

Full Length Research Paper

Brain fingerprinting

Dhiraj Ahuja* and Bharat Singh

Department of Electrical and Electronics Engineering, YMCA University of Science and Technology, Faridabad-121006 (Haryana), India.

Accepted 9 January, 2012

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 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. In the field of criminology, a new lie detector has been developed in the United States of America called “brain finger printing”. 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.

Keywords: Polygraph, electroencephalography, Farwell brain fingerprinting, electroencephalography (EEG) signals.

INTRODUCTION

Brain fingerprinting is an investigative technique which measures recognition of familiar stimuli by measuring electrical brain wave responses to words, phrases, or pictures that are presented on a computer screen. Brain fingerprinting was invented by Lawrence Farwell. Its theory explains that the suspect's reaction to the details of an event or activity will reflect if the suspect had prior knowledge of the event or activity (Farwell and Donchin, 1991). Farwell's brain fingerprinting originally used the well known P300 brain response to detect the brain's recognition of the known information (Farwell and Donchin, 1986, 1991; Farwell 1995a). Later Farwell discovered the "memory and encoding related multifaceted electroencephalographic response" (MERMER), which includes the P300 and additional features and is reported to provide a higher level of accuracy than the P300 alone (Farwell and Smith, 2001; Farwell, 1994, 1995b). One of the applications is lie detection. Farwell brain fingerprinting has been 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. In peer-reviewed publications Farwell and colleagues report over 99% accuracy in laboratory research (Farwell and Donchin, 1991; Farwell and Richardson, 2006b) and real-life field applications (Farwell and Smith, 2001; Farwell and Richardson, 2006a). In independent research William Iacono and others who followed identical or similar scientific protocols to Farwell's have reported a similar high level of accuracy (Allen and Iacono, 1997).

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 (for example, palm sweating and heart rate), while brain fingerprinting measures electrical brain activity via a fitted headband

*Corresponding author. E-mail: dahuja8978@yahoo.com. Tel: 919255947380, 918901584248.



Figure 1. Person being tested wearing a special headband with electronic sensors.



Figure 2. Victim's facial expression.

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 Farwell's 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 1). 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 (Figures 2 and 3).

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 subject's brain response to relevant words, phrases, or pictures to detect whether or not the relevant information is stored in the subject's brain (Farwell and Smith, 2001; Simon, 2005; Harrington v. State).

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; and
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 the suspect. In the computer evidence analysis, the Farwell

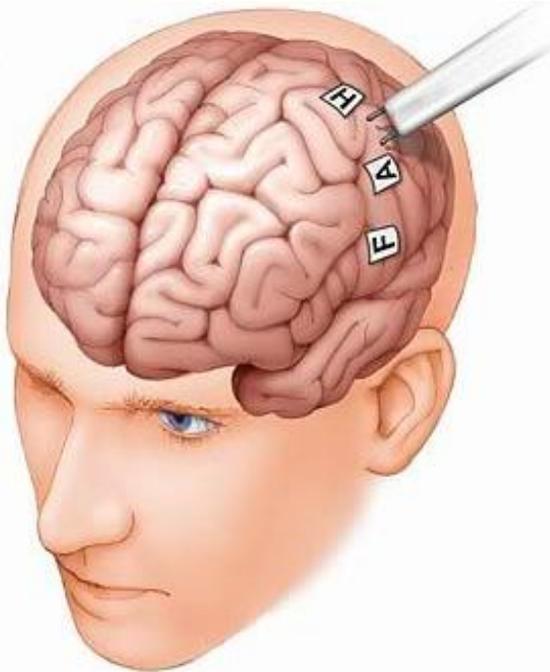


Figure 3. Victim's stimulus.

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 brain of the suspect (Figure 4).

APPLICATIONS

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.
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 (Figure 3). 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 this technology, now, terrorists and those supporting terrorism can be identified quickly and accurately.

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. In a study with the FBI, Dr. Farwell and FBI scientist Drew Richardson, former chief of the FBI's chem-bio-nuclear counterterrorism unit, used brain fingerprinting to show that test subjects from specific groups could be identified by detecting specific knowledge which would only be known to members of those groups (Farwell, 1993; Farwell and Richardson, 2006b). A group of 17 FBI agents and 4 non-agents were exposed to stimuli (words, phrases, and acronyms) that were flashed on a computer screen. The probe stimuli contained information that would be common knowledge only to someone with FBI training. Brain fingerprinting correctly distinguished the FBI agents from the non-agents.

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. 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. Brain Fingerprinting testing was also "instrumental in obtaining a confession and guilty plea" from serial killer James B. Grinder, according to Sheriff Robert Dawson of Macon County, Missouri. In August 1999, Dr. Farwell conducted a brain fingerprinting test on Grinder, showing that information stored in his brain matched the details of the murder of Julie Helton

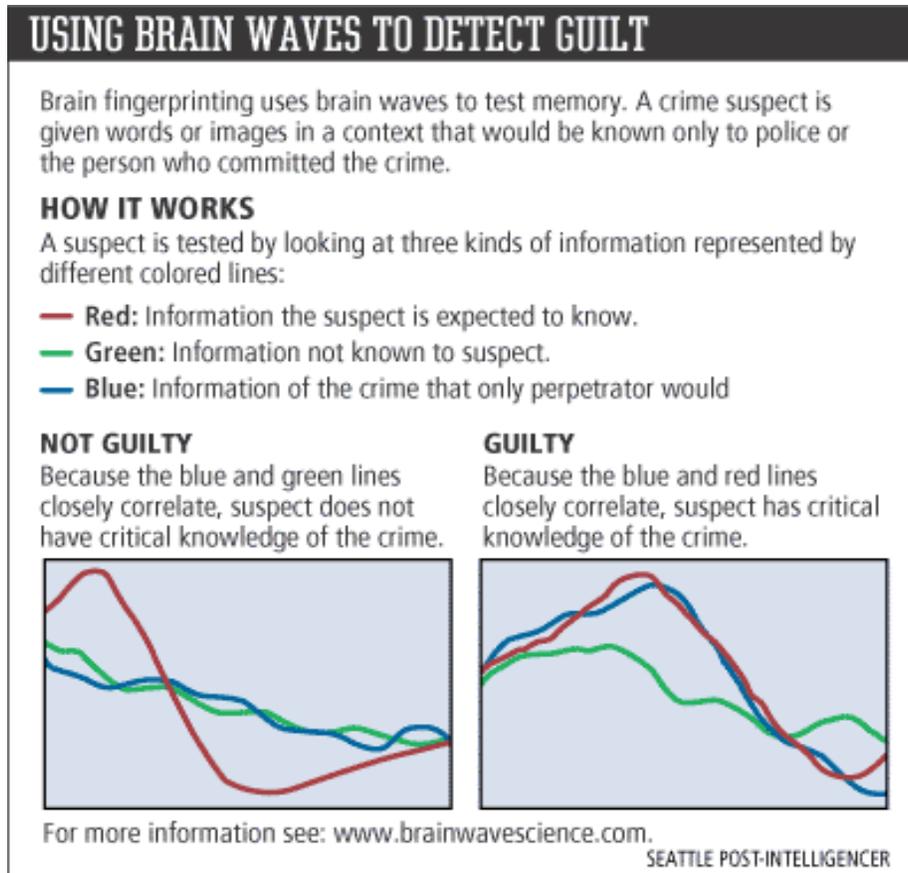


Figure 4. Use of Brain waves to detect guilt.

(Dalbey, 1999). Faced with a certain conviction and almost certain death sentence, Grinder then pled guilty to the rape and murder of Julie Helton in exchange for a life sentence without parole. He is currently serving that sentence and has also confessed to the murders of three other women.

Medical

'Brain fingerprinting' is the patented technology that can measure objectively, for the first time, how memory and cognitive functioning of Alzheimer sufferers are affected by medications. A 30 min test involves wearing a headband with built-in electrodes; technicians then present words, phrases and images that are both known and unknown to the patient to determine whether information that should be in the brain is still there. 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.

Additional applications

In advertising, Brain fingerprinting laboratories will offer significant advances in measuring campaign and media effectiveness. Most advertising programs today are evaluated subjectively using focus groups. We will be able to offer significantly more advanced, scientific methods to help determine the effectiveness of campaigns and be very cost competitive with current methodologies. This technology will be able to help determine what information is actually retained in memory by individuals. For example, in a branding campaign do people remember the brand, the product, etc. and how do the results vary with demographics? We will also be able to measure the comparative effectiveness of multiple media types.

In the insurance industry, brain fingerprinting laboratories will be able to be helpful to reduce the

incidence of insurance fraud by determining if an individual has knowledge of fraudulent or criminal acts. The same type of testing can help to determine if an individual has specific knowledge related to computer crimes where there is typically no witness or physical evidence. In a CIA-funded study, brain fingerprinting correctly detected which individuals had participated in specific real-life events, some of which were crimes, based on the record stored in their brains. Accuracy again was 100% (Farwell and Richardson, 2006a). Dr. Farwell collaborated with FBI scientist Sharon Smith in a further study in which brain fingerprinting detected real-life events that was published in the *Journal of Forensic Sciences* (Farwell and Smith, 2001).

COMPARISON WITH OTHER TECHNOLOGIES

Conventional fingerprinting and DNA match physical evidence from a crime scene with evidence on the person of the perpetrator. Similarly, brain fingerprinting matches informational evidence from the crime scene with evidence stored in the brain. Fingerprints and DNA are available in only 1% of crimes. The brain is always there, planning, executing, and recording the suspect's actions.

Brain fingerprinting has nothing to do with lie detection. Rather, it is a scientific way to determine if someone has committed a specific crime or other act. No questions are asked and no answers are given during Farwell brain fingerprinting. As with DNA and fingerprints, the results are the same whether the person has lied or told the truth at any time.

Admissibility of brain fingerprinting in court

The admissibility of brain fingerprinting in court has not yet been fully established. The following well established features of brain fingerprinting, however, will be relevant when the question of admissibility is tested in court. 1) Brain fingerprinting has been thoroughly and scientifically tested. 2) The theory and application of brain fingerprinting have been subject to peer review and publication. 3) The rate of error is extremely low -- virtually nonexistent -- and clear standards governing scientific techniques of operation of the technology have been established and published. 4) The theory and practice of brain fingerprinting have gained general acceptance in the relevant scientific community. 5) Brain fingerprinting is non-invasive and non-testimonial. There are examples where court has considered the brain fingerprinting reports. Farwell's brain fingerprinting has been ruled admissible as evidence in court in the reversal of the murder conviction of Terry Harrington (*Harrington v. State*, Farwell and Makeig, 2005). Following a hearing on post-conviction relief on November 14, 2000, an Iowa District Court held that Dr. Farwell's brain fingerprinting

P-300 test results were admissible as scientific evidence as defined in Congress Ruling 702 and in the Daubert standard. Harrington was freed by the Iowa Supreme Court on constitutional grounds.

LIMITATIONS OF BRAIN FINGERPRINTING

1. Brain fingerprinting detects information-processing brain responses that reveal what information is stored in the subject's 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 party's 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 (Farwell and Richardson, 2006b).
4. Brain fingerprinting does not detect lies. It simply detects information. No questions are asked or answered during a brain fingerprinting test. The subject neither lies nor tells the truth during a brain fingerprinting test, and the outcome of the test is unaffected by whether he has lied 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 fingerprinting depends on the memory of the subject.
6. 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 in the probe stimuli.
7. 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 (PBS 2004).

REFERENCES

- Abdollah T (2003). Brain Fingerprinting – Picture-perfect crimes. *Berkeley Med. J. Issues*, Spring 2003. Accessed July 20, 2008.
- Allen JJB, Lacono WG (1997). A comparison of methods for the analysis of event-related potentials in deception detection. *Psychophysiol.*, 34: 234-240.
- Dalbey B (1999). Brain Fingerprinting Testing Traps Serial Killer in Missouri. *The Fairfield Ledger*. Fairfield, IA, August, p. 1.
- Farwell LA, Donchin E (1986). The brain detector: P300 in the detection of deception. *Psychophysiology*, 24: 434.
- Farwell LA, Donchin E (1991). The Truth Will Out: Interrogative Polygraphy ("Lie Detection") With Event-Related Brain Potentials. *Psychophysiol.*, 28: 531-547.
- Farwell LA (1992a). The brain-wave information detection (BID) system: A new paradigm for psycho physiological detection of information (unpublished doctoral dissertation). Urbana-Champaign (IL): University of Illinois.
- Farwell LA (1993). Brain MERMERs: Detection of FBI Agents and crime-relevant information with the Farwell MERA system. *Proceedings of the International Security Systems Symposium*, Washington, D.C.
- Farwell LA (1994). Method and Apparatus for Multifaceted Electroencephalographic Response Analysis (MERA). U.S. Patent #5,363,858, Nov. 15.
- Farwell LA (1995a). Method and Apparatus for Truth Detection. U.S. Patent #5,406,956, April 18.
- Farwell LA (1995b). Method for Electroencephalographic Information Detection. U.S. Patent #5,467,777, Nov. 21.
- Farwell LA, Smith SS (2001). Using Brain MERMER Testing to Detect Concealed Knowledge Despite Efforts to Conceal. *J. Forens. Sci.*, 46(1): 135-143.
- Farwell LA, Makeig T (2005). Farwell Brain Fingerprinting in the case of *Harrington v. State*. *Open Court X*, 3: 7-10. Indiana State Bar Association.
- Farwell LA, Richardson DC (2006a). Brain Fingerprinting in Field conditions. *Psychophysiology*, 43: 5 S37-S38.
- Farwell LA, Richardson DC (2006b). Brain Fingerprinting in Laboratory Conditions. *Psychophysiol.*, 43: S38.
- Fox C (2006b). Brain Fingerprinting Skepticism. *American Observer*, March 29.
- Gaillard AKW, Ritter W (1983). *Tutorials in event-related potential research: endogenous components*. Amsterdam: North-Holland.
- Harrington v. State*, Case No. PCCV 073247. Iowa District Court for Pottawattamie County, March 5, 2001.
- PBS Innovation Series (2004). Brain Fingerprinting May 4, 2004. Brain Fingerprinting: Ask the Experts. Accessed July 20, 2008.
- Picton TW (1988). *Handbook of electroencephalography and clinical neurophysiology: Human event-related potentials*. 3: Amsterdam: Elsevier.
- Rosenfeld JP, Soskins M, Bosh G, Ryan A (2004). Simple, Effective Counter measures to P300-based Tests of Detection of Concealed Information. *Psychophysiol.*, 41: 205–219.
- Simon S (2005). What you don't know can't hurt you. *Law Enforcement Technology*, Sept., 2005.