Received: 2012-01-07
Accepted: 2012-02-10
Original Article
JMSS/ April 2012, Vol 2, No2

Assessment of Human Random Number Generation for Biometric Verification

First A. Elham Jokar[1]; Second B. Mohammad Mikaili[2]

ABSTRACT

Random number generation is one of the human abilities. It is proven that the sequence of random numbers generated by people do not follow full randomness criteria. These numbers produced by brain activity seem to be completely non stationary. In this paper, we show that there is a distinction between the random numbers generated by different people who provides the discrimination capability, and can be used as a biometric signature. We considered these numbers as a signal, and their complexity for various time-frequency sections was calculated. Then with a proper structure of a support vector machine (SVM), we classify the features. The error rate obtained in this study, shows high discrimination capabilities for this biometric characteristic.

KEYWORDS

Random number generation, verification biotelemetry, wavelet decomposition, approximate entropy, support vector machine

1. INTRODUCTION

The Longman Dictionary of Contemporary English describes 'random' as: ''happening or chosen without any definite plan, aim, or pattern''. A sequence of numbers is said to be random, if the next element can't be predicted from the previous one [2].

For many years, scientists have been checking the ability of human beings in generating true random numbers. During the random number generation, each subject has his/her own strategy and must partially memorize the previous numbers and choose the next one based on his/her own conception of randomness.

Since 1960, Alan B. Baddeley investigated in this field extensively. Recently, new statistical processing methods have been applied to discover this ability of human beings and in most of them man has been known as a bad random number generator [1]-[3].

Generally, generation of random numbers activate certain areas of the brain. If numbers are not written down, then the mind can only review those numbers held in short term memory which causes pattern suppression [3]. Because of this process, the random sequence generated by people, is biased compared to true random numbers [2]. Analysis of random numbers generated by people to investigate short term memory function and attention is a well-explored area of psychological research [3].

When someone is asked to generate random numbers, a cognitive load is implied, since there is a close interaction between executive memory and internalized decision making mechanisms. Several studies in cognitive psychology show that the generation of random rhythms is a cognitive task and has enough information for discrimination of different clinical populations.

A closely related task to number generation is random rhythms of tapping a key [4]. The first assessment of this idea is done in a study by Hornero et.al[5] in classification of schizophrenic patients from healthy subjects. He showed that the tapping rhythm of schizophrenic patients differ from healthy subjects ($p_{ANOVA} < 0.001$). The time series generated by tapping a key for schizophrenic patients had a lower complexity and variability than the healthy subjects. He used chaotic dynamic attractors and the second-order difference plots of the time series, and calculation of the correlation dimension and the central tendency measure (CTM) parameter. Then he concluded that this test could be a complementary tool to help physicians in the estimation of cognitive-motor dysfunction in schizophrenic patients.

In 2006, Hornero et.al[6], analysed the time series generated by schizophrenic patients and control subjects using three nonlinear methods of time series: CTM from the scatter plots of first differences of data, approximate entropy (ApEn), and Lempel-Ziv (LZ) complexity. He constructed a training set and a test set and used the training set for algorithm development and optimum threshold selection. Each method was assessed using the test dataset. He obtained 80% sensitivity and 90% specificity with LZ complexity, 90% sensitivity, and 60% specificity with ApEn, and 70% sensitivity and 70% specificity with CTM. His results show differences in the ability to generate random time series between schizophrenic subjects and controls, as estimated by the CTM, ApEn, and LZ.

[1] E. joker, Msc student of Engineering Department, Shahed University, Tehran, Iran (e.mail: elhamjokar@gmail.com)
[2] M. Mikaili , Assistant Professor of Engineering department, Shahed University, Tehran, Iran (e.mail: mikaili@shahed.ac.ir)

Received: 2012-01-07
Accepted: 2012-02-10

Until this time, random rhythms just used to discriminate between clinical and control subjects, but In 2009, Laskaris et.al[4] has suggested a new method in biometric verification with the repetitive pressing of a button in a random manner. Biometrics includes methods for recognizing a person, based on a physiological characteristic, like fingerprints, face, hand geometry, handwriting, iris and voice. As the level of security violations and transaction fraudulent increases, the need for highly secure identification and personal verification technologies is becoming apparent. Biometric solutions are able to provide for confidential financial transactions and personal data privacy. Utilizing biometrics for personal identification is becoming considerably more reliable and convenient than current methods. Current methods such as the utilization of passwords may be used by someone other than the authorized user and also it is required to memorize, but biometrics links the event to a particular individual and because of this reason it has the low possibility of error and fraud. The first wave of biometrics includes natural characters were distinctive and static, like recognizing a person, based on his\her fingerprints, iris, hand geometry, vein topography…When the fraud caused the loss of security, the scientists tried to find the second wave of biometrics with more dynamic characteristics like the voice and handwriting style which are difficult to be imitated. One of the biometric approach in this kind is Keystroke dynamics which known as typing recognition. It analyses the way a person types, since no extra hardware is required and typing is the most natural way for a user to interact with the system in most applications, particularly over the world-wide web. However, the passage to be typed might need to be fixed and this means a memory load, similar to remembering an extra password. Moreover, there is a potential change due to continuous practice of the same typing patterns[8]. The new biometric character introduced by laskaris was the random time intervals of tapping a key, in which the simplicity of interface is kept, while the restriction of typing specific patterns is alleviated. Key stroke dynamic is a cognitive task, since it depends on higher brain functions that can be indirectly measured in random generation. Interestingly, he demonstrated that everyone has his own Eigen-rhythms regulating spontaneous finger tapping. laskaris used this ability of humans to verifying the person's identity. His proposed method was based on graph theory and calculated similarity between two signals for identification of their generators. Their study could achieve 93% accuracy with Support Vector Machine (SVM), 95% accuracy with Minimum Class Variance Support Vector Machine (MCVSVM) classifiers[4].

In this paper a new method is suggested for distinction between the random generations of individuals. This method has been used for chaotic quantification of cerebral signals. To demonstrate the effectiveness of this method, two different protocols were designed. The first protocol is based on laskaris experiments. The second test, which is a new protocol in the field of biometrics, was established on human conception of the random numbers.

When someone is asked to generate (verbally of via keyboard) random numbers, there is a cognitive load implied, since there is a close interaction between short-term memory and internalized decision making mechanisms.

This ability of humans is very valuable, especially in a world where counterfeiting and fraud has been rampant and the need for highly secure identification and personal verification technologies is becoming obvious.

In this study, we test a new method for identification people from their random tapping and verify if a discrimination scenario which proposed, is possible by random generation of numbers. To answer these questions, two different experiments were established:

- Subjects should press the keyboard keys in a random manner. The time intervals between the hits are considered as a signal for that subject.

-In the second test, we choose a special range of the number space (1-9) as our original set, and subjects were asked to keep this set in mind and generate random numbers verbally.

Due to the non-stationary characteristics of the signals in both experiments, we used Complexity assessment methods to distinguish between number sets generated by individuals. Part 2 describes the conditions of the experiments. In section 3 the method of feature extraction will be explained. Section 4 includes the results and final

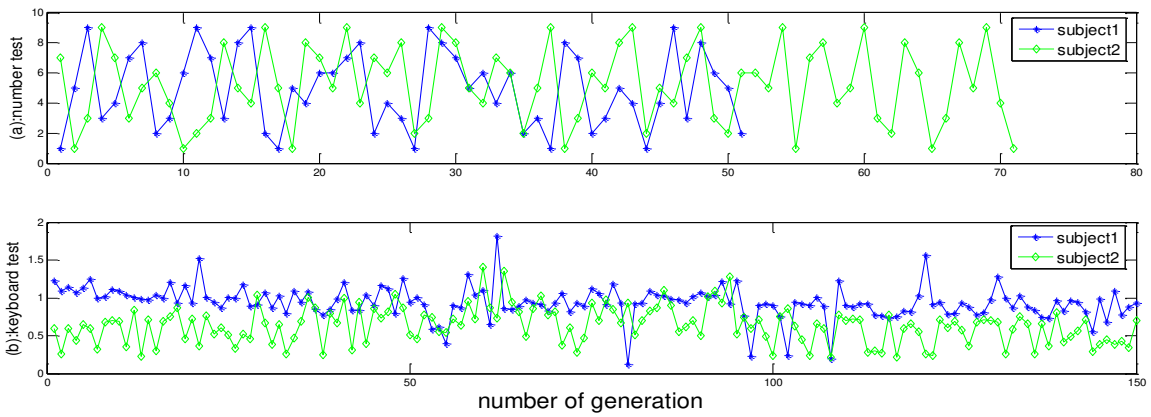

Figure 1: Example of signals generate by two subjects in different tests, (a): number test for two subjects with different length, (b): keyboard test for different subjects

Received: 2012-01-07
Accepted: 2012-02-10

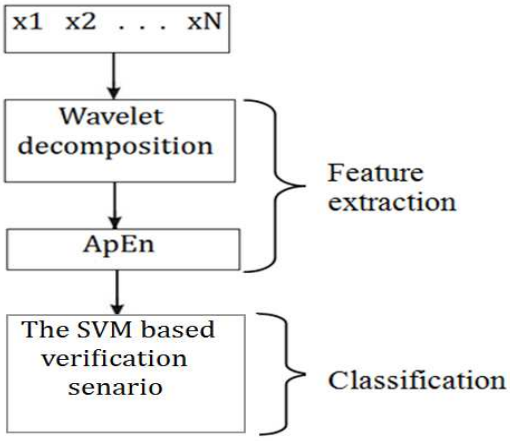

Figure 2: Schematic of our signal processing method

section contains a brief discussion on the results obtained in this study.

2. PROTOCOLS AND PARTICIPANTS

30 subjects (6 male and 24 female aged 24.6±1.505) participated in this experiment. The subjects did the tests while they were seated relaxed in a quite laboratory. During the tests, only one participant attended in the laboratory at a time. This restriction was imposed to minimize the environmental effects their performance. Each participant was asked to do the tests 10 times in five different days. In each session, two parts was performed. Each part consists of two protocols: number test and keyboard test. Subjects had a short break for a few minutes between each two parts in one session.

A. Numbers test

Due to the mental perception of subjects of decimal number space, the selection range was set from 1 to 9, and the subjects must generate a sequential series of random numbers verbally in a limited time (140 seconds per test). The meaning of the random numbers was explained with the theory of hat and nine numbered balls in it. The description of randomness was the same for all subjects, and they were not allowed to ask any questions. To generate a random number, the subject should imagine taking a ball out of the hat, read its number and return it. In this study we don't use the external paced for number generation and subjects should generate numbers with their own rhythm. We considered time limitation in this protocol because our processing was independent of the length of the signals. **Figure 1**. shows two examples of random number signals recorded from two different subjects. During the test, voice of the subjects was recorded and transcribed later by the experimenter on a personal computer and converted to a MATLAB signal.

B. Keyboard test

In this test, subjects were asked to press the keys of the keyboard with the index finger of their dominant hand in an as random manner as possible, until the screen shows the end of the exercise. In first session for each subject the meaning of random time interval for pressing the space key was explained with an example consist of a square 4×4 cm, which appears and disappears in the screen at random rhythm. In this study the number of strokes were T=150. This increase in length of the signals in compare with previous work is to eliminate the effect of subjects fatigue for two consecutive protocols (number test and keyboard test). If X[n] denotes the sequence of exact time-latencies of subjects hits X[n] = $[t_1,t_2,...,t_T]$, the corresponding signal takes the form x[n] = $[t_2-t_1,t_3-t_2,...,t_T-t_{T-1}]$. After each test, this series was reconstructed and used as input signal. Figure 1.b shows two random time interval for two subjects.

3. SIGNAL PROCESSING

The processing was performed in two stages:

A. Feature extraction
B. Classification:

In **Figure 2** a schematic of our signal processing method is shown. In following sections each of these steps is described.

A. Feature extraction

In first stage, features are extracted from the data using time–frequency domain methods. Since the signal has non-stationary characteristics in general, it is more appropriate to use time–frequency domain methods like wavelet transform for feature extraction. Wavelet transform does not require the assumption of "quasi-stationary" on the data. It supports both time and frequency aspects of a signal simultaneously, which makes it possible to capture accurately and localize transient characteristics of the data. Signals were decomposed into various frequency bands through wavelet packet decomposition. Then, the Approximate Entropy (ApEn) -subsequently described- of the wavelet coefficients is calculated at the various nodes of the decomposition tree and used as a feature set for training the proper classifier. ApEn is a measure of predictability or regularity of a time series and helps to understand the underlying chaotic behaviour of the brain that shows itself in the numbers.

Wavelet Packet Decomposition (WPD): Wavelet packet analysis is a generalized form of the discrete wavelet transform. In the wavelet packet analysis, the signal is first passed through a low-pass and a high-pass filter, in parallel. The cut-off frequencies of these filters are one-fourth of the sampling frequency. The bandwidth of the filters *is* half the bandwidth of the original signal, which allows downsampling of the output signals by two

Received: 2012-01-07
Accepted: 2012-02-10

without losing any information according to the Nyquist theorem. At each level of the decomposition, frequency resolution is doubled through filtering while the time resolution is halved by downsampling operation [7]. In this study, signals were decomposed into various frequency bands through *a two* level wavelet packet decomposition. Based on the shape of signals, Daubechi2 (Db2) mother wavelet is used for th*e decomposition. After this two* level decomposition, we have 7 vectors of wavelet coefficients for each signal; we then calculate ApEn for each of the vectors and construct the feature matrix.

Approximate Entropy (ApEn): ApEn which is derived from the Kolmogorov–Sinai entropy is a tool for calculation of the complexity of a signal. It is defined as the log likelihood (how likely is) that runs of patterns of certain length that are close to each other will remain close on next incremental comparisons [7]. A deterministic signal is expected to have a smaller ApEn value than a highly irregular or random one. To compute the ApEn of a signal, y_i ,i=1,…,N, the trajectory in the embedding space, R_m, must first be reconstructed using the reconstruction method:

$$x_i = \{y_i, y_{i+\tau}, y_{i+2\tau}, \ldots, y_{i+(m-1)\tau}\}, 1 \le N-(m-1)\tau \quad (1)$$

Where N is the length of the number signal and τ and m are the time delay and embedding dimension, respectively. The distance between two points of the trajectory can be considered as the maximum difference in their corresponding elements:

$$d(x(i), x(j)) = \max_{k=1,2,..,m}(|\, y(i+(k-1)\tau) - y(j+(k-1)\tau)\,|) \quad (2)$$

Then, the similarity between a point of the trajectory and the others are computed as:

$$C_i^m(r) = \frac{1}{N-(m-1)\tau} \sum_{j \ne i} \theta(r - d(r - d(x(i), x(j)))) \quad (3)$$

Where θ(x)=1 for x>0, and θ(x)=0 otherwise, and r is the vector comparison threshold. Finally, we define $\Phi^m(r)$ as:

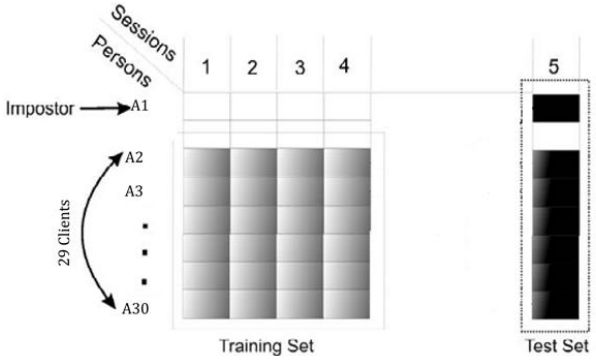

Figure 3: Verification scenario

$$\phi^m(r) = \frac{1}{N-(m-1)\tau} \sum_{i=1}^{N-(m-1)\tau} \log C_i^m(r) \quad (4)$$

For fixed m, r and τ, ApEn is defined as:

$$ApEn(m, r, \tau, N) = \phi^m(r) - \phi^{m+1}(r) \quad (5)$$

The ApEn is calculated for the wavelet coefficients obtained in the previous step and are used as our features. Thus, for each signal, 7 vectors were obtained by WPD and Entropy was calculated for each of them. Vector comparison distance (r) and the time delay (t) were set to 0.15 times the standard deviation of the coefficients and 1, respectively. Different results were obtained using different values for m.

B. Classification

After construction feature matrix from ApEn, it can be used for training a suitable classifier. For each of the 30 participants, there were ten signals, so totally we had 300 signals with 7 features for each. Therefore, the size of the feature matrix was 300x7. Due to the large number of classes (every subject is considered as a class), and a small number of data for each class, neural network was not recognized as a suitable classifier. However, the Support Vector Machine (SVM), has the required characteristics and was used as our classifier. The SVM method is based on the solution of a quadratic optimization problem that represents a trade off between the minimization of the empirical error and the maximization of the smoothness of the regression function. In the present work, different kernels were used for classification to choose the best one. To solve the problem of lack of data in each class and

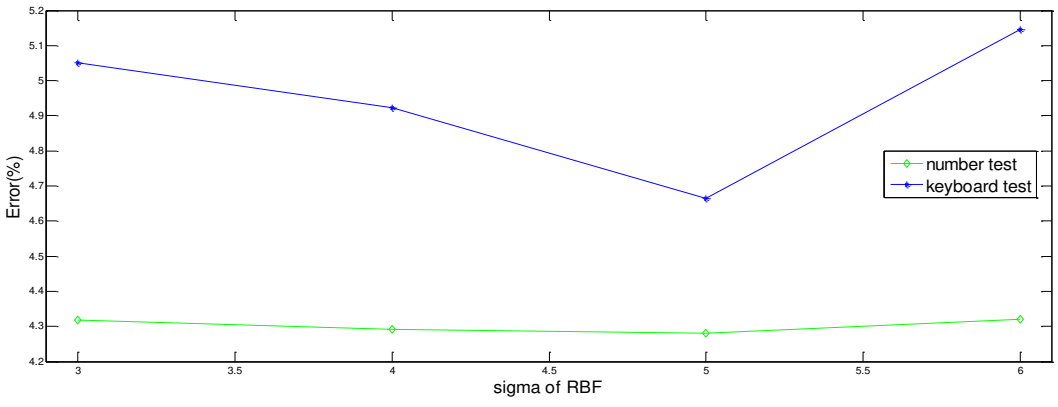

Figure 4 results of SVM based scenario for keyboard test and number test with RBF kernel

Received: 2012-01-07
Accepted: 2012-02-10

TABLE1

ERROR RATE OF VERIFICATION WITH CHENGE OF KERNELS

Kernel function		m=2 Error(%)	m=3 Error(%)
Rbf	Sigma=3	4.3088	4.3180
	Sigma=4	4.3218	4.2912
	Sigma=5	4.3207	4.2808
	Sigma=6	4.3126	4.3207

TABLE 2

COMPARISON BETWEEN ERRORS OBTAINED UNTIL NOW

Biometry protocol	Feature extraction method	The best classifier	Error(%)
Laskaris test	Embed dimension+ MST + WW-test + MDS	MSVSVM	5.40
Keyboard test	Wevelet Dec. +ApEn	SVM	4.7
Number test	Wevelet Dec. +ApEn	SVM	4.3

avoid overfitting the classifier, the standard criteria Leave-one-out (LOO) was used. In this way, for each subject, two signal left out to be used as a test set and the remaining, used for training. To complete the test set and to have an impostor claim, we moved over the 30 subjects and excluded all samples of one person from the training set in each turn along with one session (2 signals) from each of the other 29 subjects. Therefore, the training set consists of all but one of the 30 subjects. The two signals from each of the 29 subjects which was excluded from the training set was used as our test set along with all the data of the imposter (the subject who was excluded from the training set). Let A_1, A_2, A_3,..., A_{30} be the identity codes of the subjects included in the database. **Figure 3** depicts the experimental protocol, when A_1 is considered to be the Impostor and session 5 is employed as test set. It can be seen that the training set is built of four out of the five available sessions each one consisted of 29 out of the 30 available subjects. In the classifier, each subject considered as a separate class, and the SVM was built based on the concept of one against all. So, we build a classifier consist of twenty nine SVM structures each trained for recognition of one class against others.

4. RESULTS

Thirty volunteers participated in this study; two tests were established to validate the proposed method. In each test, 10 signals captured from each individual. For each signal 7 features were extracted, after applying two-level wavelet decomposition and calculating the approximate entropies, the classification scenario was trained and tested as described in previous section. in this case, the acceptance rate and the rejection rate were considered equal. The error rate was calculated as the average of the errors in all runs. The results for different kernels for number test, is given in Table 1. Parameter m is related to how to calculate the approximate entropy and shows the embedding dimension in calculation phase. It is shown that, SVM achieved a very good result of 4.3% average error rate in performance verification using linear and RBF kernels with sigma=5. Results of keyboard test and number test are compared in **Error! Reference source not found.**. As can be seen, a better accuracy is achieved in number test compared to the keyboard test. However, both tests got the best results with Sigma=5.

5. CONCLUSION

In the past, the random numbers generated by humans were only used to activate certain parts of the brain. This study showed that behind the irregular and chaotic behavior of numbers produced by people, there is a distinctive feature which is very interesting and useful and can be used to identify the producer. This ability was seen in the time series obtained by pressing a key in clinical populations. In those studies distinction between healthy

and patient populations were performed using signals from random time intervals of tapping a key. In 2009, laskaris showed that the interval between pressing the key has the

features that vary between different individuals. In laskaris experiments, adding dimensions of time series was reconstructed and the matrix of similarity between the signals using the minimum spanning tree and the multivariate Wald-Wolfowitz test was calculated. In his work, with equal acceptance rate and rejection rate he could achieve 7.55% error with SVM, and 5.44% error with MCVSVM structure. Comparison of responses obtained in this experiment and Laskaris test are summarized in Table 2. The results are remarkably similar, although the method used in this article and laskaris method is completely different. This has two important aspects:

Firstly, the method used in this study gave the correct answer to signals with a protocol similar to Laskarys protocol (using keyboard pressing instead of tapping one key). As a result our method has been properly established and implemented.

Secondly, the ability of generating random numbers can be confirmed as a biometric feature. As can be seen the random numbers make better distinction between their producers compared to random rhythms. This higher accuracy may be due to numbers range from 1 to 9 that causes more clear perception of randomness in people and then specified mental processing on the data. Despite of

Received: 2012-01-07
Accepted: 2012-02-10

lower error rate in number test, this protocol is easier to fraud than the keyboard test. Then we can say that keyboard test is safer than the number test. One of the technical challenges that need to be considered is converting of the speech signal to number signal in number test. The keyboard test doesn't have this part. With all problems listed above, results in this paper shows number test as keyboard test can considered as biometry character of each person.

A significant practical issue is the adequate number of signals in each protocol. In previous experiments the lengths of key tapping were 128 hits, however only one test were taken from the participants. In this study, subjects first participated in number test and then done the keyboard test. So to eliminate the effects of exhaustion from the previous test, and also to make a clear interpretation of the brain processes, the signal length was increased. This can be one of the reasons for error reduction in this protocol. In number test due to limitation in test time the numbers were produced by individuals were different. This variation did not affect the implementation process. However some of the individuals are very slow in number generation and their signals are short. Then if the length of data for all individuals were got equal in this protocol, perhaps a greater accuracy could be expected.

This biometric feature is very valuable, because it requires no special tool and its process is so quick and easy. Especially, the possibility for fraud and fake on it is very difficult. In the world of the Internet and webs where people should be identified virtually and remotely, it would be very useful. The number of participants in this experiment does not allow us to conclude in general, but as a Preliminary study it is very satisfactory. Of course, if this field of biometrics can reach an acceptable accuracy, this protocol could become a comprehensive tool in security–identification systems.

6. REFERENCES

[1] N. Persaud, "Humans can consciously generate random number sequences: A possible test for artificial intelligence," Medical Hypotheses, 65, 211–214, 2005.

[2] M. Figurska, M. S. czyk, K. Kulesza, "Humans cannot consciously generate random numbers sequences: Polemic study," Medical Hypotheses, 70, 182–185, 2008.

[3] W. Bains, "Random number generation and creativity," Medical Hypotheses, 70, 186–190, 2008.

[4] N. A. Laskaris, S. P. Zafeiriou, L. Garefa, "Use of random time intervals (RTIs) generation for biometric verification", Pattern Recognition, 42, 2787 – 2796, 2009.

[5] R. Hornero, A. Alonso, N. Jimeno, A. Jimeno, M. Lopez, "Nonlinear Analysis of Time Series Generated by Schizophrenic Patients," *IEEE Engineering In Medicine And Biology*, 18 (3) (1999) 84–90.

[6] R. Hornero, D. Abásolo, N. Jimeno, C. I. Sánchez, J. Poza, M. Aboy, "Variability, Regularity, and Complexity of Time Series Generated by Schizophrenic Patients and Control Subjects," *IEEE Transactions On Biomedical Engineering*, VOL. 53, NO. 2, february 2006.

[7] H. Ocak, "Optimal classification of epileptic seizures in EEG using wavelet analysis and genetic algorithm," Signal Processing, 88, 1858–1867, (2008).

[8] A. Peacock, K. Xian, M. Wilkerson, ''Typing patterns: a key to user identification'', IEEE Security & Privacy 2 (5), 40–47, (2004).