An Conventional Methodology for Brain FingerPrinting

M. Ramasubramanian
Professor & Head,
Department of CSE,
Sri Devi Women’s Engineering
College, Hyderabad, India

TKS. Rathish Babu
Professor,
Department of CSE,
Sri Devi Women’s Engineering
College, Hyderabad, India

VRS. Rajesh Kumar
Professor & Head,
Department of ECE,
Sri Devi Women’s Engineering
College, Hyderabad, India

DOI: 10.23956/ijarcsse/V7I7/0118

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. In the field of criminology, a new lie detector has been developed in the United States of America. 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 crime. According to the experts, even if the person willingly suppresses the necessary information, the brain wave is sure to trap him.

Keywords—Sensors, response, knowledge, resonance, Security

I. INTRODUCTION

Brain Fingerprinting is a controversial investigative technique that 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. The theory is 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. 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.

A. Definition

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 guilt 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.

B. Origin of The Term Brain Fingerprinting

Brain fingerprinting is so named based on the following analogy. Fingerprinting establishes an objective, scientific connection between fingerprints at a crime scene and the fingers of a suspect. DNA “fingerprinting,” as it is sometimes called, establishes an objective, scientific connection between biological samples from the crime scene and biological samples from the suspect. Brain fingerprinting was so named because like fingerprinting it detects a match between evidence from the crime scene and evidence on the person of the suspect. It establishes an objective, scientific connection between features of the crime scene and the record stored in the brain of a suspect.

C. Principles of Applying Brain Fingerprinting

The purpose of brain fingerprinting is to determine whether or not specific relevant knowledge is stored in the brain of the suspect.

In field cases, the relevant knowledge generally is information that an investigator thinks represent the details of a crime. Alternatively, it may be information that is known only to a particular group of people, such as FBI agents, skilled bomb makers, trainees of an Al-Qaeda training camp, or members of a terrorist cell. The primary example used herein
will be the case where the relevant knowledge constitutes information that an investigator believes constitutes salient features of a crime that the perpetrator experienced in the course of committing the crime. The relevant knowledge is provided by the criminal investigator to the brain fingerprinting scientist. The goal of brain fingerprinting is to determine whether or not the relevant knowledge is known to the subject.

Brain fingerprinting does not evaluate whether or not the investigator's account of the crime is accurate, or whether the putatively relevant knowledge actually correctly represents the crime. Brain fingerprinting does not detect guilt or innocence. The determination of whether the subject is guilty is a legal determination that is made by a judge and/or jury, not by a scientist or a computer.

Brain fingerprinting does not detect whether or not the subject committed the crime. It only detects whether or not the subject knows the relevant knowledge contained in the probes. The prosecution may argue that the best explanation for an “information present” determination is that the subject learned the relevant knowledge while committing the crime. (In a properly executed brain fingerprinting test, plausible alternative hypotheses such as the subject being told the information after the crime have been eliminated before the test.) The defense may argue that an “information absent” determination introduces a reasonable doubt that the subject is guilty of committing the crime, and provides support for his claims of innocence. The defense may argue, for example, that a subject should or would know the relevant knowledge if he had committed the crime.

Brain fingerprinting does not evaluate whether the subject should, could, or would know the information, and under what circumstances. It only determines whether or not the subject actually does know the relevant knowledge. The interpretation of the results of a brain fingerprinting test in terms of guilt or innocence, participation or non-participation in a crime, goes beyond the science and is outside the realm of expert testimony by a brain fingerprinting scientist.

Brain fingerprinting is similar to other forensic sciences in this regard. A DNA expert testifies that Sample A, which the investigators say came from the crime scene, matches Sample B, which the investigators say came from the subject. Similarly, an expert may testify that two fingerprints match. He does not testify, report, or attempt to scientifically determine “Therefore, the subject committed the murder.” A brain fingerprinting scientist testifies regarding only one specific fact: the subject does or does not know the specific relevant knowledge tested (Harrington v. State 2001). The degree to which this fact is probative regarding the subject’s participation in a crime is outside the realm of science. That is a matter to be debated by the prosecution and defense and decided by a judge and/or jury based on their non-scientific, common sense judgment and life experience.

In a laboratory setting, the relevant knowledge is fabricated by the experimenter. One additional step is necessary before a test can be implemented to test whether or not the subject knows the relevant knowledge. The experimenter designs and implements a knowledge-imparting procedure to impart the relevant knowledge to the subject. The imparting procedure generally constitutes a training session, a mock crime, or some combination thereof. The purpose of the knowledge-imparting procedure is to make certain that the subject knows the relevant knowledge. The accuracy of a method to detect the relevant knowledge can only be evaluated when the relevant knowledge is actually there to be detected. If the knowledge-imparting procedure fails to impart the knowledge to the subject, then the knowledge is not there to be detected. No method, no matter how perfect, can detect knowledge that is not there. As discussed above in the context of ground truth, in order to conduct a valid test of a knowledge-detection procedure in a laboratory study, the experimenter must independently assess whether the knowledge-imparting procedure actually succeeded in imparting the knowledge so it was there to be detected. This is accomplished by post-test interviews.

In a field case, the brain fingerprinting procedure begins after the criminal investigator has provided the relevant knowledge to the scientist. In a laboratory case, the brain fingerprinting procedure begins after the experimenter has fabricated the relevant knowledge and successfully implemented the knowledge-imparting procedure.

The relevant knowledge generally comprises 12–30 short phrases or pictures, along with an explanation of the significance of each in the context of the crime. The investigator also provides the scientist with a detailed account of which items in the relevant knowledge are or may be already known to the subject for any known reason. For example, the investigator notes any specific features of the crime that have been published in the newspaper or revealed to the subject in interrogation or previous legal proceedings.

The relevant knowledge generally contains six to nine or more items that have never been revealed to the subject. These will constitute the probe stimuli. If there is an insufficient number of features that are known only to the perpetrator and investigators (probes), a brain fingerprinting test cannot be conducted.

Generally there are also six or more items that have already been revealed to the subject or are commonly known. These will constitute the target stimuli. The test requires an equal number of targets and probes. If there are too few features already known to the subject for non-incriminating reasons (potential targets), the experimenter may request additional information about the crime from the criminal investigator to use for target stimuli. Alternatively, if there are ample available features of the crime that are not commonly known and have not been revealed to the subject (potential probes), the experimenter may elect to inform the subject about some of these features and use these as targets instead of probes.

D. 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 stimulus or a stimulus 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.

II. ARCHITECTURE

Brain fingerprinting can be viewed as a modern, and more accurate, lie detection test. To understand how it works, we must understand the basic difference between the guilty and the innocent. The guilty, since he has committed the crime, has the details of the crime in his memory. However, the innocent does not have the details in his memory. Brain fingerprinting is a test of whether the details are present in the memory or not. If they are, then the person is guilty, otherwise innocent as shown in Fig. 1.

Fig. 1 Architecture

Brain fingerprinting does brain fingerprinting check for these details in a person’s memory by showing certain images of objects (possible murder weapons, etc) and other stimulus. It then records the response of the person’s brain on seeing these objects. EEG sensors are used to record these responses. Further, a specific waveform called the P300 gets activated (as measured in the response) only if the person is guilty; otherwise it does not. P300 is the specific response of a brain that recognizes the object/image shown, and hence, has the object/image in his memory. This helps identify the guilty. However, the human brain is capable of generating as well as modifying thoughts. No matter what the truth is, the brain has the power to choose to believe otherwise. The guilty may modify his thoughts even on seeing the murder weapon, and choose not to respond or think of the murder incident. The solution to this problem is to record the response of the person to the stimulus within fractions of a second. The response is recorded before the person can modify it, or even be aware of his own thoughts as shown in Fig. 2.

Fig. 2 Brain Fingerprinting Setup
A. Instrumental Requirements
- Personal Computer
- Data acquisition board
- Graphic card for driving two monitors from one PC
- Four channel EEG amplifier
- Software developed by Brain fingerprinting Laboratories for data acquisition and analysis

1) Personal computer: A Pentium 4, 1 GHz IBM personal computer (CPU) is the most important unit which is the brain of the whole setup for Brain Fingerprinting. The headband measures the electroencephalographic (EEG) response from several locations on the scalp. Silver-silver chlorides disposable electrodes were held in a place by a custom headband as shown in Fig. 3.

![Fig. 3 Collection of Data from Sensors](image-url)

2) Data acquisition board: Data Acquisition board (DAQ) is used for converting the signal into a digital format i.e. digitization.

3) Brain fingerprinting software: A Brain Fingerprinting Software developed for the assistance is installed into the personal computer.

4) Electro encephalo gram (eeg): The neurons in the brain fire electrically, forming a vast network of electrical potential conduits. Electroencephalography (EEG) involves the measurement of these patterns of electrical voltage changes that originate in the brain. These measurements are made non-invasively from the scalp. When the brain conducts certain tasks, specific patterns of EEG (or “brainwave”) activity are produced. An example of such a specific task is noticing, recognizing, and processing the information contained in a significant stimulus such as a murder weapon presented on a screen in a brain fingerprinting test. These specific patterns of brainwave activity are known as event-related brain potentials, or ERPs. Brain fingerprinting technique uses event-related brain potentials to determine what information is stored in a person’s brain. This is based on how the brain processes specific information such as the features of a crime that are presented on a computer screen.

B. The Discovery of The P300-Mermer

In the initial brain fingerprinting research, Farwell and Donchin used the P300 event-related brain potential. 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 ms 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 1,000–1,500 ms (1–1.5 s). In the first brain fingerprinting study, for example, Farwell and Donchin presented a stimulus every 1,500 ms.

In dealing with real-life situations, Farwell and Richardson, Farwell et al. 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 1,500 to 3,000 ms. 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. The same thing happened to Farwell and Richardson. They were looking for the P300 response, and indeed the brain responses contained a clear P300 peak at about 500–800 ms. Surprisingly, however, this positive peak was followed by a negative peak with a latency as long as 1,200 ms. This unexpected late negative potential consistently followed the positive P300 peak. It was reliably elicited by the same “Aha” response that elicited the P300.

This more complex P300-MERMER response included both the P300 and a late negative peak (the Late Negative Potential or LNP). Farwell called this a memory and encoding related multifaceted electroencephalographic response (MERMER), or P300-MERMER. The P300 is maximal in the parietal area. The late negative potential (LNP) that constitutes the latter part of the P300-MERMER is parietally maximal yet also frontally prominent.

Experimentation (including recording without analog filters), scalp distribution (the relative amplitude at different scalp sites), and morphology (the latency and shape of the waveforms) proved that the LNP was not an artifact of the signal-detection or noise-reduction procedures or equipment, such as digital and analog filters. The recording equipment is identical for all scalp sites and all subjects. If the LNP were an artifact of the equipment, the identical equipment would produce the same effects in different instances. On the contrary, Farwell et al. found that the relative latency and amplitude of the P300 and the LNP are very different for different subjects and for different scalp sites in the same subject.

Like any new discovery, the P300-MERMER raises questions both of nomenclature and substance. The classical P300 is also known by various other names, including the P3, N2–P3 complex, P3a and P3b, late positive complex, and LPC. There has been considerable discussion as to whether the P300 is a unitary response or in fact a constellation of several responses. There has also been discussion over whether the various names refer to the same or slightly different phenomena.

The discovery of the P300-MERMER has allowed the brain fingerprinting results to be more accurate than the results obtained with the P300 alone. The P300-MERMER consists of a positive peak followed by a negative peak. The P300 includes only the positive peak. Thus, the full P300-MERMER contains more information and more distinctive features, and can be more reliably and accurately detected by a mathematical signal-detection algorithm than the P300 alone.

In all brain fingerprinting research using either the P300-MERMER or the P300 alone, there have been no false negatives and no false positives. 100% of determinations made have been correct. (See, however, the discussion below regarding the term “100% accurate.”) When Farwell and colleagues have included the full P300-MERMER in the data analysis algorithm, there have also been no in determinates. In brain fingerprinting research using the P300 alone, results have been indeterminate in 3% of cases overall, consisting of 12.5% in one experiment. As discussed below, an indeterminate response is not an incorrect response, but rather the determination that insufficient data are available to make a determination in either direction with high statistical confidence.

C. Stimuli

Three types of stimuli are presented.

- Probes
- Targets
- Irrelevants

1) Probes: 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; and
- 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, etc.

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.
2) **Target:** Target stimuli are details about the crime that the experimenter is certain the subject knows, whether or not he committed the crime. They may have been previously revealed through news accounts, interrogation, etc. In any case, the experimenter tells the subject the target stimuli and explains their significance in terms of the crime. Because they are significant in the context of the crime for all subjects, targets elicit an “Aha” response in all subjects. Targets elicit a P300-MERMER whether the subject knows the other salient features of the crime contained in the probes or not. For example, a target stimulus might be the name of the victim, which is revealed to the subject in the course of test instructions (and may be already known from news reports, etc.).

3) **Irrelevant:** Irrelevant stimuli contain information that is not relevant to the crime and not relevant to the subject. They consist of incorrect but plausible crime features. Irrelevant stimuli are designed to be indistinguishable from correct crime-relevant features (probes) to someone who does not know the features of the crime as shown in Fig.4.

If a probe stimulus is the murder weapon, a knife, then irrelevant stimuli could be other plausible (but incorrect) murder weapons such as a pistol, a rifle, and a baseball bat.

Thus, the targets and irrelevants both provide standard responses. The targets provide a standard for the subject’s brain response to relevant, significant information about the crime in question. The irrelevants provide a standard for the subject’s brain response or rather lack of a response to irrelevant information that is plausible as being crime-relevant.

It is vital in any science to isolate the critical variable. This three-stimulus design accomplishes this purpose. Targets and irrelevants differ only in whether or not they contain the critical feature being tested, that is, whether they contain known crime-relevant information. For an information-present subject, probe stimuli are virtually identical to target stimuli: both contain known features of the crime. The only difference is which button is pressed when the stimuli appear. For an information-absent subject, probes are indistinguishable from irrelevants. The probe responses are classified as being more similar to targets or irrelevants. Everything except the critical variable, namely the subject’s recognition of the probes as crime-relevant, is controlled.

![Fig.4 Brain waves used to detect guilt](image)

- **Red:** Information the suspect is expected to know. It arises due to target type stimuli.
- **Green:** Information not to suspect. The irrelevant stimuli is responsible for this type of brain waves.
- **Blue:** Information of the crime that only perpetrator would know. This occurs due to probes.

The subject is given a list of the targets and instructed to press a specific button when a target appears and another button when any other stimulus appears. Since the subject does not know which of the three types of stimulus will occur on each trial, he must read and evaluate each stimulus, and demonstrate behaviorally in each trial that he has done so by pressing the appropriate button.

For a subject who knows the relevant details about the crime, the probes, like the targets, are significant and relevant. Thus, the probes produce an “Aha” response when presented in the context of the crime. This manifests as a P300-MERMER in the brainwaves that will be virtually identical to the target response. For a subject who lacks the knowledge contained in the probes, the probes are indistinguishable from the irrelevants. Probes do not produce an “Aha” response or the corresponding P300-MERMER: the probe response will be virtually identical to the irrelevant response.

The brain fingerprinting computerized data analysis algorithm computes a mathematical determination as to whether the probe response is more similar to that of the targets or that of the irrelevants. The former yields a determination of “information present”; the latter, “information absent.” The information that is either present or absent in the brain of the subject is the information contained in the probes. The brain fingerprinting system also computes a statistical confidence for each individual determination, e.g., “information present, 99.9% confidence.” If there is insufficient data to reach either an “information present” or an “information absent” determination with a high statistical confidence, the algorithm returns the outcome of “indeterminate.”

Since the inclusion of the P300-MERMER in the brainwave data analysis algorithm, brain fingerprinting testing has made a definite determination in every case. All determinations have been correct. There have been no false negatives, no false positives, and no indeterminates. Error rate has been 0% in all studies and field applications. Accuracy has been
100%. (As discussed below, these are usually represented as “less than 1%” and “over 99%” respectively.) When brain fingerprinting data analysis has been conducted using the P300 alone, there have been no false positives or false negatives, and about 3% of the results have been indeterminate. All of these were in a single experiment wherein indeterminates comprised 12.5% of the results.

D. Electroencephalography

Electroencephalography (EEG) is the measurement of electrical activity produced by the brain as recorded from electrodes placed on the scalp. Just as the activity in a computer can be understood on multiple levels, from the activity of individual transistors to the function of applications, so can the electrical activity of the brain be described on relatively small to relatively large scales. At one end are action potentials in a single axon or currents within a single dendrite of a single neuron, and at the other end is the activity measured by the EEG which aggregates the electric voltage fields from millions of neurons. So-called scalp EEG is collected from tens to hundreds of electrodes positioned on different locations at the surface of the head. EEG signals (in the range of milli-volts) are amplified and digitalized for later processing. The data measured by the scalp EEG are used for clinical and research purposes as shown in Fig.5.

Fig.5 Electrography

E. Source of EEG Activity

Scalp EEG activity oscillates at multiple frequencies having different characteristic spatial distributions associated with different states of brain functioning such as waking and sleeping. These oscillations represent synchronized activity over a network of neurons. The neuronal networks underlying some of these oscillations are understood (such as the thalamocortical resonance underlying sleep spindles) while many others are not (e.g. the system that generates the posterior basic rhythm) as shown in Fig.6.

Fig.6 Adaptive noise module

F. EEG VS FMRI AND PET

EEG has several strong sides as a tool of exploring brain activity; for example, its time resolution is very high (on the level of a single millisecond). Other methods of looking at brain activity, such as PET and FMRI have time resolution between seconds and minutes.
EEG measures the brain’s electrical activity directly, while other methods record changes in blood flow (e.g., SPECT, FMRI) or metabolic activity (e.g., PET), which are indirect markers of brain electrical activity.

EEG can be used simultaneously with fMRI so that high-temporal resolution data can be recorded at the same time as high-spatial-resolution data, however, since the data derived from each occurs over a different time course, the data sets do not necessarily represent the exact same brain activity. There are technical difficulties associated with combining these two modalities like currents can be induced in moving EEG electrode wires due to the magnetic field of the MRI.

EEG can be recorded at the same time as MEG so that data from these complimentary high time resolution techniques can be combined. Magneto-encephalography (MEG) is an imaging technique used to measure the magnetic fields produced by electrical activity in the brain via extremely sensitive devices such as superconducting quantum interference devices (SQUIDs). These measurements are commonly used in both research and clinical settings. There are many uses for the MEG, including assisting surgeons in localizing pathology, assisting researchers in determining the function of various parts of the brain, neuro-feedback, and others.

1) **Method:** Scalp EEG, the recording is obtained by placing electrodes on the scalp. Each electrode is connected to one input of a differential amplifier and a common system reference electrode is connected to the other input of each differential amplifier. These amplifiers amplify the voltage between the active electrode and the reference (typically 1,000–100,000 times, or 60–100 dB of voltage gain). A typical adult human EEG signal is about 10μV to 100 μV in amplitude when measured from the scalp and is about 10–20 mV when measured from subdural electrodes. In digital EEG systems, the amplified signal is digitized via an analog-to-digital converter, after being passed through an anti-aliasing filter. Since an EEG voltage signal represents a difference between the voltages at two electrodes, the display of the EEG for the reading encephalographer may be set up in one of several ways.

### G. DATA ANALYSIS

The purpose of data analysis in brain fingerprinting studies is to determine whether the brain responses to the probe stimuli are more similar to the responses to the target stimuli or to the responses to the irrelevant stimuli, and to provide a statistical confidence for this determination. The determination and statistical confidence must be computed for each individual subject.

If the probe responses are mathematically more similar to the same subject’s responses to target stimuli containing known features of the crime, the subject is determined to be “information present.” If the probe responses are mathematically more similar to the same subject’s responses to irrelevant stimuli containing plausible but unknown (or incorrect) features of the crime, the subject is determined to be “information absent.”

To be valid, the statistical confidence for an individual determination of “information present” or “information absent” must take into account the level of variability in the individual brain responses that are aggregated in the average response. Farwell and Donchin and their colleagues Wasserman and Bockenholt applied bootstrapping to compute a statistical confidence for each individual determination that takes this variability into account. Bootstrapping is described in detail in these publications. It has now become a standard procedure in event-related brain potential research. Bootstrapping is a method to compute probability and statistical confidence regardless of the shape of the distribution of the data. It also provides a means to re-introduce the variability across single trials present in the original data, while preserving the feature of a smooth average that is necessary for comparing the waveforms of the three types.

The algorithm is as follows. Conduct the following procedure twice, once using the time epoch characteristic of the P300-MERMER (typically 300–1,800 ms after the stimulus) and once using the time epoch characteristic of the P300 alone (typically 300–900 ms post-stimulus).

- Sample randomly with replacement T target trials, P probe trials, and I irrelevant trials, where T, P, and I are equal to the total number of trials in the data set of the respective types. A trial consists of one stimulus presentation and the associated brain response data.
- Average the trials by trial type, yielding three average waveforms: probe, target, and irrelevant. Compare the average waveforms to determine if the probe average is more similar to the target average or to the irrelevant average.
- Repeat the above procedure 1,000 times. Each iteration yields a new set of 3 averages containing probe, target, and irrelevant trials respectively. Keep a tally of the number of times the probe average is more like the irrelevant average than like the target average.
- For each iteration, compare the probe, target, and irrelevant waveforms according to the following algorithm: (a) subtract the grand mean of all trials, or grand average waveform, from each of the 3 averages, yielding 3 adjusted averages; (b) compute the correlation between the adjusted probe average and the adjusted irrelevant average; (c) compute the correlation between the adjusted probe average and the adjusted target average; (d) compare the probe-irrelevant correlation with the probe-target correlation: if the probe-irrelevant correlation is greater, then increment the “information present” tally by one; otherwise, increment the “information absent” tally by one.
- Compute the percentage of times that the probe—target correlation is higher than the probe—irrelevant correlation. This the percentage of times that the probe waveform is more similar to the target waveform than to the irrelevant waveform. This provides the probability or statistical confidence for an “information present” result. 100% minus this figure the provides the probability that the probe response is more similar to the irrelevant response, which provides the statistical confidence that for an “information absent” result.
Compare the computed statistical confidence to a decision criterion. If the statistical confidence for an “information present” result is greater than 90%, classify subject as information present. If the statistical confidence for an information absent response is greater than 70%, classify the subject as information absent. If neither criterion is met, no determination is made: the subject is not classified as either information present or information absent; this is an “indeterminate” outcome.

In other words, if the bootstrapping procedure produces a high statistical confidence that the probe response is more similar to the target response than to the irrelevant response, then the determination is “information present.” If the bootstrapping procedure produces a high statistical confidence that the probe response is more similar to the irrelevant response, then the determination is “information absent.”

If neither the statistical confidence for “information present” nor the confidence for “information absent” is high enough to meet established criteria, the subject is not classified in either category, and the result is “indeterminate.” Typically a confidence of 90% is required for an “information present” determination. A lower criterion, typically 70%, is generally required for an “information absent” determination.

The outcome of brain fingerprinting data analysis consists of two determinations, each of the form “information present/absent, x% confidence,” e.g., “information present, 99.9% confidence.” One determination is computed using the full P300-MERMER, and one using the P300 alone. This allows us to report one result with the method that applies the most well established science and is most certain to meet the standard of general acceptance in the scientific community, and one with the method that applies the state of the art and generally produces the highest statistical confidence.

By computing bootstrapped correlation as described above, the brain fingerprinting data analysis algorithm takes into account the amplitude, latency, and morphology (shape and time course) of the brain response. This maximizes the information extracted from the data and also controls for individual differences in brain responses from different subjects.

III. ADVANTAGES AND DISADVANTAGES

Brain Fingerprinting is a powerful and proven forensic tool that can permanently change the way suspects are convicted or freed.

A. Advantages

- Fast and cost-effective way to determine the truth: The principle is simple. It has been proven that memory centers of the human brain respond to the sight of familiar stimuli with a distinct change in electrical activity. The brain waves cannot lie. As a result, brain fingerprinting is fundamentally different from polygraphs; it depends only on brain information processing, not the emotional response of the subject.

- Identifies the guilty exonerates the innocent: Just as science matches fingerprints from the crime scene with a suspect’s own fingerprints, and DNA matches biological samples from the crime with the suspect’s own DNA, Brain Fingerprinting matches information from the crime scene with information stored in the subject’s brain repository.

- Highly scientific: The accuracy of Brain Fingerprinting lies in its technological ability to pick up the brain’s electrical signal – known as a p300 wave – before the suspect has time to influence the output. This split-second bump in electrical activity – that stars anywhere from 300 milliseconds to 800 milliseconds after a recognized stimulus – is a scientifically advanced way to detect concealed language.

- Virtually eliminates deception: Many seasoned criminals have discovered ways to beat a polygraph. Deception is much more difficult with Brain Fingerprinting. When the subject recognizes the stimuli, an involuntary MERMER (brain wave response) occurs. It’s about as foolproof as it gets.

- Far more accurate than a polygraph: The polygraph determines a person’s level of deception by measuring galvanic skin response, respiration, heart rate and blood pressure. Brain Fingerprinting depends only on information processing. It eliminates the subject’s often-unreliable emotional response.

B. Limitations

- Brain fingerprinting does not detect how that information got there. This fact has implications for how and when the technique can be applied. In a case where a suspect claims not to have been at the crime scene and has no legitimate reason for knowing the details of the crime and investigators have information that has not been released to the public, brain fingerprinting can determine objectively whether or not the subject possesses that information. In such a case, brain fingerprinting could provide useful evidence. If, however, the suspect knows everything that the investigators know about the crime for some legitimate reason, then the test cannot be applied. There are several circumstances in which this may be the case.

- If a suspect acknowledges being at the scene of the crime, but claims to be a witness and not a perpetrator, then the fact that he knows details about the crime would not be incriminating. There would be no reason to conduct a test, because the resulting “information present” response would simply show that the suspect knew the details about the crime – knowledge which he already admits and which he gained at the crime scene whether he was a witness or a perpetrator.

- Another case where brain fingerprinting is not applicable would be one wherein a suspect and an alleged victim – say, of an alleged sexual assault – agree on the details of what was said and done, but disagree on the intent of the parties. 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.
In a case where the suspect knows everything that the investigators know because he has been exposed to all available information in a previous trial, there is no available information with which to construct probe stimuli, so a test cannot be conducted. Even in a case where the suspect knows many of the details about the crime, however, it is sometimes possible to discover salient information that the perpetrator must have encountered in the course of committing the crime, but the suspect claims not to know and would not know if he were innocent.

The argument that brain fingerprinting evidence should not be admitted or considered due to the limitations of human memory is without merit in any forum that admits witness testimony of any kind. Witness testimony constitutes a subjective report of the contents of memory. Brain fingerprinting constitutes objective, scientific evidence of the contents of memory. In any forum where subjective reports of the contents of memory are considered, objective evidence of the contents of human memory warrant at least the same treatment. For brain fingerprinting, witness testimony, and confessions, the well-known limitations of human memory go to the weight of the evidence, not to admissibility or applicability.

IV. APPLICATIONS

In the United States and many other jurisdictions, the error rate of a scientific technique is critical for admissibility as scientific evidence in court. The error rate is the percentage of determinations made that are either false negatives or false positives. In brain fingerprinting, this is the percentage of “information present” and “information absent” determinations that are false positives and false negatives respectively.

In order to be viable for field use or any application with non-trivial consequences, a technique must have an error rate of less than 1% overall, and less than 5% in each and every individual study. Brain fingerprinting exceeds this standard. In all laboratory and field research and field applications to date, brain fingerprinting has had an error rate of less than 1%. In each individual study, brain fingerprinting has also had an error rate of less than 1%. In fact, to date brain fingerprinting has never produced an error, neither a false positive nor a false negative, in any research or field applications.

A. National Security

Brain Fingerprinting protects the interests of a nation through the power of brainwaves. In today’s volatile world, countries must be prepared to defend their interests and protect their people. With the use of Brain Fingerprinting technology, nations can detect concealed information stored within the brains of wanted criminals and terrorists. Since the terrorist attacks on the US in 2001, the ways that nations protect their people and border have changed. With national security spending at an all time high, the focus has turned to emerging technologies. Brain Fingerprinting offers a unique and nearly flawless technology that nations can leverage to defend their people.

Brain Fingerprinting offers countries the chance to see inside the minds of criminals, foreign or domestic terrorists, and any other person who poses a threat to national security. Imagine being able to tell if a suspect has knowledge of terrorist activities without a lengthy and costly investigation. Brain Fingerprinting shows whether information is present in the brain with instantaneous and accurate results. Brain Fingerprinting embraces one commonsense premise: even if there is no external evidence left behind, the brain is an infallible witness to the plotting of a crime. Put another way, the terrorist’s brain contains knowledge of organizations, training and plans that do not exist in an innocent person’s memory bank. Brain Fingerprinting provides investigators With a whole new state-of-the-art weapon to fight terrorism. Measuring the brain’s response to stimuli has been proven to be over 99 percent accurate in detecting EOD/IED bomb knowledge, uncovering high intelligence value individuals, and establishing links between a suspect and known terrorist networks, places and events. Brain Fingerprinting has been proven to:

- Aid in determining who has participated in terrorist’s acts, directly or indirectly.
- Support investigators in identifying potential trained terrorists, even if they are in a “sleeper” cell and have not been active in years.
- Help to pinpoint those who maintain a leadership role within a terrorist organization.
- Improve security in areas like protecting classified information and evaluating immigrant visa applications.
- Validate the possible links from database analysis techniques.

Brain Fingerprinting may well be the breakthrough that investigators have hoped for, enabling them to determine who is involved with terrorist activity with a nearly infallible degree of accuracy.

B. Law Enforcement

The irreplaceable Brain Fingerprinting technology puts criminals behind bars while exonerating innocents. Brain Fingerprinting is an innovative science that many law enforcement and intelligence agencies are seeking to add to their arsenal of investigative tools. The objective of law enforcement is to seek out the correct perpetrator and see that they are punished for the crime they have committed. Once a suspect is in custody, Brain Fingerprinting can accurately establish whether or not the suspect has knowledge of the crime. This saves time and money on investigations, while keeping dangerous criminals off of the streets. Conventional fingerprinting and DNA testing match physical evidence from a crime scene with evidence found on the perpetrator. While these are tested and accepted methods, they are only available in roughly 1% of crimes. It is estimated that Brain Fingerprinting would be applicable in 60%-70% of these same cases, thus having the potential to make a profound effect on the criminal justice system. The advantages to Brain Fingerprinting are that it offers higher accuracy than other techniques, is non-invasive and has been ruled admissible in the US court.
Scanning the brain to determine guilt or innocence: Before the invention of Brain Fingerprinting, an individual could get away with a crime if he could accomplish two things: make sure that there was no physical evidence, and make sure that he was the only one who knew about the crime (or silence anyone else who knew, through bribery, coercion, intimidation, or murder).

The perpetrators of all kinds of crime know who they are, and they know what they have done. Now that Brain Fingerprinting is available, whenever the investigators know the salient facts about the crime, and the perpetrator, having committed the crime, knows these same facts as well, Brain Fingerprinting can be used to detect this knowledge stored in the brain of the perpetrator. Even when the perpetrator avoids physical evidence and makes certain that no one else knows of his crime, since he himself knows, the investigators can also know of his participation. No longer can any perpetrator plan a crime with any degree of certainty that he can avoid detection and avoid being brought to justice.

Now there’s a new way to help determine truth and justice. Brain Fingerprinting is a scientiffic computer-based technology for determining whether relevant information is stored in the brain through the measurement brain waves.

It has been proven 99% accurate in over 200 tests, including actual criminal cases, tests on FBI agents and tests on military medical experts. Investigators can identify or exonerate suspects based upon measuring brain-wave responses to crime-related photos or words displayed on a computer screen.

C. Counter-Terrorism

An innovative tool that saves lives by reducing the threat of terrorist activity and attacks. The greatest challenge in global security is it's not simply developing new ways to fight terrorism; rather, it's quickly identifying who the terrorists really are. In today's times, terrorists and their accomplices are very likely hiding in full sight among us. And they aim to keep it that way.

Now there's an infallible witness to these crimes even when fingerprints or DNA are not available. Brain Fingerprinting empowers investigators to accurately measure if specific information is hidden within a suspect's brain. With the innovative Brain Fingerprinting technology, counter terrorism officials will be able to scientifically test suspected terrorists to indict or exonerate them based on the information stored within their brain. Brain Fingerprinting can easily detect terrorist knowledge and threats—even being able to detect if a suspect has been in a sleeper cell. This can be accomplished by searching for knowledge of bomb and IED making and terrorist trainings.

In counter-terrorism, there is no comparable technology available that can help catch terrorists throughout the world. Brain Fingerprinting can identify active or inactive terrorists before and after any terrorist act happens. This innovative science aims to save lives and protect countries through its patented technology.

Brain fingerprinting test can detect:
- Knowledge characteristic of bomb makers / IED experts.
- Knowledge of specific terrorist training.
- Knowledge of terrorist financing procedures, methods, and events.
- Knowledge of particular known terrorists.
- Familiarity with the inside workings of a specific terrorist cell.
- Knowledge of terrorist codes, procedures, and locations.
- Knowledge of biological weapons.
- Knowledge of nuclear weapons.
- Knowledge of known terrorists.
- Inside knowledge of organized crime organizations.
- Affiliation with known organized crime figures.

D. Border Security

Border Security priorities have long been regarded as one of the highest challenges for national and global security. Combating transnational criminal organizations that traffic in drugs, weapons, and money, and that smuggle people across the borders has always been a test for law enforcement agencies in charge of securing nation’s borders.

As long as investigators know what they are looking for, Brain Fingerprinting can detect any kind of security-related knowledge, and in fact any kind of information stored in the brain. This can be used to identify individuals who are involved in crime or terrorism. Brain Fingerprinting can help investigators crack down on criminal networks engaging in passport and visa fraud and human smuggling. Protecting the nation’s borders—land, air, and sea—from the illegal entry of people, weapons, drugs, and contraband is vital to our homeland security, as well as economic prosperity of any country and Brain Fingerprinting can help secure and manage borders.

E. Human Trafficking

Brain Fingerprinting can detect information regarding the specific people, places, and actions involved in sexual exploitation and forced labor. The technology can detect those directly involved and in large scale operations also the planners and the leaders of the criminal organizations involved.

Brain Fingerprinting specific issue tests can also be applied in human trafficking. An individual suspected of being involved in a human trafficking ring could be tested for recognition of a series of known victims, known associates, places involved, transportation methods, financial transactions, etc., even without detailed information being available about any one specific event. The only prerequisite for applying Brain Fingerprinting is that the investigators know what information they are looking for.
F. Immigration

An immigration control system is central to any nation’s security policy. Recent events in the world shine light on the fact that in a very real sense, the primary weapons of terrorists are not the inanimate objects at all but, rather, the terrorists themselves, especially in the case of suicide attackers.

**Identifying persons with connections to known criminal or terrorist organizations:** Brain Fingerprinting has proven over 99% accurate in detecting knowledge characteristic of FBI agents, US Navy military medical experts, and bomb makers (IED/EOD experts). Similarly, individuals who are involved in criminal or terrorist organizations have specific inside knowledge that is not known to the public. Brain Fingerprinting can detect this information stored in the brains of those involved in the criminal and terrorist organizations.

**Identifying perpetrators of illegal schemes to provide entry into the country for profit:** Illegal schemes to provide entry to the country for profit involve considerable detail of plans regarding how to recruit customers surreptitiously, how to transport them, and how to avoid detection. Those involved in planning and perpetrating these schemes possess specific knowledge that is unknown to others. Brain Fingerprinting can detect this knowledge.

V. CONCLUSION

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 fulfills an urgent need for governments, law enforcement agencies, corporations, investigators, crime victims, and falsely accused, innocent suspects.

VI. FUTURE ENHANCEMENT

In the years since Dr. Farwell first began applying the technology in the real world, proponents. Critics, including some scientists, and those whose criminal activities have been thwarted by brain fingerprinting have advocated further delay in applying the technique. Farwell and colleagues as well as other, independent scientists who have precisely replicated Farwell’s research or used similar methods, have obtained accuracy rates approaching 100% in both laboratory and field conditions. Proponents of the continued use of brain fingerprinting in criminal and counterterrorism cases cite the peer-reviewed research on the accuracy of brain fingerprinting in the laboratory and the field, the fact that it has been ruled admissible in court, the vital counterterrorism applications, and the benefits of bringing criminals such as serial killer to justice and freeing innocent convicts.

REFERENCES
[5] research.omicsgroup.org