Available online at www.sciencedirect.com

ScienceDirect

Procedia Technology 25 (2016) 286 – 292

Procedia Technology

Global Colloquium in Recent Advancement and Effectual Researches in Engineering, Science and Technology (RAEREST 2016)

A New Cryptographic Key Generation Scheme Using Psychological Signals

Akhila V A[a*], Arunvinodh C [b], Reshmi K C [c], Sakthiprasad K M [d]

[a&c] *M.TECH Student,Royal College of Engineering & Technology,Chiramanangad P.O, Akkikavu, Thrissur, Kerala,680604, v.akhila93@gmail.com*

[b] *Assisstant professor,Royal College of Engineering & Technology,Chiramanangad P.O, Akkikavu, Thrissur, Kerala,680604, arunvinodh@gmail.com,*

Abstract

Ensuring confidentiality and integrity of secret information is the major concern in the field of Biometric Cryptosystems. Security of data transmission is served by the art of encrypted data called cryptography. Biometric cryptography is the emerging methodology in communication networks. Various types of biometrics are available for encryption and also for decryption. This paper introduces a new technique known as brain wave cryptography. Brain waves or signals are generated by the neuron activity of human brain. With the help of sensors brain signals can be captured. After capturing brain waves convert these into digital form. From the brain signals we can generate a secret code or key which can be used as cryptographic key or we can bind key with the help of brain waves. The security of the key can be improved because brain waves will be one of the most powerful biometrics compared to others. This novel approach will enhances the security of the data transmission. This paper also highlights a new idea of automatic ICi selection by taking an average of particular brain regions which resolves the problem of online BCI. The proposed method has been tested in EEG datasets such as .SET, .SMA which succeeds in selecting reference ICi**.**

Peer-review under responsibility of the organizing committee of RAEREST 2016

*Keywords:*Human cognition; online-BCI; ICA, automatic ICi selection; EEG;cryptography;key generation

1. Introduction

Brain consists of billions of neurons which are communicated with each other through the use of electricity. Simultaneously millions of these types of signals are sent which in turn produces enormous amount of electrical activity in the brain. This combined activity rises and falls likea wave. So it is referred to as brainwaves which can be detected by medical equipment such as EEG. It measures electricity level over area of the brain scalp, depending

Peer-review under responsibility of the organizing committee of RAEREST 2016
doi:10.1016/j.protcy.2016.08.109

on what person is doing the electrical activity in the brain will change. There is much difference between brainwaves of sleeping person with brainwave of a person is wide awake. Mental state of a person can be analyzed by observing brainwave pattern. For extreme anxious people produces high beta waves while person who has ADD/ADHD produces slow alpha/theta waves. Table I show different types of brainwaves and associated mental states. Brain waves can be classified based on frequency ranges which are explaining in Table 1.

Table 1.Types of brain waves

Wave	Frequency	Mental states
Gamma	27 Hz & up	Formation of ideas, language, memory processing and various types of learning
Beta	12Hz-27Hz	Wide awake
Alpha	8Hz-12Hz	Awake but relaxed
Theta	3Hz-8Hz	Light sleep and extreme relaxation
Delta	0.2Hz-3Hz	Deep dreamless sleep

Brain computer interface (BCI) systems convey messages from brain to computer through direct electronic interface which allow users to communicate without movement. Electroencephalogram (EEG) signals were generated by conscious electrical brain activity is monitored and patterns are analyzed by BCI system. BCI can useful for physically disabled people in order to perform many activities, which in turn improve their quality of life and productivity, offers them more independence by establishing a communication link between a subject and computer. EEG based BCI will gives insights into applications such as, gaming [1] emotional disorder verification [2], personal authentication and preventing accidents etc. separating brain signals from artifacts can be done with the help of a technique called independent component analysis (ICA).To assess the dynamics of task-related independent components (ICs) done by machine learning approaches.

For example, to predict human driving performance ICs the posterior brain region [3]-[7] can be used. Intended directions of movement are determined by temporo-parietal Ics[8]-[10]. The task of motion imagery EEG classification will be enhanced by sensorimotor ICs, and P300-BCI [11] constructed with the help of ICs associated with event related potential. However, in BCIs manual is needed for selecting ICs of interest after ICA[12] step. Predefined IC was used in most existing ICA-based models.

Research by systems neurophysiologists studying motor systems has uncovered how kinematic parameters of movement control are encoded in neuronal firing rates. BCI systems capable of multidimensional control, which are capitalizing on neuroscience findings, several groups were able to develop real-time, closed-loop. Initially, testing will be performed on nonhuman primates, but multidimensional control of a computer cursor or a robotic arm requires electrode arrays which are implanted in several severely disabled individuals. Although Intracortical recordings used by invasive BCIs (mostly single units) achieves a high level of DOF, there still retain significant and unresolved queries regarding the long-term Intracortical electrodes stability, from individual neurons, action potentials were recorded, therefore clinical applications would significantly limits.Particular brain regions independent components [8]-[10] will not be used for online-specific BCI. These methods cannot be used for application of online based BCI.

All sectors need secure data transmissions. That's why cryptography is having this much importance in the real world. Network security is having very much importance when sending confidential data within organizations or between organizations through the network. At present various kinds of cryptography techniques are exists.

A traditional biometric will be fingerprint. Fingerprints consist of minutia points which are used to check for uniqueness. Encryption of text using fingerprints [14] includes minutia extractor and minutia matcher. Biometric key is produced by analyzing minutia points of a fingerprint of human beings. Oracle database is used for storing

fingerprint template which is also used for some basic manipulations like create user, edit user, log in etc using matlab. Various encryption algorithms takes as input of this recently generated biometric for encoding information. The problem behind this approach will be use of fake fingerprint. Fake fingerprint will affect the security in biometric key generation.

Another way of encryption can be achieved with the help of DNA technology [15]. This enciphering scheme 20-mer oligo nucleotides DNA sequence designed and generated by the sender of communication used as forward primer for PCR amplification and transmits it over a secure channel to a receiver. The message-receiver Bob also designs a DNA sequence which is 20-mer oligo nucleotides long as a reverse primer for PCR amplification and transmits it to Alice over a secure channel. After a pair of PCR primers is respectively designed and exchanged over a secure communication channel, we can get an encryption key KA that is a pair of PCR primers and Bob's public key e, as well as an decryption key KB that is a pair of PCR primers and Bob's secret key d.

Another alternative is cryptography based on iris image [16]. In iris based cryptography a secret key is produced from the iris image. In the feature extraction step acquiring the image using suitable cameras and converts this image into binary 0's and 1's.

Face image based cryptography also available [17]. Face image is one of the identification factors. Face recognition is important in identification process. Key binding is used in this paper. That means cryptographic key which are generated from RNG (random number generator) binds with face image which is given as input to the bio cryptosystem

The remaining portion of paper organized as follows: independent component analysis, independent component of interest, implementation results and finally conclusion are discussed.

2. Independent Component Analysis

Independent component analysis (ICA) can be used to suppress artifacts independent in EEG recordings.ICA decomposes EEG signals into statistically independent components or sources and then followed by removal of artificial signals. Artificial signal are those signal in which we are not concentrated at all. For example if we take cerebral activity components as artificial one then that component will be removed from the EEG data.

Independent component analysis[1] tries to separate intoindependent non-gaussian signal from multivariate signal. For example sound is a signal composed of addition of signal from different sources. Problem is that separate individual contributing sources from observed total signal.

3. ICi calculation & key generation

After performing independent component analysis few components are selected as independent component of interest which is used for further processing. Mainly this paper is dealing with online brain computer interface in which dynamically selecting particular components as components of interest. There is five parts of brain called central, parietal, motor, occipital, frontal regions responsible for human cognition.

3.1 Reference ICi calculation

In this paper five scalp maps were predefined as reference ICi. To take average of frontal components of different EEG signals this procedure is repeated for all other (central, motor, parietal, occipital components) and predefined it as reference ICi.

3.2 ICi calculation

ICi calculation can be done with help of reference ICi.

Step 1: Read the EEG data.
Step 2: Perform independent component analysis using infomax algorithm
Step 3:for i=1 to n (each Independent component)

Step 4:for j=1 to 5(each reference ICi)
if ($|\rho(\Lambda_i, \hat{\Lambda}_j)| \geq 0.55$) then,
Take that component as ICi go to step 5
Else
discard that component.
End for
End for
Step 5:Finally ICi will be used for feature extraction and classification.
Step 6:Stop.

3.3 Key generation

To perform key generation some sort of tasks are given to the sender and analyzing the brain signal based on input tasks. After analyzing the brain waves finds out dominant waves generate binary value equivalent. At the receiver side the same activity will be used for checking analyses the brain waves which is passes to the signal to binary converter and produces key. That key will used for decrypting the cipher text. So no one other than sender can retrieve the secret information. This cryptographic scheme will be applicable when any confidential data stored in central database can be secured using brain signal as a biometric.

In the novel approach fig 1(a) entitles about security of saving cryptographic key by using key binding technique with the help of brain waves generated from neuron actions in brain. After binding key with brain signals which will stored as secured template. The secured template will be further analyzed for verification phase. In verification phase inputting brain waves and features are extracted from the input opposite of key binding called key releasing will happen reproduces the correct key if the inputting brain wave will be valid, otherwise error key will be appears and it will causes error while the decryption process. In fig1 (b) represents about biometric key generation from brain waves of different mental activities of the same person. In this approach initially brain signals are captured using sensors then it is given to feature extraction stage. Here relevant features are extracted and those extracted features were responsible for generation of brain biometric key. Using this key both encryption and decryption process will be performed. This paper concentrates on biometric key generation from EEG signals.

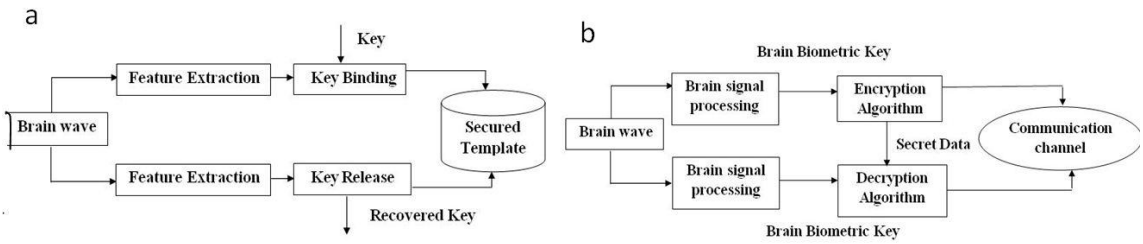

Fig. 1. (a) key binding using brain waves; (b) biometric key generation from brain waves

3. Results and discussion

This paper concentrates on calculation of independent component of interest and also this method is applicable to any type of EEG signal. This work implemented on .set data. We can also apply it for .bdf, .edf, .sma data also. EEGLAB toolbox [13] can be used for loading the EEG data and per**fo**rming ICA. Thentopograph of 32 independent components of EEG dataset was plotted which are shown in fig 2. EEG datasets will be present in different formats such as .set, .eeg, .edf, .bdf, .sma, .rdf etc.

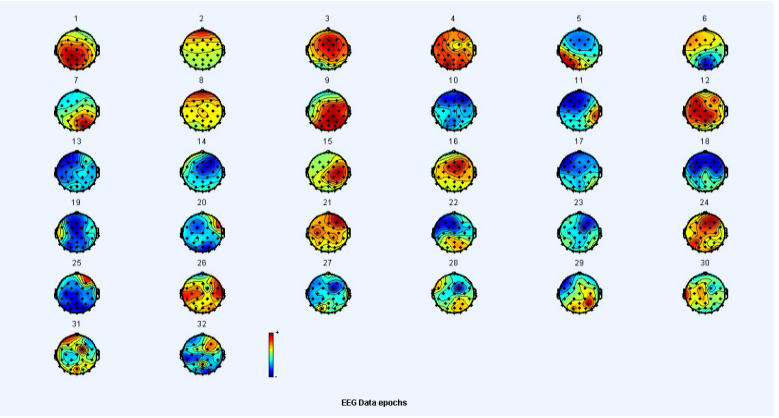

Fig. 2.Topograph of ICs of EEG dataset1

This paper performs automatic ICi selection procedure by calculating correlation coefficient between reference ICs and ICis. Finally bar graph is plotted EEG datasets. Correlation coefficients of central, motor, frontal, occipital, and parietal regions are shown in figures 3.This bar graph represents which component is closer to 5 brain regions.

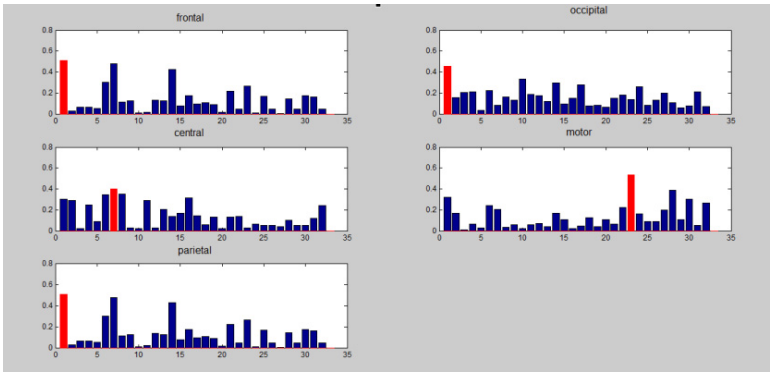

Fig. 3.Correlation coefficient calculation of eegdataset 1

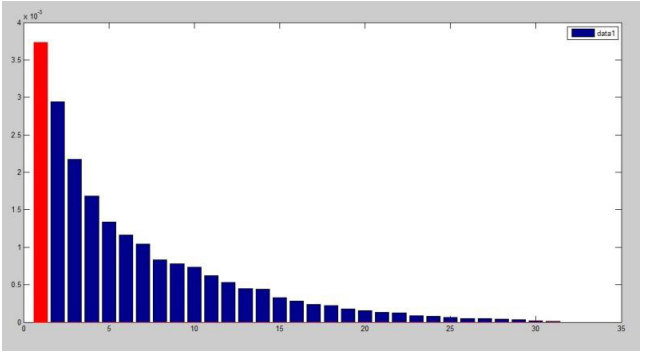

Fig 4: Extracted features of eegdataset using PCA

In Fig 3component- 1 represents frontal component-7 represents central component-1 represents parietal component-1 represents occipital and component-23 represents motor regions. Those ICs denoted as red colour in the bar graph. Fig 5 represents bar graph of eigen vectors using PCA. Red colour denotes greatest eigen value in eigen vectors which is used for biometric key generation.

By comparing the four graphs concludes that after applying PCA into ICA weight inverse matrix of N×N matrix obtaining an output of 1×N matrix. Principle component analysis is mainly used for dimensionality reduction. Output of PCA in MATLAB is a mapping. From this data mapping applying function called 'getdata' which is used to extract data from the data mapping. Then the data of mapping will be a structure. From the structure data extract an eigen value which resembles dimensionally reduced input dataset. In the above graph shows various eigenvectors of different datasets. In one graph highest value will be in the range will be 63×10^2. Second eigen vector graph displays highest value as 37×10^2. Using the highest value of Eigen vector, a secret key will be generated. This cryptographic key will be very secure because nobody can guess the key or attack the key. This key will be unique for each individual at a particular task or brain activity. This type of key generation is somewhat good because key generation is done using psychological signals like EEG etc.

In this paper key generation has an influence on various emotions. It may be taken as both positive and negative senses. The person (receiver) who is at stress stage the correct key will not be generated because of signal variation referred as negative sense. At positive sense somebody is trying to forcefully do the task for hacking secret key this situation also yields to negative result. These 2 cases occur at rare instances.

4. Conclusion

Paper proposed ensemble of independent components which combines multiple brain region features. Most of the paper highlights any one of the component like central motor or parietal. This paper highlights online base BCI selecting components dynamically. Here an automatic ICi selection procedure is introduced. In this work PCA was used as feature extraction algorithm. This work also introduces a key generation techniques using EEG signals. Dynamic cryptographic keys are generated that is why this idea produces more security in cryptography and data hiding also. This system highly effected with emotions. Signal generation depends more on mental state. This type of key generation was secured than existing methods. This paper clearly gives a path to brain based biometric cryptosystem since brain signals are not possible to generate artificially and uniqueness is good compare to other biometrics

References

[1] L.-D. Liao, C.-Y.Chen, I.-J.Wang, S.-F.Chen, S.-Y Li, B.-W.Chen,J.-Y.Chang, and C.-T. Lin, "Gaming control using a wearable andwireless EEG-based brain-computer interface device with novel dryfoam-based sensors," *J. Neuroeng.Rehabil.*, vol. 9, no. 5, pp. 1–11,Jan. 2012.

[2] R. Sitaram, S. Lee, S. Ruiz,M. Rana, R. Veit, and N. Birbaumer, "Realtime support vector classification and feedback of multiple emotional brain states," NeuroImage, vol. 56, no. 2, pp. 753–765, May 2011.

[3] F.-C. Lin, L.-W.Ko, C.-H. Chuang, T.-P.Su, and C.-T. Lin, "Generalized EEG-based drowsiness prediction system by using a self-organizing neural fuzzy system," IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 59, no. 9, pp. 2044–2055, Sep. 2012.

[4] R. N. Khushaba, S. Kodagoda, S. Lal, and G. Dissanayake, "Driver drowsiness classification using fuzzy wavelet-packet-based feature-extraction algorithm," IEEE Trans. Biomed. Eng., vol. 58, no. 1, pp. 121–131, Jan. 2011.

[5] A. J. Bell and T. J. Sejnowski, "An information-maximization approach to blind separation and blind deconvolution," Neural Comput., vol. 7, no. 6, pp. 1129–1159, Nov. 1995.

[6] T.-P. Jung, S. Makeig, M. J. McKeown, A. J. Bell, T. W. Lee, and T. J. Sejnowski, "Imaging brain dynamics using independent component analysis," Proc. IEEE, vol. 89, no. 7, pp. 1107–1122, Jul. 2001.

[7] C.-T. Lin, L.-W.Ko, I.-F. Chung, T.-Y.Huang,Y.-C. Chen, T.-P.Jung, and S.-F. Liang, "Adaptive EEG-based alertness estimation system by using ICA-based fuzzy neural networks," IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 53, no. 11, pp. 2469–2476, Nov. 2006.

[8] C. Papadelis, Z. Chen, C. Kourtidou-Papadeli, P. D. Bamidis, I. Chouvarda, E. Bekiaris, and N. Maglaveras, "Monitoring sleepiness with on-board electrophysiological recordings for preventing sleep-deprived traffic accidents," Clin. Neurophysiol., vol. 118, no. 9, pp. 1906–1922, Sep. 2007.

[9] F.-C. Lin, L.-W.Ko, C.-H. Chuang, T.-P.Su, and C.-T. Lin, "Generalized EEG-based drowsiness prediction system by using a self-organizing neural fuzzy system," IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 59, no. 9, pp. 2044–2055, Sep. 2012.

[10] R. N. Khushaba, S. Kodagoda, S. Lal, and G. Dissanayake, "Driver drowsiness classification using fuzzy wavelet-packet-based feature-extraction algorithm," IEEE Trans. Biomed. Eng., vol. 58, no. 1, pp. 121–131, Jan. 2011.

[11] O. I. Khan, F. Farooq, F. Akram, M. T. Choi, S. M. Han, and T. S. Kim, "Robust extraction of P300 using constrained ICA for BCI applications," Med. Biol. Eng. Comput., vol. 50, no. 3, pp. 231–241, Mar. 2012

[12] AapoHyvärinen and Erkki "Independent Component Analysis: Algorithms and Applications" Neural Networks Research Centre Helsinki University of Technlogy P.O. Box 5400, FIN-02015 HUT, Finland Neural Networks, 13(4-5):411-430, 2000.

[13] Arnaud Delorme, Scott Makeig "EEGLAB: an open source toolbox for analysis of single-trial EEG dynamics including independent component analysis" Swartz Center for Computational Neuroscience, Institute for Neural Computation, University of California San Diego, La Jolla, CA 92093-0961, USA

[14] Abhishek Sharma, Naredra Kumar "Encryption of Text Using Fingerprints as Input to Various Algorithms" International Journal Of Science and Research, Volume 3 Issue 4 , April 2014

[15] GuangzhaoCui ,Limin Qin, Yanfeng Wang, Xuncai Zhang "An Encryption Using DNA Technology " 2008 IEEE

[16] Sruthi B. Asok, P. Karthigaikumar, Sandhya R, Naveen Jarold K, Siva Mangai "Iris Based Cryptography" International Journal of Advanced Research in Computer and Communication Engineering, Volume 2 Issue 2 Feb 2013.

[17] Francis Minhthang Bui, Karl Martin, Haiping Lu, Konstantinos N. Plataniotis, and DimitriosHatzinakos, "Fuzzy Key Binding Strategies Based on Quantization Index Modulation (QIM) for Biometric Encryption (BE) Applications" IEEE Transaction on Information Forensics and Security, Vol. 5, No. 1, March 2010