JOURNAL OF INFORMATION, KNOWLEDGE AND RESEARCH IN ELECTRONICS AND COMMUNICATION

# BRAIN FINGERPRINTING

[1] *ASHWINI V. SHARMA* , [1]*Dr. GANESH S. SABLE*

[1, 2] **Department of Electronics Engineering, Savitribai Phule Womens Engg. college, B.A.M.U. University, Aurangabad, Maharashtra, India.**

***ashwinisharma.108@gmail.com, sable.eesa@gmail.com***

***ABSTRACT :*** *Brain fingerprinting 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 derives from studies suggesting that persons asked to lie show different patterns of brain activity than they do when being truthful. Issues related to the use of such evidence in courts are discussed. The author concludes that neither approach is currently supported by enough data regarding its accuracy in detecting deception to warrant use in court. This test uses what Farwell calls the MERMER ("Memory and Encoding Related Multifaceted Electroencephalographic Response") response to detect familiarity reaction. One of the applications is lie detection. Dr. Lawrence A. Farwell has invented, developed, proven, and patented the technique of Farwell Brain Fingerprinting, a new computer-based technology to identify the perpetrator of a crime accurately and scientifically by measuring brain-wave responses to crime-relevant words or pictures presented on a computer screen. Farwell Brain Fingerprinting has proven 100% accurate in over 120 tests, including tests on FBI agents, tests for a US intelligence agency and for the US Navy, and tests on real-life situations including actual crimes.*

## 1. Introduction

In the field of criminology, a new lie detector has been developed in the United States of America. This is called “brain fingerprinting”. This invention is supposed to be the best lie detector available as on date and is said to detect even smooth criminals who pass the polygraph test (the conventional lie detector test) with ease. The new method employs brain waves, which are useful in detecting whether the person subjected to the test, remembers finer details of the crime. Even if the person willingly suppresses the necessary information, the brain wave is sure to trap him, according to the experts who are very excited about the new kid on the block. Brain Fingerprinting is designed to determine whether an individual recognizes specific information related to an event or activity by measuring electrical brain wave responses to words, phrases, or pictures presented on a computer screen. The technique can be applied only in situations where investigators have a sufficient amount of specific information about an event or activity that would be known only to the perpetrator and investigator. In this respect, Brain Fingerprinting is considered a type of Guilty Knowledge Test, where the "guilty" party is expected to react strongly to the relevant detail of the event of activity.

Existing (polygraph) procedures for assessing the validity of a suspect's "guilty" knowledge rely on measurement of autonomic arousal (e.g., palm sweating and heart rate), while Brain Fingerprinting measures electrical brain activity via a fitted headband containing special sensors. Brain Fingerprinting is said to be more accurate in detecting "guilty" knowledge distinct from the false positives of traditional polygraph methods, but this is hotly disputed by specialized researchers.

## 2. TECHNIQUE

The person to be tested wears a special headband with electronic sensors that measure the electroencephalography from several locations on the scalp. In order to calibrate the brain fingerprinting system, the testee 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 milliseconds after it is confronted with a stimulus of special significance, e.g. a rare vs. a common stimuls or a stimulas the proband is asked to count. The novel interpretation in brain fingerprinting is to look for P300 as response to stimuli related to the crime in question e.g., a murder weapon or a victim's face. Because it is based on EEG signals, the system does not require the testee to issue verbal responses to questions or stimuli.

Brain fingerprinting uses cognitive brain responses, brain fingerprinting does not depend on the emotions of the subject, nor is it affected by emotional responses. Brain fingerprinting is fundamentally different from the polygraph (lie-detector), which measures emotion-based physiological signals such as heart rate, sweating, and blood pressure. Also, unlike polygraph testing, it does not attempt to

determine whether or not the subject is lying or telling the truth.

Brain fingerprinting technology is based on the principle that the brain is central to all human acts. 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. Until the invention of Brain Fingerprinting testing, there was no scientific way to detect this fundamental difference. 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 the Brain Fingerprinting system, a significant scientific breakthrough has now become a practical applied technology. A new era in security and intelligence gathering has begun. Now, terrorists and those supporting terrorism can be identified quickly and accurately. No longer should any terrorist be able to evade justice for lack of evidence. And there is no reason why an innocent individual should be falsely imprisoned or convicted of terrorist activity. A Brain Fingerprinting test can determine with an extremely high degree of accuracy those who are involved with terrorist activity and those who are not.

Brain Fingerprinting testing does not prove guilt or innocence. That is the role of a judge and jury. 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. The impacts on the criminal justice system will be profound. The potential now exists to significantly improve the speed and accuracy of the entire system, from investigations to parole hearings. Brain Fingerprinting testing will be able to dramatically reduce the costs associated with investigating and prosecuting innocent people and allow law enforcement professionals to concentrate on suspects who have verifiable, detailed knowledge of the crimes.

**THE DISCOVERY OF THE P300-MERMER**

In the initial brain fingerprinting research, Farwell and Donchin used the P300 event-related brain potential (Farwell and Donchin 1986; 1988b; 1991; Farwell 1992a). Later Farwell discovered that the P300 can be considered to be part of a larger response he called a memory and encoding related multifaceted electroencephalographic response or P300-MERMER.The discovery of the P300-MERMER was one more step in the ongoing progression from very short latency evoked potentials to longer and longer latency event-related potentials as the stimuli and the processing demanded by the experimental task become more rich and complex. In the 1990s when Farwell and FBI scientist Drew Richardson were conducting the brain fingerprinting research on FBI agents, P300 latencies of 600 to 700 milliseconds were typically found in experiments.

Where the stimuli were information rich and the cognitive processing required was substantial. At that time, in such research a new stimulus was typically presented every 1000 to 1500 milliseconds (1 to 1.5 seconds). In the first brain fingerprinting study, for example, Farwell and Donchin (1991) presented a stimulus every 1500 milliseconds. In dealing with real-life situations, Farwell and Richardson (2006b; Farwell, Richardson, and Richardson, 2011; in press) found it necessary to use longer and more complex stimuli to accurately communicate the necessary information to the subject. In order to present realistic stimuli that accurately represented knowledge unique to FBI agents, they found it necessary to use stimuli consisting of several words, sometimes several words of several syllables each. It took the subjects longer to read the words and evaluate their significance than in previous experiments with simpler stimuli. To give the subjects time to process the stimuli and respond appropriately, Farwell and Richardson lengthened the interval between stimuli from 1500 milliseconds to 3000 milliseconds. They recorded a longer segment of brainwave data in each trial. Recall that in the 1960s when scientists looked farther out in time after the stimulus, they found previously unseen responses such as the P300 (Sutton et al. 1965).

**What is MERMER?**

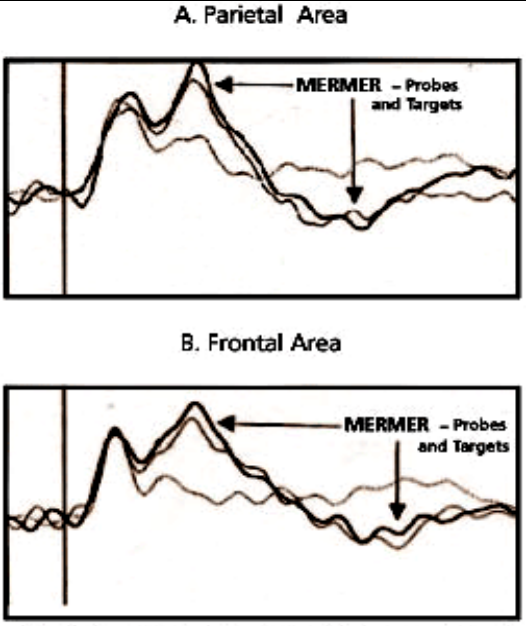


Figure 2. These are ERPs that are copied from the BF Web site, showing Pz (top) and Fz (bottom) ERPs. Positive is up, and the "MERMER" in response to targets and probes indicates two peaks with arrows; the first is the classic P300, and the second is the subsequent negative peak. The unlabelled waveforms not containing "MERMER5" are in response to irrelevant stimuli. (No timing information provided.)

Figure 1. Brain Wave

**3. Experimental design**

Brain fingerprinting tests are conducted according to the following scientific protocols. In a brain fingerprinting test, stimuli are presented to the subject in the form of words, phrases, or pictures on a computer screen. (Auditory stimuli may also be presented.) Brain responses are measured non invasively from the scalp, digitized, and analyzed to determine the presence or absence of information stored in the brain. Figure 1 outlines the stages of data acquisition and analysis in brain fingerprinting.

Three types of stimuli are presented: probes, targets, and irrelevant. Probes contain information that is relevant to the crime or other investigated situation. Probes have three necessary attributes.

- Probes contain features of the crime that in the judgment of the criminal investigator the perpetrators would have experienced in committing the crime.
- Probes contain information that the subject has no way of knowing if he did not participate in the crime.
- Probes contain information that the subject claims not to know or to recognize as significant for any reason.

For example, if a subject claims not to have been at the murder scene and not to know what the murder weapon was, a probe stimulus could be the murder weapon, such as a knife. Brain fingerprinting experimental protocols ensure that probes do not contain information that the subject knows from the news media interrogations.

The scientific question addressed by a brain fingerprinting test is whether or not the subject is knowledgeable regarding the crime or investigated situation. Specifically, the critical variable is his recognition of the information contained in the probes as significant in the context of the crime (or lack thereof). If, and only if, this is present, it is predicted that the probes will elicit a P300-MERMER. The amplitude, morphology and latency will be characteristic of the individual subject's response to such stimuli when the subject knows the relevant information. For a subject who is knowledgeable or "information present," the probes contain information describing known features of the crime. For a subject who is "information absent," the probes contain information describing plausible features of the crime that are not known to be correct. To objectively classify the probe responses into one of these two categories, it is necessary to isolate the critical variable. To accomplish this, two standards are required: a standard for the response of this subject to stimuli containing known features of the crime, and a standard for the response of this subject to stimuli containing plausible but unknown (or incorrect) features of the crime.

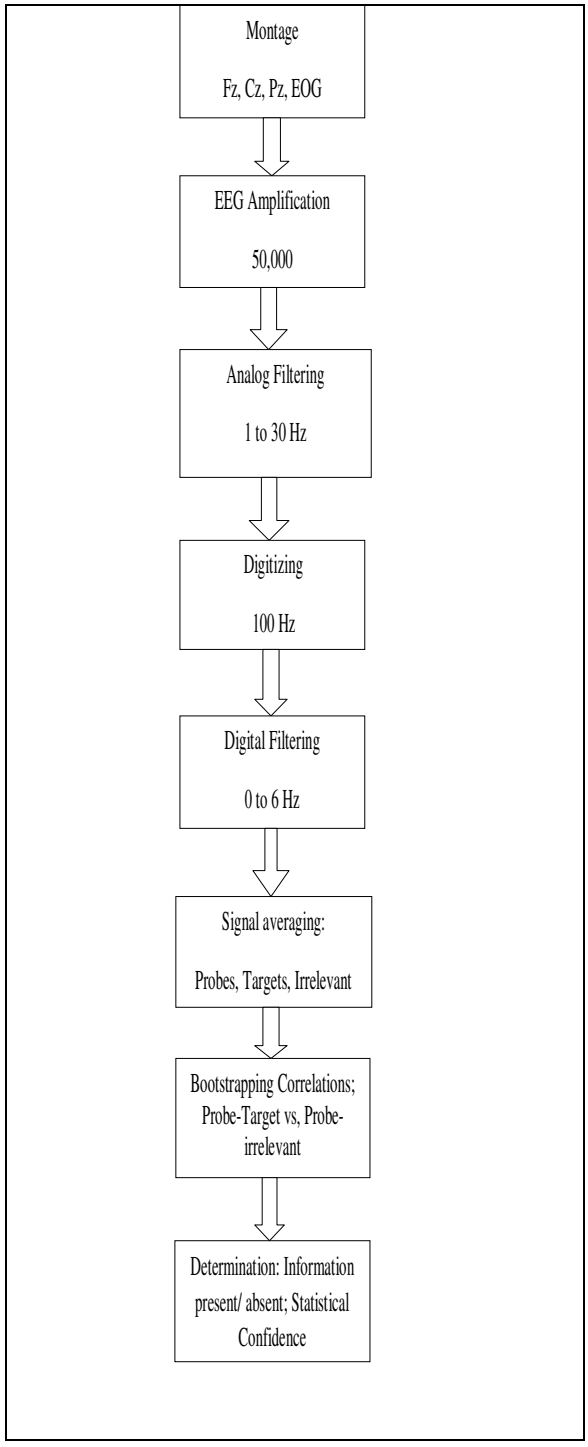


Figure 2. Flow Chart of Experimental Design

**Instrumental requirements:**

- Personal Computer
- A Data acquisition board
- A Graphics Card for driving two monitors from one PC
- A four-channel EEG amplifier system.

- Software developed by the Brain Fingerprinting laboratories for the data acquisition and analysis.

Figure 3 Person being tested wearing a special headband with electronic sensors.

Figure 4 Victims facial expression

The belt wearing in both the figures containing special sensors. Brain fingerprinting is said to be more accurate in detecting "guilty" knowledge distinct from the false positives of traditional polygraph methods, but this is hotly disputed by specialized researchers and has been criticized on a number of fronts (Abdollah, 2003; Fox 2006b). Although independent scientists who have used the same or similar methods as Farwells brain fingerprinting have achieved similar, highly accurate results (Allen and Lacono, 1997; Harrington v. State), different methods have yielded different results. J. Peter Rosenfeld used P300-based tests incorporating fundamentally different methods, resulting in as low as chance accuracy (Rosenfeld et al., 2004) as well as susceptibility to countermeasures, and criticized brain fingerprinting based on the premise that the shortcomings of his alternative technique should generalize to all other techniques in which the P300 is among the brain responses measured, including brain fingerprinting.

**Operation of the Technique**

The person to be tested wears a special headband with electronic sensors that measure the electroencephalography from several locations on the scalp (Figure 3). In order to calibrate the brain fingerprinting system, the testee 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, for example, a rare vs. a common stimulus or a stimulus the subject is asked to count (Gaillard and Ritter, 1983; Picton, 1988). 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 4**.** Victims facial expression. Because it is based on EEG signals, the system does not require the testee to issue verbal responses to questions or stimuli.

Brain fingerprinting uses cognitive brain responses and do not depend on the emotions of the subject, nor is it affected by emotional responses (Farwell, 1994). Brain fingerprinting is fundamentally different from the polygraph (lie-detector), which measures emotion-based physiological signals such as heart rate, sweating, and blood pressure (Farwell and Smith, 2001; Farwell 1992a, 1995a). Also, unlike polygraph testing, it does not attempt to determine whether or not the subject is lying or telling the truth. Rather, it measures the subjects brain response to relevant words, phrases, or pictures to detect whether or not the relevant information is stored in the subjects brain (Farwell and Smith, 2001; Simon, 2005; Harrington v. State).

**Analysis procedure**

When brain fingerprinting test is done on any suspect then this type of graph appears on the analyzer screen, by seeing these waves is comes to the conclusion that whether the information is present in the person mind or not. This graph shows three lines red, blue and green. Red line indicates the information that suspect is expected to know. Green line shows information that is not known to the suspect and the blue line indicated the information of the crime that only suspect would know. In this graph green line and the blue line are closely correlate with each other that means the related information is not present in the suspect brain. Information is not present in figure of not guilty.

In this graph since blue and red lines which indicated that the information is expected to know by the suspect and the information that only the suspect would know are correlated with each other that shows the information is present in the suspect brain. This is how analyzes is done in brain fingerprinting. The whole procedure of brain fingerprinting consists of four phases.

**Comparison of waveform**

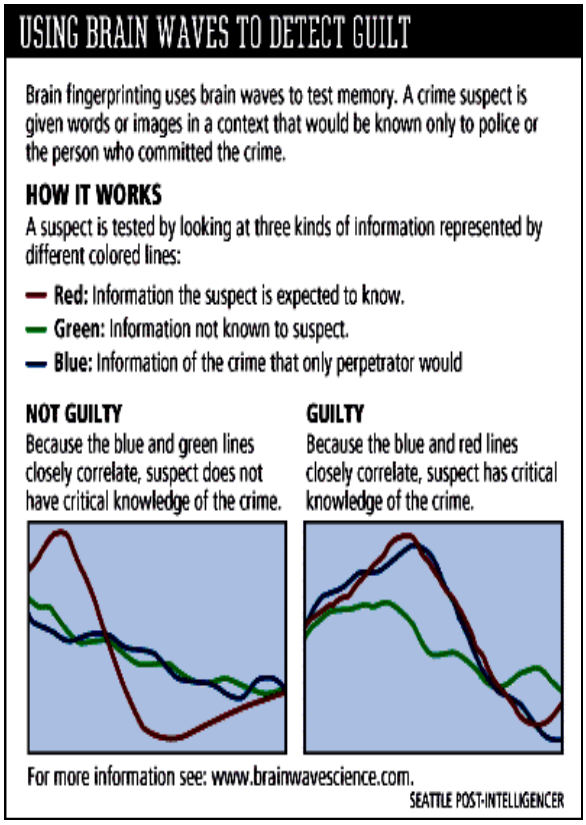


Figure 5. Waveform of Brain Fingerprinting

A Suspect is tested by looking at three kinds of information represented by Different colored lines:

-----Red: information the suspect is expected to know

-----Green: information not known to suspect

-----Blue: information of the crime that only perpetrator would know.

**NOT GUILTY:**

1. Because the blue and green
2. Lines closely correlate, suspect does
3. Critical knowledge of the crime

**GUILTY:**

1. Because the blue and red
2. Lines closely correlate, and suspect does not
3. Critical knowledge of the crime.

**Four phases of Farwell brain fingerprinting**

In fingerprinting and DNA fingerprinting, evidence is recognized and collected at the crime scene, and preserved properly until a suspect is apprehended, is scientifically compared with evidence on the person of the suspect to detect a match that would place the suspect at the crime scene. Farwell Brain fingerprinting works similarly, except that the evidence collected both at the crime scene and on the person of the suspect (that is, in the brain as revealed by electrical brain responses) is informational evidence rather than physical evidence.

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.
4. Brain fingerprinting scientific result.

In the crime scene evidence collection, an expert in Farwell brain fingerprinting examines the crime scene and other evidence connected with the crime to identify detail of the crime that would be known only to the perpetrator. The expert then conducts the brain evidence collection in order to determine whether or not the evidence from the crime scene matches evidence stored in the brain of suspect. In the computer evidence analysis, the Farwell 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" –the details of the crime are stored in the brain of the suspect – or "information absent" – the details of the crime are not stored in the of the suspect.

**Record of 100% of accuracy**

At the time of this first field application, Dr. Farwell's successes in the scientific laboratory with his invention were already well known. In collaboration with FBI scientist Dr. Drew Richardson, Dr. Farwell achieved 100% accuracy in using Farwell Brain Fingerprinting to identify FBI agents based on their brain responses to words and phrases only an FBI agent would recognize. Tests conducted by Dr. Farwell for the US Navy in collaboration with Navy LCDR Rene S. Hernandez, Ph.D., also resulted in 100% accurate results. In research on contract with a US government intelligence agency, Farwell Brain Fingerprinting achieved 100% accuracy in proving the presence or absence of a wide variety of evidence stored in the brains of individuals involved in over 120 cases. Dr. Farwell has published extensively in the scientific literature and presented his research to many scientific and technical audiences throughout the worl. Farwell Brain Fingerprinting has been subjected to rigorous peer review under US government sponsorship, and has been found scientifically viable as well as revolutionary in its implications.

**4. CONCLUSIONS AND FUTURE SCOPE**

Brain Fingerprinting is a revolutionary new scientific technology for solving crimes, identifying perpetrators, and exonerating innocent suspects, with a record of 100% accuracy in research with US government agencies, actual criminal cases, and other applications. The technology investigators fulfill an urgent need for governments, law enforcement agencies, corporations, crime victims, and falsely accused innocent suspects.

**APPLICATIONS**

The various applications are as follows:-

1. Test for several forms of employment, especially in dealing with sensitive military and foreign intelligence screening.
2. Individuals who were "information present" and "information absent".
3. A group of 17 FBI agents and 4 non-agents were exposed to stimuli.
4. To detect symptoms of Alzheimer's disease, Mental Depression and other forms of dementia including neurological disorders.
5. Criminal cases.
6. Advertisements (researches are being carried on).
7. Counter-Terrorism.
8. Security Testing.

**Counter Terrorism**

Brain fingerprinting can help address 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.3
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.
5) 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.
6) A Brain Fingerprinting test can determine with an extremely high degree of accuracy those who are involved with terrorist activity and those who are not.

**ADVANTAGES**

1) The primary advantage of brain fingerprinting is that in most crimes very few such features can be found. In some crimes none are available. The record stored in the brain of the perpetrator is often a rich source of information that can be connected to the crime scene. Except in rare cases where the crime has been recorded on video, the record stored in the brain is generally the most comprehensive available record of the crime, even though it is not perfect.
2) Brain fingerprinting also has advantages in comparison to witness testimony. It provides an objective, scientific way to detect the record of the crime stored in the brain directly. Witness testimony provides an indirect, subjective account of this record. Witnesses may lie. The brain never lies. If the information is stored in the brain, it can be objectively detected regardless of the honesty or dishonesty of the subject.
3) Identify criminals quickly and scientifically.
4) Record of 100% accuracy.
5) Identify terrorists and members of gangs, criminal and intelligence organizations.
6) Reduce expenditure of money and other resources in law enforcement.
7) Reduce evasion of justice.
8) Access criminal evidence in the brain.
9) Fingerprints and DNA, though accurate and highly useful, can only be collected in approximately 1% of all criminal cases brain is always there.
10) Human Rights Oriented.

**DISADVANTAGES**

1) Brain fingerprinting detects information-processing brain responses that reveal what information is stored in the subjects brain. It does not detect how that information got there, be it a witness or a perpetrator.
2) Brain fingerprinting detects only information, and not intent. The fact that the suspect knows the uncontested facts of the circumstance does not tell us which partys version of the intent is correct (Simon, 2005).
3) Brain fingerprinting is not applicable for general screening, for example, in general pre-employment or employee screening wherein any number of undesirable activities or intentions may be relevant. If the investigators have no idea what crime or undesirable act the individual may have committed, there is no way to structure appropriate stimuli to detect the telltale knowledge that would result from committing the crime. Brain fingerprinting can, however, be used for specific screening or focused screening, when investigators have some idea what they are looking for. For example, brain fingerprinting can be used to detect whether a person has knowledge that would identify him as an FBI agent, an Al-Qaeda-trained terrorist, a member of a criminal organization or terrorist cell, or a bomb maker.
4) Brain fingerprinting does not detect lies. It simply detects information. No questions are asked a brain fingerprinting test, and the outcome of the test is unaffected by whether he has lied or answered during a brain fingerprinting test. The subject neither lies nor tells the truth during or told the truth at any other time. The outcome of "information present" or "information absent" depends on whether the relevant information is stored in the brain, and not on what the subject says about it (Farwell, 1994; Simon, 2005; PBS 2004). 5) Just as all witness testimony depends on the memory of the witness, brain on the fingerprinting depends memory of the subject.
5) In the probe stimuli. 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. A DNA test determines only whether two DNA samples match, it does not determine whether the investigator did an effective job of collecting DNA from the crime scene. Similarly, a brain fingerprinting test determines only whether or not the information stored in the suspect's brain matches the information contained.

6) Brain fingerprinting is not a substitute for effective investigation on the part of the investigator or for commonsense and good judgment on the part of the judge and jury.

**REFERENCES**

[1] Allen, JJ, Mertens, R(2009) Limitations to the detection of deception: true and false recollection are poorly distinguished using an event-related potential procedure. Social Neuroscience 4(6), 473-90.

[2] Basar-Eroglu C, Basar E, Demiralp T, Schumann M (1992) P300-response: possible psychophysiological correlates in delta and theta frequency channels. A review. International Journal of Psychophysiology, 13, 2, 161-79.

[3] Daubert v. Merrell Dow Pharmaceuticals, Inc. 509 U.S. 579, 594 (1993).

[4] Farwell, L A (1992a) the Brain-Wave Information Detection (BID) System: A New Paradigm for Psychophysiological Detection of Information. Doctoral Dissertation, University of Illinois at Urbana-Champaign p. 1-165.

[5] Farwell, L A (1992b) Two new twists on the truth detector: brain-wave detection of occupational information. Psychophysiology 29(s4A), S3.

[6] Farwell LA, inventor. Method and apparatus for multifaceted electroencephalographic response analysis (MERA). US patent 5,363,858. 1994 Nov 15.

[7] Farwell LA, Donchin E. The truth will out: interrogative polygraphy ("lie detection") with event-related brain potentials. Psychophysiology 1991;28:531-541.

[8] Allen, J (2008). Not devoid of forensic potential, but... The American Journal of Bioethics 8(1), 27-28

[9] Allen, J, Iacono, WG (1997) A comparison of methods for the analysis of event-related potentials in deception detection. Psychophysiology 34, 234 - 240.

[10] Erickson, M J (2007) Daubert's Bipolar Treatment of Scientific Expert Testimony -- From Frye's Polygraph to Farwell's Brain Fingerprinting. Drake Law Review 55, 763-812.

[11] Farwell LA and Smith SS. Using Brain MERMER Testing To Detect Concealed Knowledge Despite Efforts To Conceal Journal of Forensic Sciences 2001