**A Seminar Report**

**on**

**TWO LEVEL AUTHENTICATION USING BRAINWAVES**

Submitted in partial fulfillment of the requirements for the award of degree

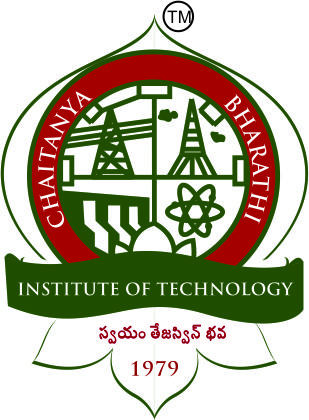
**BACHELOR OF ENGINEERING**

**in**

**COMPUTER SCIENCE AND ENGINEERING**

***by***

**SHALINI KOTHURU(1601-16-733-013)**



Department of Computer Science and Engineering

**CHAITANYA BHARATHI INSTITUTE OF TECHNOLOGY (A)**

**(Affiliated to Osmania University; Accredited by NBA(AICTE) and NAAC(UGC), ISO Certified 9001:2015)**

**GANDIPET, HYDERABAD – 500 075**

**Website: www.cbit.ac.in**

**[2019-2020]**

**CERTIFICATE**

Certified that seminar work entitled **“Two level authentication using brain waves”** is a bonafide work carried out in the eighth semester by **“Shalini Kothuru (1601-16-733-013)”** in partial fulfilment for the award of Bachelor of Engineering in Computer Science and Engineering from Chaitanya Bharathi Institute of Technology (A), Gandipet during the academic year 2019-2020.

**Seminar Incharges Mentor**

**Dr.K.Sagar Sri M. Venkata Krishna Reddy**

**Professor Asst.Professor**

**Dr.Sangeeta Gupta**

**Assoc.Professor**

**Smt.E.Kalpana**

**Asst.Professor**

ii

**TABLE INDEX**

**Table Page number**

3.2. Performance of different biometrics 7

4.1 Frequencies of different brain waves 9

iii

**FIGURE INDEX**

**Figure Page number**

1 Authentication 2

4.4 Simplified block diagram 11

4.4.1 Brain computer interface 11

4.4.2 Level Differentiator Unit 12

4.4.3 Checker Module 13

iv

**LIST OF ABBREVIATIONS**

EEG Electroencephalography

BCI Brain Computer Interface

LDU Level Differentiator Unit

ARM Advanced RISC Machines

LCD Liquid Crystal Display

ASCII American Standard Code for Information Exchange

BMI Brain Machine Interface

v

**ABSTRACT**

*Authenticity means identity of proof. It has become an essential part of our everyday lives. It is needed almost everywhere from banks to experimental labs, from car automation to home automation and even to personal computers and mobile phones. This proof of identity might be something like a password, pin or pattern, fingerprint, hand geometry or retina scans, card and keys. But these techniques are immune to shoulder-surfing problem and cards can be lost. An adult brain contains about 100 billion interconnected neurons. Each of them generates and leads electrical charges while brain works. The electrical activity (recorded using Electroencephalography) in a human brain is used to confirm a person's identity. The pattern of interconnections between billions of neurons is represented as thoughts and emotions. Change in emotions and thoughts or actions will differ from person to person, so it provides more integrity and authenticity. And also differently disabled person can’t use system which uses fingerprints or retina scans but they can use brain waves since they are always present. Using Brain waves as a biometric to provide authentication is very beneficial. A system is designed and implemented which allows user to set a pattern of brain waves which must be provided as an unlock pattern to get the access. This pattern can be any combination of eye blink, attention and various brain rhythms like Alpha, Beta, Theta and Delta. The system described in this paper provides two-level authentication. First level of which is brain waves. Once the correct pattern of brain signal is provide the system will ask for a pass key as a second level of authentication.*

vi

**TABLE OF CONTENTS**

**TOPIC PAGE NUMBER**

**Cover page** i

**Certificate**  ii

**Table Index** iii

**Figure Index**  iv

**List of abbreviations**  v

**Abstract**  vi

1. **Introduction**  1
   1. What is authentication 1
   2. What is biometrics 1
   3. How does it work 2
2. **Existing Work 3**
3. **Review on biometrics 5**

3.1 Commonly used biometrics 5

3.1.1 Fingerprint Recognition 5

3.1.2 Facial Recognition 5

3.1.3 Iris Recognition 6

3.2 Performance of different biometrics 6

3.3 Biometric attacks 7

3.3.1 Adversary Attacks 7

3.3.2 Denial of Service 8

3.3.3 False Enrolment 8

3.3.4 Fake Physical Biometrics 8

**4. Methodology 9**

4.1 EEG as biometric 9

4.2 Advantages of EEG 10

4.3 Disadvantages EEG 10

4.4. Implementation 11

4.4.1 Brain Computer Interface 11

4.4.2 Level Differentiator Unit 12

4.4.3 Checker Module 13

**5. Conclusion 14**

**References**

**1. INTRODUCTION**

**1.1 What is authentication?**

Authentication is process of verifying claimed identity of a person for a service or request. Due to advancement in technology, authentication has become an essential part of our everyday lives which is used at almost every place from banks to experimental labs, from car automation to home automation and even to personal computers and mobile phones.

Some commonly used authentication systems are passwords, pin codes, card readers etc. Now some biometrics, like finger print, retina are also being used for authentication. The service provided from authentication aims to facilitate the integrity of the system, as well as the authorization service. It also serves as a method of verification of sources, uniqueness, and integrity of messages. In essence, the basic functionality of authentication is to prevent requests from fraudulent users in a multiuser environment. But card and keys can be lost and there is a problem of shoulder surfing using passwords and code. So we use one of biometrics as our authentication method in this paper.

**1.2 What is biometrics?**

Biometrics is the technical term for body measurements and calculations. It refers to metrics related to human characteristics. Biometrics authentication (or realistic authentication) is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance. Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological versus behavioral characteristics. Physiological characteristics are related to the shape of the body. Examples include, but are not limited to fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina and odour/scent. Behavioral characteristics are related to the pattern of behavior of a person, including but not limited to typing rhythm, gait, and voice.

1

Since behavioral characteristics will differ from person to person, we use brain waves as our authentication method. Even physically handicapped person who can’t type password or use fingerprint can use their brain waves to authenticate and there is no problem of shoulder surfing problem.

**1.3 How does it work?**

An adult brain contains about 100 billion interconnected neurons. The pattern of interconnections between billions of neurons will differ from person to person. A system is designed which allows user to set a pattern of brain waves (also called EEG signals) which must be provided as an unlock pattern to get the access. This pattern can be any combination of eye blink, attention and various brain rhythms like Alpha, Beta, Theta and Delta. The system described in this paper provides two-level authentication. First level of which is brain waves. The System captures brain signals from user using brain wave sensor and it is verified with pattern already stored in computer. Once the correct pattern of brain signal is provide the system will ask for a pass key as a second level of authentication.

****

**Figure : 1 Authentication**

2

**2. EXISTING WORK**

Initially brain signals are studied and analyzed over a century ago to cure brain diseases and spinal cord diseases. Due to its unique characteristics, the scientific community identified it as automatic person recognition system to authenticate person identity. Because of its robustness against spoofing attacks, possibility to perform continuous identification, intrinsic liveness detection, and universality, brain signals is more beneficial compared to other biometric authentication methods like iris, retina, face and fingerprint recognition.

In paper [1], Patrizio Campisi and Daria La Rocca, reviewed some issues related to EEG as authentication, which forms an obstacle in the implementation of biometric systems to provide authentication based on brain waves. EEG techniques have a high temporal resolution, in the range of milliseconds, which allows dynamic studies to understand the underlying mechanisms by means of computational methods. In fact, information concerning for instance psycho-physiological state, neuro-logical and neuromuscular health, emotions, memory, the course of concentration, attention, levels of arousal, mental fatigue or workload during special tasks, and sensitiveness to external stimulation can be extracted from EEG inspection and manipulation. These kind of evidence has led in last decades to use brain signals to convey conscious volition in EEG-based systems, like brain computer interface (BCI) and brain machine interface (BMI) , aiming at controlling remote devices by means of the interpretation of the brain electrical activity.

Although some isolated attempts to use EEG to discriminate people have been performed in the past, only recently the scientific community has started a more systematic investigation on the use of EEG signals as human distinctive traits which can be potentially used in a biometric system. In fact the way the brain regions are organized and coordinated during specific cognitive functions or mental states, such as the response to audio or visual stimuli, during real or imagined body movements, imagined speech, resting states, etc., or during emotional states, can provide relevant information about the brain conditions which, in the studies conducted so far, have shown to have some discriminant capabilities among subjects

3

due to both morphological and anatomical traits, and functional plasticity traits.

In paper [1], Patrizio Campisi and Daria La Rocca, elaborates that how much understanding level has been reached in using brain waves as a Biometric identifier and how much still to be achieved. Specially, they covered and discussed several issues which need to be taken into account to design an EEG based user recognition system and to perform a fair comparison among the existing systems in terms of usability and recognition performance. EEG biometrics poses several new challenges to be tackled by researchers. For example, permanence and uniqueness are two basic requirements that need to be well analyzed for each candidate biometrics to be employed in more authenticated brain systems.

4

**3. REVIEW ON BIOMETRICS**

**3.1 Commonly used biometrics**

**3.1.1 Fingerprint Recognition**

An identification system based on fingerprint recognition looks for specific characteristics in the line pattern on the surface of the finger. The bifurcations, ridge endings and islands that make up this line pattern are stored in the form of an image.

The disadvantage of capturing an image of an external characteristic is that this image can be replicated – even if it is stored in encoded form. It can be spoofed also.It also requires large amount of computer resources.

**3.1.2 Facial recognition**

A facial recognition system analyses the shape and position of different parts of the face to determine a match. Surface features, such as the skin, are also sometimes taken into account.

Facial recognition for security purposes is an offshoot of face detection technology, which is used to identify faces in complex images in which a number of faces may be present. This technology has developed rapidly in recent years and is therefore an excellent candidate if a system is needed for remote recognition. Another plus is that the technology allows ‘negative identification’, or the exclusion of faces, making it a good deal easier to scan a crowd for suspicious individuals.

However, facial recognition also has a number of significant drawbacks. For example, the technology focuses mainly on the face itself, i.e. from the hairline down. As a result, a person usually has to be looking straight at the camera to make recognition possible.

5

**3.1.3 Iris recognition**

When an iris scan is performed a scanner reads out the unique characteristics of an iris, which are then converted into an encrypted (bar) code. Iris scanning is known to be an excellent security technique, especially if it is performed using infrared light.

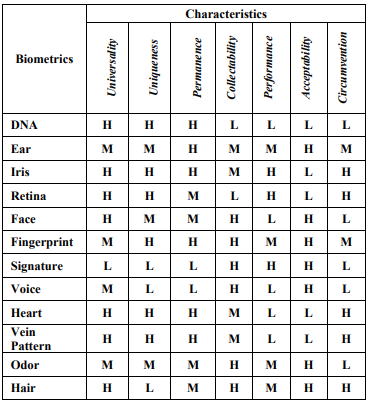
However, one problem frequently encountered when the technology is introduced is resistance from users. Quite a few people find having their eyes scanned a rather unpleasant experience. You also have to adopt a certain position so the scanner can read your iris, which can cause discomfort. Hygiene is another frequently cited drawback, as many systems require users to place their chin on a chin rest that has been used by countless people before them.

**3.2 Performance of different bio metrics**

**T**he table below shows various biometric based technologies based on the perception of the author, which is rated High, Medium, and Low, which is denoted by H, M, and L respectively. These biometrics are then rated against characteristics which complements biometrics which are:

* Universality, how present it is in the general population.
* Uniqueness, how can it be used as an identifier on individuals.
* Permanence, how long can the identifiers last.
* Collectability, how easy the identifiers are captured and quantified.
* Performance, how fast and accurate it is.
* Acceptability, how individuals can accept the biometric.
* Circumvention, how secure and fool proof the biometric is.

6



**Table: 3.2 Performance of different biometrics**

**3.3 Biometric attacks**

**3.3.1 Adversary Attacks**

An adversary attack is essentially an attack which relies on the biometric system’s loopholes in design and its availability of resources. This form of attack can further be broken down into three categories which is firstly administration attack(insider attack). This attack refers to system vulnerabilities due to improper administration of the system. After that, we have, the no secure infrastructure, which is comprised of hardware, software, and communication channel vulnerabilities which can eventually lead to breaches. Finally, we have biometric overtness, which refers to the attacker’s ability to acquire the actual users biometric, in other words, imitating a legitimate user’s biometric characteristic which would be used for authentication.

7

**3.3.2 Denial of Service**

One of the most devastating attack vectors is denial of service, which aims to essentially corrupt or render a biometric system unusable. Introducing environmental elements such as light, dust, and heat can potentially degrade biometric sensors and alter the quality of the data. However, Denial of Service attacks are considered to be ‘noisy’, in which it means that they are noticed quickly, although sometimes the aim is to create confusion from such events.

**3.3.3 False Enrolment**

False enrolment is also a prevalent threat for biometrics. The essential basic for biometric data is founded upon legitimate enrolment. If such data were to be falsified, then the identity will be incorrectly matched. Such a threat can be in systems such as passport applications.

**3.3.4 Fake Physical Biometrics**

Another threat that has been very prominent with biometrics is fake physical biometrics. Such an attack is easily conducted and requires little to no technical knowledge. Whilst at the same time certain materials required to create such a fake item is generally cheap and easily obtainable by any individual. Such a risk creates a threat for biometrics where characteristics can easily be reproduced.

It is important to ensure the security of biometrics from the very start, security should be incorporated into both the design and inception, especially since the usage of biometric systems has gained popularity

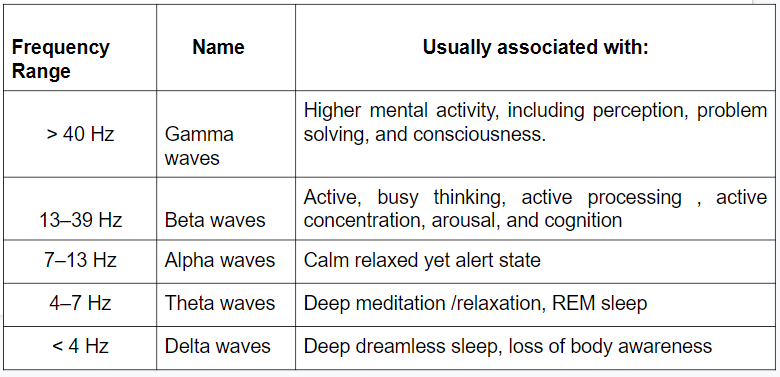
8

**4. METHODOLOGY**

**4.1 EEG signals as biometric**

An adult brain contains about 100 billion interconnected neurons. Each of them generates and leads electrical charges while brain works. The sum of all these very small electrical charges contributes to the generation of an electric field with fluctuating electrical potentials around our scalp. The fluctuating potentials are typically in the μV range. These fluctuations can be measured using sensors. The potentials are measured between two or more points called electrodes or sensors, which is placed on the scalp at different locations according to some standard configurations. These measurements are called as Electroencephalography (EEG). That is why the term brain waves can also be used when referring EEG signals. The pattern of interconnections between billions of neurons is represented as thoughts and emotions. Change in emotions and thoughts or actions will change the interconnections of neurons which will in term change the electric field. So, changes in thoughts can be interpreted by sensing brain signals.

Brain consists of 5 different types of brain waves; Delta, Theta, Alpha, Beta and Gamma brain waves. The table below gives overview of the primary function of brain waves.

****

**Table 4.1 Frequencies of different brain waves**

9

**4.2 Advantages of EEG**

EEG has more advantages compared to other biometrics

Since each individual reaction will be different from others

* EEG is much more confidential due to the fact that it corresponds to a secret mental task created from a stimulus, which in no way is observable. The common spoofing attacks previously mentioned would not be as viable in this scenario as compared to traditional biometric schemes.
* EEG is the fact that signals are very difficult to mimic, due to the fact that mental tasks are dependent on each individual. This means that, when presented with a stimulus, each individual would have a different way of processing it. These signals can also be affected by things such as mood, mental stress, and an individual’s mental state, this makes it much more complicated for attackers to obtain authentication from an individual who are subjected to force and threat
* EEG signals can only be recorded if the living individual is functional and receptive. This means that there is no possibility that a non-living brain can possibly produce EEG signals, which in hindsight prevents attackers from stealing this characteristic from the user.

**4.3 Disadvantages of EEG**

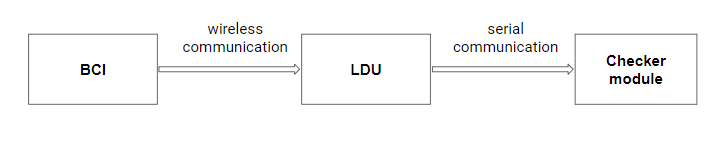
* Low spatial resolution on scalp
* EEG determines neural activity that occurs below the upper layers of brain poorly
* Signal to noise ratio is poor
* Since brain signals change according to person condition it is difficult to capture brain waves similar to brain waves pattern stored in computer when a person is drunken or after work outs.

10

**4.4 Implementation**

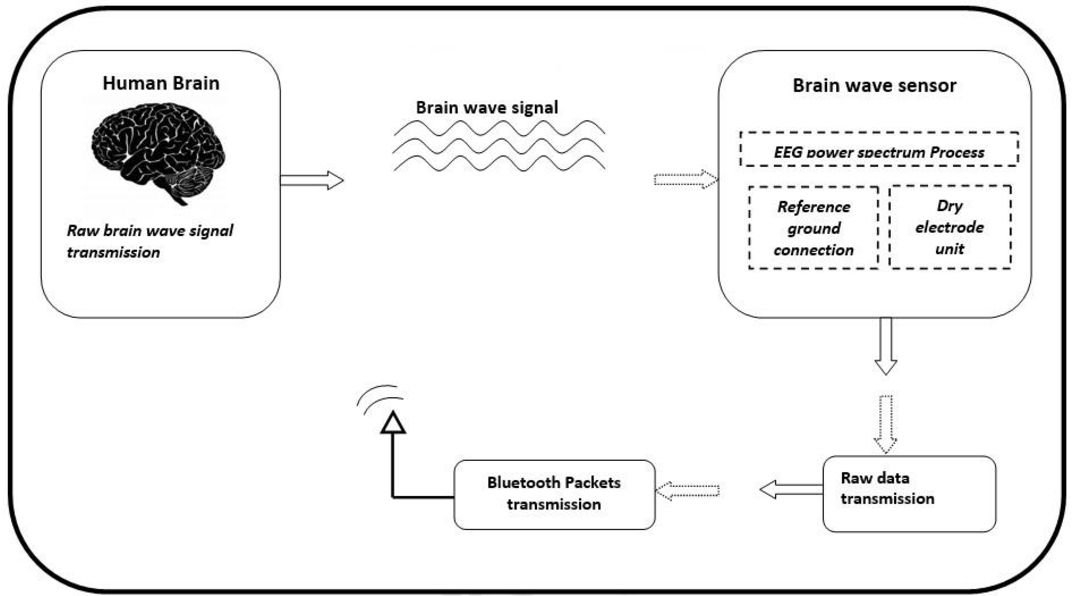
The following block shows simplified block diagram. The system is divided into 3 main blocks:

* Brain Computer Interface
* Level Differentiator Unit
* Checker Module



**Fig : 4.4 Simplified block diagram**

**4.4.1 Brain Computer Interface**

****

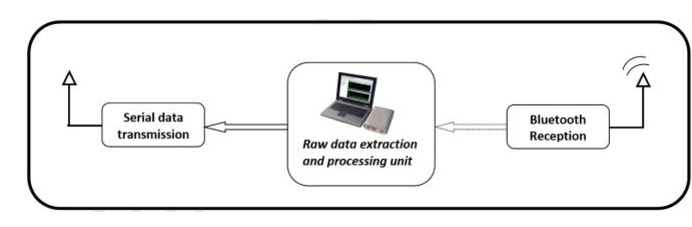
**Fig : 4.4.1 Brain computer interface**

11

In generalized term, we can say, this block has the responsibility to connect human brain to the computer system. In our case, computer system is nothing but a level differentiator unit. Brain computer interface system uses brain wave sensors to acquire electrical equivalent brain signals generated due to activities of billions of neurons. Brain wave sensor consists of dry electrodes and a reference electrode. The captured raw data is then converted in the form of packets. These data packets are then transmitted to level differentiator unit using wireless Bluetooth transmission.

Brain sense headband is used as brain sensor. It uses single electrode configuration. One electrode is placed on forehead at frontal lobe of brain. Headband uses one reference electrode which is connected to the left ear lobe as a reference node. This headband is battery powered and requires three 1.5V dry batteries. Brain sense headband is a Bluetooth enabled device which transmits brain signals in the form of packets through wireless communication.

**4.4.2 Level Differentiator Unit**

****

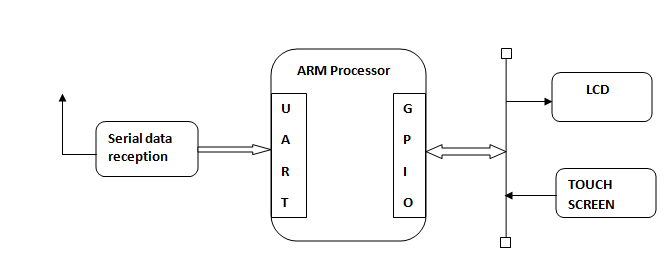
**Fig : 4.4.2 Level Differentiator Unit**

This block receives wireless data and performs data extraction from raw data that is captured. This block uses Matlab platform for data extraction and interpretation from brain waves that are received. A specific pattern of brain waves is pre-defined in level differentiator unit as an unlock pattern of brain waves for authentication. User needs to generate the authentic pattern to get the access. Level differentiator unit receives the brain waves in real-time and checks

12

whether the pattern generated now matches with the pre-defined pattern. It then sends ASCII keys to the checker module accordingly. Level differentiator unit uses serial communication for connection to checker module.

**4.4.3 Checker Module**

****

**Fig : 4.4.3 Checker Module**

This block is used to provide two-level authentication. It receives ASCII key from level differentiator unit if authorized pattern of brain waves is generated. After satisfying brain wave condition checker module asks for a pass-key which is second level of authentication. Checker module consists of an ARM processor interfaced with a touch panel and a LCD. Touch panel is used as an input device and LCD as an output device. User enters the pass-key on touch screen and then authenticated or unauthenticated entry is indicated on LCD. Note here that Pass-key will be asked only if the brain waves are matched.

13

**5. CONCLUSION**

In his study, we have seen what is authentication and importance of authentication today, where multi-user systems are at large and different biometrics used for authentication. Since authentication plays important role everywhere, we have to choose the authentication method which is less prone to attacks and more unique. Due to that we looked at an authentication method which was different compared to traditional methods, with the use of biometrics. Hence, the usage of EEG-based biometrics solves certain problems that other biometrics like fingerprint, retina and password face due to its uniqueness. A system is designed where EEG signals are captured from user by using brain wave sensor is used as first level authentication and second level authentication is done using passkey if brain waves are matched only. Since brain waves changes from person to person and depending on person’s condition, it is difficult to mimic. So using brain waves to authenticate is person’s identity is more beneficial compared to other authentication methods.

14

**REFERENCES**

[1] G Patrizio Campisi and Daria La Rocca, “Brain Waves for Automatic Biometric-Based User Recognition”, *IEEE Transactions on Information Forensics and Security, Vol. 9, No. 5, pp 782-800, May 2014.*

[2] A. Jain, A. Ross and S. Pankanti, "Biometrics: A Tool for Information Security", *IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp. 125-143, 2006.*

[3] M. Schatten, M. Baca, and M. Cubrilo, "Towards a general definition of biometric systems." *arXiv preprint arXiv:0909.2365, 2009.*

[4] Authentication with brainwaves: a review on the application of EEG as an authentication method, *https://ieeexplore.ieee.org/document/8776850*

[5] Survey of EEG based biometric authentication, *https://ieeexplore.ieee.org/document/82564 71*

[6] Biometrics**,** *https://en.wikipedia.org/wiki/Biometrics*

[7] Commonly used biometrics, *https://www.recogtech.com/en/knowledge-base/5-common-bio metric-techniques-compared*

[8] Performance of different biometrics, *https://www.virtualcasemanagement.com/bio.aspx*

[9] Types of brain waves, *https://itsusync.com/different-types-of-brain-waves-delta-theta-alpha -beta-gamma* [10] E. Zion-Golumbic, “What is EEG?” [Online]. Available: https://www.mada.org.il/ brain/ articles/ faces-e.pdf. [Accessed: 30-Sep2018].