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