International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-4 Issue-3, July 2015

A New Paradigm for Automatic Unveiling of Human Thoughts by Reading Brain Signals

L. Amudha, T.M. Nithya

Abstract—we now live in the age of deception. Existing techniques to detect deception uses polygraph methods to assess whether a suspect is guilt or not. These methods rely on measurement of autonomic arousal like palm sweating, facial expressions, words uttered, and answer to queries, actions and heart rate to get knowledge about any crime scene. No criminal would ever accept his crime. And a practiced user can conceal the emotions mentioned above. The most detailed knowledge of any crime is locked away in the brain of the person who committed it. The fact is that no person has control over his brain signals. Use of functional magnetic resonance imaging in lie detection derives from studies suggesting that persons asked to lie show different patterns of brain activity than they do when being truthful. There are over a billion neurons in the brain that communicate with each other using electrochemical signal. Since no person can hide his brain signals, a novel and easy method of detecting concealed information, brain fingerprinting using EEG (Electroencephalogram) is gaining wide attention among investigating agencies. The issues and applicability of brain fingerprinting is discussed in the following sections and a wide range of research scope is also proposed.

Keywords: Polygraph, Electroencephalography (EEG), Brain fingerprinting, P300-MERMER, ERP signals.

I. INTRODUCTION

EEG is a neural amplifier that records the signals denoting brain wave pattern. The electrodes are placed in the scalp in an ordered way. Brain is about 1 cm from the scalp. To detect even the microvolt level potential differences signals from brain is amplified. The brain responses from the amplifiers are then conveyed to the computer where they are analyzed to detect knowledge. If the computer detects P300/MERMER waves it indicates that specific information relevant to the situation under investigation is stored in the brain. In the field of criminology, a new lie detector has been developed in the United States of America called “brain finger printing”. This paper reports field/real-life studies using event related potentials in the detection of concealed information. Another major purpose of the research reported herein is to identify the scientific principles and specific methods unveiled in the recent years for knowledge detection.

Revised Manuscript Received on 30 July 2015.
***** Correspondence Author
L. Amudha*, Assistant Professor, Department of Computer Science and Engineering, K. Ramakrishnan College of Engineering, Trichy 621 112, (Tamil Nadu). India.
T.M. Nithya, Assistant Professor, Department of Computer Science and Engineering, K. Ramakrishnan College of Engineering, Trichy 621 112, (Tamil Nadu). India.

II. TYPES OF BRAIN FREQUENCIES

The four types of brain waves Beta, Alpha, Theta and Delta with their specific frequency ranges discriminates the levels of arousal and excitability within the brain. The frequency ranges of the 5 types of brain waves are specified in Fig. 1

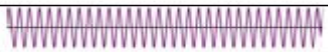
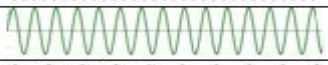
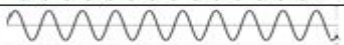
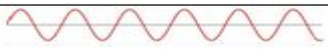
Type of brain wave	Brain wave image	Frequency ranges
Gamma		31Hz and up
Beta		12 and 30 Hz
Alpha		7.5 to 12 Hz
Theta		3.5 to 7.5 Hz
Delta		0.5 to 3.5 Hz

Fig.1. Types of brain waves and its frequencies

These four basic frequency ranges discriminate the levels of arousal or excitability within the brain. After viewing a picture or scene or listening a music ERP (Event Related Potential) signals are generated. ERP signals constitutes positive and negative fluctuations. These signals are labeled as P1, P2, N1, N2, N400, P300. The P300 ERP helps us in lie detection. P300 is a specific electric brain wave that is triggered whenever a person sees a familiar object. After 300 ms the P300 waves will appear on the EEG machine. Due to the specificity of brain wave response the technique has been labeled as brain fingerprinting.

III.BRAIN FINGERPRINTING TECHNIQUE

Brain finger printing is based on finding that the brain generates a unique brain wave pattern when a person encounters a familiar stimulus. Use of functional magnetic resonance imaging in lie detection suggests that persons asked to lie show different patterns of brain activity than they do when being truthful. In Fig.2 the subject wears a head band of electrodes, faces a computer screen that flashes photographs.

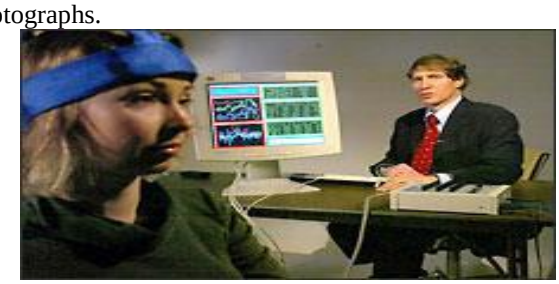


Fig.2. A suspect wearing a headband fitted with special sensors

Brain fingerprinting system makes a mathematical determination as to whether or not this specific evidence is stored in the brain and computes a statistical confidence for that determination. This determination and statistical confidence constitute the scientific result of Farwell brain fingerprinting: either "information present" or "information absent". The details of the crime are stored in the brain of the suspect or the details of the crime are not stored in the brain of the suspect.

This technique can be applied only when investigators have a sufficient amount of specific information about an event or activity that would be known only to the person under investigation and investigator. Brain fingerprinting is considered as a type of guilty knowledge test, where the "guilty" party is expected to react strongly to the relevant detail of the event of activity. Polygraph procedures for assessing the validity of a suspect's "guilty" knowledge rely on measurement of autonomic arousals like palm sweating, heart rate, etc, while brain fingerprinting measures electrical brain activity via a fitted headband with special sensors.

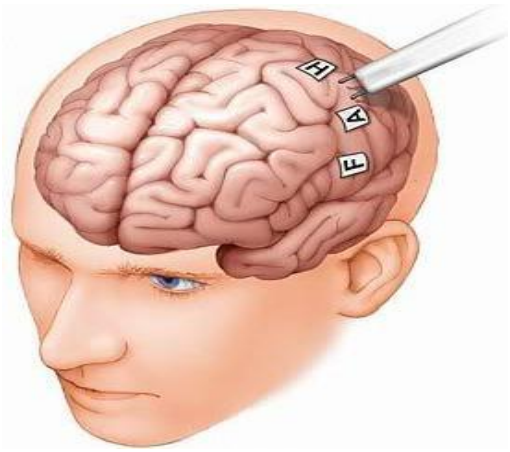


Fig.3. Stimulus generated in suspect brain

In order to calibrate the brain fingerprinting system, the suspect is presented with a series of irrelevant stimuli, words, and pictures, and a series of relevant stimuli, words, and pictures. The test subject's brain response to these two different types of stimuli allow the tester to determine if the measured brain responses to test stimuli, called probes, are more similar to the relevant or irrelevant responses. The technique uses the well known fact that an electrical signal known as P300 is emitted from an individual's brain approximately 300 ms after it is confronted with a stimulus of special significance. The novel interpretation in brain fingerprinting is to look for P300 as response to stimuli related to the crime in question for example a murder weapon or a victim's face (Figure 3).

A. Signal Characteristics of The P300-Mermer

(Farwell and Smith 2001) have shown that in the brain fingerprinting paradigm this positive peak is followed by a late negative peak (the Late Negative Potential or LNP). The two together have been termed P300 MERMER (memory and encoding related multifaceted electroencephalographic response). Both the P300 and the P300-MERMER undoubtedly have other features beyond the simple time-domain pattern that becomes apparent through the usual ERP signal-averaging procedures. The positive–negative-peaked pattern in the time domain (or negative–positive–negative pattern if the N2 preceding the P300 is included), however, is sufficient to define the response, and is all that is necessary to detect it.

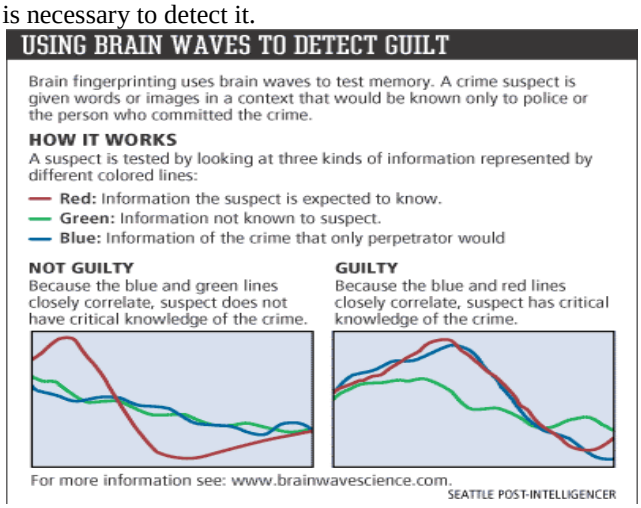


Fig. 4 Discrimination of signals for not guilty and guilty

Fig 5 shows the brain response of serial killer J. B. Grinder to information relevant to the murder of Julie Helton . There is a clear P300-MERMER in response to the known targets. The P300 is the positive voltage peak at the upper left. The P300-MERMER contains both the P300 peak and the late negative potential (LNP) at the lower right. There is no P300-MERMER in response to the irrelevant. Grinder's brain response to the crime-relevant probes clearly contains a P300-MERMER. This shows that the record in the brain of J. B. Grinder contains salient details of the murder. Determination: ''information present.'' statistical confidence: 99.9%

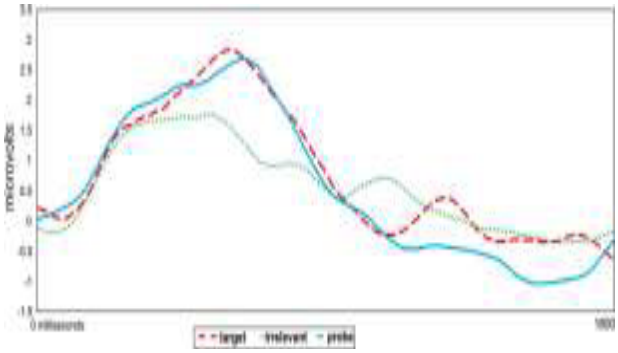


Fig. 5 ''Information present'' brain response of a serial killer.

Brain fingerprinting studies analyze the data based on either the P300-MERMER, or the P300 alone, or both.

B. Four Phases of Farwell Brain Fingerprinting

There are four stages to Farwell brain fingerprinting, which are similar to the steps in fingerprinting and DNA fingerprinting:

1. Brain fingerprinting crime scene evidence collection;
2. Brain fingerprinting brain evidence collection;
3. Brain fingerprinting computer evidence analysis; and
4. Brain fingerprinting scientific result.

Brain fingerprinting testing provides an accurate, economical and timely solution to the central problem in the fight against terrorism. It is now possible to determine scientifically whether or not a person has terrorist training and knowledge of terrorist activities. With this technology, now, terrorists and those supporting terrorism can be identified quickly and accurately.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

C. Why and How Brain Activity Can Be Measured

In EEG, brain-related electrical potentials are recorded from the scalp. Pairs of conductive Electrodes made of silver, for example, are used to read this electricity. The difference in voltage between the electrodes is measured, and since the signal is weak (30-100 V) it has to be amplified.

Current occurs when neurons communicate. The simplest event is called action potential, and is a discharge caused by fast opening and closing of Na^+ and K^+ ion channels in the neuron membrane. If the membrane depolarize to some threshold, the neuron will"fire" Tracking these discharges over time reveals the brain activity.

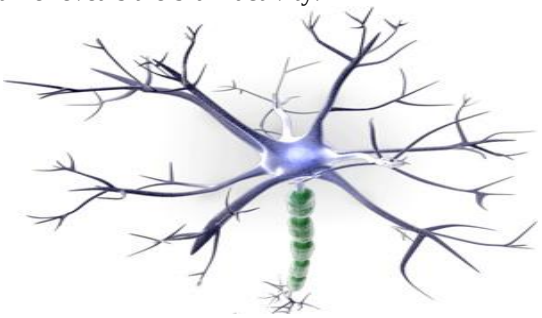


Fig. 6. Artistic illustration of a single neuron and its synapses

D. Stages of Data Acquisition and Analysis

Electroencephalograph (EEG) data are collected from midline frontal, central, and parietal scalp sites (Fz, Cz, and Pz respectively). Electrooculograph (EOG) data are collected from the forehead to monitor artifacts generated by eye movements. Data are amplified, digitized, filtered, and analyzed Fig.7.

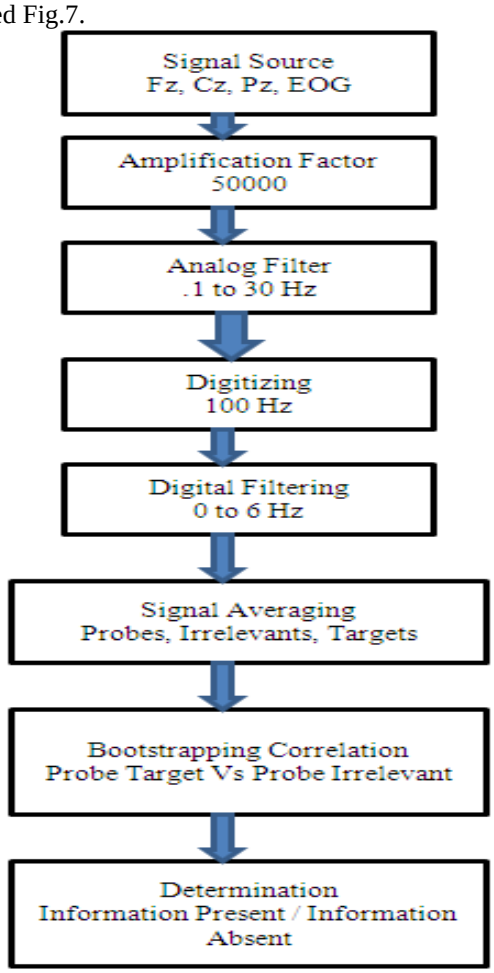


Fig. 7. Stages of data acquisition and analysis

Stimuli are presented for duration of 300 milliseconds at an inter-stimulus interval of 3000 milliseconds. A fixation point is presented for 1000 milliseconds prior to each stimulus presentation. Figure 8 outlines the timing parameters for stimulus presentation, data acquisition, and data analysis.

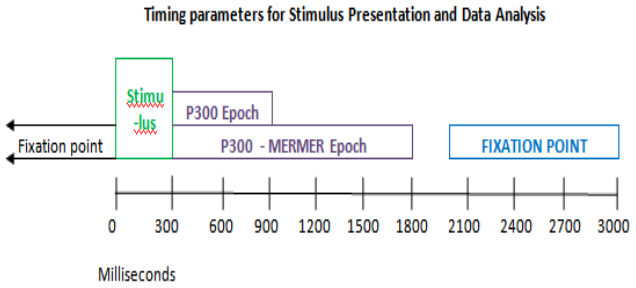


Fig. 8. Timing parameters for individual events in brain

The analysis epoch is 300 – 900 milliseconds post stimulus for the P300 analysis, and 300 – 1800 milliseconds apost-stimulus for the P300-MERMER analysis.

E. Summary of Previous Results Of The P300-Mermer-Based Analysis

In the brain fingerprinting studies [5],the observed error rate was 0 %. Accuracy was 100 %. 100 % of determinations were correct. There were no false negatives and no false positives. There were also no indeterminate. This analysis used a priori criteria of 90 % statistical confidence for an information-present determination and 70 % statistical confidence for an information-absent determination.

Therefore brain fingerprinting is 100% accurate in all previous analysis and experimentation.

I. Applications of Brain Fingerprinting

1. Criminal Justice
2. Counter terrorism
3. Medical

A. Criminal Justice

A critical task of the criminal justice system is to determine who has committed a crime. The key difference between a guilty party and an innocent suspect is that the perpetrator of the crime has a record of the crime stored in their brain, and the innocent suspect does not. Until the invention of Brain Finger printing testing, there was no scientifically valid way to detect this fundamental difference. This exciting technology gives the judge and jury new, scientifically valid evidence to help them arrive at their decision. DNA evidence and fingerprints are available in only about 1% of major crimes. It is estimated that Brain fingerprinting testing will apply in approximately 60 to 70% of these major crimes.

B. Counter Terrorism

Brain fingerprinting can help in addressing the following critical elements in the fight against terrorism:

1. Aid in determining who has participated in terrorist acts, directly or indirectly.
2. Aid in identifying trained terrorists with the potential to commit future terrorist acts, even if they are in a "sleeper" cell and have not been active for years.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

3. Help to identify people who have knowledge or training in banking, finance or communications and who are associated with terrorist teams and acts.
4. Help to determine if an individual is in a leadership role within a terrorist organization.

In a terrorist act, there may or may not be peripheral evidence such as fingerprints or DNA, but the brain of the perpetrator is always there, planning, executing, and recording the crime. The terrorist has knowledge of organizations, training and plans that an innocent person does not have. Brain fingerprinting testing provides an accurate, economical and timely solution to the central problem in the fight against terrorism.

C. Medical Diagnosis

This technique can be used to identify how memory and cognitive functioning of Alzheimer sufferers are affected by medications. When presented with familiar information, the brain responds by producing MERMERs, specific increases in neuron activity. The technician can use this response to measure how quickly information is disappearing from the brain and whether the drugs they are taking are slowing down the process.

In a study funded by the CIA, Farwell and colleagues (Farwell and Richardson, 2006b) used brain fingerprinting to detect which individuals had US Navy military medical training. All 30 subjects were correctly determined to have or not to have the specific information regarding military medicine stored in their brains.

IV. LIMITATIONS AND ISSUES TO BE CONSIDERED DURING FALSE POSITIVE SITUATIONS

1. Publicly known information cannot be considered during the test process. Standard brain finger printing systems eliminate all such information from their investigation test procedures. Many details not known to the public through media or newspaper can be included in the test.
2. Brain fingerprinting does not detect lies. It simply detects information. No questions are asked or answered during a brain fingerprinting test.
3. If the suspect knows everything the investigators know, since he has been exposed to all information about the crime in the previous trials, a test may not be fruitful. Then there must be some critical information that might be known only to the perpetrator. If a suspect does not have any such information in his brain, then he is innocent.
4. If a suspect claims to be a witness but not a perpetrator, then he knows the details about the crime scene. Brain fingerprinting shows that he is guilty when he may not be a perpetrator.
5. Like all forensic science techniques, brain fingerprinting depends on the evidence-gathering process which lies outside the realm of science to provide the evidence to be scientifically tested.
6. Brain fingerprinting is not a substitute for effective investigation on the part of the investigator or for common sense and good judgment on the part of the judge and jury

V. RESEARCH SCOPE

A. Person Identification

Brain fingerprinting is a new emerging technology that can also be used in person identification as a good alternative for fingerprint, palm print, secret pin number.

B. Non Vocal Communication

Interpretation of human thought from brain activity without depending on speech or action is one of the most provoking and challenging frontiers of modern neuroscience. This technique specifically would be of more helpful for patients who are fully conscious and awake, yet due to brain damage are unable to show any behavioral responsibility.

C. Mind Speech

With severely-epileptic patients who were going to have the seizure-stricken parts of their brain removed, the researchers opened the skull and put microelectrodes directly on to the Face-Motor Cortex and Wernicke's area of brain that are crucial for speech. This could in the future make it possible for disabled people to communicate, using a speech synthesizer to read the matched words out loud.

Even physically good persons can use this technique for mind to mind communication, similar to SMS service available through mobile phones.

D. Interface The Brainmonitor Program With Existing Games

There are many open source games available, that could be interesting to connect with the EEG equipment. The advantage is that a lot of work is already done, like the graphical display and game play, so the focus can remain on what and how the EEG function should be.

E. Advertising

It allow advertisers to determine what information from an ad is retained in memory as

(i) What elements do people pay attention to?
(ii) What type of media is most effective?
(iii) How to attract people all over the world?

VI. CONCLUSION

This type of testing can also help to determine if an individual has specific knowledge related to computer crimes where there is typically no witness or physical evidence. If investigating agencies adopt this brain reading technique, they will be able to narrow down the most likely suspects in much shorter time. Also it prevents sentencing of innocent people. The main purpose of this paper is discussion of the emerging success in accurate analysis in extracting the thoughts of a human brain. Also the recent developments in hardware in terms of size and speed pave way for new researches to convert human brain signals into other forms of communication like text or speech or to transfer human thoughts from one person to another without vocal communication.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

REFERENCES

1. Lawrence A. Farwell, Brain fingerprinting: a comprehensive tutorial review of detection of concealed information with event-related brain potentials, Cogn Neurodyn (2012) 6:115–154
2. Farwell LA, Smith SS (2001). Using Brain MERMER Testing to Detect Concealed Knowledge Despite Efforts to Conceal. J. Forens. Sci., 46(1): 135-143.
3. Farwell LA. The brain-wave information detection (BID) system: a new paradigm for psychophysiological detection of information [unpublished doctoral dissertationl. Urbana-Champaign (IL): University of Illinois, 1992.
4. Farwell LA, Richardson DC (2006b). Brain Fingerprinting in Laboratory Conditions. Psychophysiol., 43: S38.
5. ”Brain fingerprinting field studies comparing P300-MERMER and P300 brainwave responses in the detection of concealed information” Lawrence A. Farwell, Drew C. Richardson, Graham Richardson, Cogn Neurodyn (2013) 7:263–299
6. Schalk, G., McFarland, D. J., Hinterberger, T., Birbaumer, N., & Wolpaw, J. R. (2004, June). BCI2000: A General-Purpose Brain Computer Interface (BCI) system. (Vol. 51) (No. 6).
7. Rosenfeld JP, Angell A, Johnson M, Quan J. An ERP-based, control question lie detector analog: algorithms for discriminating effects within individual's average waveforms. Psychophysiology 1991; 28 (3): 3 t 9-35.
8. Farwell LA, Hemandez R. Brain-wave detection of concealed information. Office of Research and Development of the Central Intelligence Agency (CIA); 1993.
9. Sabeti M, Moradi E, Katebi, S (2011) Analysis of neural sources of p300 event-related potential in normal and schizophrenic participants. Advances in Experimental Medicine and Biology, 696, 589-97.
10. Verschuere B, Ben-Shakhar G, Meijer E (2011) Memory Detection: Theory and Application of the Concealed Information Test. Cambridge: Cambridge University Press; 1 edition.
11. Dhiraj Ahuja and Bharat Singh, Brain fingerprinting, Journal of Engineering and Technology Research Vol. 4(6), pp. 98-103, November 2012.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)