Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 126 (2018) 713–722

Procedia Computer Science

www.elsevier.com/locate/procedia

22nd International Conference on Knowledge-Based and Intelligent Information & Engineering Systems

On the Study of Impacts of Brain Conditions on EEG-based Cryptographic Key Generation Systems

Dang Nguyen[a], Dat Tran[a], Dharmendra Sharma[a], Wanli Ma[a]

[a] *Faculty of Science and Technology*
University of Canberra, ACT 2601, Australia

Abstract

In this paper, we investigate impacts of brain conditions on an EEG-based cryptographic key generation system. Brain disorders, such as epilepsy and alcohol, involve in the EEG signal and hence it may have impacts on the system. This issue has not been analyzed in the literature. To solve this issue, we introduce a method for key generation from EEG signals, and implement experiments on the Australian EEG and the Alcoholism datasets. We use parametric spectrum estimate technique for feature exaction, and devised a error-correction quantization technique that is useful for a noisy data such as EEG. For experimental methodology, we perform on two groups of subjects, epileptic and non-epileptic, alcoholic and non-alcoholic to investigate the impact of brain conditions on the success rate of system. Experimental results show that both epilepsy and alcoholic actually have impacts on the performance of system.

Keywords: Knowledge discovery, EEG, Cryptographic key, Epilepsy, Alcohol, NIST

1. Introduction

Biometric-based cryptographic key generation is regarded as a data mining application that uses knowledge discovery techniques to extract biometric information to generate cryptographic keys. The applications of keys can be used in cryptographic primitives such as encryption and decryption algorithms. In general, people can use their biometrics (including voice, face, iris, and fingerprint) as good alternatives, or supplements, to PINs and passwords for cryptographic key generation. It has been shown that electroencephalogram (EEG) can be also used as a biometric for key generation.

Accuracy is one of the crucial requirements of any biometrics-based key generation system, including EEG-based. Factors which may affect the accuracy of an EEG-based key generation system can be signal noises, feature extraction methods, and/or error-correction algorithms. Mental disorder (such as epilepsy and alcohol) may also have some

* Corresponding author. Tel.: +61405639877
E-mail address: Dang.van.Nguyen@canberra.edu.au

10.1016/j.procs.2018.08.005

effects on the performance as it has been shown that, brain state changes from less to more ordered state, from more to less chaotic, or from more to less complexity during epileptic and alcoholic seizures.

1.1. Epilepsy

Approximately 1% of the people in the world suffer from epilepsy. Epilepsy is chronic neurological disorder which is generally characterized the sudden and the recurrent seizures [16]. Epileptic seizures are manifestations of epilepsy, which are caused by the sudden development of synchronous neuronal firing in the cerebral cortex and are recorded using the EEG. They may be partial seizures, which occur only in a few channels of the EEG recording, or generalized seizures the whole brain, which involve in every channel of the EEG recording [16]. The shape of wave may contain useful information relating to the different psychological states of the brain [15]. Therefore, EEG signal parameters, extracted and analyzed using computers, are useful in diagnosing and assessing brain state, especially epilepsy [15]. So far, studies have focused on detecting epilepsy such as in [16], and there have been no reports on the impacts of epilepsy on the performance of cryptographic key generation.

In recent years, a few attempts have been reported on seizure detection and prediction from EEG analysis using two different approaches: 1) Examination of the waveforms in the preictal (before a seizure) EEG to find markers or changes in neuronal activity such as spikes which may be precursors to seizures; 2) Analysis of the nonlinear spatio-temporal evolution of the EEG signals to find a governing rule as the system moves from a seizure-free to seizure state [2]. Srinivasan et al. [28] proposed a neural-network-based automated epileptic EEG detection system that uses approximate entropy (ApEn) as the input feature. ApEn is a statistical parameter that measures the predictability of the current amplitude values of a physiological signal based on its previous amplitude values. In [2], Adeli et al. presented a wavelet-chaos methodology for analysis of EEG for detection of seizures and epilepsy. In their research, the nonlinear dynamics of the original EEG are quantified in the form of the correlation dimension (CD, representing system complexity) and the largest Lyapunov exponent (LLE, representing system chaoticity). Their new wavelet-based methodology detects the changes in CD and LLE in delta (0-4 Hz), theta (4-8 Hz), alpha (8-12 Hz), beta (13-30 Hz) and gamma (30-60 Hz) sub-bands and classifies the EEG signals into Healthy EEG, Interictal (seizure-free) EEG and Ictal (during a seizure) EEG based on it.

1.2. Alcohol

Alcohol is one of the most commonly used substance in the world. Alcoholic beverages containing ethanol, a psychoactive drug with relaxant and euphoric effects [23], have been part of social life throughout the world for many years. Alcohol intoxication causes changes in various aspects of psychological function including changes in subjective mood (from states and feelings of relaxation to exhaustion and depression), or vomiting and loss of consciousness in cases of higher doses [23]. Alcoholism is also associated with brain defects and impairments in behaviour, psychomotor performance and cognitive processes. Alcohol, at the same time, increases sexual risk-taking, aggressive behavior, and traffic accidents [10].

Ethanol ingestion has been claimed as a cause of systematic changes in the characteristics of the normal, waking, background human EEG [21]. Studies in neuroimaging, physiology, neuropathology and neuropsychology concerned with alcoholics have indicated alcohol may cause damage and dysfunction in the frontal lobes, limbic system and cerebellum [23]. It has also been shown that neurophysiology parameters, which are affected by alcohol, can be detected through EEG signals. O'Boyle et al. [21] pointed out the impact of alcohol in the significant rise of absolute power, hence, the total absolute power in the theta and low alpha sub-band. There was also a significant increase of relative power in the low alpha while an opposite trend was seen in the high alpha and high beta. In [24], Porjesz and Begleiter reported that the alcohol-dependent people had higher resting theta power at all scalp locations. This reflected a deficiency in the information processing capacity of the central nervous system. In alcoholics, unstable poor alpha rhythm was found while there was also an increase in power in beta in frontal brain regions. While in the active brain condition, alcohol caused an increase in absolute power (amplitude) of delta, theta and alpha rhythms in both the frontal mid-line and parietal regions of the brain in both high and low load task conditions [14]. Similarly, the prefrontal region of the brain decreased the absolute power regarding to an increase in the amount of alcohol intake [14].

In this study, we tackle this issue by presenting a system for EEG-based key generation. We employ power spectral density estimate technique based on Autoregressive (AR) model from Burg's method for feature extraction

on EEG signals to obtain EEG features for EEG-based key generation systems. The AR model is used to find a set of parameters to describe the best of signal, and has been shown to be suitably used for epileptic seizure detection[20], and classification between alcoholic and non-alcoholic subjects[22]. Then, we investigate the impacts of brain conditions by the success rates of system. If brain conditions has impacts on the system, the success rates of disorder groups will be different from the normal groups. Moreover, we investigate the impacts of brain conditions on the length of keys generated, and the randomness of keys that is tested at a high level of significance by comprehensive battery of tests recommended by the National Institute of Standard and Technology (NIST)[5].

2. Related works

Keystroke biometric is among the first to be used to generate biometric keys[19]. By combining a user's typing patterns and a password to form a hardened password, each keystroke feature is discretized to be a single bit and uses error tolerance for feature variation, and a short bit string is obtained by concatenating these bits. Then, a more reliable implementation from voice was proposed using the same methodology[18]. This method has an improvement in performance to increase the entropy of key up to 46 bits, and decreases the false rejection rate to 20%[18].

Fingerprint is one of reliable biometrics used for key generation with its long history of use for criminal investigations[27]. Biometric information is extracted from fingerprint images by using the Fourier transform that decreases the variation of features. Keys are finally generated as follows: a predefined random key is locked with a biometric sample, and then unlocked by another biometric sample. This is a promising idea to generate random biometric key, however the system performance is not presented. Moreover, Clancy et al. proposed a "fuzzy vault" technique for a similar application that 69-bit keys can be generated with a high false negative rate of 30%.

Another biometric used is face that was proposed by Goh and Ngo[11]. They exploited the biometric-locking technique to extract eigen-projections as features of face images, then combined with a random string and quantized to obtain a single bit. These bits were concatenated and coded to generate a binary key. Goh and Ngo reported an implementation to generate 80-bit keys with a small false negative rate of 0.93%. However, the dataset for experiments is from a continuous video source that has minor variations instead of a face database.

Hao et al. are among the first to use iris for a similar application[12]. They propose an error-correction technique that combines Hadamard and Reed-Solomon codes. A key is generated from iris image and auxiliary data, and adversary needs both of them to recover the key. They generate keys up to 140 bits with 0.47% false negative rate.

3. EEG-based Cryptography Key Generation Method

Before presenting technical details of the construction, we first introduce some relevant cryptographic primitives and notation. We use the notation $\|$ to refer to string concatenation, and $L[i]$ is the i^{th} element in the list L. π is notated as a password of an user and $x \xleftarrow{R} X$ be the uniform selection of x at random from a set X, and $x \leftarrow A$ is to show that x is an output of algorithm A. Let $[a,b]_k = \{a + ik : i \in [0, \lfloor (b-a/k) \rfloor]\}$. E and D are 192-bit AES encryption and decryption algorithms. Four cryptographic hash functions are used: H_0 and H_1 are two functions that map a password in a set of passwords into two different elements in the key space. H_{ver} is a hash function used to generate a token to check whether a generated key is correct, and H_{key} is a hash function to generate a cryptographic key. We notate $B = \{\beta_1, \ldots, \beta_{M+1}\}$ to be a set of $(M+1)$ biometric samples from a user, $\Delta = 1 + max_i(\delta_i)$, and $\Phi = \{\phi_1, \ldots, \phi_N\}$ be a set of N feature vectors extracted from B that will be presented in the next section. Our method comprises of three phases: feature extraction, enrollment and key generation.

3.1. Feature Extraction

For feature extraction, in order to extract the individual EEG sub-bands, the autoregressive (AR) spectral analysis with Burg method is used to obtain the Power Spectral Density (PSD) of the signal. AR process is chosen due to its ability to handle short segment of data (in our case, 1 second of data) while giving high frequency resolution, and smooth power spectra[26]. Autoregressive process is given by $x(i) = \sum_{k=1}^{d} a_k x(i-k) + e(n)$ where $x(i)$ is the ith sampled data, d is the model order, a_k is the AR coefficients, and $e(i)$ is the prediction error term. Burg's method

is used to estimate the AR coefficients, because this method is more accurate than it used the data directly, whereas inaccuracies occur when Yule-Walker equations were directly used, or error source like bias in the autocorrelation function estimate happen in other parameter estimation methods[26]. Power spectral density (PSD) of a signal is a positive real function of a frequency variable associated with a stationary stochastic process. The PSD is defined as the discrete time Fourier transform (DTFT) of the covariance sequence[29]: $\psi(\omega) = \sum_{k=-\infty}^{\infty} r(k)e^{-i\omega k}$ with the auto-covariance sequence $r(k) = E(y(t)y^*(t-k))$ and $y(t)$ is the discrete time signal assumed to be a sequence of random variables with zero mean. After PSD estimate, the average power is computed to obtain a feature vector represented as $\Phi = (\phi_1, ..., \phi_N)$. The method consist of two algorithms: Enroll (Algorithm 1) and KeyGen (Algorithm 3).

3.2. Enrol

The Enrol phase is a process of 3 steps: threshold estimation, error correction, key generation and template creation. We assume IV to be a random and secrete number of 128-bit length used to protect the template.

Threshold Estimation. First, a user provides M biometric samples $\phi_i(\beta_1), \ldots, \phi_i(\beta_M)$, $i = 1, 2, ..., N$ and a password π. The system computes EEG features used for key generation, and determine thresholds to correct features of an user in algorithm 2.

Error-Correction Codes. In this step, we correct EEG features using the vector quantization technique. Its purpose is to correct features into a single, repeatable value by partitioning them into intervals, and performed as follows (see algorithm 1, step 4(a)-4(d)). First, we compute μ_i as the mean of $\phi_i(\beta_1), \ldots, \phi_i(\beta_M)$ for each index $i \in L$. Then, the range $R_i = [0, r_i]$ of each feature ϕ_i is partitioned around μ_i into intervals $([\alpha_i + k\delta_i, \alpha_i + (k+1)\delta_i, k \in [0, \lfloor (r_i/k) \rfloor] - 1)$ of length δ_i by computing a lowest boundary: $\alpha_i =$ if $\mu_i \geq \delta_i/2$, otherwise $\lfloor \mu_i + \delta_i/2 \rfloor$. Finally, an offset ρ_i of quantization is randomly chosen in the range $[\alpha_i, \Delta]_{\delta_i}$ with $\Delta = \max(\delta_i)_i$, and $x_i = \max(0, \lfloor \mu_i - \delta_i/2 \rfloor)$ is computed as the border of partition that contains μ_i.

Key generation. A key is derived from a password π, the feature indexes, and the quantized feature by computing $K_j = L[j] || x_{L[j]}$ with $j = 0, 1, ..., N-1$, and $K = H_{key}(\pi \parallel K_0 \parallel \ldots \parallel K_{|\Psi|-1})$. It means that K is the output of a hash function applied to the password, feature indexed and the lower boundary of partition.

Template creation Our goal is to protect the feature indexes and the quantization information so that only an user who has π and the ability of reproduction EEG signal that is close to the samples in enrollment phase can regenerate the correct key (step 3(e+f) in algorithm 1). The template is: $T = (C, v) = ((C_0, \ldots, C_{|L|-1}), H_{ver}(\pi \parallel K_0 \parallel \ldots \parallel K_{|\Psi|-1}))$, where C is used to store the feature indexes and the quantization offsets, and v is used for only verification, but is different from the key K because of two different hash functions H_{ver} and H_{key}.

3.3. Key Generation

The input the algorithm is a password π, the template $T = (C, v)$, and a new biometric sample β_{M+1}. This algorithm (see algorithm 3) consists of the following steps:

Firstly, features $\phi_1(\beta_{M+1}), ..., \phi_N(\beta_{M+1})$ are extracted from the sample β_{M+1}.

Secondly, the vector C is decrypted to reproduce the list L and the quantization offsets $\rho_{L[j]}$, $j = 0, ..., |C| - 1$. The value in list L are a list of feature indexes. After that, computing x_i to be the largest boundary of partition that is smaller than or equal to $\phi_i(\beta_{M+1})$ for $i = L[j]$, $j \in [0, |C| - 1]$, then letting $K_j = i || x_i$ and concatenating these values to produce a temporary key (see Steps 2(a)-2(c)).

Lastly, the temporary key $H_{ver}(\pi \parallel K_0 \parallel ... \parallel K_j)$ is hashed to check the result with v. If they are equal, the key $K = H_{ver}(\pi \parallel K_0 \parallel ... \parallel K_j)$ is output, otherwise the algorithm fails (see Steps 2(d) and 2(e)).

3.4. Security Analysis

To successfully unlock the cryptographic key (K) an adversary would require a) The password, b) The user biometric, and c) The template. The compromise of any one of these factors only is not enough to aid an adversaries to regenerate the correct key K. The password or user biometric cannot be used only to regenerate the correct key without the stored template (contained either in a smart card or central database store). Alternatively even if the template is compromised by an adversary, what an adversary can do is to guess a biometric β', a password π', and run the algorithm 3 with T, and hope the output matches K. However, no information about the user biometric and the key

Algorithm 1 Enroll

Input: Password π, sample set $\{\beta_1, \ldots, \beta_M\}$, and feature set $\Phi_u = \{\phi_1, \ldots, \phi_N\}$ of an user u, and multi-thresholds $\delta_1, \ldots, \delta N$ with $\Delta = max_i(\delta_i)$
Output: Key K and template T

1. $L \leftarrow Permute\{1, ..., N\}$
2. $k_0 \leftarrow H_0(\pi \oplus IV)$, $k_1 \leftarrow H_1(\pi \oplus IV)$
3. For $j = 0$ to $\mid L \mid -1$
   (a) $i \leftarrow L[j]$
   (b) $\mu_i \leftarrow Mean(\phi_i(\beta_1), \ldots, \phi_i(\beta_M))$
   (c) $\alpha_i \leftarrow \lfloor \mu_i - \delta_i/2 \rfloor \bmod \delta_i$ if $\mu_i \geq \delta_i/2$. Otherwise, $\lfloor \mu_i + \delta_i/2 \rfloor$
   (d) $x_i \leftarrow \max(0, \lfloor \mu_i - \delta_i/2 \rfloor)$
   (e) $\rho_i \overset{R}{\leftarrow} [\alpha_i, \Delta]_{\delta_i}$
   (f) $C_j = (E^N_{k_0}(i), E^{\Delta}_{k_1}(\rho_i))$
   (g) $K_j = i \parallel x_i$
4. $K \leftarrow H_{key}(\pi \parallel K_0 \parallel \ldots \parallel K_{|\Psi|-1})$
5. $T \leftarrow (C, v) = ((C_0, \ldots, C_{|L|-1}), H_{ver}(\pi \parallel K_0 \parallel \ldots \parallel K_{|\Psi|-1}))$
6. Return K and T

Algorithm 2 Multi-Threshold Estimation

Input: Feature set $\Phi = \{\phi_1, \ldots, \phi_N\}$ and sample set $\{\beta_1, \ldots, \beta_M\}$ of a user u.
Output: Quantization thresholds $\delta_1, \ldots, \delta_N$

1. For $i = 1 \ldots N$
   (a) Sorting $\phi_i(\beta_1), \ldots, \phi_i(\beta_M)$ in ascending order
   (b) $\lambda_i = mean(\phi_i(\beta_1), \ldots, \phi_i(\beta_M))$
   (c) $t_i = max(\phi_i(\beta_M) - \lambda_i, \lambda_i - \phi_i(\beta_1))$
   (d) $\epsilon_i = \frac{1}{M-1} \sum_{k=1}^{M-1} (\phi_i(\beta_{k+1}) - \phi_i(\beta_k))$
   (e) $\delta_i = 2(t_i + \epsilon_i)$
2. Return $\delta_1, \ldots, \delta_N$

K can be leaked. The template is derived from C and v which is generated independently from completely separate random process. C is produced from any cryptographically secure encryption algorithm whose outputs do not leak any information about its inputs because IV is sufficient secure[5], therefore it will not leak no information about the user biometric, and protect the template better than RBTs. Moreover, K and v produced from independently hash functions whose outputs are random, so there is no information about K to be leaked if v is compromised.

On the other hand, if the K is badly comprised, an adversary is unable to find a collision to discover the user biometric with knowledge of password and the template because of secure hash function and random permutation used. In this case, a new key can be issued, and the user will be required to provide a new biometric measurement to

Algorithm 3 KeyGen

Input: Template $T = (C, v)$, passwords π, sample β_{M+1}, feature $\Phi_{M+1} = (\phi_{M+1,1}, ..., \phi_{M+1,N})$ of this sample, and multi-thresholds $\delta_1, ..., \delta_N$

Output: Key K or $\perp$

1. $k_0 \leftarrow H_0(\pi \oplus IV), k_1 \leftarrow H_1(\pi \oplus IV)$
2. For $j = 0$ to $| C | -1$
   (a) $i \leftarrow D^N_{k_0}(C[j][0])$
   (b) $\alpha_i \leftarrow D^N_{k_1}(C[j][1])$s
   (c) $x_i \leftarrow \max_{x \in 0 \cup [\alpha_i, \phi_{M+1,i}(\beta_{M+1})]_{\delta_i}} x$
   (d) $K_j = i \parallel x_i$
   (e) if $H_{ver}(\pi \parallel K_0 \parallel ... \parallel K_j) = v$ then $K = H_{key}(\pi \parallel K_0 \parallel \ldots \parallel K_j)$
   (f) Return K
3. Return $\perp$

the system, and the old biometrics will be cancelled. This method is flexible for EEG signals, but the new biometrics may be derived from the old template[4] for iris (cannot be changed) to generate a new key.

4. Experiments and Results

Our experiment was conducted on the Australian EEG (AEEG) dataset[13] and the Alcoholism dataset[6] that are summarized in Table 1.

The AEEG dataset was collected in the John Hunter Hospital, New South Wales, Australia, over a period of 11 years. The recordings were made by using 23 electrodes placed on the scalp of a subject with the sampling rate of 167 Hz for about 20 minutes, on patients aged 2-10 years with epilepsy, cognitive disability and language regression with autism or autistic features, and patients aged 16-25 years where psychotic symptoms were noted in the history field. Exclusion criteria were a confirmed history of clinical seizures and acute physical illness or injury. The subset of the data used for our experiments consists of the EEG data of 80 subjects.

The Alcoholism dataset comes from a study to examine EEG correlations of genetic predisposition to alcoholism. The dataset was obtained from the University of California, Irvine Knowledge Discovery in Databases (UCI KDD) Archive, and consisted of EEG recordings of 122 alcoholic and control subjects. Each of these subjects was measured by placing 64 electrodes on their scalps sampled at 256 Hz for one second. In the recording stage, each subject was exposed to either a single stimulus (S1) or to two stimuli (S1 and S2) which were pictures of objects chosen from the 1980 Snodgrass and Vanderwart picture set. When two stimuli were shown, they were presented in either a matched condition where S1 was identical to S2 or in a non-matched condition where S1 differed from S2. The full dataset contains data of 77 alcoholic and 45 control subjects.

Table 1: EEG Dataset Descriptions

Datasets	Group	Number of Subjects	Number of Channels	Number of trials	Number of sessions	Trial length (seconds)
AEEG	Non-epileptic	40	23	60	1	15
	Epileptic	40	23	60	1	15
Alcoholism	Non-alcoholic	45	64	120	1	1
	Alcoholic	45	64	120	1	1

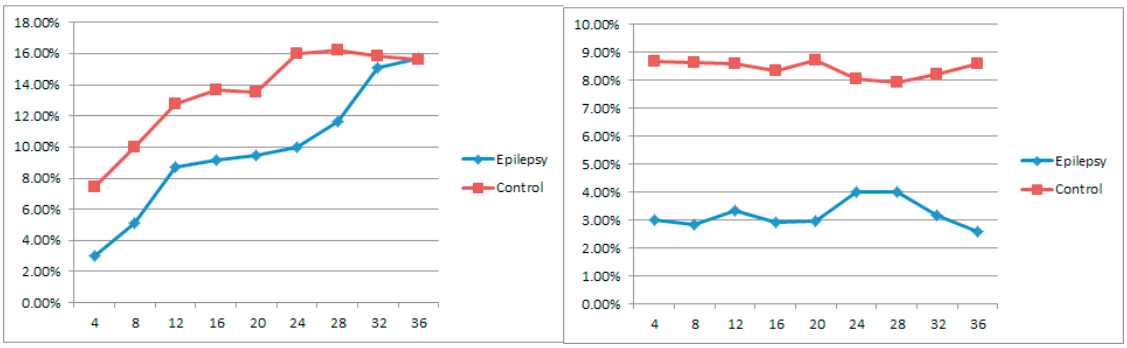
We use the equal error rate (EER) when the false rejection rate (FRR) equals to the false acceptance rate (FAR) to evaluate this method. To compute the FRR we use the repeated leave-out-κ cross validation method. Given ν enrollment samples, we random choose $\nu - \kappa$ samples to create a training data for generating a key and a template in

Table 2: Optimal Order of EEG datasets. StD = Standard Deviation

Datasets	Groups	Mean	Std
Alcoholism	Alcoholic	26.6	8.27
	Control	30.48	5.24
AEEG	Epilepsy	6.52	4.23
	Control	10.8	3.76

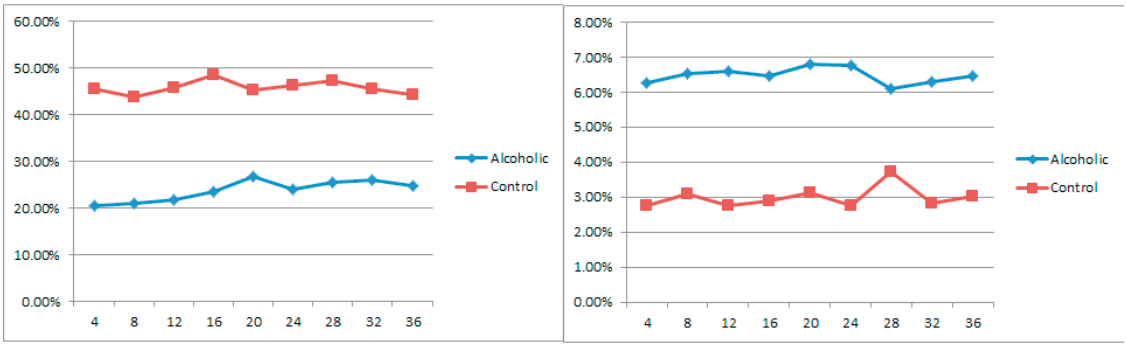
the enrollment phase. Then we use the remaining κ samples to create a testing data to regenerate the key with this template, and measure the number of samples that the key are not regenerated. We set the ratio of ν and κ to be 3:1. This process is repeated 10 times and averages across all 10 runs are used to compute FRR. To compute FAR, we use all of samples of a user from a training data to create a key and a template, and all samples from a testing data of remaining users to test the ability of forgers to regenerate the correct key.

Among the criteria for selection of the optimal order of the AR model, the Akaike information criterion (AIC)[3] were evaluated in this work. AR-based spectral analysis has an inconvenience that the order of AR model have to be estimated prior to the spectral analysis[8]. The technique used in this paper is similar to the approach presented in[8] in order to determine optimal AR model orders for spectral analysis of short segments of the time series including EEG. Table 2 shows that range of AR order is selected from 4 to 36.



(a) (b)

Fig. 1: EERs of the method for AEEG dataset by orders (a) EEG wave and (b) Gamma



(a) (b)

Fig. 2: EERs of the method for Alcoholism dataset by orders (a) EEG wave and (b) Gamma

Table 3: Error equal rates (%) of AEEG dataset

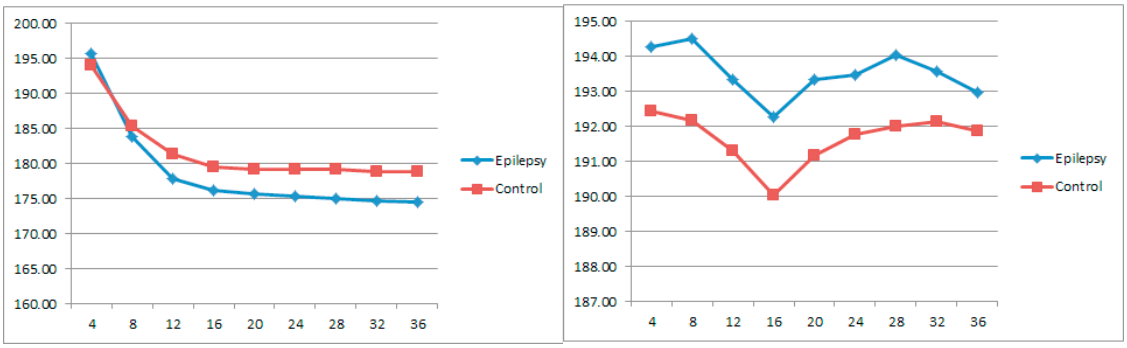
Wavebands	EEG	Gamma
Epileptic	2.99	**2.58**
Non-epileptic	7.43	7.92

Table 4: Error equal rates % of Alcoholism dataset

Wavebands	EEG	Gamma
Alcoholic	20.60	6.11
Non-alcoholic	43.86	2.78

Experimental results are presented in two figures 1, 2, and two tables 3, 4. First, we do investigation the variation of EERs between epileptic group and non-epileptic group by a variation of an order of Autoregressive model for EEG wave and gamma. The other sub-bands (alpha, beta, delta and theta) provides poor performance and they are not presented further. We are not aiming to compare the EERs on the same feature extraction method, but we can have a remark on why the epileptic group has a smaller error rates than others. As shown in the figure 1, the performance between EEG wave and the gamma band are very similar, and the smallest of EEG is 2.58% observed at order 36 from the gamma. In addition, the EERs of the epileptic group are always smaller than of the normal group for all three bands. While the maximum difference is 6.01% observed at order 36 in the gamma band, the minimum difference is 4.44 at order 4 in EEG wave as seen in table 3. Although it is not significant to see whether random difference between the two datasets or epilepsy has contributed to the performance of key generation system, the later case would be appropriate as epileptic EEG signals are less chaotic and complex than normal EEG signals [16,25]. As a result, this may make epileptic EEG signals more suitable with linear methods such as Autoregressive model, thus, it probably helps to increase the accuracy of EEG-based cryptographic key generation system.

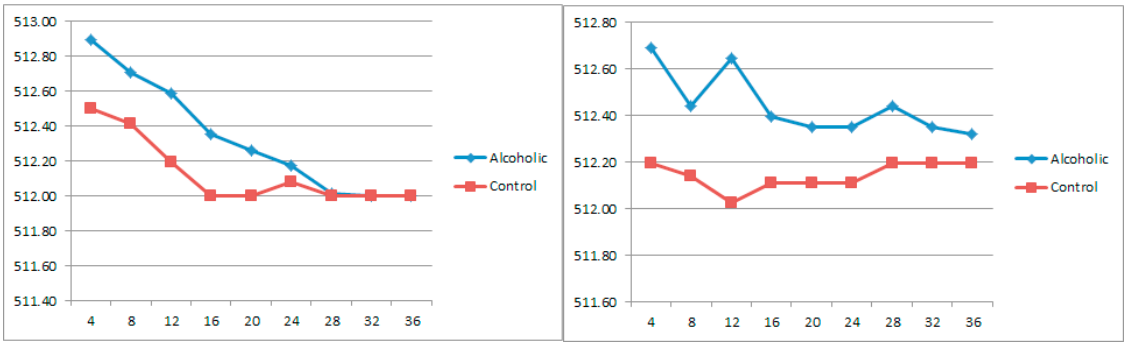
In contrast, the alcoholic group always have higher equal error rates than of the normal group as shown in figure 2 for three bands. As demonstrated in table 4, the difference of EER between EEG wave and the gamma is large at a maximum of 41.08% observed at the normal group. Moreover, the EER of alcoholic group has a minimum of 6.11%, recorded at order 28 in the gamma band, larger than the normal group of 2.78%. This would support the hypothesis that that alcoholic has impact on the performance of key generation system [22]. As stated in [1,22], alcoholic EEG signals are more chaotic and complex than normal EEG signals. In addition, Autoregressive model is a tool to discriminate chaotic levels, i.e, the higher values reflects the more chaotic signals, and vice versa [9]. As a result, the more chaotic property of the alcoholic EEG signals makes the higher values. Therefore, it causes the higher inter-class variation which results in the higher equal error rates of alcoholic group. Our design achieves a good performance which the accuracy is very close to Monrose's work [18], 97.42% versus 98%.



(a) (b)

Fig. 3: The average of key length for AEEG dataset by orders (a) EEG wave and (b) Gamma

In the next experiments, we used a comprehensive battery of tests from NIST [5] to evaluate for randomness of keys generated. First, for key length selection, we measure the average of key length for users in the datasets. As shown in figure 3 and 4, key length is affected by frequency bands, and selected to be 192 bits for AEEG and 512 for Alcoholism that is the largest for both gamma band and EEG wave, and suitably used for 192-bit and 512-bit AES application. The reason is that each channel generated a character containing at least 8 bits as seen in the step 3(g) on algorithm 1. Next, for randomness tests, we use six out of fifteen tests in the NIST Test Suite as other tests requires more than



(a) (b)

Fig. 4: The average of key length for Alcoholism dataset by orders (a) EEG wave and (b) Gamma

Table 5: Results of NIST Test Suite for randomness from AEEG dataset of EEG wave and gamma band. Values in table are percentage of passing rates. Results for beta band is not presented because of small key length.

Wavebands	EEG		Gamma	
	Epilepsy	Non-Epilepsy	Epilepsy	Non-Epilepsy
Frequency	97.37	100.00	100.00	100.00
Block Frequency	100.00	100.00	97.37	100.00
Runs	73.68	78.95	78.95	86.84
Longest Run of ones	100.00	100.00	100.00	100.00
Approximate Entropy	100.00	100.00	100.00	100.00
Serial	97.37	94.74	100.00	94.74
Serial	97.37	97.37	100.00	100.00
Success Rate	**95.11**	**95.86**	**96.62**	**97.37**

Table 6: Results of NIST Test Suite for randomness from Alcoholism dataset of EEG wave and gamma band. Values in table are percentage of passing rates.

Wavebands	EEG		Gamma	
	Alcoholic	Non-Alcoholic	Alcoholic	Non-Alcoholic
Frequency	100.00	100.00	100.00	100.00
Block Frequency	100.00	100.00	100.00	100.00
Runs	77.94	83.33	83.82	83.33
Longest Run of Ones	97.06	97.22	95.59	91.67
Approximate Entropy	100.00	100.00	100.00	100.00
Serial	94.12	97.22	94.12	97.22
Serial	97.06	97.22	97.06	97.22
Success Rate	**95.17**	**96.43**	**95.80**	**95.63**

1000-bit length. Six testes include frequency, block frequency, runs, longest run, approximate entropy, and serial that has two tests. As shown in table 5 and 6, generated keys pass the most of six tests with high success rates, it means that the keys are good random. Moreover, the success rate of normal group is similar to the disorder group of both alcohol and epilepsy for all three bands, and it shows that brain disorders do not has impacts on the randomness of keys. Moreover, the success rates approach the best results from other existing RNGs such as Blum Blum Shub[7], and Micali Schnorr[17].

Overall, we can see the changes on EERs of EEG-based cryptographic key generation system for the epileptic and alcoholic datasets, but they do not have impacts on the randomness of keys generated.

5. Conclusion

In this paper, we have found that brain conditions have impacts on the performance of EEG-based cryptographic key generation systems. This implies that a cryptographic key generation system will provide high performance on the users that have mental disorder such as epilepsy and alcoholic. For further investigation, we will conduct experiments on other feature extraction methods as well as on a larger scale of datasets for confirming the influences of brain conditions on cryptographic key generation systems.

References

1. U. R. Acharya, S. V. Sree, S. Chattopadhyay, and J. S. Suri, "Automated diagnosis of normal and alcoholic eeg signals," *International journal of neural systems*, vol. 22, no. 03, p. 1250011, 2012.
2. H. Adeli, S. Ghosh-Dastidar, and N. Dadmehr, "A wavelet-chaos methodology for analysis of eegs and eeg subbands to detect seizure and epilepsy," *IEEE Transactions on Biomedical Engineering*, vol. 54, no. 2, pp. 205–211, 2007.
3. H. Akaike, "A new look at the statistical model identification," *IEEE transactions on automatic control*, vol. 19, no. 6, pp. 716–723, 1974.
4. L. Ballard, S. Kamara, and M. K. Reiter, "The practical subtleties of biometric key generation." in *USENIX Security Symposium*, 2008, pp. 61–74.
5. E. Barker, "Nist special publication 800-57 part 1 revision 4 recommendation for key management–part 1: General," 2016.
6. H. Begleiter, "Eeg alcoholism database," *Online: https://kdd.ics.uci.edu/databases/eeg/eeg.data.html*, 1999.
7. L. Blum, M. Blum, and M. Shub, "A simple unpredictable pseudo-random number generator," *SIAM Journal on computing*, vol. 15, no. 2, pp. 364–383, 1986.
8. A. Boardman, F. S. Schlindwein, and A. P. Rocha, "A study on the optimum order of autoregressive models for heart rate variability," *Physiological measurement*, vol. 23, no. 2, p. 325, 2002.
9. V. Cuomo, V. Lapenna, M. Macchiato, and C. Serio, "Autoregressive models as a tool to discriminate chaos from randomness in geoelectrical time series: an application to earthquake prediction," *Annals of Geophysics*, vol. 40, no. 2, 1997.
10. M. Field, R. W. Wiers, P. Christiansen, M. T. Fillmore, and J. C. Verster, "Acute alcohol effects on inhibitory control and implicit cognition: implications for loss of control over drinking," *Alcoholism: Clinical and Experimental Research*, vol. 34, no. 8, pp. 1346–1352, 2010.
11. A. Goh and D. C. Ngo, "Computation of cryptographic keys from face biometrics," in *Communications and Multimedia Security. Advanced Techniques for Network and Data Protection*. Springer, 2003, pp. 1–13.
12. F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," *Computers, IEEE Transactions on*, vol. 55, no. 9, pp. 1081–1088, 2006.
13. M. Hunter, R. L. Smith, W. Hyslop, O. A. Rosso, R. Gerlach, J. Rostas, D. Williams, and F. Henskens, "The australian eeg database," *Clinical EEG and neuroscience*, vol. 36, no. 2, pp. 76–81, 2005.
14. G. Janvale, S. Kendre, and S. Mehrotra, "Mental and behavioural disorders related to alcohol and their effects on eeg signals–an overview," *Procedia-Social and Behavioral Sciences*, vol. 133, pp. 116–121, 2014.
15. N. Kannathal, M. L. Choo, U. R. Acharya, and P. Sadasivan, "Entropies for detection of epilepsy in eeg," *Computer methods and programs in biomedicine*, vol. 80, no. 3, pp. 187–194, 2005.
16. Y. Kumar and M. Dewal, "Complexity measures for normal and epileptic eeg signals using apen, sampen and sen," *IJCCT*, vol. 2, no. 7, pp. 6–12, 2011.
17. S. Micali and C. Schnorr, "Pseudo-random sequence generator," Jul. 24 1990, uS Patent 4,944,009.
18. F. Monrose, M. K. Reiter, Q. Li, and S. Wetzel, "Cryptographic key generation from voice," in *Security and Privacy, 2001. S&P 2001. Proceedings. 2001 IEEE Symposium on*. IEEE, 2001, pp. 202–213.
19. F. Monrose, M. K. Reiter, and S. Wetzel, "Password hardening based on keystroke dynamics," 1999.
20. S. Mousavi, M. Niknazar, and B. V. Vahdat, "Epileptic seizure detection using ar model on eeg signals," in *Biomedical engineering conference, 2008. CIBEC 2008. Cairo International*. IEEE, 2008, pp. 1–4.
21. D. J. O'Boyle, F. Van, and K. I. Hume, "Effects of alcohol, at two times of day, on eeg-derived indices of physiological arousal," *Electroencephalography and clinical Neurophysiology*, vol. 95, no. 2, pp. 97–107, 1995.
22. K.-M. Ong, K.-H. Thung, C.-Y. Wee, and R. Paramesranle, "Selection of a subset of eeg channels using pca to classify alcoholics and non-alcoholics," in *Proceedings of the 2005 IEEE Engineering in Medicine and Biology 27th Annual Conference (Shanghai, China, 2005)*, 2005.
23. M. Oscar-Berman and K. Marinković, "Alcohol: effects on neurobehavioral functions and the brain," *Neuropsychology review*, vol. 17, no. 3, pp. 239–257, 2007.
24. B. Porjesz and H. Begleiter, "Alcoholism and human electrophysiology," *Alcohol research and health*, vol. 27, no. 2, pp. 153–160, 2003.
25. S. Sanei and J. A. Chambers, *EEG signal processing*. John Wiley & Sons, 2013.
26. R. Shiavi, *Introduction to applied statistical signal analysis: Guide to biomedical and electrical engineering applications*. Academic Press, 2010.
27. C. Soutar and G. Tomko, "Secure private key generation using a fingerprint," in *Cardtech/Securetech Conference Proceedings*, vol. 1, 1996, pp. 245–252.
28. V. Srinivasan, C. Eswaran, and N. Sriraam, "Approximate entropy-based epileptic eeg detection using artificial neural networks," *IEEE Transactions on information Technology in Biomedicine*, vol. 11, no. 3, pp. 288–295, 2007.
29. P. Stoica and R. L. Moses, *Spectral analysis of signals*. Pearson Prentice Hall Upper Saddle River, NJ, 2005, vol. 452.