Journal of Ubiquitous Computing and Communication Technologies (ISSN: 2582-337X)
www.irojournals.com/jucct/

A Study on Brain Fingerprinting Technology

S. Deepika[1], B. Kaviyadharshini[2], S. Sharmila[3], S. N. Sangeethaa[4], S. Jothimani[5]

[1-3]UG Scholar, Department of Computer Science and Engineering, Bannari Amman Institute of Technology, Erode, India
[4,5]Assistant Professor, Department of Computer Science and Engineering, Bannari Amman Institute of Technology, Erode, India

E-mail: [1]deepika.cs20@bitsathy.ac.in, [2]kaviyadharshini.cs20@bitsathy.ac.in, [3]sharmila.cs20@bitsathy.ac.in, [4]sangeethaasn @bitsathy.ac.in, [5]jothimanis@bitsathy.ac.in

Abstract

The detection and resolution of any crime is made possible with the use of modern technology. The crime is discovered, the suspect is named, and then the court is presented with sufficient proof to show that the crime was committed by the named suspect. The proofs could be mental or physical. The best lie detector now in existence, according to this invention, is reported to be able to catch even sneaky crooks who successfully pass the standard polygraph test. Criminal investigators gather physical evidence, which can be destroyed, while mental evidence is preserved in the brain and cannot be erased. The brain wave reaction of an individual to crime-related images or phrases displayed on a computer screen can be used to analyze those evidences, using Electroencephalography (EEG). This novel Brain Fingerprinting technique uses brainwaves, which can be used to determine if the test participant remembers the specifics of the incident. The brain wave issuer will trap him even if they are consciously hiding the required information. Over 120 studies, including testing on Federal agents, testing for the United States intelligence agency and the US Navy, tests on actual cases, including felony crimes, have demonstrated that brain fingerprinting is 100 percent accurate.

Keywords: Brain fingerprint technology, electroencephalography (EEG), crime, brain wave response

1. Introduction

A novel computer-based technique called "Brain fingerprinting," also known as "Brain Electrical Oscillation Signature Profiling" (BEOSP), is used to identify a criminal by

DOI: https://doi.org/10.36548/jucct.2022.3.001
Received: 05.07.2022, received in revised form: 30.07.2022, accepted: 14.08.2022, published: 24.08.2022

observing their brain's response to images or words associated with the crime [1]. This cutting-edge technique is used to solve crimes, identify juvenile offenders, and prove a criminal's innocence with 100% accuracy. Dr. Lawrence A. Farwell created this technology in 1995.As of August 21, 2004, the word "100% accurate" on Farwell's websites suggested that the method has flawless accuracy [3]. In peer-reviewed articles, Farwell and co-workers claimed that their laboratory studies (Farwell and Donchin, 1991; Farwell and Richardson, 2006b) and field applications (Farwell and Smith, 2001; Farwell and Richardson, 2006a) have above 99 percent accuracy [2]. William Iacono and others who used the same or related scientific procedures have reported a similarly high level of accuracy in independent study. Figure 1 shows the model of Brain Fingerprinting Technology.

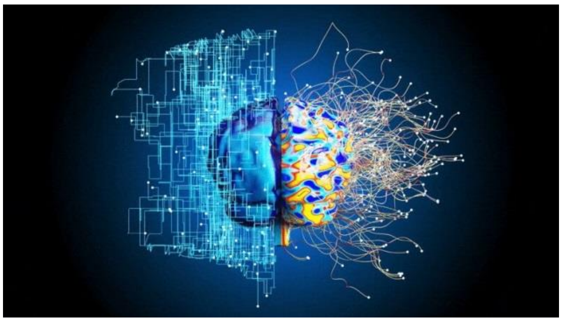

Figure 1. Brain fingerprinting technology

In a court case in 1999, Farwell applied this strategy to establish the innocence of a suspect. He showed each participant a photo of the crime site and then analysed their brain waves to discover who had previously witnessed the event. He persuaded the judge to grant the convicted person's parole by arguing that the test was 99.99 percent accurate [4]. The technique is used in circumstances when investigators have access to enough particular information about an incident or behaviour, that would be known only to the culprit and investigator.

This makes brain fingerprinting a form of guilty knowledge test, where the "guilty" participant is anticipated to have strong emotional responses to the pertinent information about the incident or activity. While the current (polygraph) methods determines whether a suspect is guilty by measuring autonomic arousal (such as heart rate and palm perspiration), brain fingerprinting uses a fitted headband with specialised sensors to capture electrical brain activity[2]. The claim that brain fingerprinting is more effective than traditional polygraph methods in identifying "guilty" knowledge is widely contested by experts and has drawn criticism on a number of fronts.

2. Brain Fingerprinting

In a criminal case, evidences gathered through investigations are used to pinpoint the specifics of the crime that a perpetrator would have to have come across during the commission of the crime and that the brain records and remembers. In a typical crime scene investigation, some crime details are unimportant, but they become crucial information in a brain fingerprinting test [5]. These consist of details that a criminal might recall doing or seeing while committing a crime, such as tipping over a pink flamingo on the lawn, rushing through long grass, the sort of weapon used, etc. Once a sizable number of memorable details are obtained, they are sorted into those that would be known to the public (via newspaper coverage, etc.) and those would only be known to the police investigators and the criminal. By using this data, the actual Brain Fingerprinting test, which consists of targets, probes, and unrelated stimuli can be created. In the process of measuring the brain wave patterns associated with visuals that are both important and irrelevant to the crime scene, brain fingerprinting technology shows relevant and irrelevant images. Figure 2 shows block diagram of Brain finger technology.

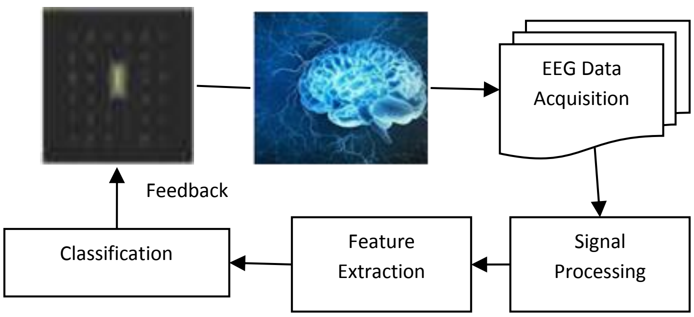

Figure 2. Architecture diagram of brain finger technology

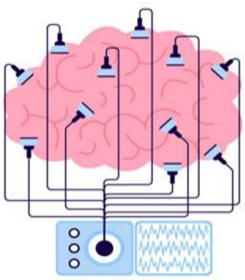

Figure 3. Digital EEP signal technique

The recollections are sparked by the pertinent imagery. This method is based on the discovery that when a person encounters a familiar environment, their brain produces a distinctive wave pattern. The features of a crime that are retained in a suspect's brain are described using Electroencephalography (EEG) [6]. The Memory and Encoding Related Multifaceted Electroencephalographic Response (MERMER) is a wavelike reaction that the brain extorts when it encounters something familiar [7]. Figure 3 shows an example of Digital electroencephalography signal technique. The P300 brain response is then contained in the MERMER. Figure 4 shows an element of ERP, or an Event Related Brain Potential, P300.

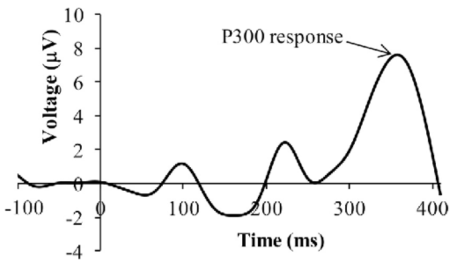

Figure 4. Graph for P300 response

A positive voltage that peaks 300ms after the occurrence of the consequential event is the P300 signal. It is sufficient to show that the person in question is aware of that specific occurrence by looking at the time domain plot of this P300 signal. The P300-MERMER signal is investigated to support the notion even more. A negative peak known as late negative potential follows the P300's positive peak [8]. P300-MERMER is the name of this pair of potentials combined. Despite having additional capabilities in addition to the straightforward time domain patterns, the P300 & P300 MERMER are not required for defining response.

3. Methodology

A series of words, sounds, or images are presented to the person taking the Guilty Knowledge Test via computer, one at a time for a limited amount of time. Each of these stimuli is labelled as a "Target," "Irrelevant," or "Probe" by the test-giver. The target stimuli are chosen to be significant information to the subject being evaluated in order to generate a baseline brain response. To react to targets, the subject must press one button, and to react to all other inputs, a different button. The bulk of non-target stimuli are irrelevant, that is, they have no bearing on the situation that the participant is testing. In this case, unrelated stimuli do not trigger a MERMER in order to create a baseline neural responses for data that is

ISSN: 2582-337X

unrelated to the patient. Figure 5 and Figure 6 shows the Parietal area and Frontal area responses.

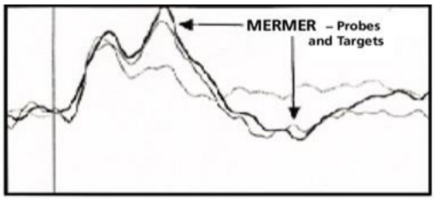

Figure 5. Parietal area response [3]

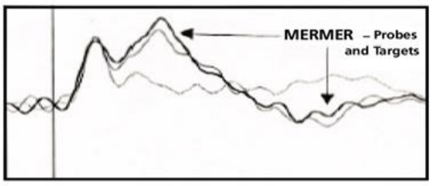

Figure 6. Frontal area response [3]

Some of the non-target is relevant to the situation the test subject is facing. These stimuli, sometimes referred to as Probes, are significant to the test subject and pertinent to the probes. They will trigger a MERMER response from the patient, showing that they have understood the meaning of the stimuli. In an individual whose brain lacks this knowledge, the response to the Probe stimulus will be the same as the response to the irrelevant stimulus. This response do not elicit a MERMER, indicating that the respondent was unable to recall the information. Due to the fact that the test only considers differences in recognition reactions to the stimuli, it is related to the Oddball effect [9]. It should be highlighted that no kind of emotional reaction to the stimulus is necessary.

Probe Stimuli: The probing test is used to determine whether a subject is knowledgeable about the problem being probed or not [10]. Thus, the investigations are always connected to the crime site. The probe's features are:

- 1st feature: Contains information about the crime learned by the perpetrator.
- 2nd feature: Contains information relevant to the crime scene but not known to the subject.
- 3rd feature: Contains information that the subject refuses to acknowledge

Irrelevant Stimuli: This stimulus presents accurate information that is credible. It compares the material from the investigation and determines if the subject has the necessary understanding of the offence [11]. Therefore, it may be determined whether or not the subject lacks the necessary information by comparing these two responses to irrelevant stimuli and probe stimuli.

Target Stimuli: It gives the probe stimulus and the reference signal waveform for comparison. Target stimuli includes information the subject is aware of, that is pertinent to the circumstance. Information that is revealed to the individual after the crime or other scenario under investigation is contained in the target stimuli [12].

4. Scientific Procedure

Each stimulus is displayed for a brief period of time. Typically, a picture is displayed for 1800 milliseconds whereas a word or phrase is displayed for a lesser time. Once the non-invasive electrodes are attached to the subject's scalp, a computer-controlled video monitor displays a series of words or images. To obtain the reference waveform, the patient is first presented the target and unrelated stimuli. The participant is then given probe stimuli, which causes the brain to produce a P300-MERMER response. As a result, the individual is exposed to numerous such stimuli, and the resulting data is subsequently analysed.

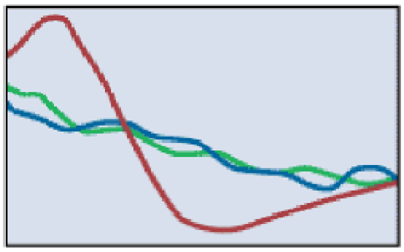

Figure 7. Not guilty [4]

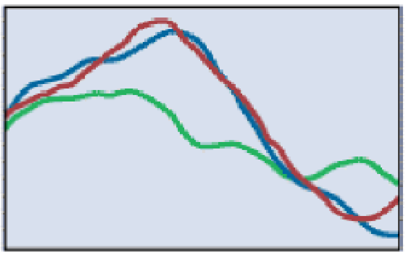

Figure 8. Guilty [4]

The probe, target, and irrelevant waveforms are compared for each iteration. Target stimuli have a red waveform, irrelevant stimuli have a green waveform, and probe stimuli have a blue waveform [4]. As seen in the figures 7 and 8, the blue line and green line are strongly associated whether the suspect is not guilty or if he lacks the necessary information. The probe and unrelated stimuli have a strong correlation that demonstrates the suspect's innocence. When the blue and red lines nearly coincide, this establishes a connection between the probe and target stimuli and the guilty status of the suspect.

The following guidelines determine whether the person is guilty or innocent:

Not Guilty: According to figure 7, a person is not guilty when the blue and green lines closely coincide.

Guilty: Based on the figure 8, guilt is present when the lines in blue and red are correlated.

5. Phases of Brain Fingerprint

The evidence gathered from the crime scene is maintained during DNA fingerprinting and compared to the evidence on the suspect. Similar principles govern the operation of brain fingerprint technology [12], but the evidence is informational rather than tangible.

The four stages of Farewell Brain Fingerprinting Technology are:

1. Collection of crime scene evidence via brain imaging
2. Using a brain print collection of brain evidence
3. Computer evidence analysis using brain fingerprinting
4. Scientific finding on brain fingerprinting.

Collection of crime scene evidence: It explains that the investigators go to the crime scene and gather evidence of the crime. For further research, terms relating to crime must be provided. When compared to many scientific studies, brain fingerprinting technology provides courts with highly useful evidence.

Collection of brain evidence: Checking to see if the evidence matches the suspects after submitting it for inquiry is helpful. EEG sensors are used in it [13]. It is an investigation of the conflict between evidence from the suspect's brain and information about the crime scene. If the information provided by the subject by the investigator does not match, then it is turned to fingerprint matching. If the fingerprint doesn't match and the individual was at the crime scene for some other reason, they will look into it for real.

Computer evidence analysis: Using complicated mathematics in the scheme and test of brain waves, it is possible to determine whether the suspect is guilty or not by looking at the results. The input is obtained in the form of probes from the preceding processes. With a combination of algebraic guarantees, the output determines if the information is present or absent for these probe stimuli.

Scientific Analysis: Brain wave patterns will determine whether the information is present based on the screen. Only scientific testing is what that leads to this conclusion. This method effectively separates informational evidence obtained from the scene of the crime and from the suspect from physical evidence. The specific information is based on the three coloured lines.

RED: The suspect is simply anticipated becoming aware of the facts surrounding the incident.

GREEN: The suspect is uninformed about the details of the crime.

BLUE: The suspect just has knowledge of the crime's details.

The following figures 9 and 10 define whether the information is obtained on the screen or not.

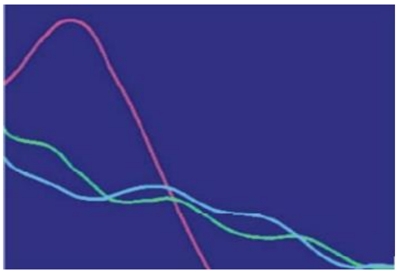

Figure 9. Information absent [4]

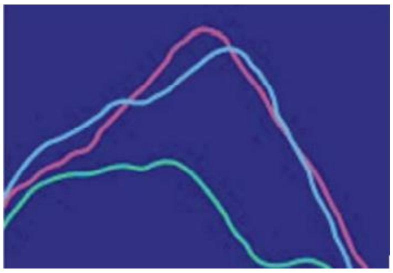

Figure 10. Information present [4]

6. MERMER Technology

MERMER technology involves the use of a customised headband that has extra electronic sensors (electrodes) and generates waveforms on the EEG. Typically, two different types of electrodes are used.

ISSN: 2582-337X

- Invasive: (electrodes are attached directly to the brain tissue).
- Non-invasive: (electrodes are placed directly on the scalp).

A collection of unrelated stimuli, words, and images or relevant stimuli, words and images are presented to the test subject. This approach employs a variety of irrelevant, target, and probe stimuli. Everybody's brain contains the electrical signal P300, which is used by this system. Once the culprit is located, it generates unique stimuli, once in every 300 milliseconds. The explanation verifies the P300's response to the queries about crime. The weapons that the criminal employed are shown on the screen. It is independent of vocal responses to stimuli by using EEG readings. The accuracy of brain fingerprinting technology is independent of the subject's emotional state. Alpha, beta, delta, and theta waves are the four waves that make up the EEG [14]. Figure 11 represents the types of brain waves.

Alpha waves: Normal occurrence of alpha waves includes deep relaxation, imaginative states, and intuitive thought. It oscillates between 8 and 12 Hz.

Beta waves: Only when a person is active, beta waves appear. It has a frequency range of 12 Hz and higher.

Theta waves: Theta waves appear when people are emotionally stressed, disappointed, daydreaming, or sleepy, for example. 4 to 8 Hz is the range of its frequencies.

Delta waves: Deep sleep and extreme deep meditation both produce delta waves. Its frequency is between 0.5 and 4Hz.

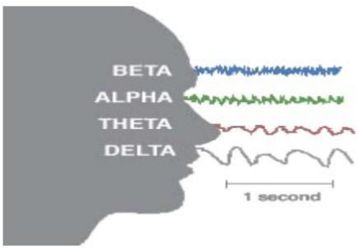

Figure 11. Types of brain waves

7. Evidence for Brain Fingerprinting

Dr. Farwell has a patented system of analysis for EEG P300 lie detection called the P300 MERMER [15]. According to Farwell, Brain Fingerprinting is a valid and trustworthy tool that assisted in the conviction of a serial killer and the release of an innocent man who had been wrongfully imprisoned for 22 years for murder (Farwell, Richardson, & Richardson, 2013) [7]. According to Larry Farwell's website, the test revealed Grinder had knowledge of the murder stored in his brain.

Before the Brain Fingerprinting test, Grinder admitted his guilt to the County Sheriff, but the Sheriff demanded proof, according to Farwell's website [16] Grinder entered a guilty plea and avoided the death penalty in exchange for a life sentence. In 2000, Terry Harrington, who was serving a life sentence for murder and contesting the verdict, also had his brain analysed[7]. According to the results of the Brain Fingerprinting test, Harrington had knowledge unique to his alibi but not knowledge specific to the specifics of the crime. The District Court recognised the P300 effect's legitimacy following a one-day hearing on the admissibility of Brain Fingerprinting evidence. The Court, however, ruled that the evidence was not convincing to give a fresh trial (Farwell & Makeig, 2005) [7].

Due to a Brady violation (prosecutors failing to disclose material that aids the defence), Harrington was later granted a second trial, and the Supreme Court overturned the District Court's ruling. Farwell asserts that after presenting the key prosecution witness with the results of the Brain Fingerprinting study, the witness changed his testimony. Harrington's conviction was overturned and he was released from prison as a result of the recanted evidence (Farwell & Makeig, 2005).

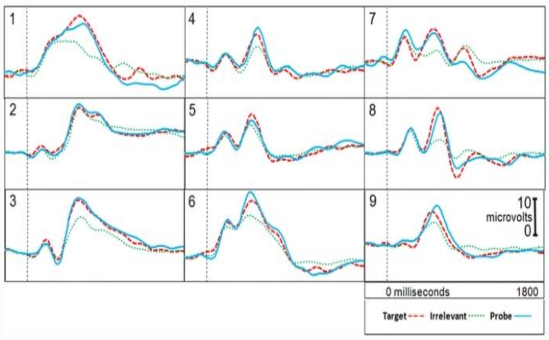

Figure 12. Brain responses of information-present subjects [7]

In his discussion of the Harrington case, Farwell emphasises how the court recognised the legitimacy of brain fingerprinting. However, the Court accepted the P300 MERMER response rather than Farwell's particular technique of analysis (Farwell & Makeig, 2005) [7]. Farwell, Richardson, and Richardson (2013) conducted "real-life" research to address this issue. These investigations covered both minor and severe crimes as well as job-specific knowledge for FBI, CIA, and U.S. Navy employees.

Perhaps the only researchers who test high-stakes lying with actual criminals regarding actual crimes are Farwell, Richardson, and Richardson. Because Farwell evaluated criminal suspects and informed them that if they passed the test, it may be used as supporting evidence for them in court, their research had a high ecological validity [7]. Figure 12 represents the Brain responses of information-present subjects

He taught the participants countermeasures (such as thinking of something else when presented with the irrelevant stimuli) that have been effectively used in prior P300 research to demonstrate that the test could not be "beaten" (Farwell et al., 2013). In 2013, effectiveness of countermeasures when using Brain Fingerprinting [7]. Their research revealed that the countermeasures had no effect on Brain Fingerprinting.

8. Applications

- Test candidates for various positions, particularly those involving sensitive military and foreign intelligence screening.
- To identify signs of neurological illnesses, Alzheimer's disease, mental depression, and other types of dementia.
- Legal proceedings: Finding the criminal is an essential component of the legal system. There was no clinically supported method of making a critical distinction prior to the development of the science of brain fingerprinting[13].
- Advertisements: This technique aids in identifying whether a specific person has information about a product concept stored in his memory.
- Antiterrorism: It is the most effective way to find terrorists who have directly or indirectly engaged in terrorist activity. It aids in determining who has leadership positions within the terrorist group. Additionally, it aids in locating sleeper cells who been dormant for years.

9. Limitations

Brain fingerprinting cannot be applied to every case or to every suspect because there are circumstances in which the detectives may not be aware of the crime scene when the criminal vanishes from the view. Therefore, no interpretation could be reached. In some circumstances, the offender may assert that he was just an eyewitness present at the crime scene. So, in this instance, although the person is fully aware of the crime scene, they did not commit the crime. As a result, no data can be interpreted.

10. Comparison with Other Technologies

Physical evidence from a crime scene is matched with evidence on the perpetrator's person using DNA and conventional fingerprinting. Brain fingerprinting works in a similar way by comparing informational evidence from the crime scene with material that is stored in the brain. Only 1% of crimes have available fingerprints and DNA. The suspect's activities are always being planned, carried out, and recorded by the suspect's brain[14]. Brain fingerprinting is not a tool for detecting lies. Instead, it is a methodical approach to determining if a specific crime or other conduct has been committed. Neither inquiries nor responses are made during the Farwell Brain Fingerprinting process. The outcomes are the same whether the person has lied or stated the truth at any moment, just like with DNA and fingerprints.

11. Conclusion

With a track record of 100% accuracy in studies with US government agencies, actual criminal cases, and other uses, brain fingerprinting is a cutting-edge new scientific tool for solving crimes, identifying criminals, and exonerating innocent individuals. The technology satisfies a critical requirement for governments, law enforcement organisations, businesses, investigators, crime victims, and people who have been wrongfully accused but are innocent. Due to the research's limited sample size, it would not be suitable to generalise its findings. However, the 100 percent accuracy and high level of confidence results offer additional support for findings from earlier studies that used brain MERMER testing.

References

[1] Başar-Eroglu, Canan, Erol Başar, Tamer Demiralp, and Martin Schürmann. "P300-response: possible psychophysiological correlates in delta and theta frequency channels. A review." International journal of psychophysiology 13, no. 2 (1992): 161-179.

[2] Farwell, Lawrence A. "Method for electroencephalographic information detection." U.S. Patent 5,467,777, issued November 21, 1995.

[3] Farwell, Lawrence A., and Emanuel Donchin. "The brain Detector-P300 in the detection of deception." In Psychophysiology, vol. 23, no. 4, pp. 434-434. 1010

VERMONT AVE NW SUITE 1100, WASHINGTON, DC 20005: SOC PSYCHOPHYSIOL RES, 1986.

[4] Rosenfeld, J. Peter. "Brain fingerprinting: A critical analysis." The Scientific Review of Mental Health Practice 4, no. 1 (2005): 20-37.

[5] Gao, Junfeng, Xiangguo Yan, Jiancheng Sun, and Chongxun Zheng. "Denoised P300 and machine learning-based concealed information test method." Computer methods and programs in biomedicine 104, no. 3 (2011): 410-417.

[6] Cavanagh, James F., Michael X. Cohen, and John JB Allen. "Prelude to and resolution of an error: EEG phase synchrony reveals cognitive control dynamics during action monitoring." Journal of Neuroscience 29, no. 1 (2009): 98-105.

[7] Farwell, L. A., and T. H. Makeig. "Farwell brain fingerprinting in the case of Harrington v." State, Open Court X [10] 3 (2005): 7-10.

[8] Allen, John J., William G. Iacono, and Kurt D. Danielson. "The identification of concealed memories using the event-related potential and implicit behavioral measures: A methodology for prediction in the face of individual differences." Psychophysiology 29, no. 5 (1992): 504-522.

[9] Erickson, Megan J. "Daubert's Bipolar Treatment of Scientific Expert Testimony-From Frye's Polygraph to Farwell's Brain Fingerprinting." Drake L. Rev. 55 (2006): 763.

[10] Lykken DT. The GSR in the detection of guilt. J Appl Psychol. 1959; 43:385–388. doi: 10.1037/h0046060.

[11] PICTON, Terence W. "Human event-related potentials." Handbook of Electroencephalography and Clinical Neurophysiology Revised Series 3 (1988).

[12] Roberts, Alexandra J. "Everything new is old again: brain fingerprinting and evidentiary analogy." Yale JL & Tech. 9 (2006): 234.

[13] Verschuere, Bruno, Gershon Ben-Shakhar, and Ewout Meijer, eds. Memory detection: Theory and application of the Concealed Information Test. Cambridge University Press, 2011.

[14] Meegan, Daniel V. "Neuroimaging techniques for memory detection: scientific, ethical, and legal issues." The American Journal of Bioethics 8, no. 1 (2008): 9-20.

[15] Wasserman, Stanley, and Ulf Bockenholt. "Bootstrapping: Applications to psychophysiology." Psychophysiology 26, no. 2 (1989): 208-221.

[16] https://larryfarwell.com.