Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Neurokey: Towards a new paradigm of cancelable biometrics-based key generation using electroencephalograms

Garima Bajwa [*], *Ram Dantu*

Department of Computer Science and Engineering, University of North Texas, Denton, TX 76203, USA

ARTICLE INFO

Article history:
Received 24 July 2015
Received in revised form 17 April 2016
Accepted 7 June 2016
Available online 15 June 2016

Keywords:
Authentication
Biometrics
Cryptography
Cryptographic keys
Electroencephalograms
Key generation
Security

ABSTRACT

Background. Brain waves (electroencephalograms, EEG) can provide conscious, continuous human authentication for the proposed system. The advantage of brainwave biometry is that it is nearly impossible to forge or duplicate as the neuronal activity of people are distinctive even when they think about the same thing. *Aim*. We propose exploiting the brain as a biometric physical unclonable function (PUF). A user's EEG signals can be used to generate a unique and repeatable key that is resistant to cryptanalysis and eavesdropping, even against an adversary who obtains all the information regarding the system. Another objective is to implement a simplistic approach of cancelable biometrics by altering one's thoughts. *Method*. Features for the first step, Subject Authentication, are obtained from each task using the energy bands obtained from discrete Fourier transform and discrete wavelet transform. The second step constituting the Neurokey generation involves feature selection using normalized thresholds and segmentation window protocol. *Results*. We applied our methods to two datasets, the first based on five mental activities by seven subjects (325 samples) and the second based on three visually evoked tasks by 120 subjects (10,861 samples). These datasets were used to analyze the key generation process because they varied in the nature of data acquisition, environment, and activities. We determined the feasibility of our system using a smaller dataset first. We obtained a mean subject classification of 98.46% and 91.05% for Dataset I and Dataset II respectively. After an appropriate choice of features, the mean half total error rate for generating Neurokeys was 3.05% for Dataset I and 4.53% for Dataset II, averaged over the subjects, tasks, and electrodes. A unique key was established for each subject and task, and the error rates were analyzed for the Neurokey generation protocol. NIST statistical suite of randomness tests were applied on all the sequences obtained from the Neurokey generation process. *Conclusions*. A consistent, unique key for each subject can be obtained using EEG signals by collecting data from distinguishable cognitive activities. Moreover, the Neurokey can be changed easily by performing a different cognitive task, providing a means to change the biometrics in case of a compromise (cancelable).

[*] Corresponding author.
E-mail addresses: garimabajwa@my.unt.edu (G. Bajwa), rdantu@unt.edu (R. Dantu).

http://dx.doi.org/10.1016/j.cose.2016.06.001
0167-4048/© 2016 Elsevier Ltd. All rights reserved.

1. Introduction

The design of cryptographic systems has two parts; a cryptographic algorithm (complex mathematical function) and a cryptographic key. According to Kerckhoffs' principle, a cryptosystem should be secure even if everything about the system, except the key, is public knowledge (Petitcolas, 2011). Hence, the strength of the cryptographic systems depends on the secrecy of the weakest link, i.e., cryptographic keys (crypto keys). The majority of encryption algorithms desire long, random keys that are difficult to memorize. Alternately, these crypto keys are stored in a database and released upon presentation of an authentication token (password). Such a scenario increases the likelihood of tokens being compromised by sharing (willfully or coercively), losing or stealing.

Generating truly random numbers to be used as cryptographic keys has been an age old problem. Biometrics alleviates the problem of remembering passwords or PINs, providing a stronger defense against repudiation. It is significantly harder to forge, copy, share, and distribute biometrics compared to passwords or PINs (Jain et al., 2004). The authors believe that strong cryptographically secure keys can be obtained from biometric-dependent key generation systems given the appropriate selection of enrollment schemes, feature descriptors/vectors, and entropy mixers as surveyed by Rathgeb and Uhl (2011). Advancements in biometrics-based cryptographic systems provide a better solution to the key management practices that address the security weakness of conventional key release systems using passcodes, tokens or pattern recognition (Zheng et al., 2006). Biometrics such as iris recognition, fingerprints, voice, hand geometry, and facial recognition are being employed at present to derive cryptographic keys (Jain et al., 2008; Uludag et al., 2004). The immutability and non-repudiability of these biometrics make them a strong tool for biometric-dependent key generation systems (Bolle et al., 2002; Dodis et al., 2004).

For an individual, the number of biometric features is limited. We only have ten fingerprints, a single set of face features, and two iris images. Though it is hard to replicate these biometrics, the key problem is that once they are compromised, there are not many alternatives. Thus, the present biometric key generation (BKG) systems suffer from the problem of permanent loss of one's biometric feature in case of a compromise by an adversary, and a user may run out of their limited unique identity features. The advantage of using other forms of cryptographic generators such as password-based or thermal noise is that they can be revoked and re-issued in the case of a breach. This is not a natural advantage in biometrics-based cryptosystems. If a person's DNA is compromised in the database, it is impossible to create a different cryptographic key. To overcome this, the system of cancelable biometrics has emerged.

Ratha et al. (2001) first introduced the system of cancelable biometrics where distortions on the biometric features are varied to provide various versions of a biometric template. As a result, it can be revoked or changed like generic passwords and yet remain unique for intended applications. The catch here is that the "evil eve" can still plan a feasible attack based on the auxiliary or helper distortion data. Hence, it is extremely challenging for cancelable biometrics to scale up to both performance and non-invertibility of transformed features (Cheung et al., 2005; Jin and Hui, 2010).

We propose a biometric key generation approach using the human brain waves (electroencephalograms – EEG signals) as a solution to this problem. The brain is what gives a sense of identity and a unique personality to a person. The brain sits at the head of the human body, both literally and figuratively, controlling and regulating all bodily processes. It achieves this by sending electric signals through neurons (nerve cells) to all parts of the body, and in turn receiving signals from them through the same route. The unique patterns of the electrical activity form the language of the brain. These electric pulses can be most easily detected on the scalp as changes in electric potentials due to currents flowing through scalp tissue, arising from synchronous activity/firing of neurons. This process of measuring electric potentials at the scalp is called Electroencephalography (EEG). EEG measurements vary depending on a person's state of mind, the activity being performed, and his/her mood. A set of measurements made during a particular activity represents an individual's brain state for that activity. Brain state not only varies from activity to activity, but also from person to person. Thus, an individual's brain state is his/her unique signature, just like his/her fingerprints or DNA.

1.1. *Motivation*

Noninvasive brain-computer interfaces (BCI) have enhanced our capabilities to study the neural circuits and utilize them for applications ranging from those in the medical field like neuroprosthetics to entertainment like neurogaming. In this paper, we propose a new modality for generating crypto keys (Neurokeys) from an individual's EEG signals while a subject performs certain mental tasks. As the tasks can be easily substituted by altering the passthoughts (Thorpe et al., 2005), these EEG signals extend a simplistic approach to implementing cancelable biometrics-based crypto key generation. Empirical reasons to exploit EEG for a plausible Neurokey are as follows:

- *Physical unclonable function (PUF)*: EEGs are nearly impossible to forge because the neuronal wiring of each person is unique and will result in a different pattern of EEG between subjects while performing similar mental activities (Zhao et al., 2010) analogous to PUFs.
- *Cancelable*: EEG readings enable us to develop cancelable biometric keys since taking a reading requires having the user engage in a specific cognitive task that can be changed if the user's biometric information is compromised.
- *Entropy*: The measured EEG biometrics have a high entropy across populations, i.e. the amount of uncertainty in the key from an adversary's point of view is large.
- *Coercion Attack*: Biometric keys from EEG signals could possibly provide prevention under coercion attacks as the brain responses change under threat (DeLaRosa et al., 2014; Öhman, 2005). Gupta and Gao (2010) showed that detecting changes in a user's skin conductance provided good resistance against coercion attacks when the keys were generated using both voice and skin conductance.

We believe our breakthrough idea will interest a diverse research community including machine learning, cryptography, and computer security.

1.2. *Problem definition*

The goal of this research initiative is to provide portable, on-the-go, cognitive keys with a possibility of regeneration even on mobile devices. This eliminates the problem of key management for encryption of user-specific data which can now be protected by the Neurokey obtained from one's EEG signals. The solution to the following research question is intended: *Can we consistently generate a Neurokey in any environment to differentiate between individuals based on their cognitive activity?* We aim to validate how the existing challenges affect the usefulness of EEG signals as a key generation scheme.

2. Related work

There are four fundamental requirements to use a biometric as a cryptographic key generation system (Jain et al., 2004). *Universality*: it should be possible to generate keys from the biometric features of all individuals. *Uniqueness*: the system should be able to separate keys of different persons with a reasonably low failure probability. *Consistency*: biometric characteristics of the individuals should remain fairly constant for a reasonable time. *Collectable*: biometric values should be easy to obtain, easy to quantify, and cause no discomfort.

EEG signals can be easily recorded using a headband containing dry or wet electrodes on a desktop or mobile device. Early works by Poulos et al. (1999) and Paranjape et al. (2001) studied the possibility of using the brain signals as a means for a new biometric authentication system. The theory of neurologists that the EEG carries genetic information of an individual (Anokhin et al., 1992; Lykken et al., 1974; Vogel, 1970) influenced their studies. Since then, several researchers have contributed toward establishing the feasibility of using EEG for biometric authentication systems, with a focus on improving the accuracy (Abdullah et al., 2010; Chang et al., 2004; He, 2009; Klonovs et al., 2013; Marcel and Millan, 2007; Nakanishi et al., 2009; Palaniappan and Ravi, 2003, 2006; Poulos et al., 2002; Revett et al., 2010).

On similar lines, Thorpe et al. (2005) describe a system that uses pass-thoughts as opposed to a conventional text-based password for user authentication, making it resistant to dictionary and shoulder-surfing attacks. Chuang et al. (2013) performed usability studies to advance the idea that consumer grade single electrodes in a non-clinical setting are sufficient to fulfill the requirements of accuracy for classification. Also, various mental tasks based on difficulty, enjoyability and recall ability were evaluated for the performance of the system. Another interesting work by Yeom et al. (2013) was based on the paradigm that unique subject-specific brain wave patterns exist in response to the visual stimuli of self and non-self face images. The validation of the stability of the EEG waves over time was established by comparing the inter-individual variation in spectral observations to the intra-individual stability over more than a year (Näpflin et al., 2007).

Only a few research studies have explored the possibility of employing the brain signals to generate keys for cryptographic applications. Palaniappan et al. (2011) present one of the early ideas about the use of EEG for PIN generation. Their system was based on P300 based BCI design incorporating an external visual stimulus paradigm. They identified Cz electrode to be appropriate, considering a limited number of trials. Lokeshwari et al. (2013) proposed data encryption using a genetic algorithm with EEG. Their system intends to feed a pseudorandom number generator with a seed obtained from EEG feature extraction. Their system represents a theoretical idea with a lack of implementation analysis.

2.1. *Contributions of the paper*

To our knowledge, no one has extensively studied the performance of a biometric system using EEG for both authentication and cryptographic key generation, utilizing different types of online EEG datasets varying in the nature of data collection, the number of electrodes, and the types of activities.

Our EEG key generation is based on a cascade system of EEG authentication followed by key generation. It is similar to a key binding system that binds a random key with a user's biometric data at the time of enrollment and releases the key upon successful authentication (Soutar et al., 1998; Uludag et al., 2004). The difference is that our system derives the random key also by using the subject's EEG biometrics itself. The inherent property of authentication ensures that the subject whose EEG signals are being used to generate his/her cryptographic key is the one whom he/she claims to be. An adversary also has to obtain access to both the authentic features and the feature vectors (of keys) to attack the system. It helps increase the overall resistance of the system to forgery as the key is never retrieved if the authentication fails.

The key generation scheme does not require original biometrics data to be stored. The feasibility of changing Neurokeys for the same subject by switching to a different mental activity is also studied, thus, providing a usable and comparable alternative to cancelable biometrics-based key generation schemes. In summary, the paper explores the following:

- empirical evaluation of using EEG for Neurokey generation
- experimental feasibility of using EEG for Neurokey generation
- potential as a cancelable biometrics-based key generation

3. System overview

Our proposed cancelable Neurokey generation scheme, shown in Fig. 1, has three phases:

Enrollment: In this phase, an individual establishes the authentic regions of his EEG features for a chosen activity using his training samples. These regions are stored as a template to authenticate later and generate the cryptographic keys. We shall not dig into the biometric template security in this paper (Ballard et al., 2008; Jain et al., 2008).

Authentication: The second part of the system will authenticate a subject using the classic biometric approach. The

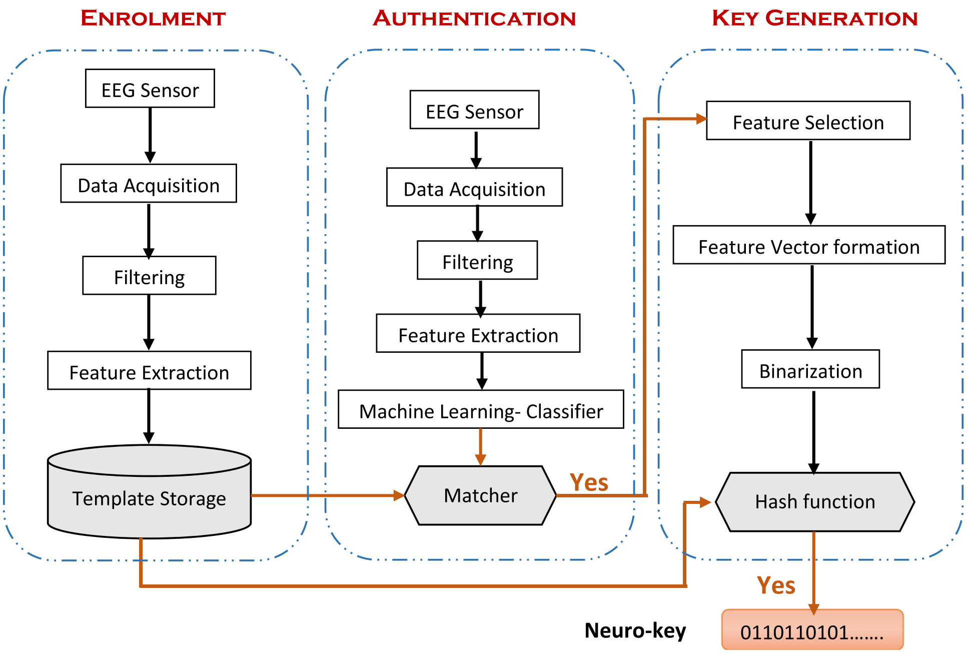


Fig. 1 – The flow of key generation from EEG of the subjects.

key is generated directly from the EEG features of an individual after the person has been authenticated using those same signals.

Key Generation: The key generation scheme does not require original biometrics data to be stored. It accepts the EEG signals of the established mental activity and generates the feature vectors after the appropriate feature selection. The feature vectors are binarized using the authentic regions of an individual in the template to generate the key. Though authentication phase is a screening process itself, the generated key is matched to the stored hash value of the genuine key to be accepted or rejected.

Lastly, the feasibility of changing a Neurokey for the same subject by switching to a different mental activity is also studied, thus providing a usable and comparable alternative to other distortion-based cancelable biometric key generation schemes.

4. Experimental data

Currently, the approaches to obtain biometrics from EEG data are derived from brain responses to either visually evoked stimuli or mental tasks. Our goal was to study the key generation process from such EEG datasets, varying in nature of data collection equipment, environment and activities, and their subsequent impact on the generation of keys.

In our investigation, we applied our methodology to two public EEG datasets to determine:

Dataset 1: Experimental feasibility using seven subjects dataset (mental task activations)
Dataset 2: System's general applicability using 120 subjects dataset (visually evoked stimuli)

4.1. *Dataset I*

This dataset has been obtained previously by Keirn and Aunon (Keirn, 1988; Keirn and Aunon, 1990; Brain-Computer Interfaces Laboratory). It consists of EEG signals from seven subjects performing five mental tasks. The tasks were chosen in a way to invoke hemispheric brainwave asymmetry.

4.1.1. *Task description*

The five mental tasks are described as follows:

Baseline Task: This task was considered as a reference or a base that was used to control and measure EEG signal activity. The subjects were asked not to engage in any specific mental task and relax as much as possible with very few movements, and to think of nothing in particular.
Letter Task: In this task the subjects were instructed to mentally compose a letter to a friend or relative without vocalizing it.
Math Task: The subjects were shown images consisting of some multiplication problems, such as 49 times 78, and were asked to solve them, again without vocalizing or making any physical movements.
Geometric Figure Rotation: The subjects were instructed to visualize a particular three-dimensional block figure being rotated about an axis.
Visual Counting: The subjects were asked to imagine a blackboard and to visualize numbers being written on the board sequentially.

4.1.2. *Data collection*

Signals were recorded from six channel placements C3, C4, P3, P4, O1, and O2 specified by 10–20 electrode placement via an Electro-Cap elastic electrode cap. The standard electrodes placement is shown in Fig. 2.

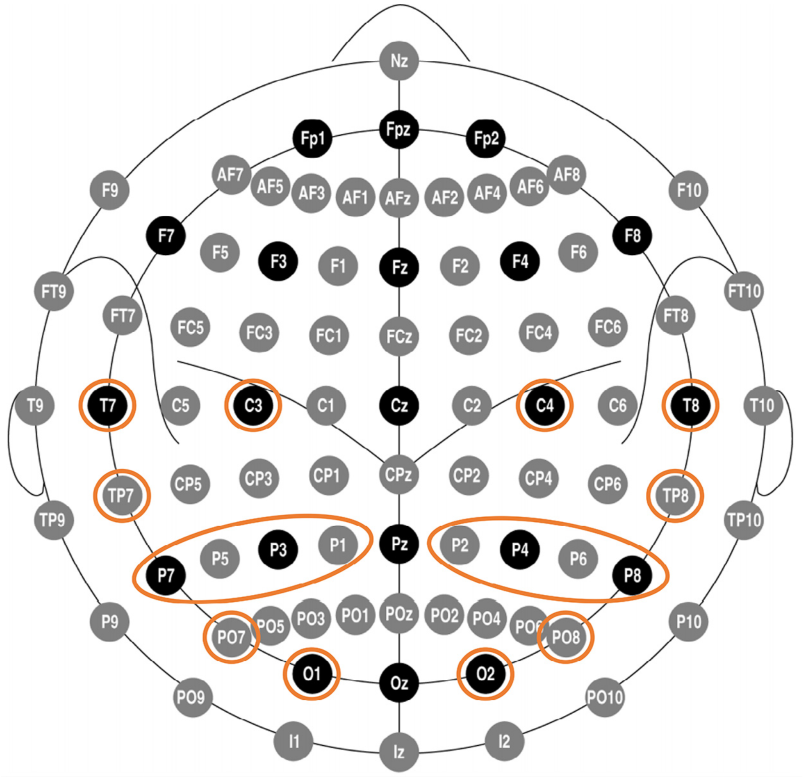


Fig. 2 – Black circles indicate positions of the original 10–20 system (Jasper, 1958), gray circles indicate additional positions introduced in the 10-10 extension (Oostenveld and Praamstra, 2001). The occipitotemporal region of interest is marked in color.

The subjects were asked to sit in a sound controlled booth with dim lighting and noiseless fans for ventilation. The electrodes were connected through a bank of Grass 7P511 amplifiers and band pass filters (0.1–100 Hz). Data recording was done at a sampling rate of 250 Hz with a Lab Master 12 bit A/D converter mounted in an IBM-AT computer. Eye blinks were detected using a separate channel of data recorded from two electrodes placed above and below the subject's left eye.

All tasks were performed with the subjects eyes open. Subject 1, left handed, aged 48, and Subject 2, right-handed, aged 39, were employees of a university. Subjects 3–7 were right-handed college students between the ages of 20 and 30. All were male subjects except Subject 5. They performed five trials of each task in one day. Each task lasted for 10 seconds, and they returned to do another five-trial session on a different day. Subjects 2 and 7 completed only one five-trial session. Subject 5 completed three such sessions and the rest completed only two sessions.

4.2. *Dataset II*

This dataset was taken from UC Irvine Machine Learning Repository (Ingber, 1997). It was collected to examine EEG correlates of genetic predisposition to alcoholism. The dataset is described below (Zhang et al., 1995).

4.2.1. *Task description*

There were two groups of subjects: alcoholic and control. Each subject was exposed to either a single visual stimulus (S1) or to two stimuli (S1 and S2). These stimuli were composed of pictures of objects obtained from the picture set of Snodgrass and Vanderwart (1980). In the case of second stimuli (S2), it was presented in either a matched condition where S1 was identical to S2 or in a non-matched condition where S2 differed from S1. The duration of each picture stimulus in each test trial was 300 ms. The interval between each trial was fixed to 3.2 s. The occurrence of matching and non-matching stimuli were randomized.

So, we divided the data into three sub-tasks; S1_task, S2_NoMatch, and S2_Match to study the generation of keys in these three scenarios. An important consideration is that we will generate the keys from 1 s of EEG data as compared to 10 s in the previous dataset. The comparison of datasets is given in Table 1.

Table 1 – Comparisons of the datasets.

Datasets	Dataset I	Dataset II
Subjects	7	120
Electrodes	6	64
Activities	5	3
Frequency	250 Hz	256 Hz
Total trials	325	10,861
Recording duration per trial per activity	10 s	1 s

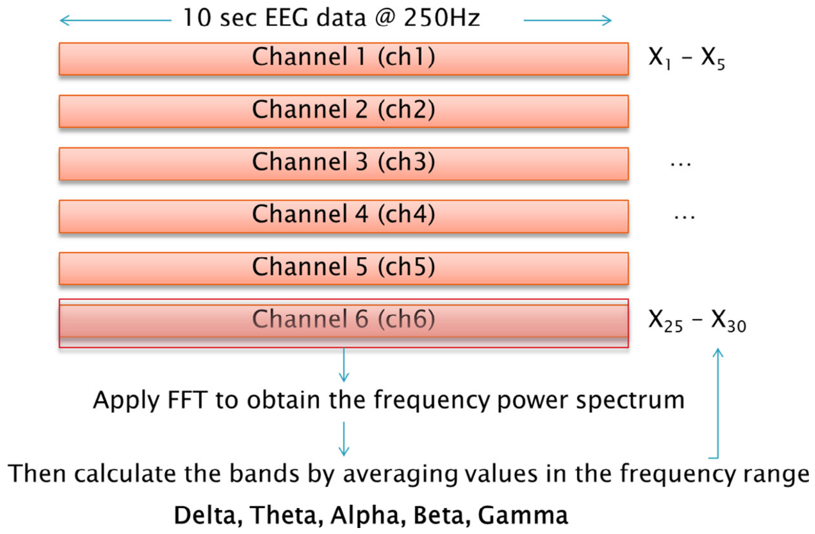

10 sec EEG data @ 250Hz
Channel 1 (ch1)
Channel 2 (ch2)
Channel 3 (ch3)
Channel 4 (ch4)
Channel 5 (ch5)
Channel 6 (ch6)
X1 – X5
…
…
X25 – X30
Apply FFT to obtain the frequency power spectrum
Then calculate the bands by averaging values in the frequency range
Delta, Theta, Alpha, Beta, Gamma

Fig. 3 – Process of FFT feature extraction from frequency distribution of different channels.

4.2.2. *Data collection*

The dataset contains EEG measurements from 64 electrodes placed on a subject's scalp at a sampling rate of 256 Hz for 1 second duration. There were 122 subjects and each subject completed 120 trials of the three visually evoked stimulus presented in a random fashion. We removed the data of two subjects as the EEG signals were noisy and contained many error trials. The data were recorded in a sound attenuated RF shielded room with the subject seated in a reclining chair. The signals were amplified with a gain of 10,000 by EpA2 amplifiers (Sensorium, Inc) with a bandpass between 0.02 and 50 Hz. Data readings involving eye and body movements (>73.3 uV) were rejected as noise.

5. Feature extraction process

Several methods can be used to extract features from the EEG signals. Different methods produce different size of feature vectors. We take advantage of both discrete Fourier transform (DFT) and discrete wavelet transform (DWT) to extract the relevant features from the EEG signals. DFT breaks down the signal into its constituent sinusoids of different frequencies whereas the DWT breaks the signal into its wavelets, using scaled and shifted versions of a mother wavelet. Wavelet properties of temporal localization and Fourier's frequency localization make them an ideal combination for extracting properties of non-stationary signals such as EEG.

5.1. *Discrete Fourier transform*

Time domain signal of each channel was converted into the frequency domain using fast Fourier transform (FFT), an efficient algorithm for computing the DFT of a sequence. The standard EEG frequency bands obtained are:

Delta (δ) – rhythmic activity between 1 and 4 Hz
Theta (θ) – rhythmic activity between 4 and 8 Hz
Alpha (α) – rhythmic activity between 8 and 12 Hz
Beta (β) – rhythmic activity between 12 and 30 Hz
Gamma (γ) – rhythmic activity between 30 and 44 Hz

These bands were calculated for each channel. Therefore, the FFT feature vector consisted of five features for an electrode. Fig. 3 shows the process of obtaining DFT features of subject classification for the authentication process.

5.2. *Discrete wavelet transform*

We used the Daubechies family of wavelets to create robust features for the subject classification. The general decomposition of the signal into its detail and approximate coefficients was achieved by applying a series of high and low pass filters to the signal. Fig. 4 shows the sequential application of the filters. Unlike FFT, DWT provides a time-frequency representation of the signal and the Daubechies wavelet's irregular shape and compact nature help in analyzing signals with discontinuities or sharp changes. Each wavelet characterized by the vanishing moments is used to represent the polynomial information in a signal. We compared "db4", "db6" and "db8" and found "db8" to be the most appropriate for capturing the underlying changes in the EEG signals. The decomposed coefficients at DWT levels have been approximated to the nearest standard EEG frequency bands as shown in Table 2.

Instead of using all the coefficients at each decomposition level, we extracted the following statistical information from the wavelet coefficients at every level.

- Mean of the absolute values of the coefficients in each level (both high and low sub-band)
- Average power of the wavelet coefficients in each sub-band
- Standard deviation of the coefficients in each sub-band

The DWT feature vector was composed of 18 features for an electrode (six energy bands × 3 statistical features per band). Thus, the combined DWT-FFT feature vector for a subject had 23 features per electrode.

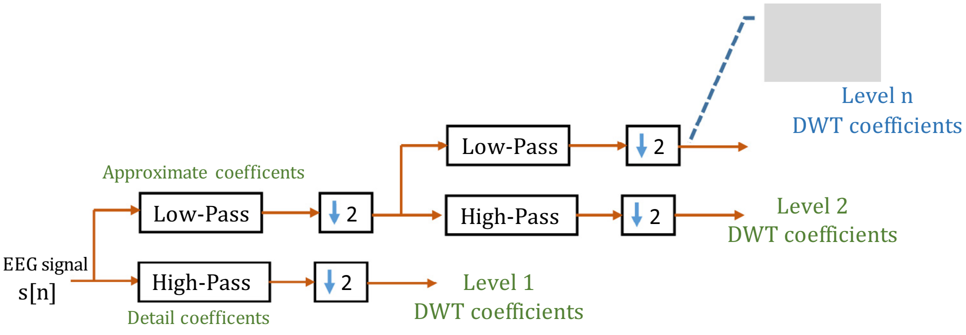


Fig. 4 – Decomposition structure of the discrete wavelet transform.

6. Authentication

6.1. Repeatability

Measurements of an individual's EEG samples taken at multiple time frames are almost never identical. We studied the problem of repeatability of the EEG biometrics for the identification process by using various sessions of EEG recordings, obtained at different time intervals (different days and times) for training and testing in the classifier. Random samples were chosen from the datasets, 66% as train set and rest as a test set, and classification was carried out using 10-fold cross validation. The mean of 10 such sampling processes were used to calculate the results. Similarly, the Neurokeys were tested by splitting the dataset into genuine and imposter users for each subject.

6.2. Classification

We performed discretization of feature vectors as another preprocessing step before the classification. Supervised discretization transforms numeric attributes to nominal attributes and takes into account the class labels as compared to unsupervised discretization like equal binning or frequency. The WEKA (Waikato Environment for Knowledge Analysis) tool was used to analyze the dataset (Hall et al.). The tool accepts ARFF (attribute relationship file format). Our MATLAB dataset in a cell array format was converted into appropriate ARFF for each of the feature extraction methods. For each of the ARFF file, two types of classification models, support vector machine and Bayesian network, were used.

Table 2 – Wavelet-decomposition level and EEG sub-bands relationship (A – approximate coefficients, D – detail coefficients).

Energy band	Frequency range (Hz)	Decomposition level
Delta	0–4	A5
Theta	4–8	D5
Alpha	8–16	D4
Beta	16–32	D3
Low gamma	32–64	D2
High gamma	64–128	D1

Support vector machine (SVM) was used as a classifier because of its accuracy and ability to separate the classes using the concept of hyperplane separation to the data, mapping the predictors onto a new, higher-dimensional space in which they can be separated linearly. The performance metrics were compared with Bayesian network classifier. Neural networks including multilayer perceptron took a considerably long time to build and classify and hence, not included in comparisons. The extracted features from each record were corresponding to the task performed by the subjects. Once the classification was performed, the results were analyzed, and the performances were compared using the following metrics.

$$Accuracy = \frac{T_p + T_n}{T_p + T_n + F_p + F_n} \quad (1)$$

$$Precision = \frac{Tp}{Tp + Fp} \quad (2)$$

$$Recall = \frac{Tp}{Tp + Fn} \quad (3)$$

$$F - measure = \frac{2 \cdot Precision \cdot Recall}{Precision + Recall} \quad (4)$$

where T_p = true positive, T_n = true negative, F_p = false positive and F_n = false negative.

We based our results on the datasets described in the previous section that consists of 325 records from Dataset I and 10,861 records from Dataset II. For Dataset II, the initial feature extraction was carried out with 61 electrodes (excluding the reference electrodes). Our aim was to empirically derive a subset of electrodes (features) in such a manner that it does not affect the subject classification significantly. In the dataset, the topographical distribution of the event-related potentials to picture stimuli containing objects was mainly located in the occipitotemporal area of the brain (Zhang et al., 1995) as shown in Fig. 2 (marked in color). We achieved a higher distinguishability in the activities using occipital, temporal and central lobes of the brain, compared to the other electrode positions.

Table 3 – Subject classification for each classifier across various tasks for Dataset I.

	Support vector machine			Bayesian network		
	Accuracy (%)	F-measure	ROC area	Accuracy (%)	F-measure	ROC area
Baseline	96.92	0.969	0.982	98.45	0.985	1
Count	98.46	0.985	1	100	1	1
Letter	96.92	0.968	1	95.38	0.953	0.999
Multiply	100	1	1	100	1	1
Rotation	100	1	1	100	1	1

We were able to isolate a subset of 18 electrodes from 61 electrodes (T7, T8, O1, O2, PO7, PO8, TP8, TP7, P3, P4, P5, P6, C3, C4, P8, P7, P1 and P2).

Table 3 shows the classification performance of Dataset I. Table 4 displays the classification accuracies and F-measures for successive empirical combination of electrodes for S1_task in Dataset II. Having empirically established the 18 best electrodes from this activity, the classification metrics for other activities of Dataset II were obtained only using these electrodes in Table 5. Measures were derived from the confusion matrix to evaluate the performance of the models using the metrics in Equations 1–4. Bayesian Network performed better for the smaller dataset (Dataset I) while SVM provided improved measures as the dataset became bigger (Dataset II).

7. Neurokey generation

The authentication ensures that the subject whose EEG signals are being used to generate his personal cryptographic key is the one who he claims to be. As stated before, the feature extraction process here should be different because the classifier used for subject authentication can handle variations in the values of the feature set. Contrary to this, even a small variation will change the key by a significant number of bits. The following subsections describe the feature selection and binary feature vectorization processes.

7.1. *Feature selection*

We used a similar approach by Chuang et al. (2013) to study the self-similarity within the subjects and cross-similarity among different subjects' EEG feature vectors across multiple trials. Self-similarity refers to similarity of the feature vectors arising from multiple trials of the same task within a subject. Cross-similarity measures similarity of the feature vectors arising from every combination of the trials of the same task between different subjects. The following equation represents a general case to determine similarity between feature vectors based on the cosine distance.

Table 4 – Subject classification with SVM for S1_task in Dataset II using successive empirical combination of electrodes.

Electrode combinations for classification	Accuracy (%)	F-measure	ROC area
T7 T8 O1 O2 PO7 PO8	80.81	0.803	0.803
T7 T8 O1 O2 PO7 PO8 P8 P7	82.63	0.822	0.912
T7 T8 O1 O2 PO7 PO8 PO1 PO2	82.20	0.817	0.91
T7 T8 O1 O2 PO7 PO8 TP8 TP7	85.61	0.852	0.927
T7 T8 O1 O2 PO7 PO8 TP8 TP7 P3 P4	86.81	0.865	0.933
T7 T8 O1 O2 PO7 PO8 TP8 TP7 P5 P6	88.97	0.887	0.944
T7 T8 O1 O2 PO7 PO8 TP8 TP7 P3 P4 P5 P6	89.70	0.895	0.948
T7 T8 O1 O2 PO7 PO8 TP8 TP7 P3 P4 P5 P6 C3 C4	90.91	0.907	0.954
T7 T8 O1 O2 PO7 PO8 TP8 TP7 P3 P4 P5 P6 C3 C4 P8 P7	91.22	0.911	0.956
T7 T8 O1 O2 PO7 PO8 TP8 TP7 P3 P4 P5 P6 C3 C4 POZ OZ	90.94	0.907	0.961
T7 T8 O1 O2 PO7 PO8 TP8 TP7 P3 P4 P5 P6 C3 C4 P8 P7 PO1 PO2	90.96	0.908	0.954
T7 T8 O1 O2 PO7 PO8 TP8 TP7 P3 P4 P5 P6 C3 C4 P8 P7 P1 P2	**92.28**	**0.921**	**0.954**
FP1 FP2 F7 F8 AF1 AF2 FZ F4 F3 FC6 FC5 FC2 FC1 T8 T7 CZ C3 C4	79.56	0.794	0.813
F7 F8 AF1 AF2 FZ F4 F3 FC6 FC5 FC2 FC1 T8 T7 CZ C3 C4 CP5 CP6	75.27	0.7515	0.787
AF1 AF2 FZ F4 F3 FC6 FC5 FC2 FC1 T8 T7 CZ C3 C4 CP5 CP6 CP1 CP2	74.14	0.741	0.752
FZ F4 F3 FC6 FC5 FC2 FC1 T8 T7 CZ C3 C4 CP5 CP6 CP1 CP2 P3 P4	82.70	0.8235	0.844
All electrodes	96.17	0.961	0.981

Table 5 – Subject classification for each classifier across various tasks for Dataset II.

	Support vector machine			Bayesian network		
	Accuracy (%)	F-measure	ROC area	Accuracy (%)	F-measure	ROC area
S1_task	92.28	0.921	0.954	87.46	0.875	0.993
S2_NoMatch	90.45	0.899	0.952	87.54	0.876	0.995
S2_Match	90.43	0.898	0.952	88.22	0.882	0.995

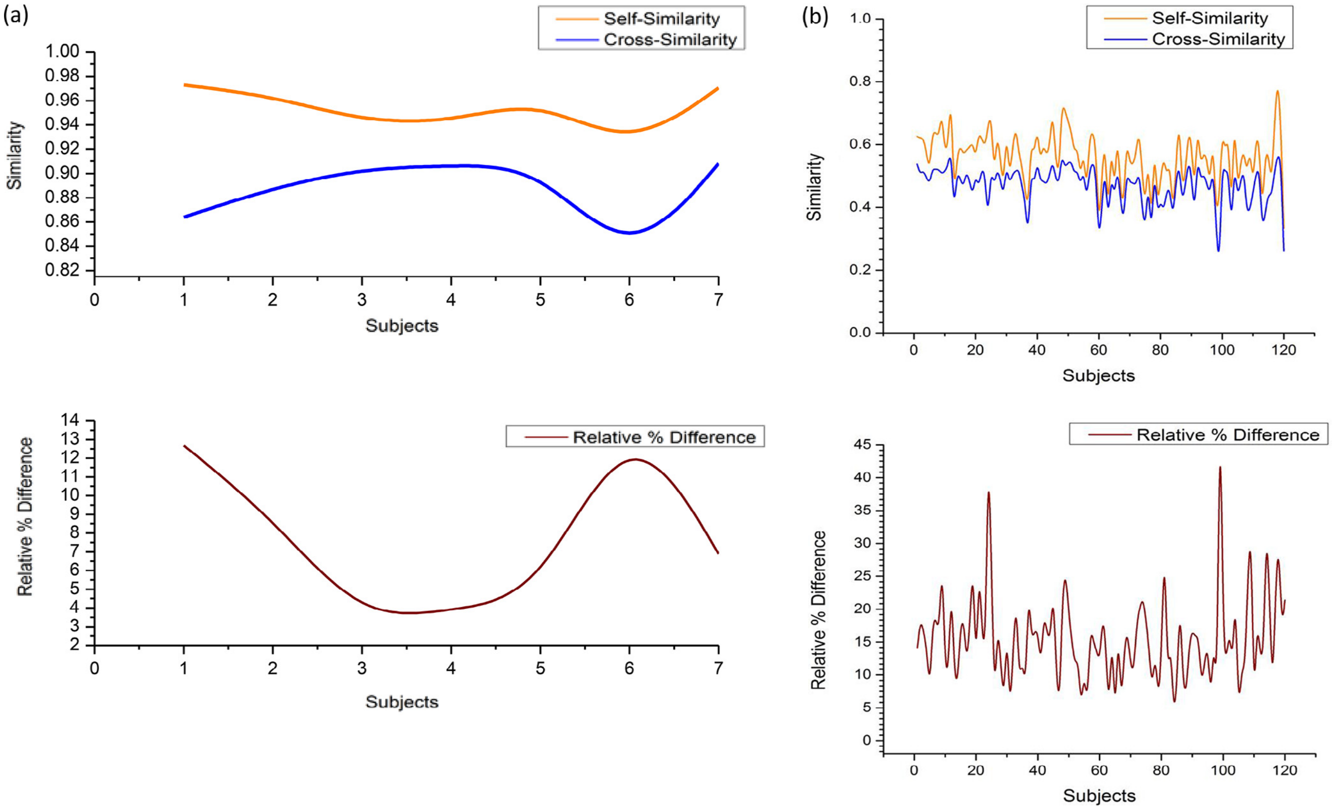


Fig. 5 – Similarity scores obtained across each subject of the Dataset I (a) and Dataset II (b).

$$similarity = \cos(\Theta) = \frac{A \cdot B}{\|A\|\|B\|} = \frac{\sum_{i=1}^{n} A_i \times B_i}{\sqrt{\sum_{i=1}^{n} A_i^2} \times \sqrt{\sum_{i=1}^{n} B_i^2}} \tag{5}$$

$$if \quad A == B : self\text{-}similarity, \quad A \neq B : cross\text{-}similarity$$

Fig. 5a and b shows the self-similarity and cross-similarity scores for both the datasets averaged over the tasks. The self-similarity scores were higher than the cross-similarity across all the subjects. The relative percentage difference between the two scores was used to determine the distinguishability between the feature vectors. The subjects that scored low on self-similarity also showed less relative percentage difference to cross similarity. This is a probable contributing factor to false acceptance rates in the system. As observed by Chuang et al. (2013), there was a good variation between the subjects for the relative difference scores. This difference was useful in deriving a unique key for a person's authenticated feature region.

The distribution of feature vectors for every subject was obtained from the training samples of each mental activity. We assumed that these distributions would also be distinguishable if the feature vectors of the subjects could be differentiated based on the variations in relative percentage difference of the similarity scores. The global feature segmentation protocol used to generate the Neurokeys was adopted from Chang et al. (2004) who extended the original Monrose et al. (2001) scheme of stable key generation. The procedure for the approach is as follows:

- First, the features were calculated from the time domain EEG signals using FFT and DWT across all electrodes, activities and subjects. Feature vectors for key generation from each electrode were formed by

$$Feature\_vector = \frac{(\delta)^3 + (\theta)^3 + (\alpha)^3 + (\beta)^3 + (\gamma)^3}{(\delta) + (\theta) + (\alpha) + (\beta) + (\gamma)} \tag{6}$$

- The distribution of feature vectors for each electrode and activity was obtained from the training samples of a subject and parameters such as mean and standard deviation were calculated for each distribution.
- The width of the global distribution was defined using the global mean and standard deviation via a segmentation parameter, k_seg.

$$Window\_start = \mu_{global} - k\_seg \times \sigma_{global}$$
$$Window\_end = \mu_{global} + k\_seg \times \sigma_{global}$$

- Equiprobable interval bins were derived in the global distribution using the authentication region of each subject's feature vector.

$$Auth\_region_{(sub,feature)} = [\mu_{sub,feature} - k_{sub,feature} \times \sigma_{sub,feature}, \; \mu_{sub,feature} + k_{sub,feature} \times \sigma_{sub,feature}]$$

The maximum value of $k_{sub,feature}$ parameter was calculated using the distinguishability criterion (Chang et al., 2004) as

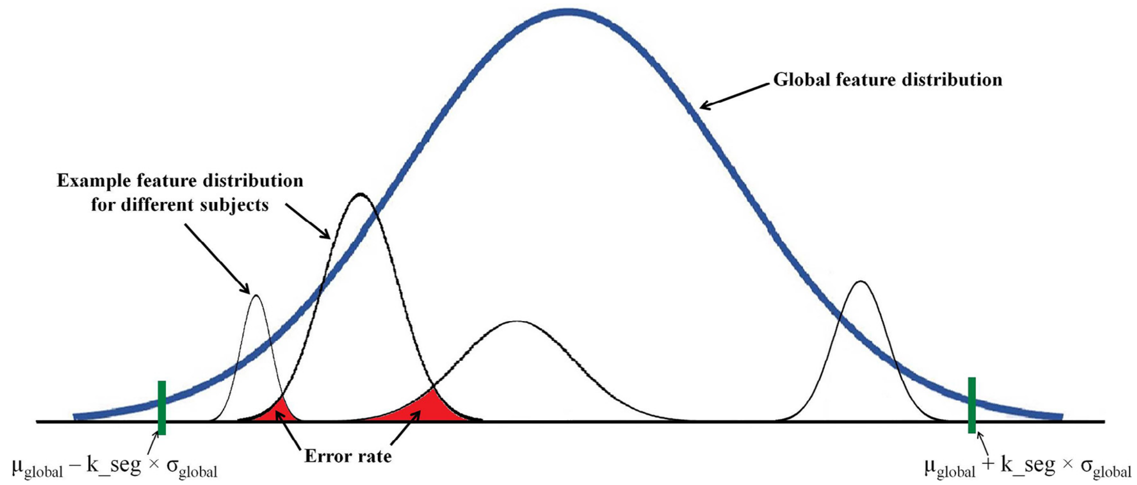

Global feature distribution
Example feature distribution for different subjects
Error rate
$\mu_{global} - k\_seg \times \sigma_{global}$
$\mu_{global} + k\_seg \times \sigma_{global}$

Fig. 6 – Example key generation process from the global feature distribution of an electrode for a subject (Chang et al., 2004).

$$k_{sub,feature} = (\mu_{global,feature} - \mu_{sub,feature})/\sigma_{sub,feature}$$

- Each feature vector from the training samples was mapped to an appropriate bin in the global distribution. The bin containing the maximum feature vector samples of the subject was used to represent that feature.

$$\begin{aligned} &if \quad (feature\_vector \geq (Window\_start + increment \times step\_size) \\ &\quad \&feature\_vector \leq (Window\_start + (increment + 1) \times step\_size)) \end{aligned}$$

The step size was proportional to the authentication region of a subject's feature vector, thus varying the number of equiprobable bins in the global distribution with each subject, electrode, and activity. Fig. 6 shows an example of key generation region using a feature of a subject in the global distribution.

- The key bits were computed from the feature vector using the binary feature quantization explained in the next subsection.
- This process was repeated for the six electrodes of Dataset I and the chosen 18 electrodes of Dataset II across all the subjects to generate the keys. The length of keys can be changed by combining different electrodes as required by the user conditioned to a particular application.

7.2. Binary feature quantization

To use the keys for any cryptographic application, the feature vectors have to be binarized appropriately without compromising the inherent security properties of the biometrics. The statistical evaluation of the Neurokeys is detailed in the next section. The basic idea to extract the bits was to use the binary value of the feature vectors and perform the mixing function using the authentication regions of each subject's electrode. We can also use the SHA-1 hash function to spread the bits more uniformly in the keys. The index of the circular shift was obtained using the number of segments in the global feature window. After all the concatenation rounds for the desired number of electrodes (18 in this case), the average key length of 230 bits was derived from each subject and activity. The pseudo code for the quantization is shown in Algorithm 1.

```
Algorithm 1 Binary feature vector quantization
Require: Biometric feature vector Fv , number of segments $N$, Authentic region Ar
Ensure: Neurokey N_key
  for $i \leftarrow 1$ to $N\_sub$ do                                ▷ Number of subjects
    for $j \leftarrow 1$ to $N\_elec$ do                             ▷ Number of electrodes
      $temp\_key[0] \leftarrow dec$ to $bin(F_v[i][j])$                ▷ Binary quantization
      $seed \leftarrow F_v[i][j]$ mod $Ar[i][j]$        ▷ Determine seed for temporary key
      $temp\_key[k] \leftarrow XOR(temp\_key[k-1], seed)$
      $key[k] \leftarrow circularshift(temp\_key[k], N[i][j])$        ▷ Use the number of segments to perform the circular shift
      $N\_key[i] \leftarrow (N\_key[i] || key[k])$         ▷ Concatenate the bits from each round to form the key
    end for
  end for
  return N_key
```

7.3. Key evaluation

The amount of data with various parameters can restrict the ability to derive a unique and repeatable key from the entire data set for each subject as outlined in Table 6. The number of possible combinations of electrodes to determine an optimal combination given by $\sum_{k=0}^{n-1}\binom{n}{k}$ is significantly large. Therefore, a subset of electrodes derived during the subject classification will be used in key generation.

Table 6 – Complexity of deriving the key.

Parameters (n)	Frequency
No. of electrodes (Ne)	1 to 61
Frequency windowing (Fw)	5
Time-Frequency windowing (Tw)	18
Distribution of data (Dd)	1
Segmentation parameter (Sk)	1
Number of subjects (Sub)	7–120
Complexity	(Ne x Fw × Tw) + (Dd × Sk × Sub) = $O(n^3)$

The following metrics were considered to evaluate the keys generated from the subjects.

False Acceptance Rate (FAR) is the measure of the likelihood that the Neurokey system will incorrectly accept the derived key from an unauthorized user. As there is only one legitimate user, keys of all other subjects in the dataset apart from the authorized user were used to assess this error rate.

False Rejection Rate (FRR) is the ratio of the number of times the Neurokey system will incorrectly reject the derived key of a genuine user to the total attempts. The dataset of the subjects was randomly split into 40% train and 60% test sets to assess this error rate.

Half Total Error rate (HTER) is an average of the FAR and FRR, defined as:

$$HTER = \frac{FAR + FRR}{2} \tag{7}$$

K_seg, the number of segments in the global window, was a crucial parameter in determining the width of the global window for the feature key and the initialization of the seed in Neurokey binarization. Fig. 7 shows the variation of HTER with the segmentation parameter averaged across subjects and electrodes. The graph is an exponential variation and K_seg = 10 was chosen to be an optimal number for the window segmentation.

We also wanted to study the error rates corresponding to the number of trials needed to enroll a user in the key generation process. Fig. 8 shows the HTER versus the number of trials for both the datasets. In each dataset, the subjects did not perform an equal number of trials. So the curves in this figure are plotted up to thirteen trials for Dataset I and five trials for Dataset II. These were the minimum of the number of trials performed by the subjects in each dataset. Thus, it gave a measure of the average number of trials required to enroll a user.

Fig. 9 shows the HTERs for Dataset I, averaged over the electrodes. The mean HTERs for Dataset II (4.53%) were slightly higher compared to Dataset I (3.05%). Since Dataset II represents a larger population, we shall analyze it in greater detail than Dataset I. We compared the FARs and FRRs of the Neurokeys obtained using FFT, DWT and combined FFT-DWT feature vectors in Figs 10a, 10b and 10c for the S1_task. The error rates for other two tasks of Dataset II using DWT-FFT feature vectors are shown in Figs 11a and 11b. We also studied an alternate view of the error rates for the subjects averaged across all electrodes in Fig. 12. It shows the fraction of users versus the probability of failure of generating their own genuine Neurokey.

FFT features were more suited for the key generation as both average FAR and FRR were less compared to DWT features. Combining the two features, FAR further reduced to nearly zero in many electrodes. This could be an excellent feature to keep away adversaries. However, the increased FRR would comparatively degrade the overall performance of the system.

7.4. *Randomness measures – NIST statistical test suite*

We utilized the guidelines of the statistical test suite for random number generators by NIST to evaluate the output of our biometric key generator (Rukhin et al., 2001). These tests are helpful in determining the suitability of a generator for the cryptographic application. We tested our sequences with nine out of the fifteen tests that applied to our system (Table 7). It is difficult to include the details of all NIST tests in this paper. We briefly list the parameters that help to understand the evaluation of each test.

- **Ho**: The null hypothesis that the sequence being tested is random.
- **Ha**: The alternative hypothesis that the sequence is not random.
- α: The level of significance of the test. It is the probability that a test will indicate that the sequence is not random when it really is random. The default value of significance is 0.01.
- A p-value $\geq\alpha$ would mean that the sequence would be considered to be random with a confidence of 99%. A p-value $< \alpha$ would mean that the sequence is non-random with a confidence of 99%.

Each test was carried out for Dataset II for a sample size = 360 sequences resulting from 120 subjects, and 3

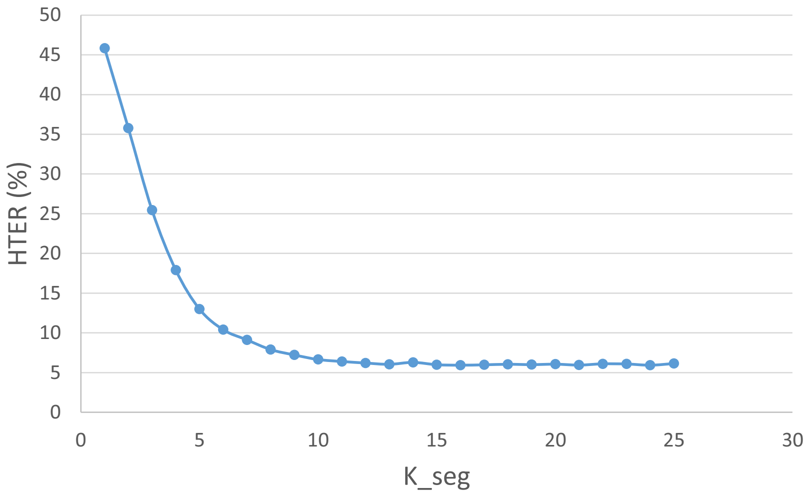


Fig. 7 – HTERs for varying the segmentation parameter values averaged across electrodes and subjects.

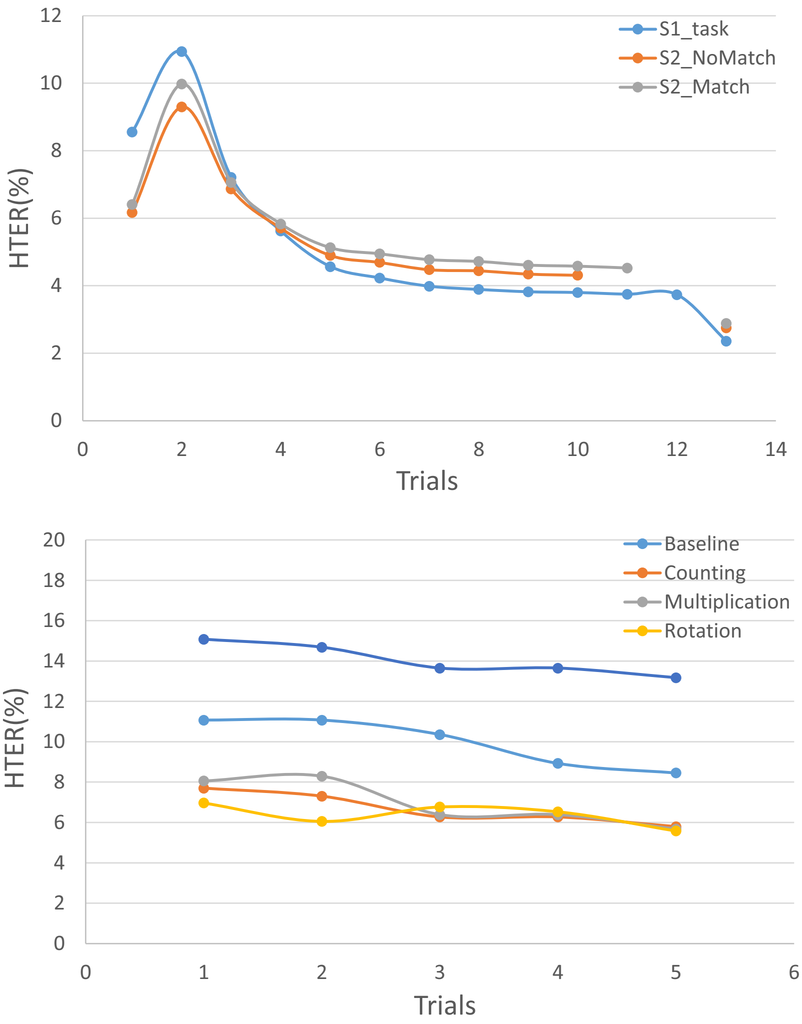


Fig. 8 – HTERs variation with number of trials for Dataset I (top) and Dataset II.

activities combined for 18 electrodes. A useful interpretation of the 3240 results (120×3×9 tests) is necessary. Two approaches outlined by NIST include (1) examining the proportion of sequences that pass a statistical test and (2) verifying the distribution of p-values from a test for uniformity.

7.4.1. Proportion

The acceptable range of proportions that pass the test is given using α, the level of significance, and m, the sample size.

$$Range = \tilde{p} \pm 3\sqrt{\frac{\tilde{p}(1-\tilde{p})}{m}} \quad (8)$$

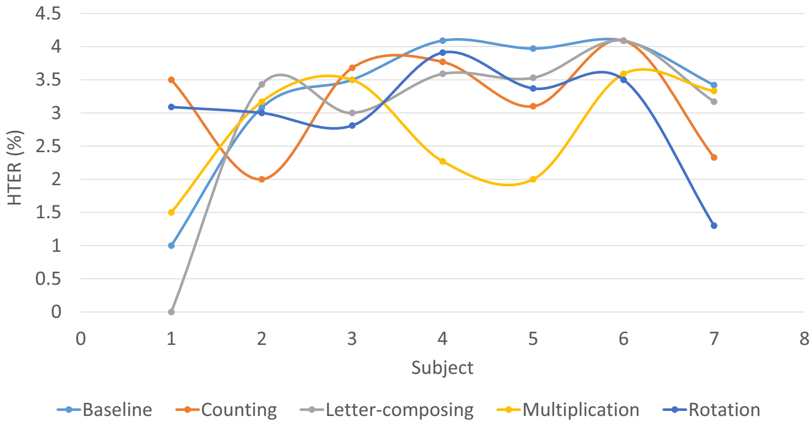


Fig. 9 – HTERs variation for Dataset I for each subject and activity averaged over the electrodes.

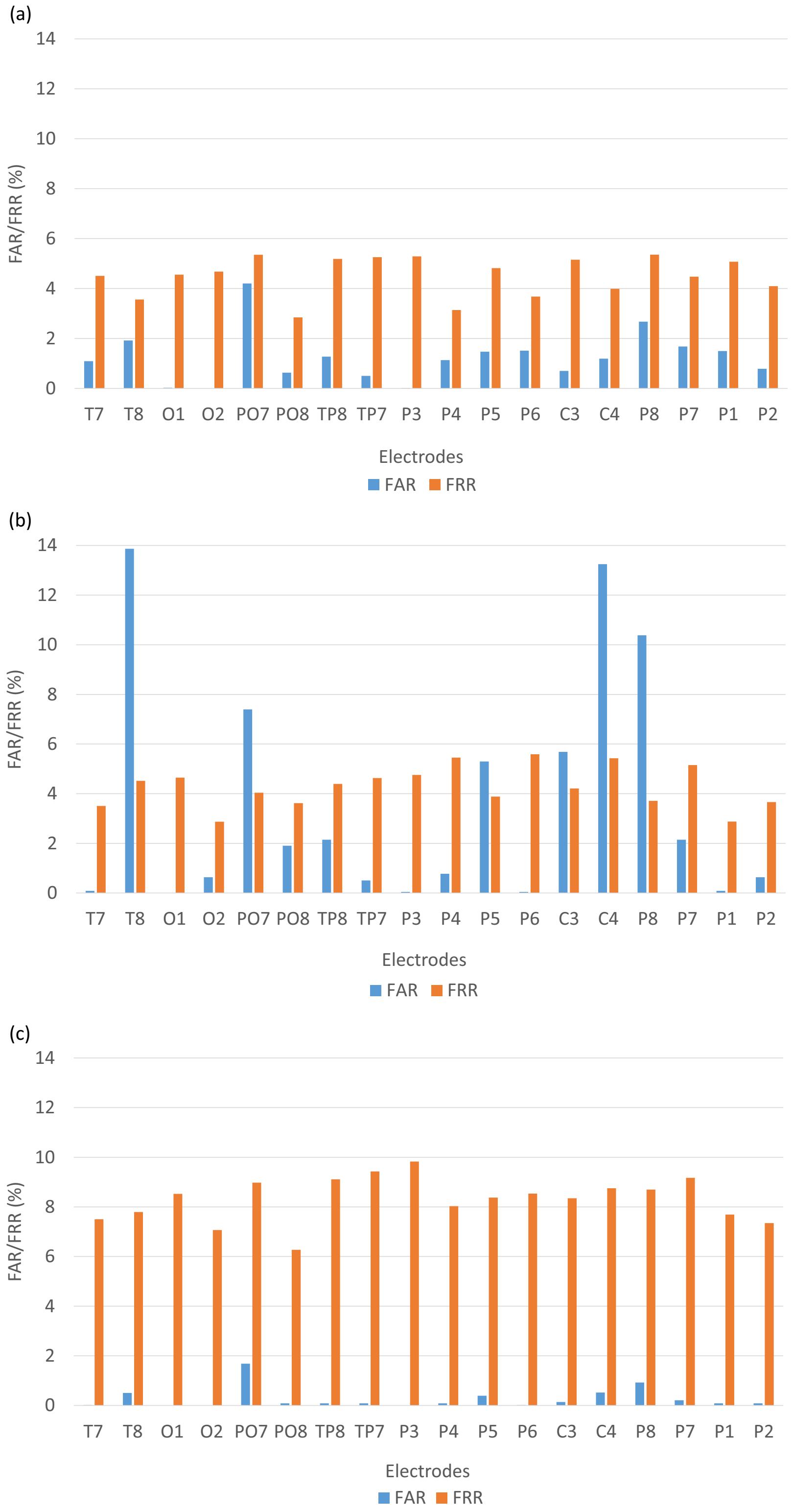
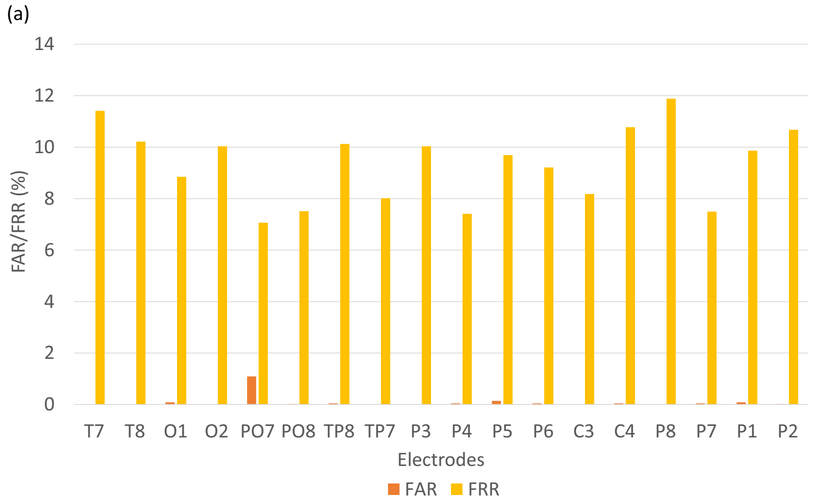


Fig. 10 – False acceptance and rejection rates for each electrode averaged across the subjects for S1_task (Dataset II) using different feature vectors (FFT feature vectors (a), DWT feature vectors (b), DWT-FFT feature vectors (c)).



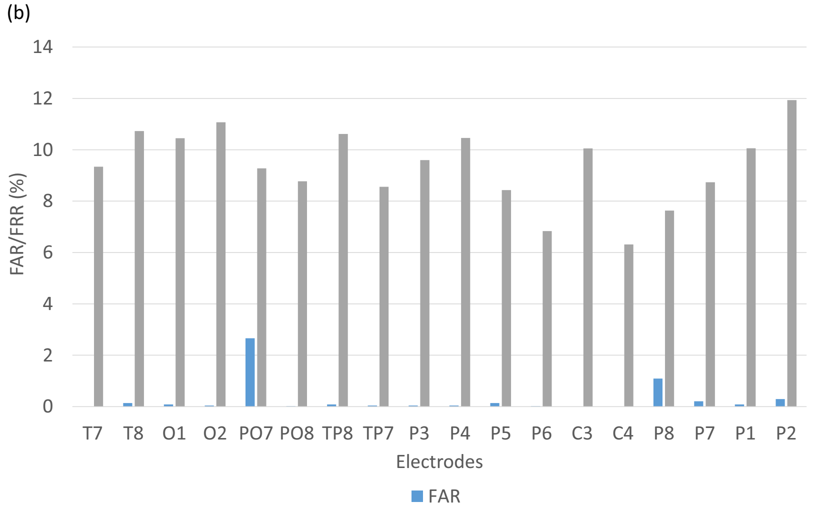


Fig. 11 – False acceptance and rejection rates for each electrode averaged across the subjects for S2_NoMatch (a) and S2_Match tasks (b), using DWT-FFT feature vectors for Dataset II.

where $\tilde{p} = 1 - \alpha$, $\alpha = 0.01$ and m = 360 sequences, we get range = 0.99 ± 0.01573213272 (i.e. proportions should lie above 0.97426786).

7.4.2. Distribution

The distribution of p-values of a test is evaluated by dividing the interval between 0 and 1 into 10 sub-intervals. The frequency of p-values that lie within each sub-interval is calculated. Uniformity is statistically determined by χ^2 test and finding the p-value of all p-values for a test (Kim et al.). If p-value ≥0.0001, then the sequences can be considered to be uniformly distributed.

$$\chi^2 = \sum_{1}^{10} \frac{(F_i - m \times S_i)^2}{m \times S_i} \tag{9}$$

$$P\ value = igamc(9/2, \chi^2/2) \tag{10}$$

where F_i gives the frequency of p-values in the *i*th sub-interval, m is the sample size, S_i denotes the rate of each *i*th bin which is computed from the histogram of p-values and *igamc* is the incomplete gamma function.

8. Discussion

The accuracies and F-measures of the subject classification using support vector machine and Bayesian network are shown in Tables 3 and 4. Dataset I (using six electrodes) had a mean accuracy of 98.46% whereas Dataset II (using selected 18 electrodes) had a mean accuracy of 91.05%, averaged over the activities. It is due to the vast difference in the number of subjects in the two datasets. The F-measures and ROC areas were reasonable given that the EEG signals were recorded over multiple sessions separated in time. From the observations, we can conclude that Bayesian network can be used to classify small datasets, and SVM can be used for large datasets. Dataset II will be analyzed and discussed more as it represents a larger population set.

Our system faces the trade-offs such as entropy vs practicality and number of features vs accuracy. All subsets of electrodes shown in Table 4 showed lower classification accuracies compared to using 61 electrodes together (96.17%). But clearly some subsets obtained better classification than the rest (mainly frontal electrodes). For instance, using a subset of 18

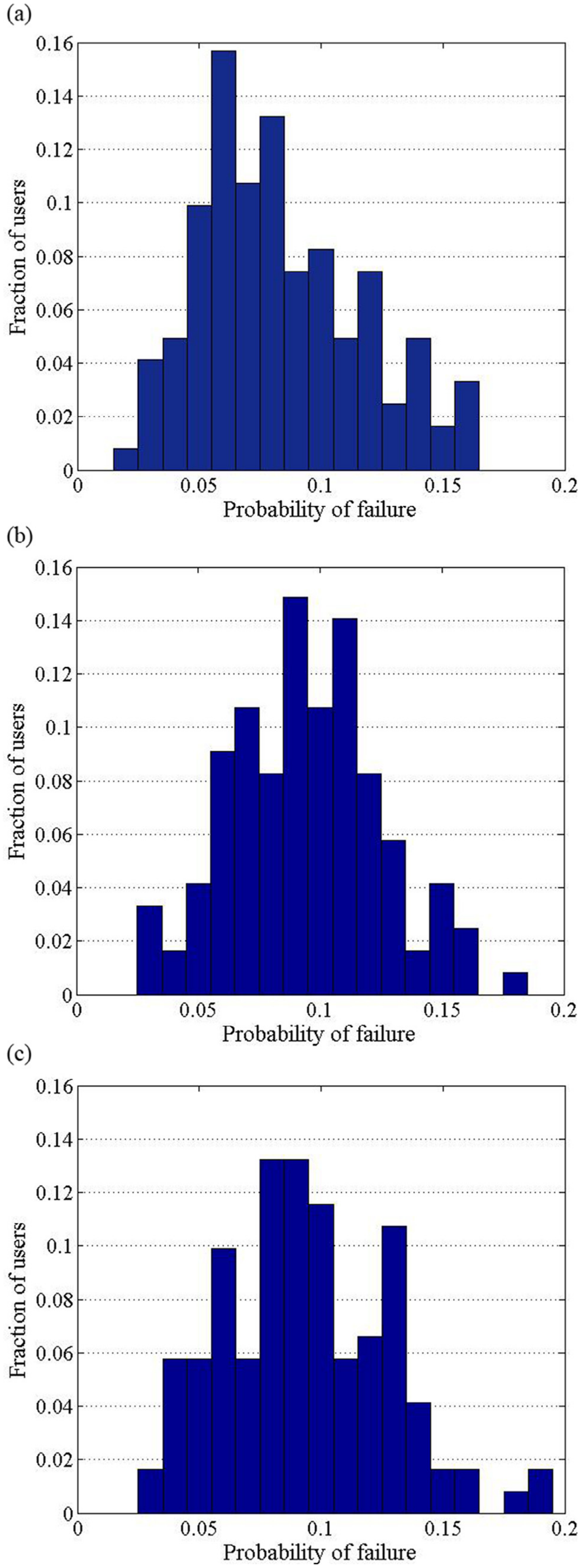


Fig. 12 – The fraction of users versus the probability of failure of generating their own genuine Neurokey for Dataset II (S1_task (a), S2_NoMatch task (b), S2_Match task (c)).

electrodes (bold in Table 4) achieved an accuracy of 92.28% whereas the subset of 18 electrodes containing FP1 through C4 (italics in Table 4) showed an accuracy of 79.56%. The reasons for this could be:

- Feature reduction is sensitive to type of electrode because its characteristics are dependent upon underlying brain activations. Zhang et al. (1995) showed that the topographical distribution of event-related potentials to picture stimuli were mainly located in the occipito-temporal areas of the brain, and these regions play a key role in high level visual information processing. We also observed that using occipital, temporal and central brain areas of the brain (P3, P4, O1, O2, C3, C4), resulted in higher distinguishability of the activities compared to other electrode positions.
- The features from biometrics such as fingerprints (Maltoni et al., 2009) are well established but feature extraction from EEG is still an active area of research. Hence, estimating the entropy contribution of each electrode to the system is a challenging endeavor. Using all the 61 electrodes increases the total number of features that may account for accommodating the variations in EEG among the trials.

For key generation process, we observed that using the same feature vectors of authentication for key generation indeed caused avalanche effect in error rates. The mean HTERs were nearly nine to 10 times lower using the global feature segmentation (Chang et al., 2004) feature selection process for key generation. It is not feasible to detail all these comparisons currently in this paper. The activities that provided better classification among subjects also produced lower error rates for the Neurokey generation process. For example, the rotation and multiplication activities had F-measures of 1 for subject classification. They also had low mean HTER values in the range of 2–3% (averaged over the subjects and electrodes). Similarly, S1_task of Dataset II with 0.961 F-measure provided a better subject distinguishability compared to other visually evoked stimulus tasks. It had a mean HTER of 4.28% (FAR 0.27%, FRR 8.30%). Thus, combining the activity with certain electrodes will help to generate strong cryptographic keys. The flexibility to change an activity upon compromise is an attribute not yet offered by most of the existing biometrics. The mean HTERs of Neurokeys from other activities were also low (S2_NoMatch 4.78%, S2_Match 4.8%). It has been shown that brain responses change during threat (DeLaRosa et al., 2014), providing a resilient solution to coercion attacks. Another possible solution could be to think of a different activity than the enrollment activity when forced to reveal one's authentic biometric key. However, it requires further work to test the performance of our scheme to key generation under a threat/coercion attack model.

As observed previously in Fig. 10, Neurokeys from the DWT (FAR 3.60%, FRR 4.27%) and FFT (FAR 1.23%, FRR 4.50%) feature vectors had lower mean error rates compared to the combined DWT-FFT feature vectors (FAR 0.27%, FRR 8.30%). The failure rate of our system has similar implications as other biometrics-based cryptographic systems. The UK Biometrics Working Group has suggested a scheme for understanding relative biometric strengths – FAR of 1.0% as basic security strength, 0.01% as medium and 0.0001% as high security strength (Patrick;

Table 7 – Results for the proportion of sequences passing the tests and the uniformity of p-values.

Statistical test	Proportion	Decision	P-value of the p-values	Decision
Frequency (Monobit) Test	0.975222	Pass	0.983235	Uniform
Frequency Test within a Block	0.988889	Pass	0.985372	Uniform
Runs Test	0.997222	Pass	0.989165	Uniform
Longest Run of Ones in a Block	0.979444	Pass	2.82E-19	Non-uniform
Spectral Test	0.172222	Fail	1.49E-06	Non-uniform
Non-overlapping Template	0.979889	Pass	8.46E-06	Non-uniform
Serial Test –a	0.983333	Pass	0.978447	Uniform
Serial Test –b	0.983333	Pass	0.882427	Uniform
Approximate Entropy Test	0.975	Pass	0.982684	Uniform
Cumulative Sums Test	0.727778	Fail	0.996361	Uniform

U. K. Government Biometrics Working Group (BWG)). Our Neurokey system fulfills this criterion of basic strength with a best FAR of 0.27%. However, the current FRR of 8.30% implies that a user will be falsely denied permission to his/her encrypted content in one out of nearly 12 access requests (when used as a private key). This leads to user annoyance while also rendering the system undeployable in large settings. False acceptance rate (FAR) is the most critical accuracy metric in a cryptographic system because an imposter break-in is certainly a more critical event than other failures of a biometric key system. Therefore, the keys generated from DWT-FFT features were accepted to be tested against the NIST randomness tests. We are currently working toward improving the FRR metrics to make it a more usable system.

With any biometric data, there will be changes in a user's characteristics – fingerprints change with time, scarring, aging and general wear, voice-scan system is influenced by sore throats, and facial-scan is affected by changes in weight. There will be a need to update the EEG feature vectors of the subjects whenever there is a biological or emotional change in the brain so that the EEG signals can effectively authenticate a genuine user and reject an imposter. Five to seven trials were needed to establish a key for the user (Fig. 8), which is relatively small. We also studied the probability of failure to generate a genuine key for the users from their biometric samples collected over different sessions in time, as shown in Fig. 12. For the S1_task, 19 users failed to generate their genuine keys with a maximum failure probability of 6%. For S2_NoMatch task, 18 users failed to generate their genuine keys with a 9% maximum failure probability. For the S2_Match task, 16 users did not generate their genuine keys with a 9% failure probability. This shows that some tasks are better for certain group of users to generate their Neurokeys. Nonetheless, there is an alternative task to switch one's Neurokey in the case of a compromise.

We performed the NIST tests on the sequences obtained from the tasks of Dataset II. The average length of key bits generated from each activity using 18 electrodes was 230 bits. Most of the sequences passed these tests. However, Spectral Test and Cumulative Sums Tests were not able to produce the proportion of the sequences that should pass the threshold of 0.9742. Majority of the NIST tests recommend a minimum input size of 100 bits. The recommended input size for Spectral Test is 1000 bits and our system was tested with an average length of 230 bits. This could be a possible reason for the test failure by a big margin. This test is based on the discrete Fourier transform to detect periodic features in the bit strings. These features play an important role in cryptanalysis (Hamano, 2005). Also, the proportion of sequences passing the Cumulative Sums test was below the threshold. It implies that some of the sequences had too many zeros or ones in the beginning or at the end, which can be easily detected by an adversary by cryptanalysis of a few sequences. For a sequence to have good random properties, the cumulative sum of the partial sequences should be near zero. For the uniform distribution test, Longest-Run-of-Ones in a Block and Non-overlapping Template Test showed non-uniform distribution of p-values. This is because the variety of p-values in these tests was limited even though the sequences passed the tests.

Using the results of Datasets I and II, we prove the feasibility of deriving random bits from the EEG biometrics of a person. Irrespective of the differences in activities, electrodes, and recording conditions, a key can be derived with a low error rate. A smaller dataset provides better authentication capability and lower error rates for the Neurokeys. For a larger data set, despite having acceptable mean HTERs for the keys, we need better feature vectorization for subject authentication.

9. Security analysis

Template Security: The information regarding the global feature segmentation protocol and an individual's authentic region needs to be stored. The authentic region windows of all subjects and feature vectors are equiprobable in the global window. However, the authentic window widths are not equal for any subject or feature, i.e. equiprobable ! = equal interval. Hence, an imposter gains no information regarding the feature vector or EEG biometric sample from the equiprobable authentic regions. The template can be secured using techniques suggested by Ballard et al. (2008) and Jain et al. (2008).

Key Space: It is a crucial factor of a cryptographic system and refers to the set of all possible keys (2^n combinations for n bits key). Average key space for the Neurokey generation is 230 bits per activity. Combining different activities will change the maximum length of keys for subjects. Thus, the range theoretically is 230 to 690 (230×3) bits. However, the effective key space is given by 1/false acceptance rate (FAR) (Gorman, 2003). Comparing with other biometrics, we see that Token (10^{12}) > Password (10^{14}–10^6) > Iris (10^6) > Fingerprint, PIN

(10^4) > Neurokeys (1/0.0027 ~ 370) > Face (6.25) (Gorman, 2003). Our current effective key space performs better than face biometrics only. A reasonable defense against guessing and search attacks would be similar to the conventional systems that restrict the number of failed attempts by a user. We hope to increase the Neurokey space in the future by exploring better entropy mixers for our system.

Entropy: It is the amount of uncertainty to guess the key from an adversary's perspective. The maximum is n bits for a truly randomized key and zero for a guessable key.

$$Entropy = \sum_{i}^{n} p(x) log_2 p(x) \tag{11}$$

where n = the total number of possible locations for a feature vector in the global window and p(x) = the probability of a feature vector occurring at each location in the global window. The overall entropy is less than n, i.e. 230 bits as stated above, since we accommodate variations among the genuine EEG samples of the subjects using the mean and standard deviation of the EEG features. The average entropy for the subjects, averaged over the tasks and electrodes, was 82 bits for our system.

10. Practical considerations

Brain-computer interface (BCI) applications were considered impractical just two decades ago. In the last 6 years, with the advent of affordable, comfortable, more sensitive, and dry EEG headsets possessing high resolutions (up to 512 Hz) (Stamps and Hamam, 2010; Zhang et al., 2010), BCI is now used routinely to control prosthetics (Lebedev and Nicolelis, 2006), wheelchairs (Huang et al., 2012; Stamps and Hamam, 2010) and gaming applications (Nijholt, 2009). Not very far in the future, we will be using EEG for cryptographic purposes similar to today's commonplace biometrics like fingerprinting. This study is a step in that direction and was aimed to explore the challenges and study the outcomes of a system using EEG as a cancelable biometric identifier for key generation.

Social engineering attacks, dictionary attacks, and phishing attacks have not been studied in a systematic fashion for the EEG-derived keys. The attacks can be countered depending on the strength of the derived key and process. We outline some of the practical limitations of using BCI technology for the cryptographic key generation.

Ethical issues: Abusing the BCI technology to trick a user into inputting a thought for deriving meaningful interpretations. *Protection from user non-compliance*: The EEG biometric template should not be easy to transfer to other parties so as to share the key using the same BKG system. This can be prevented by not storing the EEG in a raw form. *Electrodes*: There is no consensus on the number of electrodes and electrode positions for authentication or key generation processes. *Emergency*: Performing a behavioral activity or task in an emergency, as opposed to a normal situation, will result in a change in the brain signals due to emotional stress. The system should still be able to generate a key. *Coercion Attack*: Similar to an emergency situation, performing an activity under duress will also result in a change in the EEG patterns. However, in this case, the system should not generate a key.

11. Conclusion and future work

A unique key for each subject was obtained using EEG signals by collecting data from distinguishable mental activities. We studied the feasibility of deriving a cancelable biometrics-based Neurokey using various mental tasks. Uniqueness and consistency among the subjects and their keys can be asserted from the results achieved using different datasets. Cryptographic systems based on biometrics such as fingerprinting have evolved over time, with extensive research work and marketing technologies leading to a reduction in their error/failure rates. It is a challenging task to characterize EEG variations for cryptographic purposes but we envision to bring the error rates down with better grade recording devices and feature fusion mechanisms. Hybrid algorithms for feature mapping to binary codewords are under progress. We ascertained the strength of the obtained Neurokeys by using entropy and NIST's statistical tests. Additionally, it seems promising to combine other synchrony measures with EEG features.

12. Dataset acknowledgements

We would like to acknowledge the late Prof. Henri Begleiter at the Neurodynamics Laboratory at the State University of New York Health Centre at Brooklyn, USA, who generated the data and UCI Machine Repository for making it available online. The authors also thank the assistance of Dr. Charles Anderson of Colorado State University, USA, for maintaining a repository of the 1989 Keirn and Aunon data and making them available for experimentation.

Acknowledgements

This work is partially supported by the National Science Foundation under grants CNS-0751205, CNS-0821736 and CNS-1229700.

REFERENCES

Abdullah MK, Subari KS, Loong JLC, Ahmad NN. Analysis of the EEG signal for a practical biometric system. World Acad Sci Eng Technol 2010;68:1123–7.

Anokhin A, Steinlein O, Fischer C, Mao Y, Vogt P, Schalt E, et al. A genetic study of the human low-voltage electroencephalogram. Hum Genet 1992;90(1–2):99–112.

Ballard L, Kamara S, Monrose F, Reiter MK. Towards practical biometric key generation with randomized biometric templates. In: Proceedings of the 15th ACM conference on computer and communications security. ACM; 2008. p. 235–44.

Bolle RM, Connell JH, Ratha NK. Biometric perils and patches. Pattern Recognit 2002;35(12):2727–38.

Chang Y-J, Zhang W, Chen T. Biometrics-based cryptographic key generation. In: 2004 IEEE International Conference on Multimedia and Expo. ICME'04, vol. 3. IEEE; 2004. p. 2203–6.

Cheung K-H, Kong A, Zhang D, Kamel M, You JT, Lam H-W. An analysis on accuracy of cancelable biometrics based on bioHashing. In: Knowledge-based intelligent information and engineering systems. Springer; 2005. p. 1168–72.

Chuang J, Nguyen H, Wang C, Johnson B. I think, therefore I am: usability and security of authentication using brainwaves. In: Financial cryptography and data security. Springer; 2013. p. 1–16.

DeLaRosa BL, Spence JS, Shakal SK, Motes MA, Calley CS, Calley VI, et al. Electrophysiological spatiotemporal dynamics during implicit visual threat processing. Brain Cogn 2014;91:54–61.

Dodis Y, Reyzin L, Smith A. Fuzzy extractors: how to generate strong keys from biometrics and other noisy data. In: Advances in cryptology-Eurocrypt 2004. Springer; 2004. p. 523–40.

Gupta P, Gao D. Fighting coercion attacks in key generation using skin conductance. In: USENIX security symposium. 2010. p. 469–84.

Hall M, Frank E, Holmes G, Pfahringer B, Reutemann P, Witten IH. The WEKA data mining software: an update, vol. 11, issue 1. 10–18. ACM SIGKDD Explorations Newsletter; 2009 <http://www.cs.waikato.ac.nz/ml/weka>.

Hamano K. The distribution of the spectrum for the discrete Fourier transform test included in SP800-22. IEICE Trans Fundamentals Electron Commun Comput Sci 2005;88(1): 67–73.

He C. Person authentication using EEG brainwave signals [Master's thesis]. University of British Columbia; 2009.

Huang D, Qian K, Fei D-Y, Jia W, Chen X, Bai O. Electroencephalography (EEG)-based brain–computer interface (BCI): a 2-d virtual wheelchair control based on event-related desynchronization/synchronization and state control. Neural Syst Rehabil Eng IEEE Trans 2012;20(3): 379–88.

Ingber L. EEG database, UCI machine learning repository, University of California, Irvine, School of Information and Computer Sciences, <http://archive.ics.uci.edu/ml/datasets/EEG+Database>; 1997.

Jain AK, Ross A, Prabhakar S. An introduction to biometric recognition. Circuits Syst Video Technol IEEE Trans 2004;14(1):4–20.

Jain AK, Nandakumar K, Nagar A. Biometric template security. EURASIP J Adv Signal Process 2008;113:2008.

Jasper HH. The ten twenty electrode system of the international federation. Electroencephalogr Clin Neurophysiol 1958;10:371–5.

Jin ATB, Hui LM. Cancelable biometrics. Scholarpedia 2010;5(1):9201. revision - 91098.

Keirn ZA. Alternative modes of communication between man and machine [Master's thesis]. Purdue University, 1988.

Keirn ZA, Aunon JI. A new mode of communication between man and his surroundings. Biomed Eng IEEE Trans 1990;37(12):1209–14.

Kim S-J, Umeno K, Hasegawa AS-J Umeno K Hasegawa A. Corrections of the NIST statistical test suite for randomness, arXiv preprint nlin/0401040, 2004.

Klonovs J, Petersen C, Olesen H, Hammershoj A. ID proof on the go: development of a mobile EEG-based biometric authentication system. Vehicular Technol Mag IEEE 2013;8(1):81–9. doi:10.1109/MVT.2012.2234056.

Brain-Computer Interfaces Laboratory, Keirn and aunon eeg dataset, [Online] http://www.cs.colostate.edu/eeg/main/data/1989_Keirn_and_Aunon [accessed 10.01.11].

Lebedev MA, Nicolelis MA. Brain–machine interfaces: past, present and future. Trends Neurosci 2006;29(9):536–46.

Lokeshwari G, Udaya S, Aparna G. A novel approach for data encryption using EEG, SPIHT and genetic algorithm for secured applications. Int J Power Control Signal Comput 2013;5:23–7.

Lykken D, Tellegen A, Thorkelson K. Genetic determination of EEG frequency spectra. Biol Psychol 1974;1(4):245–59.

Maltoni D, Maio D, Jain A, Prabhakar S. Handbook of fingerprint recognition. Springer Science & Business Media; 2009.

Marcel S, Millan J. Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation. Pattern Anal Mach Intell IEEE Trans 2007;29(4):743–52. doi:10.1109/TPAMI.2007.1012.

Monrose F, Reiter MK, Li Q, Wetzel S. Cryptographic key generation from voice. In: 2001 IEEE Symposium on Security and Privacy. S&P 2001 Proceedings, IEEE. 2001. p. 202–13.

Nakanishi I, Baba S, Miyamoto C. EEG based biometric authentication using new spectral features. In: International Symposium on Intelligent Signal Processing and Communication Systems. ISPACS 2009. 2009. p. 651–4 doi:10.1109/ISPACS.2009.5383756.

Näpflin M, Wildi M, Sarnthein J. Test–retest reliability of resting EEG spectra validates a statistical signature of persons. Clin Neurophysiol 2007;118(11):2519–24.

Nijholt A. BCI for games: a "State of the Art" survey. In: Entertainment Computing-ICEC 2008. Springer; 2009. p. 225–8.

O. Gorman L. Comparing passwords, tokens, and biometrics for user authentication. Proc IEEE 2003;91(12):2021–40.

Oostenveld R, Praamstra P. The five percent electrode system for high-resolution EEG and ERP measurements. Clinical Neurophysiology 2001;112(4):713–19.

Öhman A. The role of the amygdala in human fear: automatic detection of threat. Psychoneuroendocrinology 2005;30(10):953–8.

Palaniappan R, Ravi K. A new method to identify individuals using signals from the brain. In: Proceedings of the 2003 Joint Conference of the Fourth International Conference on Information, Communications and Signal Processing, 2003 and Fourth Pacific Rim Conference on Multimedia, vol. 3. IEEE; 2003. p. 1442–5.

Palaniappan R, Ravi K. Improving visual evoked potential feature classification for person recognition using PCA and normalization. Pattern Recognit Lett 2006;27(7):726–33.

Palaniappan R, Gosalia J, Revett K, Samraj A. PIN generation using single channel EEG biometric. In: Advances in computing and communications. Springer; 2011. p. 378–85.

Paranjape R, Mahovsky J, Benedicenti L, Koles Z. The electroencephalogram as a biometric. In: Canadian Conference on Electrical and Computer Engineering, vol. 2. IEEE; 2001. p. 1363–6.

Patrick AS. Fingerprint concerns: performance, usability, and acceptance of fingerprint biometric systems. National Research Council of Canada; 2008 [accessed 01.04.16.] [Online] <http://www.andrewpatrick.ca/essays/fingerprint-concerns-performance-usability-and-acceptance-of-fingerprint-biometric-systems/>.

Petitcolas FA. Kerckhoffs principle. In: Encyclopedia of cryptography and security. Springer; 2011. p. 675.

Poulos M, Rangoussi M, Chrissikopoulos V, Evangelou A. Person identification based on parametric processing of the EEG. In: Proceedings of ICECS'99. The 6th IEEE International Conference on Electronics, Circuits and Systems, vol. 1. IEEE; 1999. p. 283–6.

Poulos M, Rangoussi M, Alexandris N, Evangelou A. Person identification from the EEG using nonlinear signal classification. Methods Inf Med 2002;41(1):64–75.

Ratha NK, Connell JH, Bolle RM. Enhancing security and privacy in biometrics-based authentication systems. IBM Syst J 2001;40(3):614–34.

Rathgeb C, Uhl A. A survey on biometric cryptosystems and cancelable biometrics. EURASIP J Inf Secur 2011;2011(1):1–25.

Revett K, Deravi F, Sirlantzis K. Biosignals for user authentication – towards cognitive biometrics? In: International Conference on Emerging Security Technologies (EST). 2010. p. 71–6 doi:10.1109/EST.2010.32.

Rukhin A, Soto J, Nechvatal J, Smid M, Barker E. A statistical test suite for random and pseudorandom number generators for cryptographic applications, Tech. rep., DTIC Document 2001.

Snodgrass JG, Vanderwart M. A standardized set of 260 pictures: norms for name agreement, image agreement, familiarity, and visual complexity. J Exp Psychol [Hum Learn] 1980;6(2):174.

Soutar C, Roberge D, Stoianov A, Gilroy R, Kumar BV. Biometric Encryption: enrollment and verification procedures. In: Aerospace/defense sensing and controls, international society for optics and photonics. 1998. p. 24–35.

Stamps K, Hamam Y. Towards inexpensive BCI control for wheelchair navigation in the enabled environment–a hardware survey. In: Brain informatics. Springer; 2010. p. 336–45.

Thorpe J, van Oorschot PC, Somayaji A. Pass-thoughts: authenticating with our minds. In: Proceedings of the 2005 workshop on new security paradigms. ACM; 2005. p. 45–56.

U. K. Government Biometrics Working Group (BWG), Biometric security concerns, [Online]. <http://docplayer.net/12457008-Biometric-security-concerns-v1-0-september-2003.html> [accessed 01.04.16.

Uludag U, Pankanti S, Prabhakar S, Jain AK. Biometric cryptosystems: issues and challenges. Proc IEEE 2004;92(6):948–60.

Vogel F. The genetic basis of the normal human electroencephalogram (EEG). Humangenetik 1970;10(2):91–114.

Yeom S-K, Suk H-I, Lee S-W. Person authentication from neural activity of face-specific visual self-representation. Pattern Recognit 2013;46(4):1159–69.

Zhang B, Wang J, Fuhlbrigge T. A review of the commercial brain-computer interface technology from perspective of industrial robotics. In: IEEE International Conference on Automation and Logistics (ICAL). IEEE; 2010. p. 379–84.

Zhang XL, Begleiter H, Porjesz B, Wang W, Litke A. Event related potentials during object recognition tasks. Brain Res Bull 1995;38(6):531–8.

Zhao Q, Peng H, Hu B, Liu Q, Liu L, Qi Y, et al. Improving individual identification in security check with an EEG based biometric solution. In: Brain informatics. Springer; 2010. p. 145–55.

Zheng G, Li W, Zhan C. Cryptographic key generation from biometric data using lattice mapping. In: 18th International Conference on Pattern Recognition. ICPR 2006., vol. 4. IEEE; 2006. p. 513–16.

Garima Bajwa is a PhD candidate in the Department of Computer Science and Engineering, University of North Texas. She is involved in inter-disciplinary research including Computer Science, Neuroscience and Signal Processing. She is currently working on mathematical modeling of EEG, commonly known as brain signals, with a focus on the ability to extract clinically significant information for real time applications. She completed her Master's in Electrical and Computer Engineering from University of Waterloo, Canada. In her free time, she loves to dig deep into things that grab her attention, spend time hiking and explore nature.

Ram Dantu has 15 years of industrial experience in the networking industry, where he worked for Cisco, Nortel, Alcatel, and Fujitsu, and was responsible for advancing technology products from concept to delivery. He is a full professor at the Department of Computer Science and Engineering, University of North Texas (UNT). He has received several NSF awards in collaboration (lead PI) with Columbia University, Purdue University, University of California at Davis, Texas A&M University and MIT. In addition to more than 150 research papers, he has authored several Requests For Comments (RFCs) related to MPLS, SS7 over IP, and routing.