A NEW COMPUTER-BASED BRAIN FINGERPRINTING TECHNOLOGY

Sai Srinivas Vellela[1], Roja D[2], Venkateswara Reddy B[3], Khader Basha Sk[4], M Venkateswara Rao[5]

[1,2,3,4]Asst. Professor, Dept. of CSE, Chalapathi Institute of Technology, Guntur, AP, India

[5]Dr. M Venkateswara Rao, Professor, Dept. of CSE, NRI Institute of Technology, Pothavarappadu, Vijayawada, AP, India.

ABSTRACT

Brain Fingerprinting is 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. 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 felony crimes.

Key Words – Brain, Fingerprinting, Crime.

1. INTRODUCTION

Brain Fingerprinting is based on the principle that the brain is central to all human acts. In a criminal act, there may or may not be many kinds of peripheral evidence, but the brain is always there, planning, executing, and recording the crime. The fundamental difference between a perpetrator and a falsely accused, innocent person is that the perpetrator, having committed the crime, has the details of the crime stored in his brain, and the innocent suspect does not. This is what Brain Fingerprinting detects scientifically When a crime is committed, a record is stored in the brain of the perpetrator. Brain Fingerprinting provides a means to objectively and scientifically connect evidence from the crime scene with evidence stored in the brain. (This is similar to the process of connecting DNA samples from the perpetrator with biological evidence found at the scene of the crime; only the evidence evaluated by Brain Fingerprinting is evidence stored in the brain.) Brain Fingerprinting measures electrical brain activity in response to crime-relevant words or pictures presented on a computer screen, and reveals a brain MERMER (memory and encoding related multifaceted electroencephalographic response) when, and only when, the evidence stored in the brain matches the evidence from the crime scene. Thus, the guilty can be identified and the innocent can be cleared in an accurate, scientific, objective, non-invasive, non-stressful, and non-testimonial manner

2. MERMER METHODOLOGY

The procedure used is similar to the Guilty Knowledge Test; a series of words, sounds, or pictures are presented via computer to the subject for a fraction of a second each. Each of these stimuli are organised by the test-giver to be a "Target," "Irrelevant," or a "Probe." The Target stimuli are chosen to be relevant information to the tested subject, and are used to establish a baseline brain response for information that is significant to the subject being tested. The subject is instructed to press on button for Targets, and another button for all other stimuli. Most of the non-Target stimuli are Irrelevant, and are totally unrelated to the situation that the subject is being tested for. The Irrelevant stimuli do not elicit a MERMER, and so establish a baseline brain response for information that is insignificant to the subject in this context. Some of the non-Target are relevant to the situation that the subject is being tested for. These stimuli, Probes, are relevant to the test, and are significant to the subject, and will elicit a MERMER, signifying that the subject has understood that stimuli to be significant. A subject lacking this information in their brain, the response to the Probe stimulus will be indistinguishable from the irrelevant stimulus. This response does not elicit a MERMER, indicating that the information is absent from their mind. Note that there does not have to be an emotional response of any kind to the stimuli- this test is entirely reliant upon recognition response to the stimuli, and relies upon a difference in recognition- hence the association with the Oddball effect

3. THE FANTASTIC FOUR

The four phases of Brain Fingerprinting

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

1. Brain Fingerprinting Crime Scene Evidence Collection;

2. Brain Fingerprinting Brain Evidence Collection;

3. Brain Fingerprinting Computer Evidence Analysis; and

4. Brain Fingerprinting Scientific Result.

In the Crime Scene Evidence Collection, an expert in Brain Fingerprinting examines the crime scene and other evidence connected with the crime to identify details of the crime that would be known only to the perpetrator. The expert then conducts the Brain Evidence Collection in order to determine whether or not the evidence from the crime scene matches evidence stored in the brain of the suspect. In the Computer Evidence Analysis, the Brain Fingerprinting system makes a mathematical determination as to whether or not this specific evidence is stored in the brain, and computes a statistical confidence for that determination. This determination and statistical confidence constitute the Scientific Result of Brain Fingerprinting: either "information present" ("guilty") – the details of the crime are stored in the brain of the suspect – or "information absent" ("innocent") – the details of the crime is not stored in the brain of the suspect

## Scientific Procedure, Research, and Applications

1. Informational Evidence Detection- The detection of concealed information stored in the brains of suspects, witnesses, intelligence sources, and others is of central concern to all phases of law enforcement, government and private investigations, and intelligence operations. Brain Fingerprinting presents a new paradigm in forensic science. This new system detects information directly, on the basis of the electrophysiological manifestations of information-processing brain activity, measured non-invasively from the scalp. Since Brain Fingerprinting depends only on brain information processing, it does not depend on the emotional response of the subject.

2 The Brain MERMER- Brain Fingerprinting utilizes multifaceted electroencephalographic response analysis (MERA) to detect information stored in the human brain. A memory and encoding related multifaceted electroencephalographic response (MERMER) is elicited when an individual recognizes and processes an incoming stimulus that is significant or noteworthy. When an irrelevant stimulus is seen, it is insignificant and not noteworthy, and the MERMER response is absent. The MERMER occurs within about a second after the stimulus presentation, and can be readily detected using EEG amplifiers and a computerized signal-detection algorithm.

3. Scientific Procedure- Brain Fingerprinting incorporates the following procedure. A sequence of words or pictures is presented on a video monitor under computer control. Each stimulus appears for a fraction of a second. Three types of stimuli are presented: "targets," "irrelevants," and "probes." The targets are made relevant and noteworthy to all subjects: the subject is given a list of the target stimuli and instructed to press a particular button in response to targets, and to press another button in response to all other stimuli. Since the targets are noteworthy for the subject, they elicit a Mermer. Most of the non-target stimuli are irrelevant, having no relation to the crime. These irrelevants do not elicit a Mermer. Some of the non-target stimuli are relevant to the crime or situation under investigation. These relevant stimuli are referred to as probes. For a subject who has committed the crime, the probes are noteworthy due to his knowledge of the details of the crime, and therefore probes elicit a brain MERMER. For an innocent subject lacking this detailed knowledge of the crime, the probes are indistinguishable from the irrelevant stimuli. For such a subject, the probes are not noteworthy, and thus probes do not elicit a MERMER.

4. Computer Controlled - The entire Brain Fingerprinting System is under computer control, including presentation of the stimuli and recording of electrical brain activity, as well as a mathematical data analysis algorithm that compares the responses to the three types of stimuli and produces a determination of "information present" ("guilty") or "information absent" ("innocent"), and a statistical confidence level for this determination. At no time during the testing and data analysis do any biases and interpretations of a system expert affect the stimulus presentation or brain responses.
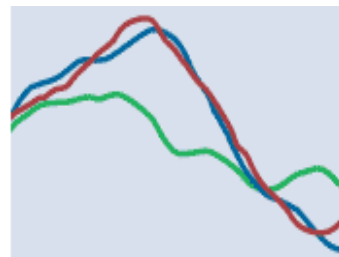
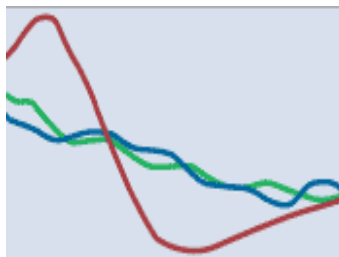## The devices used in brain fingerprinting
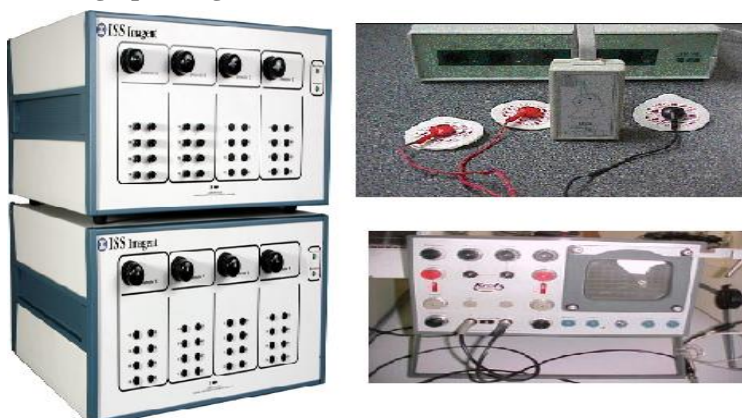
Brain waves:
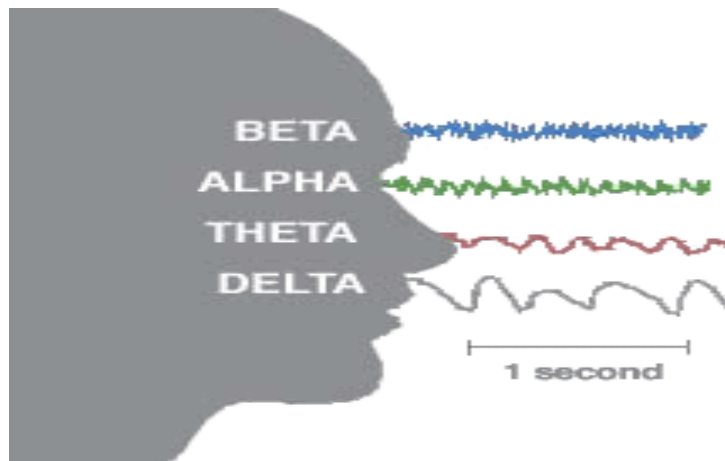
Using brain waves to detect guilt

How it works

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

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

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

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

NOT GUILTY:

Because the blue and green Lines closely correlate, suspect does Not have critical knowledge of the crime

GUILTY:

because the blue and red Lines closely correlate, and suspect has critical knowledge of the crime

Scientific Experiments, Field Tests, and Criminal Cases

Scientific studies, field tests, and actual criminal cases involving over 120 individuals described in various scientific publications and technical reports by Dr. Lawrence A. Farwell have verified the extremely high level of accuracy and overall effectiveness of Brain Fingerprinting. The system had 100% accurate scientific results in all studies, field tests, and actual cases conducted at the Federal Bureau of Investigation, a US intelligence agency, the Alexandria (VA) Police Department, the offices of the Macon County (MO) Sheriff, and other organizations and individuals. Some of these tests are described below.

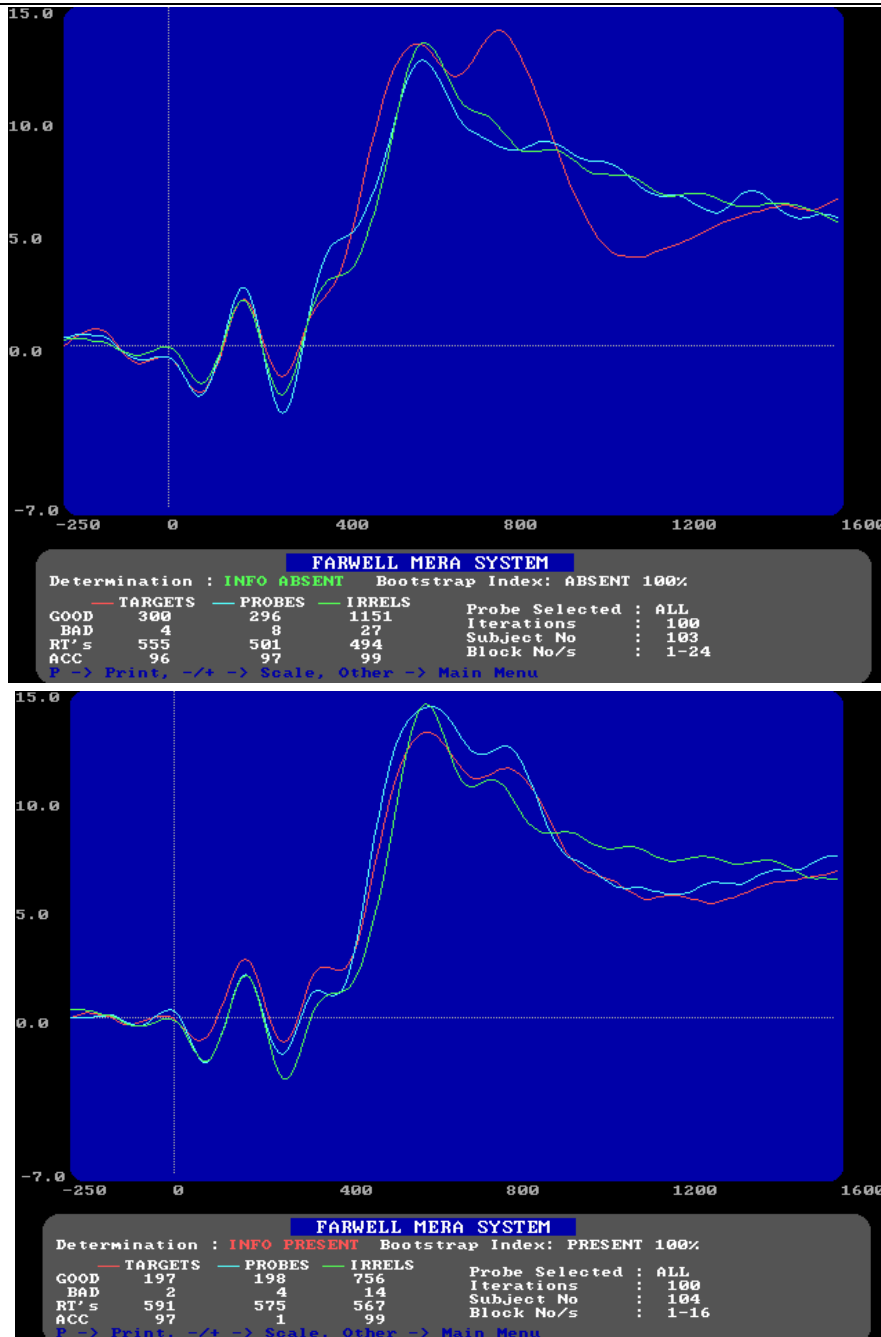**Terry Harrington's Brain-Wave Responses**

Y-axis: voltage in micro volts at the parietal (Pz) scalp site.

X-axis: time in milliseconds (msec). Stimulus was presented at 0 msec.

Determination: information absent.

Statistical Confidence: 99.9%

Conclusion: Certain significant details of the murder of John Schweer are not stored in Terry Harrington's brain

Determination: information present.

Statistical Confidence: 99.9%

Conclusion: Certain significant details of the murder of John Schweer are stored in Terry Harrington's brain.

Results of the Brain Fingerprinting test on Terry Harrington

For the test on Schweer's murder, the determination of Brain Fingerprinting was "information absent," with a statistical confidence of 99.9%. The information stored in Harrington's brain did not match the scenario in which Harrington went to the crime scene and committed the murder. The determination of the Brain Fingerprinting test for alibi-relevant information was "information present," with a confidence of 99.9%. The information stored in Harrington's brain did match the scenario in which Harrington was elsewhere (at a concert and with friends) at the time of the crime.

4. 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.

5. REFERENCES

[1] Lambourne GTC. The Use of Fingerprints in Identification. Med. Sci Law 1979.Knowledge Despite Efforts To Conceal Journal of Forensic Sciences 2001.

[2] Wasserman S, Bockenholt U. (1989). Bootstrapping: applications to bioinformatics and secure authentication analysis Dept.of Defence Research.

[3] Vellela, S.S., Balamanigandan, R. Optimized clustering routing framework to maintain the optimal energy status in the wsn mobile cloud environment. Multimed Tools Appl (2023). https://doi.org/10.1007/s11042-023-15926-5

[4] "MOBILE RFID APPLICATIONS IN LOCATION BASED SERVICES ZONE", International Journal of Emerging Technologies and Innovative Research (www.jetir.org | UGC and issn Approved), ISSN:2349-5162, Vol.10, Issue 6, page no. ppd851-d859, June-2023, Available at : http://www.jetir.org/papers/JETIR2306410.pdf

[5] Vellela, S. S., Reddy, B. V., Chaitanya, K. K., & Rao, M. V. (2023, January). An Integrated Approach to Improve E-Healthcare System using Dynamic Cloud Computing Platform. In 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT) (pp. 776-782). IEEE.

[6] VenkateswaraRao, M., Vellela, S., Reddy, V., Vullam, N., Sk, K. B., & Roja, D. (2023, March). Credit Investigation and Comprehensive Risk Management System based Big Data Analytics in Commercial Banking. In 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS) (Vol. 1, pp. 2387-2391). IEEE.

[7] Vellela, S. S., & Balamanigandan, R. (2022, December). Design of Hybrid Authentication Protocol for High Secure Applications in Cloud Environments. In 2022 International Conference on Automation, Computing and Renewable Systems (ICACRS) (pp. 408-414). IEEE.

[8] Vellela, S. S., Basha Sk, K., & Yakubreddy, K. (2023). Cloud-hosted concept-hierarchy flex-based infringement checking system. International Advanced Research Journal in Science, Engineering and Technology, 10(3).

[9] Rao, M. V., Vellela, S. S., Sk, K. B., Venkateswara, R. B., & Roja, D. (2023). SYSTEMATIC REVIEW ON SOFTWARE APPLICATION UNDERDISTRIBUTED DENIAL OF SERVICE ATTACKS FOR GROUP WEBSITES. Dogo Rangsang Research Journal UGC Care Group I Journal, 13(3), 2347-7180.

[10] Vullam, N., Vellela, S. S., Reddy, V., Rao, M. V., SK, K. B., & Roja, D. (2023, May). Multi-Agent Personalized Recommendation System in E-Commerce based on User. In 2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC) (pp. 1194-1199). IEEE.

[11] Sk, K. B., & Vellela, S. S. (2019). Diamond Search by Using Block Matching Algorithm. DIAMOND SEARCH BY USING BLOCK MATCHING ALGORITHM", International Journal of Emerging Technologies and Innovative Research (www. jetir. org), ISSN, 2349-5162.

[12] Vellela, S. S., Balamanigandan, R., & Praveen, S. P. (2022). Strategic Survey on Security and Privacy Methods of Cloud Computing Environment. Journal of Next Generation Technology (ISSN: 2583-021X), 2(1).

[13] Vellela, S. S., & Krishna, A. M. (2020). On Board Artificial Intelligence With Service Aggregation for Edge Computing in Industrial Applications. Journal of Critical Reviews, 7(07), 2020.

[14] Madhuri, A., Jyothi, V. E., Praveen, S. P., Sindhura, S., Srinivas, V. S., & Kumar, D. L. S. (2022). A New Multi-Level Semi-Supervised Learning Approach for Network Intrusion Detection System Based on the 'GOA'. Journal of Interconnection Networks, 2143047.

[15] Madhuri, A., Praveen, S. P., Kumar, D. L. S., Sindhura, S., &Vellela, S. S. (2021). Challenges and issues of data analytics in emerging scenarios for big data, cloud and image mining. Annals of the Romanian Society for Cell Biology, 412-423.

[16] Praveen, S. P., Sarala, P., Kumar, T. K. M., Manuri, S. G., Srinivas, V. S., &Swapna, D. (2022, November). An Adaptive Load Balancing Technique for Multi SDN Controllers.In 2022 International Conference on Augmented Intelligence and Sustainable Systems (ICAISS) (pp. 1403-1409).IEEE.

[17] Sk, K. B., Roja, D., Priya, S. S., Dalavi, L., Vellela, S. S., & Reddy, V. (2023, March). Coronary Heart Disease Prediction and Classification using Hybrid Machine Learning Algorithms. In 2023 International Conference on Innovative Data Communication Technologies and Application (ICIDCA) (pp. 1-7). IEEE.

[18] SRINIVAS, V. S., PUSHPALATHA, D., SARATHKUMAR, G., KAVITHA, C., & HARSHITHKUMAR, D. ADVANCED INTELLIGENCE HEALTH INSURANCE COST PREDICTION USING RANDOM FOREST.

[19] D, Roja and Dalavai, Lavanya and Javvadi, Sravanthi and Sk, Khader Basha and Vellela, Sai Srinivas and B, Venkateswara Reddy and Vullam, Nagagopiraju, Computerised Image Processing and Pattern Recognition by

Using Machine Algorithms (April 10, 2023). TIJER International Research Journal, Volume 10 Issue 4, April 2023, Available at SSRN: https://ssrn.com/abstract=4428667

[20] Sk, K. B., Vellela, S. S., Yakubreddy, K., & Rao, M. V. (2023). Novel and Secure Protocol for Trusted Wireless Ad-hoc Network Creation. Khader Basha Sk, Venkateswara Reddy B, Sai Srinivas Vellela, Kancharakunt Yakub Reddy, M Venkateswara Rao, Novel and Secure Protocol for Trusted Wireless Ad-hoc Network Creation, 10(3).

[21] Venkateswara Reddy, B., Vellela, S. S., Sk, K. B., Roja, D., Yakubreddy, K., & Rao, M. V. Conceptual Hierarchies for Efficient Query Results Navigation. International Journal of All Research Education and Scientific Methods (IJARESM), ISSN, 2455-6211.

[22] Yakubreddy, K., Vellela, S. S., Sk, K. B., Reddy, V., & Roja, D. (2023). Grape CS-ML Database-Informed Methods for Contemporary Vineyard Management. International Research Journal of Modernization in Engineering Technology and Science, 5(03).

[23] Pratap, V. K. (2020). An Effective Automatic Automobile Safety Method Using AI and Convolutional Neural Network. International Journal for Innovative Engineering and Management Research, 9(09).

[24] Gajjala Buchi Babu, Mutyala Venu Gopal, Vellala Sai Srinivas, V. Krishna Pratap, Efficient Key Generation for Multicast Groups Based on Secret Sharing, (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 1, Issue 4, pp.1702-1707.

[25] Karthik, J. V., & Reddy, B. V. (2014). Authentication of secret information in image stenography. International Journal of Computer Science and Network Security (IJCSNS), 14(6), 58.