IOSR Journal of Computer Science (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727
PP 29-32
www.iosrjournals.org

Uncrackable Password Authentication Using Brain Fingerprinting

Nikhil M. Palekar[1], Vaishnavi P. Rakhunde[2], Aaysha Shaikh[3], Dipak Kardel[4]
[1,2,3,]Computer Science and Engineering Department, Jawaharlal Darda Institute of Engineering and Technology, Yavatmal, India
[4]Information Technology Department, Government College of Engineering,Amravati,India

ABSTRACT : *Brain Fingerprinting is a technique used to find the unique brain-wave pattern generated by brain when a person encounters a familiar stimulus. It is based on fact that brain is central to all human acts. Brain is always there, planning, executing and recording the objects to which we encounters in the form of image, video or text. So my research says that, if we think about very personal object then something unique related to that strikes in our mind and unique brain-wave will be generated by our brain which can be used as passwords. As no one can read our mind or personal object in this case, it will be the most unbreakable password.*

Keywords –*Brain-Waves, EFG, MERA, MERMER*

I. INTRODUCTION TO BRAIN FINGERPRINTING

Brain Fingerprinting is a controversial proposed 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.

II. MERMER TECHNOLOGY

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 organized 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 is 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.

III. BRAIN MERMER

The 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.

III. 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.

IV. COMPUTER CONTROLLED SYSTEM

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 person to be tested wears a special headband with electronic sensors that measure the EFG from several locations on the scalp.The devices used in Brain fingerprinting are :

Fig. (1) Equipment of Brain Fingerprinting

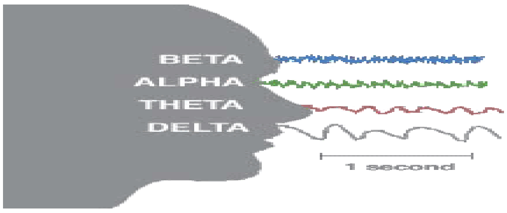

Fig. (2) Brain Waves

V. HOW IT WORKS

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

RED line: information the suspect is expected to know

GREEN line: information not known to suspect

BLUE line: information of the crime that only perpetrator would know

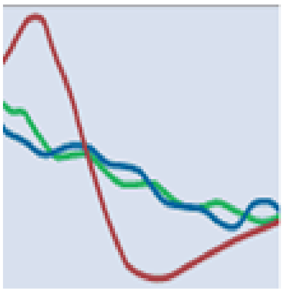

Fig. (3.1) Not Guilty

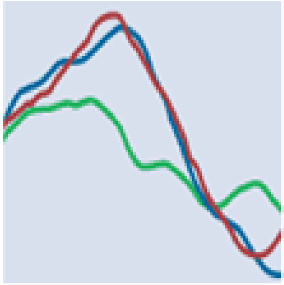

Fig. (3.2) Guilty

As the blue and green lines closely correlate, suspect does not have critical knowledge of the crime. Hence it is Not Guilty.

As the blue and green lines are apart from each other and they closely correlate, suspect have the critical knowledge of crime and hence it is Guilty.

VI. PASSWORD AUTHENTICATION

As we know that human brain is central to all the human acts, everything what we see is stored in the brain in the form of music, video or text. And according to Brain Fingerprinting technology, unique brain wave is created by an individual's brain. So we can use these brain waves as a password. We can use single brain-wave or a combinations of brave-wave as a password according to our password storage capacity and authentication technology.

If we think about very personal object then unique brain-wave will create. We have to store this wave in a computer controlled device. Then again when we think about that personal thing then brain-wave will create which will be the same as previous one. If the both brain-wave matches then password matches and we can get access. As everyone generates their own unique brain-wave, no brain-wave will be the same until brain-wave is created by the same person.

There are 4 different waveforms considered in Brain Fingerprinting but here we are considering only 2 waveforms here. One is expected brain-wave(Red in color) which will be stored in computer controlled device and other is one(any other color) which we get when person thinks about that personal thing. Password can be authenticate only when expected brain-wave matches with other.

In the case, if any other people know the personal object which we are considering to generate unique brain-wave then also they cannot generate the same brain-wave. Because when other person thinks about that object then different brain –wave will generate. Hence this can be the Uncrackable Password Authentication technique because no one can know what the person thinks about something. It is not yet practically implemented but it is implementable.

Only the disadvantage is that it will be very costly as the required devise for Brain Fingerprinting are very costly.

VII. CONCLUSION

Brain Fingerprinting is 100% proven and implemented technique. Brain-wave generated by brain plays very important role in this. It is usedto 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. But these brain-waves can be used for password authentication. Brain-waves can be created by thinking any personal object. Unique brain-wave will create by brain which can be used as password.

This is the world of hackers so nothing is safe. They are able to crack everything. So we need a technique which cannot be cracked, a technique on which we can trust blindly. And if we implement Password Authentication Technique by using Brain Fingerprinting by considering unique brain-waves as a password then it will be Uncrackable Password Authentication Technique.

References

[1] Prof. Dinesh Chandra Jain and Dr. V.P. Pawar, The Brain Fingerprinting Through Digital. Electroencephalography Signal Technique, *International Journal on Computer Science and Engineering, IJCSE11-03-03-047*.

[2] Dr. Farwell and Smith SS, Brain Fingerprinting, *Journal of Forensic Sciences, 2001*.

[3] Farwell LA and Smith SS, Using Brain MERMER Testing To Detect Concealed Knowledge Despite Efforts To Conceal *Journal of Forensic Sciences 2001.*

[4] Vrushen Pawar, S.C.Meherotra and Arun Marwale, Digital EEG through sensitivity analysis of Electrography signal to human expression, *IEEE Transaction MAN and Sybaritic, Manuscript Number SMCA06-08-0244,USA 2007.*

[5] Frances M.Dyro, *The EEG Handbook, Clinical Neurophysiology,* Laboratory Massachusetts, London,1989**.**