



Study on Advancing Cognitive Neuroscience: Brain Fingerprinting for Enhanced Neurological Research

Rishita sri kotapati

Department of Computer Science and Engineering , Alliance University Bangalore
rishitakotapati@gmail.com

Abstract

Brain fingerprinting is an advanced technique for positively and scientifically identifying criminals by analysing brain wave reactions to crime-related words or images displayed on a computer screen. The theory behind brain fingerprinting technology is that when people experience certain events, their brains generate unique brain wave patterns [10]. P300MERMER EEG event-related potential elicited by stimuli relevant to the current situation [14]. P300-MARMER answers to terms or visuals related to crime scene, terrorist instruction, bomb making experience, etc. Determined by BF. BF's cognitive information processing was assessed for data identification [5]. There is no lie, tension or emotion that BF can reveal. The level of statistical confidence is determined by BF if there is data or the lack of it for each individual opinion. There are no false positives or negatives in laboratory or field tests conducted by the FBI, CIA, US Navy and other agencies. All the results obtained were even correct. Only 3% of findings are considered "indeterminate". The use of BF has been authorized in criminal proceedings. The new method uses brain waves to determine whether a test taker can recall the specifics of an event. Even if the subject deliberately withholds the necessary information, the brain wave transmitter will pick it up.

Keywords: P300-MERMER, EEG, perpetrator, brain wave patterns, cognitive, indeterminate, data identification

1. Introduction

Finding the truth is an ongoing struggle in criminal justice, security, and intelligence research. The main purpose of investigations and inquiries is to detect deception [4], distinguish between truth and falsehood, and reveal hidden facts. The polygraph test is an example of a traditional approach that has been used but has limitations and is controversial. The development of brain fingerprinting creates curiosity and optimism in the search for more reliable and accurate methods [3]. EEG brain responses, or brain waves, are continuously monitored by head-mounted sensors in a process called "brain fingerprinting," [13] an unbiased scientific way to uncover information hidden in the brain. It involves the presentation of words, sentences, or pictures containing important facts about crime or other issues on a computer screen [7], followed by a series of unrelated stimuli. We measure how stimuli affect the brain. By computer analysis of brain responses, certain brain wave patterns can be identified when the brain is processed in certain ways. A brain wave pattern called P300-MARBLE best describes this reaction by analyzing the subject's brain wave response, we can find out whether the subject has retained the specific material being evaluated. This method is claimed to be more effective than the lie detector test. Dr. Lawrence Farwell, who developed the method, says it is 99.99% accurate. It only takes ten minutes to complete this test. The most important changes that occur in criminals and witnesses cannot be directly observed by the trial method. In fact, both the perpetrators and the witnesses to the crime are aware of their involvement. They usually have a complete understanding of what is happening and who is involved, apart from the trivial facts. More detailed information on this matter can be found in the recording of the perpetrator and the witness recalling certain aspects of the crime scene and certain characteristics of the perpetrator [19]. Investigators can only use this tactic if they have sufficient, specific knowledge of an incident or case that will be known to them and the perpetrator.



2. Methodology

A sequence of words, sounds, or images, each presented briefly by the computer [8]; The process is similar to the knowledge test. Subjects categorized each of these stimuli as “Target,” “Irrelevant,” or “Evaluation.” The brain's primary response to meaningful information for the subject is determined by using Target stimuli selected as relevant information. Pressing one button will activate the Objective, pressing another button will activate the remaining 80 triggers. Most of the nontarget stimuli are irrelevant, that is, they are unrelated to the condition being tested. Irrelevant stimuli provide the brain's primary response to information that is irrelevant to humans in this context because they do not generate marbles. Part of the non-target question refers to the scenario in which the person is being assessed. This stimulus, called investigation [9], is related to the test and related to the topic. It will also produce marbles indicating that the subject has recognized the significance of the stimulus. If the participant's brain does not have this knowledge, they will not be able to tell the difference between an unrelated stimulus and a probe stimulus. This shows that they are unaware of the information as marble is not available in response. It should be noted that no emotional response is required for this test; rather, it only depends on the subject's ability to recognize stimuli and the difference in recognition, hence the Oddball effect.

3. Literature review

The Four Steps of Brain Fingerprinting When fingerprints or DNA fingerprints are used, the evidence is detected, collected, and properly stored before a suspect's arrest is scientifically compared to determine whether there is a reasonable match with the suspect's personal record [15]. A similar procedure applies to brain fingerprinting, where data instead of physical evidence is collected from the suspect's body at the crime scene (i.e., electrical brain reactions). Similar to fingerprinting and DNA fingerprinting procedures, brain fingerprinting is a four-step process.

1. Collect Braille fingerprint collision evidence
2. Collect internal evidence
3. Collect and analyze computer evidence and
4. Scientific results of brain fingerprinting.

When evidence is collected from the crime scene, brain fingerprint experts examine the scene and related materials to find information about the crime that only criminals know about.

Experts then collect evidence from the suspect's brain to determine if it matches evidence at the crime scene. This process is known as brain evidence collection [12]. In computer evidence analysis, the brain fingerprint method calculates the statistical confidence in the mathematical conclusion that this particular piece of evidence is stored in the brain. A brain fingerprint result of "data present" (i.e., "incorrect") or "no information" (i.e., "innocent") is determined with statistical confidence.

4. Results and Discussion

Dr. Farwell testified in the trial on November 14 and is subject to probation based on his test results.

In addition, Dr. Two other psychophysicologists with EEG expertise, William Iacono from the University of Minnesota and Emanuel Donchin from the University of Illinois, testified about Dr. Farwell's expertise, test results, and the basis of brain fingerprinting. At Harrington's request, Iacono



testified with the state named Donchin. Both experts recognize Dr. Farwell's beliefs and support the science of brain fingerprinting. Donchin said that the choice of the examiner and the presentation of the special test represent the beginning of art and the end of science during the research to build a brain fingerprint test, because it shows the main characteristics of the crime that is used as a stimulus. from research. Iacono, on the other hand, asserts the scientific case for P300 based on his own experience. The experience and judgment of the criminal investigator will determine this. Brain fingerprinting is a scientific field that determines how a person's brain responds to probes, producing objective results such as "information present" or "information absent." It has nothing to do with the results of the subjective evaluation of the scientist conducting the test. Test results are sent to fact finders to help determine whether or not they are wrong. Brain fingerprinting scientists interpret whether a suspect's brain contains crime-related information found during the investigation, the suspect's guilt or innocence, or whether the suspect actually committed the crime.

4.1 Results of Terry Harrington's Brain Fingerprinting Test

US homicide brain fingerprinting results "no data" with 99.9% statistical confidence. Harrington's crime-scene-and-murder scenario doesn't match the knowledge stored in his brain. The details in [22] Harrington's memory fit the theory that he was elsewhere (at a concert with his friends) when the crime was committed.

5. Applications

5.1.Criminal Justice

Prosecution is an important responsibility of the criminal justice system [20]. The memory of an innocent suspect of crime is not in his mind, but a criminal is. The main difference between innocent suspects and criminal participants is this. Before the invention of the BF test, this important difference could not be determined by a reliable scientific approach. No guilt or innocence can be established by brain fingerprinting. Judges and juries play such a role. Using this innovative technology, judges and juries can reach conclusions with the help of new, scientifically based evidence. On August 5, 1999, Dr. Lawrence Farwell performed brain imaging tests on murder suspect J.B. Grinder. The purpose of this study was to determine whether Grinder's brain contained memories related to the rape and death of Julie Helton. While working as a scientist in the FBI laboratory, crime investigator Drew Richardson developed a research stimulus. According to the results of the brain fingerprinting test, Grinder's brain contains information about the characteristics of the crime stored there. The available data resulted in a statistical confidence level of 99.9%.

5.2.Counter terrorism

It helps identify people who directly or indirectly support terrorism. This helps in finding trained terrorists who are "sleeping" and may not be active for a long time but can do more terrorist attacks. Assistance in identifying individuals with experience or training in the banking, financial, or communications industries associated with terrorist organizations and activities. Find out if anyone is acting as a leader in a terrorist group. Terrorist acts may or may not contain evidence such as DNA or fingerprints, but the criminal's mind is always active when the crime is being planned, executed and recorded. Terrorists ask for information about groups, training and plans that innocent people do not. Before brain fingerprinting experiments began, there was no objective way to determine this important difference. Using brain fingerprinting, [18] Dr. Farwell and FBI scientist Drew Richardson, former head of the bureau's chemical, biological, and nuclear counterterrorism division,



have shown that test subjects can be identified from a specific group by identifying specific knowledge known only to their members. this group in research with the FBI (Farwell, 1993; Farwell & Richardson, 2006b). A group of 17 FBI agents and 4 non-agents viewed stimuli (words, phrases, and acronyms) on a computer screen. The search prompt contains information that only a person with FBI experience would find common knowledge. Brain fingerprinting has successfully separated FBI agents from non-agents. Improve the ability to quickly and reliably identify terrorists and supporters of terrorism. No longer should terrorists be allowed to escape justice due to lack of evidence. There is no reason for innocent people to be arrested or convicted of terrorism.

5.3. Medical

A patented technique called "brain fingerprinting" allows for the first objective measurement of the drug's effects on the memory and cognitive function of Alzheimer's patients [1]. First-generation tests are more accurate than commonly used tests and may be on the market in 18-25 months. During the 30-minute test, the patient wears a headband with integrated electrodes. Next, the technician asks the patient to identify words, phrases, and pictures in familiar and new contexts [2]. This allows the technician to scan the patient's brain for any remaining information. When the brain encounters familiar information, a special increase in the activity of cells called MERMERS is created. Technicians can use this reaction to measure how fast the brain is firing and see if there are drugs that slow it down [17].

5.4. Other Applications

Brain fingerprinting labs will make significant improvements in advertising metrics and campaign effectiveness. Focus groups are now used for subjective evaluation of most advertising campaigns. We can offer more sophisticated scientific methods to evaluate the success of campaigns and be cheaper than existing methods [11]. This technology will allow us to find out what people store in their memories. Brain fingerprinting labs can help the insurance industry reduce the prevalence of insurance fraud [6] by assessing whether people are aware of fraud or other bad behaviour. In computer crimes where there are no witnesses or physical evidence, the same test can help determine whether a person has specific knowledge related to the crime.

6. Limitations of Brain Fingerprinting

In every crime, the brain of the offender is a significant factor. Criminals are practically always aware of their participation in the crime and often fully understand its elements. However, brain fingerprinting is not always suitable for every person or case. Details that criminal investigators believe the perpetrator encountered during the crime must be part of the investigation. The investigation must include information that the suspect claims not to know. As a result, there are situations where it is not possible to compile an investigation of a specific crime involving a specific person. It is evident that a brain fingerprint test is not possible under these conditions. For example, when someone inexplicably disappears and foul play is suspected, the police are unable to identify the manner in which the crime was committed and cannot plan an investigation. Cannot be tested for brain fingerprinting. A person may claim to have been at the crime scene as a witness rather than as an accomplice. In such a scenario, there would be no information that the individual would say they did not know. As a result, a brain fingerprint test could not be arranged and there could be no probes. Brain fingerprinting is a technique that detects the brain's information-processing responses and can be used to identify the types of information stored in an individual's brain. Regardless of whether the



information came from a witness or a perpetrator, it is impossible to determine how it got there. Brain fingerprinting only finds information; misses the point. Knowledge of the suspect's undeniable facts does not indicate that either side's view of the other's motivations is correct. Brain fingerprints cannot detect fraud. It only recognizes information. No questions or answers are asked during a brain imaging scan. Whether or not the participant ever lied or told the truth has no bearing on the results of the brain fingerprinting test. It is not what someone says that affects whether something is considered "present" or "absent", but rather the information that is stored in the brain. Like other forensic science methods, brain fingerprinting [21] relies on an evidence-gathering procedure that is beyond the scope of science to produce data that can be used in scientific testing. DNA testing only assesses whether two DNA samples are the same, it does not determine whether the investigator has successfully extracted DNA from the murder scene. In a similar vein, the brain fingerprint test is only regardless of whether the data stored in the suspect's brain matches the data in the probe stimuli

7. Conclusion

In more than 200 experiments by Farwell and colleagues, brain imaging produced no false positives or false negatives. [16] The results drawn have zero percent error rate and 100% accuracy rate. Decisions are made about "data available" and "data not available" and statistical confidence levels are added to each result. Because P300-MERMER is included in the data analysis procedure, there is no meaning. P300 was the only device used in 3% of cases before P300MERMER was developed. In this case, the data analysis algorithm shows that there is not enough information for both sides to make a decision with high statistical confidence. No result; The result is "undetermined". Acceptance of the brain fingerprinting law is still being proven. However, the following well-established characteristics of BF will be important when the issue of admissibility is discussed in court.

Brain imaging has undergone extensive and rigorous testing. The hypothesis behind brain fingerprinting has been published and peer reviewed. The error rate is very low, almost non-existent, and the technology that has been developed and published has precise guidelines that govern the method of scientific work. The idea and application of brain fingerprinting has received wide attention in the relevant scientific community. One of the metaphorical non-proof methods is brain fingerprinting. Tests that use brain fingerprinting to diagnose certain problems can reveal details about specific events, such as terrorist attacks or crimes in specific locations. Special tests for brain fingerprints can reveal some kind of knowledge or skills, such as specific details for FBI agents, bomb makers, or Al-Qaeda-trained terrorists. Brain imaging is not suitable for extensive testing when the investigator does not understand the information sought. Brain imaging has been allowed to be used as scientific evidence in court and has been successfully used in clinical settings. It is effectively used today when studied by American scientists.

8. Acknowledgements

I extend my deepest gratitude to all those who played a crucial role in the successful completion of this project. Special thanks to my professor Dr . Geetha A ,whose unwavering guidance and expertise shaped the direction of this work. Their insightful feedback and continuous support were invaluable throughout the entire process.

References



- [1] Safa Silath and Lipsa Sadath, “Behavioural Biometrics in Feature Profiles-Engineering Healthcare and Rehabilitation Systems”, Journal of International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), (2021).
- [2] Lucio Amelio and Alessia Amelio , “Classification Methods in Image Analysis with a Special Focus on Medical Analytics” , Part of the Intelligent Systems Reference Library book series (ISRL ,volume 149), (2018), pp : 31-69.
- [3] Ikram Ud Din and Ahmad Almogren, “NeuroTrust—Artificial-Neural-Network-Based Intelligent Trust Management Mechanism for Large-Scale Internet of Medical Things”, IEEE internet of things journal, Volume: 8, Issue: 21.
- [4] Douglas Cirqueira, Markus Helfret, “Scenario-Based Requirements Elicitation for User-Centric Explainable AI”, International Cross-Domain Conference for Machine Learning and Knowledge Extraction ,(2020).
- [5] Roman V Yampolskiy, “Behavioral, Cognitive and Virtual Biometrics”, Computer analysis of human behavior pp 347-385, (2011).
- [6] Wanting Ji and Ruili Wang, “Computational Intelligence for Information Security: A Survey”, IEEE Transactions on Emerging Topics in Computational Intelligence, (2020).
- [7] Ajith Abraham and Vaida luksaite, “A Review of AI Cloud and Edge Sensors, Methods, and Applications for the Recognition of Emotional, Affective and Physiological States”, (2022).
- [8] R Sheela and R Suchitra, “Unmasking the Masked: Face Recognition and Its Challenges Using the Periocular Region – A Review”, IGI Global, (2022).
- [9] S Bansal and M Agarwal, “Security Designs for the Cloud, Iot, and Social Networking”, Wiley, (2019).
- [10] Lawrence A. Farwell, “Brain fingerprinting: a comprehensive tutorial review of detection of concealed information with event-related brain potentials”, NCBI, (2012).
- [11] Mohammad S Obaidat, “State of the art and perspectives on traditional and emerging biometrics: A survey”, Wiley, (2018).
- [12] Shulan Lu and Derek Harter, “Towards Collaborative and Intelligent Learning Environments Based on Eye Tracking Data and Learning Analytics: A Survey”, IEEE, (2021).
- [13] Arif I Sarwat and Alexander Pons, “A Survey on Modality Characteristics, Performance Evaluation Metrics, and Security for Traditional and Wearable Biometric Systems”, ACM, (2019).
- [14] Hosang Kolivand and Fares, “A robust brain pattern for brain-based authentication methods using deep breath”, computers and security, (2023).
- [15] Cogn Neurodyn,” Brain fingerprinting: a comprehensive tutorial review of detection of concealed information with event-related brain potentials”, National library of medicine, (2012).
- [16] J. Peter Rosenfeld, “Brain fingerprinting: A critical analysis”, Research gate, (2005).
- [17] Zack Shan, “Brain fingerprinting: A promising future application for predicting mental illness”, ScienceDirect, (2023).
- [18] Amit Joshi and Prashanth Kumar, “Brain Fingerprinting: The New Era of Truth and Lie Detection”, SSRN, (2023).
- [19] Bibin Abraham and S.L Vaya, “BRAIN FINGERPRINTING TECHNOLOGY: A UNIQUE TECHNIQUE THAT DETECT THE CULPRIT”, worldwide journals, (2023).
- [20] Mancy Thomas, “Brain Fingerprinting: An Overview”, Ijert, (2015).
- [21] Walter Zhao and Tipparedy, “Magnetic resonance fingerprinting: an overview”, Springer, (2021).
- [22] Rosenfeld,” Brain fingerprinting: a critical analysis”, Semantic scholar, (2005).