INTRODUCTION

The most common biometric method to identify the individuals is through fingerprint [1] recognition. In recent years, there has been significant interest in using other biometrics for identifying individuals. These include techniques that rely on:- DNA, hand geometry, palm print, face (both optical and infrared), iris, retina, signature, ear shape, odor, keystroke entry pattern, gait, and voice [2]. Other emerging biometrics such as ear force fields [3], heart signals [4], and electroencephalogram (EEG) or brain signals [5-7] have also been proposed in recent years. As signal recording from the brain is rather complicated, biometrics based on brain signals has not been studied extensively though it is one of the most fraud resistant biometrics.

As the EEG based method uses features computed from 61 Visual Evoked Potential (VEP) signals, it is unlikely that different persons will have similar activity in all parts of the brain. Thus VEP signals are most suitable for identification of individuals. Fischer Discriminant Ratio (FDR) has been used to find the optimal EEG channels to reduce the computational time. However, the fusion of Genetic Algorithm (GA) with Linear Discriminant Analysis (LDA) classifier shows that the identification performance is improved compared to FDR.

As for bio-encryption, generic cryptographic system is possession based, where possession of decrypting key is sufficient to decrypt the cipher text into plaintext. As most of the cryptographic keys are lengthy and in random order, they are normally stored on a computer or smart card and released through simple password authentication [8]. As different persons have different thought processes, the generated key is unique to each individual and hence the encryption is robust to fraudulent attacks as compared to other encryption systems. Biometric cryptosystems are obviously more advantageous compared to generic cryptographic systems as the encrypting key is more difficult to be stolen or compromised.
Thus, the objective of this study is to identify the feasibility of using brain signals to identify the individuals and to generate biometric cryptographic key for encryption and decryption process.

**VEP Data**

To obtain EEG signals in gamma frequency range, filtering was performed, and the energies of these filtered signals were used as a set of features. The EEG signals were recorded from subjects while being exposed to a stimulus, which consist of drawings of objects chosen from Snodgrass and Vanderwart picture set [9]. These pictures represent common black and white objects, such as, for instance, airplane, banana, and ball. The subjects (totalling 40) were seated in a reclining chair located in a sound attenuated RF shielded room. Measurements were taken from 61 active channels placed on the subject’s scalp, sampled at 256 Hz. The subjects were asked to remember or recognise the stimulus. Stimulus duration of every picture was 300 ms with an inter-trial interval of 5.1s. All the stimuli were shown using a display located 1 meter away from the subjects. One-second EEG measurements after each stimulus onset were stored. Figure 1 illustrates a stimulus presentation.

![Figure 1. Example of visual stimulus presentation](image)

EEG signals contaminated with eye blink artifacts were not considered in the classification, and were detected using a 100 $\mu$V threshold. This is a common threshold value in EEG studies, and is used since blinking produces 100-200 $\mu$V potential lasting 250 milliseconds [10]. A total of 40 artifact free trials were considered for every subject, to make a total 1600 EEG data sets. The EEG signals were filtered using a forward and reverse Elliptic band-pass digital filter, to obtain zero phase distortion. The 3-dB pass-band was chosen to be between 30 and...
50Hz, whereas the stop-band was fixed at 28 and 52 Hz. The minimum stop-band attenuation was set at 20 dB. To form the EEG features, the energy of the EEG signal from each channel was computed and normalised according to the total energy from all 61 channels.

**Methodology**

1. **LDA Classifier**

   This classifier uses hyperplanes to separate the input vectors (features) into different classes (Duda et al, 2001). For a two-class problem with two features, the boundary is simply a straight line. For classifying several classes, the general strategy is multi-levels of 'one versus the rest' classification though one level of multi-class classification is also possible with the generation of several hyperplanes. LDA is simple to use and in general gives acceptable levels of performance (Lotte et al, 2007) though VEP data is generally non-linear but its low complexity makes it particularly suitable for VEP based biometric systems.

2. **Optimal Channel Selection**

   Channel optimization is used to select channels or electrodes that are discriminatory to minimize the number of channels while maintaining similar individual identification performance using EEG biometric with reduced computation time. This study focused by using FDR and fusion of GA with LDC.

**FDR**

FDR was used to select the optimal channels for Fuzzy ARTMAP classification of individuals using Gamma Band Power (GBP) of VEP signals. The higher FDR values denote channels that were more discriminatory between the classes. The following relation shows the FDR function:

\[
FDR_k = \sum_{i=1}^{N} \sum_{j=1}^{N} \frac{(\mu_i^k - \mu_j^k)^2}{(\sigma_i^k)^2 + (\sigma_j^k)^2}
\]
where $N$ is the number of classes i.e. 40 subjects, $\mu^i_k$ is the mean of $k^{th}$ feature for $i^{th}$ class, $\sigma^i_k$ is the standard deviation of the $k^{th}$ for $i^{th}$ class and $i$ is varied from 1 to 40 subjects. The optimal channel set (27 channels) provides improved performance with lower computation time when compared to 61 channels [11].

**GA with LDC**

In this study, the dataset of 40 patterns from each subject is split randomly into four non-overlapping sets with each consisting of 10 patterns, i.e. each dataset consist of 400 patterns. GA uses datasets 1 and 2. LDC is used with datasets 3 and 4, which GA has not seen earlier. Classification is performed using a 20 fold equal class cross validation procedure. From the results it is evident that, by using only 23 channels instead of 61 channels will reduce the design complexity and lower in computation time. By comparing the performance with FDR, GA with LDC yields better performance [12].

**Classifier Selection**

In this study, the following classifiers are used to identify the individuals using VEP signals:

- Multilayer Perceptron – Backpropogation (MLP-BP) [3]
- Simplified fuzzy ARTMAP (SFA) [5, 13 & 14]
- Linear Discriminant Analysis (LDA) [15]
- Elman Backpropagation Network (EBP) [16]
- Grow and Learn Network (GAL) [17]
- k-Nearest Neighbour (k-NN) [14,15]

From the experimental results, it shows that, EBP gives better performance. Cross validation was used to ensure the reliability of the results.
Biometric Cryptosystem

Basic Biometric Cryptosystem using EEG signals

A novel method of data encryption using event-related EEG has been studied [18]. EEG from gamma band spectral range from specific channels was used to generate the biometric encryption key. This key was then used to shuffle leaf nodes in the Huffman tree generated from the data with Huffman coding, thereby changing the codewords that would be necessary during decoding. The complete key generation process takes slightly more than one second (therefore comparable to any other bio-encryption method) and combined with the simple but effective Huffman tree shuffling/de-shuffling, the whole procedure is fast enough for system implementation.

Improved EEG Cryptosystem using Elman Neural Network

An EEG based bio-cryptosystem has been proposed. In this approach, EEG from gamma band spectral range was used as inputs to ENN to generate the encryption key [19]. This key was then used to shuffle leaf nodes in the Huffman tree generated from the data with Huffman coding, thereby changing the codewords that would be necessary during decoding. The complete key generation process takes slightly more than one second (therefore comparable to any other bio-encryption method) and combined with the simple but effective Huffman tree shuffling/de-shuffling, the whole procedure is fast enough for system implementation.

Conclusion

Since, individual thought process is different from others it is possible to identify the individuals using their brain signals and to generate a key for biometric cryptographic systems. Though it is a tedious process to record the EEG signals, the use of active electrodes simplifies the set-up and minimises the preparation time. Also, dry electrodes (that do not require any wet gel to achieve the necessary impedance) are being investigated. So, though currently, it is cumbersome, the recording procedure will be simpler in future and the fraud resistance will outweigh any difficulty and the study shows that it would be used in multimodal biometric applications to improve the security.
Acknowledgement

I thank the late Prof. Henri Begleiter at the Neurodynamics Laboratory at the State University of New York Health Centre at Brooklyn, USA who generated the raw VEP data and Mr. Paul Conlon, of Sasco Hill Research, USA for sending the data.

References


