. Palaniappan, Two-stage biometric authentication method using thought activity brain waves," International Journal of Neural Systems, vol. 18, issue 1, pp.59-66, 2008.

[5] C. N. Gupta, Y.U. Khan, R. Palaniappan, and F. Sepulveda, Wavelet framework for improved target detection in oddball paradigms using P300 and gamma band analysis, Special issue on Bio-signals: Data Acquisition, Processing and Control, International Journal of Biomedical Soft-computing and Human Sciences, vol.14, no. 2, pp.61-67, 2009.

[6] C. N. Gupta, J. J. Wilson, R. Palaniappan, and C. S. Syan, Single trial P300 amplitude for pass-code brain-machine interface design, Proceedings of International Conference on Advanced Computing, Chikhli, Maharashtra, India, 21-22 February 2008.

[7] C. N. Gupta, R. Palaniappan, and R. Paramesran, Exploiting the P300 paradigm for cognitive biometrics, International Journal of Cognitive Biometrics, vol.1, no.1, pp.26-38, 2012.

[8] C. N. Gupta and R. Palaniappan, Using high-frequency electroencephalogram in visual and auditory-based brain-computer interface designs, EContact! 14.3 – Biotechnological Performance Practice, Canadian Electroacoustic Society, June 2012.

Heart Waves as Emerging Biometrics

Biometrics can also be obtained from the heart waves (signals) and this was explored in another study [3]. The use of ECG signals for the purpose of identifying individuals is relatively new as compared to the other biometric technology and has not matured as sufficiently. Nevertheless, a brief summary of the method is given here for the sake of completeness when studying emerging forms of biometric technology. The study in [3] used the QRS complex of the ECG waveform that was extracted from a single lead (channel) when the user was at rest and a feature called form factor that measures the shape of the ECG wave was computed in addition to commonly used medical diagnosis features like R-R interval, R amplitude, QRS interval, QR amplitude and RS amplitude. Identification success rate of 96.17% was obtained when tested over ten users. Changes over a period of time and under different health conditions (for example, when user has just finished exercising) will likely affect the heart wave and the performance of the biometric system. Clearly this was a pilot study and more development will be necessary before such technology can be used for biometric applications.

Conclusion

This article has given an introduction to the currently emerging biometric technology – mainly brain responses to audio and visual were covered for biometric authentication and identification but also touching lightly on heart waves for individual identification. Overall, the current advances in the related technologies indicate that it is highly likely that biometric technologies based on brain waves will be a reality in the coming decade, if not years.

RAMASWAMY PALANIAPPAN

Ramaswamy Palaniappan PhD is a senior lecturer in Department of Engineering, School of Technology, University of Wolverhampton, Telford, UK. His research interest lie in the area of biosignal analysis and machine learning for biometric and brain-computer interface applications. He has published over 140 research papers in addition to two text books in engineering. His pioneering work in using brain signals for biometrics has received international recognition.

IAN SILLITOE

Ian Sillitoe is currently Professor of Robotics at the Department of Engineering, University of Wolverhampton, UK and has previously held visiting professorships at a number of European Universities. His research interests include sensor and distributed control systems, applied to autonomous and semi-autonomous systems and more recently has been studying biometric technologies.