Vision Related Brain Activity for Biometric Authentication

Ramaswamy Palaniappan
Dept. of Computer Science
University of Essex
Wivenhoe Park
Essex, CO4 3SQ, United Kingdom
rpalan@essex.ac.uk

Abstract – **Brain activity based biometric in the context of authentication of individuals is investigated. Specifically, a novel two-stage authenticating procedure to authenticate the claimed identity of the user using evoked potentials obtained when the user perceives a visual stimulus is proposed. A thorough analysis is performed on the proposed pilot approach, which validates the success of the approach.**

I. INTRODUCTION

With the advent of internet banking and e-commerce, authentications of individuals have become an important issue. These are also crucial in ensuring security for access to confidential documents or to restricted areas. Biometrics often surpasses other measures such as the use of personal identification number and password for authentication. Though the much established biometric is fingerprint, nevertheless, there have been significant interests in utilizing other biometrics such DNA, hand geometry, palm print, face (both optical and infrared), iris, retina, signature, ear shape, odor, keystroke entry pattern, gait, and voice [2].

More recently, other emerging biometrics have mushroomed. These are like ear force fields [3], electrical activity of the heart [4], and brain [5-7]. The least studied is the electrical activity of the brain; perhaps due to the difficulties in the recording procedures. However, it is probably the best biometric in terms of fraud resistance and this overweighs the cumbersomeness of data recording.

Some of the studies on using electrical activity of the brain as biometric include the work by Paranjape et al [5] who examined the use of autoregressive (AR) models of various orders computed from EEG signals recorded from the subjects with eyes open and eyes closed. Poulos et al [6] used a Learning Vector Quantizer[1] network to classify AR parameters describing the alpha rhythm EEG feature. Palaniappan [7] utilized energy of the gamma band potentials from visual evoked potential (VEP) as a feature to identify individuals. The underlying mechanism behind this approach was that the perception of a visual stimulus (black and white drawings of common objects) evokes brain activity related to recognition and memory, which is known to be particularly reflected in gamma oscillations. These are known to be distinct between humans, thereby proving to be suitable as a biometric.

Until now, all the few studies on using electrical activity of the brain as biometric concentrated on identification of a user from a pool of users. In this study, authentication of the user using vision related brain activity similar to the previous study in [7] is explored. A novel two threshold authentication procedure is proposed which gives improved accuracy as compared to existing authentication methods that adjusts a single threshold to balance false accept error (FAE) and false reject error (FRE).

FAE is the error made by the authentication system when wrongly accepting an impostor as client while the latter is made when wrongly rejecting a client as impostor. Client is the actual user claiming the identity while impostor is the user claiming another person's identity.

II. BRAIN ACTIVITY DATA

A total of 40 subjects participated in the study. The subjects were seated in a reclining chair located in a sound attenuated RF shielded room and their brain signals, typically known as VEP were recorded when subjects visualized a common black and white line drawing like a ball, a banana, a house, etc. The pictures were easily recognizable and thus would evoke parts of the brain related to visual perception and recognition.

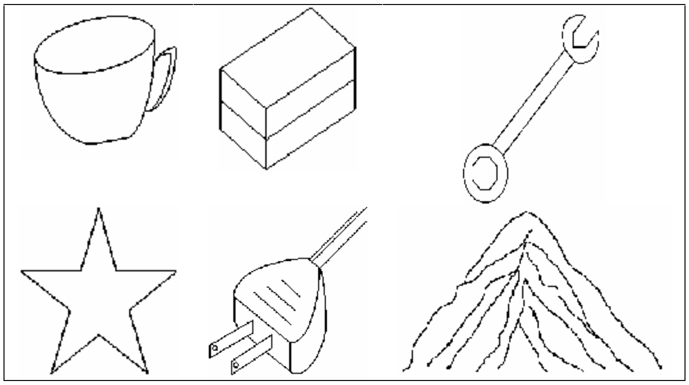


Fig. 1. Examples of shown pictures.

Measurements were taken from 61 active channels placed on the subject's scalp, which were sampled at 256 Hz. The electrode positions were located at standard sites using extension of Standard Electrode Position Nomenclature, American Encephalographic Association.

[1] In the paper, it is referred as Learning Vector Quantizer, though the common name is Learning Vector Quantization.

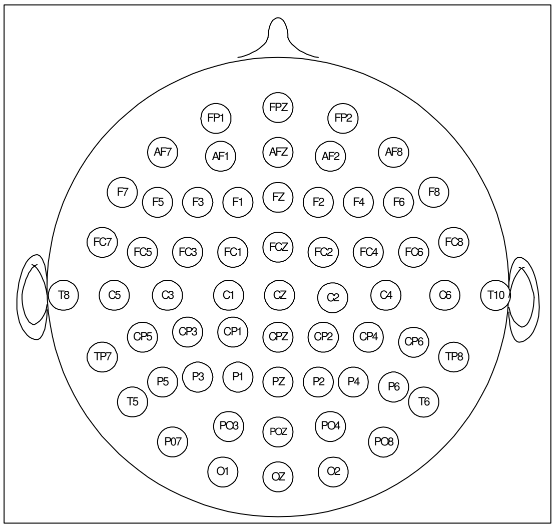


Fig. 2. Electrode locations for the 61 channel VEP recording system.

Stimulus duration of each picture was 300 ms. All the stimuli were shown using a computer display unit located 1 meter away from the subject's eyes. One-second measurements after each stimulus onset were stored. This data set is actually a subset of a larger experiment designed to study a quantitative marker for visual short-term memory [8].

III. PRE-PROCESSING AND FEATURE EXTRACTION

VEP signals with eye blink artifact contamination were removed using a computer program written to detect VEP signals with magnitudes above 100 μV. These VEP signals detected with eye blinks were then discarded from the experimental study. The threshold value of 100 μV was used since blinking produces 100-200 μV potential lasting 250 milliseconds [9]. After the removal of VEP signals with eye blinks, there were 40 VEP signals from a subject giving a total of 1600 VEP signals.

These VEP signals were re-referenced to common average using

$$z[n] = x[n] - \frac{1}{61}\sum_{i=1}^{61} x_i[n], \tag{1}$$

where *x[n]* is the original signal, while *z[n]* is the new re-referenced signal. This would be useful in reducing the intra-subject variance of the VEP signals.

Notice that there is a possibility that the same subject exhibits similar energy patterns in different sessions, however, the recorded signal power is not likely to be the same. In order words, there are strong indications that the ratios among the energies across the channels do not vary over time but instead the subjects exhibit scaling of energies in all the channels. The baseline measure using common spatial average (2) serves to reduce this intra-class variance.

Figure 3 shows the reduction in intra-class standard deviation through the use of common spatial average as a baseline measure for one subject (from 40 VEP signals) over 61 channels.

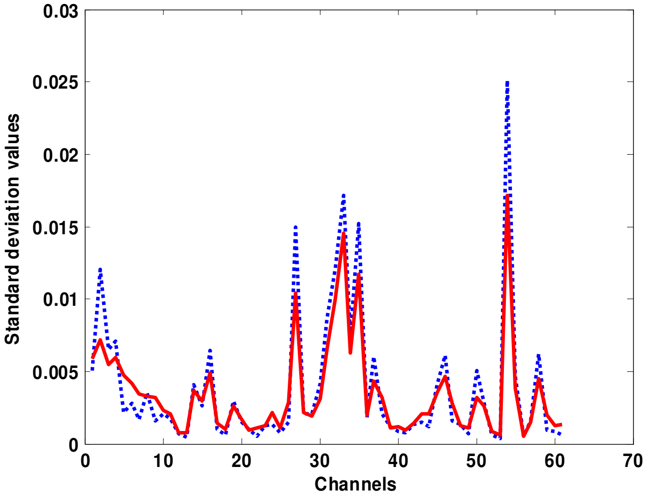
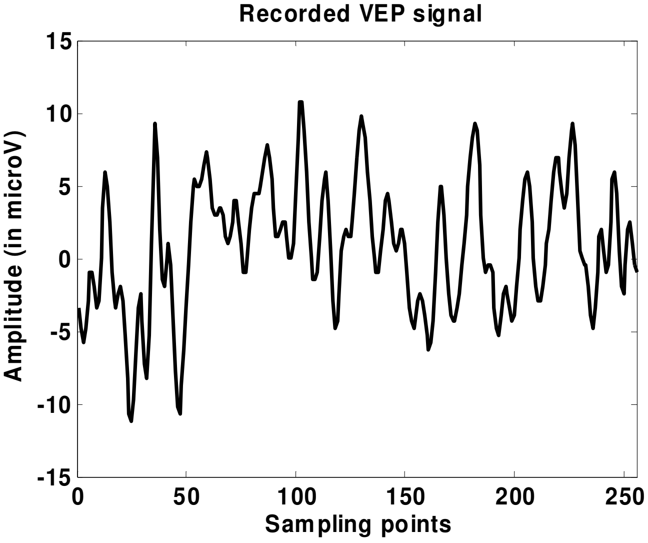


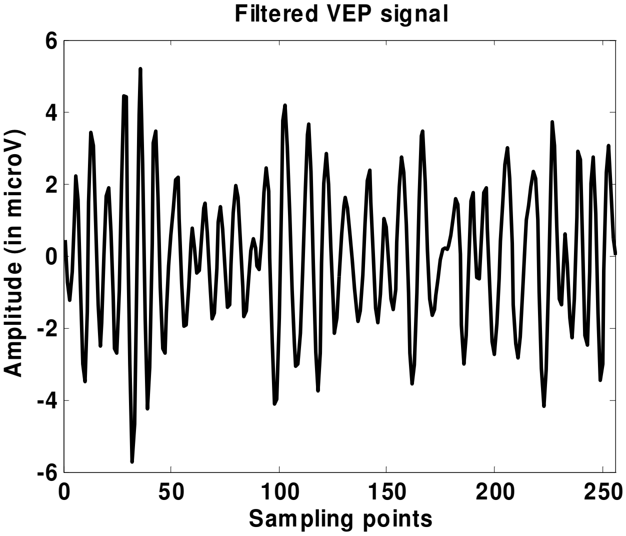
Fig. 3. Standard deviation values for 40 VEP signals over 61 channels. Solid line: the values with spatial average as baseline measure. Dotted line: the values without the use of spatial average.

Features were extracted for all 61 channels from every 1600 VEP signals. The VEP signals were filtered with pass-band width from 20 to 50 Hz using Elliptic filter. Forward and reverse operations were performed to ensure no phase distortion. The stop-band width of the filter was 1 Hz beyond the pass-band width on both sides. The filter orders were chosen to give a minimum of 20 dB attenuation in the stop-bands and a maximum of 0.1 dB ripple in the pass-bands.

Next, powers of these filtered signals from each channel were computed as features to form a feature vector of 61 values.



(a)



(b)

Fig. 4. Example of VEP (a) before filtering (b) after filtering.

IV. AUTHENTICATION PROCEDURE

The 1600 feature vectors (each with length 61) were split into

- Train patterns using 10 randomly selected client feature vectors;
- Validation patterns using 10 randomly selected client feature vectors (with no overlap to train patterns);
- Test patterns using 20 remaining client feature vectors and all 1560 impostor feature vectors.

The Manhanttan (city block) distances *D*, were computed between 10 validation patterns and 10 training patterns. Next, *Dmax* and *Dmin*, the maximum and minimum validation-training distances for each validation pattern were computed. Thresholds, Th_1 and Th_2 were obtained using

$$Th_1 = \min(D\min) \text{ and } Th_2 = \max(D\max)\,. \qquad (2)$$

The Th_1 will be useful in reducing FAE, i.e. reducing the error of wrongly accepting impostors as clients while *Th2* will be useful in reducing FRE, i.e. reducing the error of wrongly rejecting the clients as impostors.

The *Dt*, Manhanttan distances of the 1580 test patterns from the 10 training patterns were computed. Next, maximum and minimum of these *Dt, Dtmax* and *Dtmin* were computed.

The threshold Th_1 was used to determine whether each pattern was client or impostor using the rule that the test pattern belonged to the client category if $Dtmax<Th_1$. Else, the test pattern was detected as from the impostor category. The focus of this authentication level was to reduce FAE only. No doubt, the FRE would be very high but the 2nd level authentication would solve this problem.

This level was used only for those test patterns that were detected as impostors. The threshold Th_2 was used to determine whether the test patterns detected as impostors from 1st level authentication were really clients or impostors. Client was detected if $Dtmin<Th_2$. Else, it was impostor. The focus of this level was to reduce FRE. Next, FRE and FAE were computed using

$$\begin{aligned}&\textit{FRE=(no. of client patterns incorrectly detected as}\\&\qquad\textit{impostor patterns/20)*100\%;}\\&\textit{FAE=(no. of impostors patterns incorrectly detected}\\&\qquad\textit{as client patterns/1560)\%100\%.}\end{aligned} \qquad (3)$$

It should be noted here that there was no overlap between the test, validation or training patterns. This was no ensure that accurate FRE and FAE would be reflected. A cross validation (CV) was conducted to ensure the reliability of the results. These steps were repeated four times with different train, validation and test patterns from client feature vectors. Test feature vectors from impostor VEP data remained the same. The averaged FAE and FRE from the cross validations were stored. Figure 5 shows a block diagram of these steps.

These steps were repeated for every subject. When a subject was being considered for authentication, 40 feature vectors from the subject were treated as client data while the rest 1560 feature vectors were treated as impostor data.

V. RESULTS AND DISCUSSION

Figure 6 shows the results of the experimental study. As mentioned earlier, the FAE and FRE were obtained using the two-threshold procedure with CV. All the subject gave perfect accuracy in rejecting impostors (i.e. zero FAEs). FREs for most of the subjects were less than 5%, with only four subjects giving more than 20%.

The overall mean (std) of FRE from all the subjects was 3.5(6.9)%. Since the FAE from all the subjects were 0, the overall mean (std) of FAE was 0. A lower FAE is generally accepted as more important than corresponding FRE as it is more important to prevent any impostors from cheating as clients rather than having some clients turned away as impostors. The zero FAEs result show that the proposed authentication procedure could prevent any impostors from cheating as clients, while maintaining a high level of client detection.

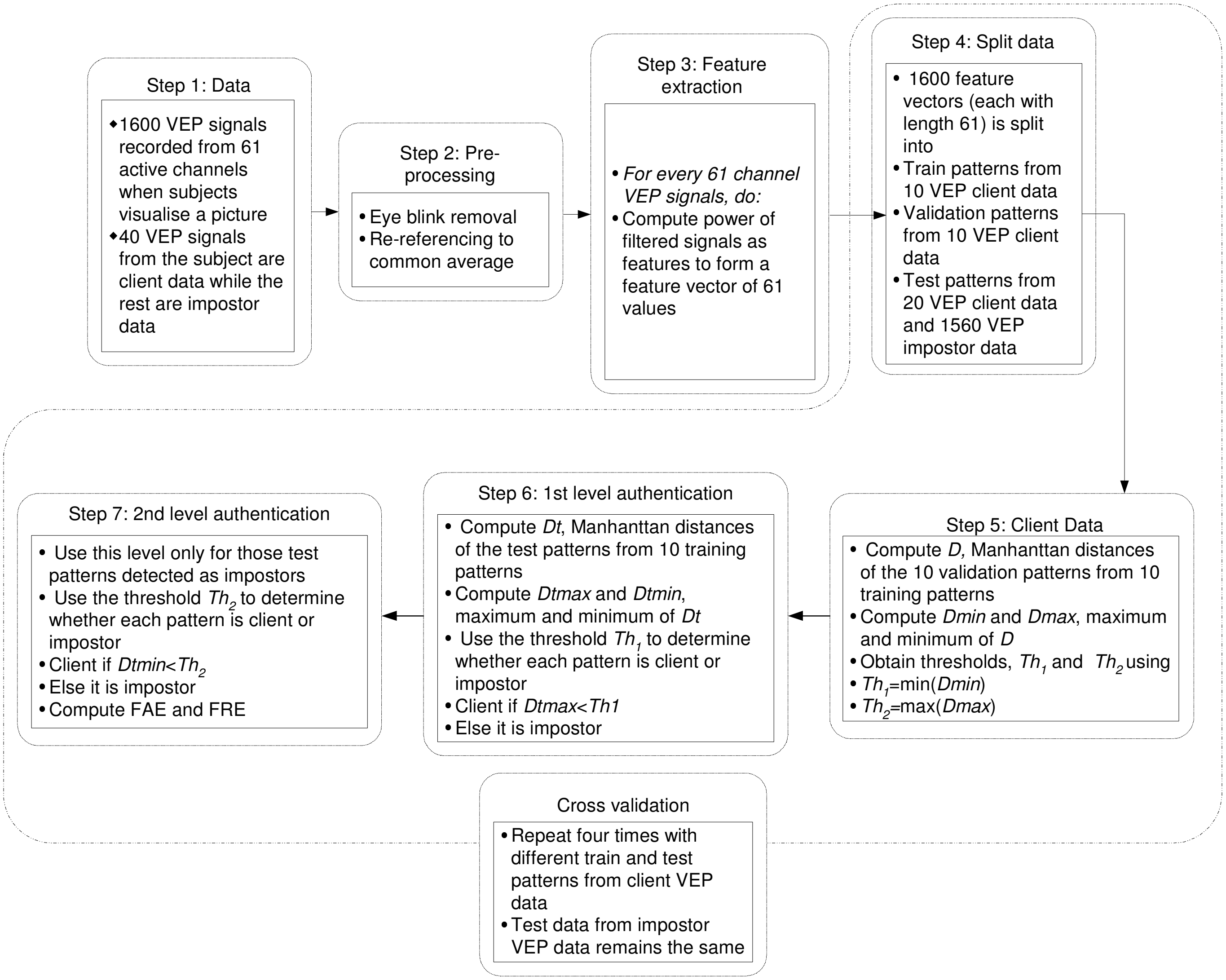

Step 1: Data
•1600 VEP signals recorded from 61 active channels when subjects visualise a picture
•40 VEP signals from the subject are client data while the rest are impostor data
Step 2: Pre-processing
• Eye blink removal
• Re-referencing to common average
Step 3: Feature extraction
• For every 61 channel VEP signals, do:
• Compute power of filtered signals as features to form a feature vector of 61 values
Step 4: Split data
• 1600 feature vectors (each with length 61) is split into
• Train patterns from 10 VEP client data
• Validation patterns from 10 VEP client data
• Test patterns from 20 VEP client data and 1560 VEP impostor data
Step 5: Client Data
• Compute D, Manhanttan distances of the 10 validation patterns from 10 training patterns
• Compute Dmin and Dmax, maximum and minimum of D
• Obtain thresholds, Th1 and Th2 using
• Th1=min(Dmin)
• Th2=max(Dmax)
Step 6: 1st level authentication
• Compute Dt, Manhanttan distances of the test patterns from 10 training patterns
• Compute Dtmax and Dtmin, maximum and minimum of Dt
• Use the threshold Th1 to determine whether each pattern is client or impostor
• Client if Dtmax<Th1
• Else it is impostor
Step 7: 2nd level authentication
• Use this level only for those test patterns detected as impostors
• Use the threshold Th2 to determine whether each pattern is client or impostor
• Client if Dtmin<Th2
• Else it is impostor
• Compute FAE and FRE
Cross validation
• Repeat four times with different train and test patterns from client VEP data
• Test data from impostor VEP data remains the same

Fig. 5. Steps in the proposed method.

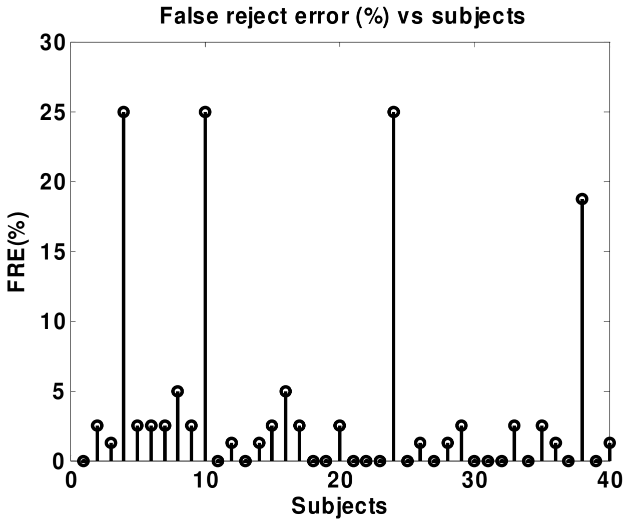


Fig. 6. Experimental FAE results

VI. CONCLUSION

In this paper, a novel method using brain signals has been proposed to authenticate the claimed identity of a user. The novelty of the method lies in the two-stage authentication procedure. Though there are difficulties in recording the brain signal (for example the use of wet electrodes, pre-setup preparatory time, etc.), the overall low FAE and FRE error rates indicate that this modality is worth further exploration especially since it has high fraud resistance.

VII. ACKNOWLEDGMENT

The author is grateful to Prof. Henri Begleiter from the Neurodynamics Laboratory, State University of New York Health Center, Brooklyn, USA, who recorded the raw VEP data and Mr. Paul Conlon, of Sasco Hill Research, USA for sending the data.

V. REFERENCES

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

[2] A.K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, pp. 4-20, vol. 14, no. 1, 2004.

[3] D. Hurley, M. Nixon, and J. Carter, "Force field feature extraction for ear biometrics," *Computer Vision and Image Understanding*, vol. 98, no. 3, pp. 491-512, 2005.

[4] L. Biel, O. Pettersson, L. Philipson, and P. Wide, "ECG analysis: a new approach in human identification," *IEEE Transactions on Instrument and Measurement*, vol. 50, no.3 pp. 808-812, 2001.

[5] R.B. Paranjape, J. Mahovsky, L. Benedicenti, and Z. Koles, "The electroencephalogram as a biometric," *in Proceedings on Canadian Conference on Electrical and Computer Engineering*, 2001, vol. 2, pp. 1363-1366.

[6] M. Poulos, M. Rangoussi, V. Chrissikopoulos, and A. Evangelou, "Person identification based on parametric processing of the EEG," *in Proceedings on IEEE International Conference on Electronics, Circuits, and Systems*, 1999, vol. 1, pp. 283-286.

[7] R. Palaniappan, "Method of identifying individuals using VEP signals and neural network," *IEE Proceedings - Science, Measurement and Technology*, vol. 151, no. 1, pp.16-20, 2004.

[8] X.L. Zhang, H. Begleiter, B. Porjesz, W. Wang, and A. Litke, "Event related potentials during object recognition tasks," *Brain Research Bulletin*, vol. 38, no. 6, pp. 531-538, 1995.

[9] K.E. Misulis, *Spehlmann's Evoked Potential Primer: Visual, Auditory and Somatosensory Evoked Potentials in Clinical Diagnosis,* Butterworth-Heinemann, 1994.